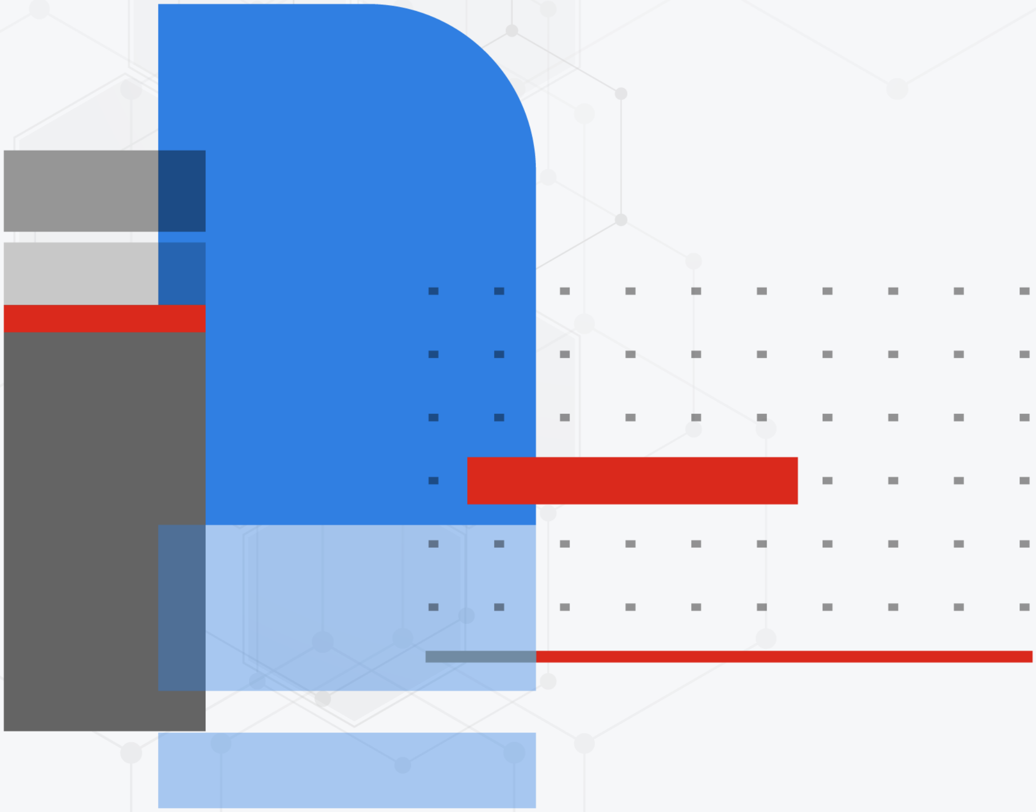
FORTINET

User Guide

FortiRecon 23.4.0



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

November 09, 2023
FortiRecon 23.4.0 User Guide
75-234-970006-20231109

TABLE OF CONTENTS

Change Log

Date	Change Description
2023-11-09	Initial release.
2023-12-06	Updated Default alerts topic.

Introduction

FortiRecon is a Digital Risk Protection (DRP) service that operates alongside existing security solutions to provide you with the visibility that an adversary can have of your infrastructure. This early warning of any malicious activity targeted at your organization enables swift detection and mitigation. Operating purely from outside the organizational boundary, the service maps an organization’s digital footprint and monitors it for abnormal activity. The service gives organizations the intelligence to mitigate credible security threats in a controlled manner as part of ongoing security efforts.

FortiRecon scans the organization's attack surface and identifies risks to assets while FortiGuard Threat Intelligence delivers early warning of risks to the organization through targeted, curated intelligence to provide an early warning of any malicious activity targeted to the organization.

The FortiRecon portal includes the following modules:

EASM	The External Attack Surface Management (EASM) module provides an adversary’s view of the organization digital attack surface and prioritizes risks and exposures, enabling administrators to mitigate threats in a controlled manner before the threats become a problem. See EASM on page 28.
Brand Protection	The Brand Protection (BP) module continually monitors the organization’s public-facing visibility for unauthorized changes, including web-based phishing attacks, typo-squatting, rogue applications, credential leaks, and brand impersonation in social media, which may impact brand value, integrity, and trust. See Brand Protection on page 60.
ACI	The Adversary Centric Intelligence (ACI) module leverages FortiGuard Threat Analysts to provide comprehensive coverage of dark web, open source, and technical threat intelligence, including threat actor insights. This information enables administrators to proactively assess risks, respond faster to incidents, better understand their attackers, and protect assets. See Adversary Centric Intelligence on page 88.
Profile Settings	The Profile Settings module allows you to personalize your FortiRecon account and provide information on your organization. See Profile settings on page 133.

FortiRecon APIs are available on the Fortinet Developer Network (FNDN). You must first register an account on FNDN to gain access.

Requirements

A FortiCloud account is required to access the FortiRecon portal. The FortiRecon Admin for your organization also needs to create an account within FortiRecon. If either of these accounts is not created, you will not be able to log in to the FortiRecon portal. See the FortiCloud New Account Onboarding document and Getting started on page 13 for more information on registering your accounts.

If you need to create a support ticket, the FortiCloud account must be linked to your entitled license. There are two methods to link the FortiCloud account to your license:

- The account owner must create sub user accounts for all of the users in your organization. See User permissions in the FortiCloud Asset Management Administration Guide.
- Contact FortiCare support to request that your account be linked to the license in your organization. See Creating support tickets in the FortiCloud Asset Management Administration Guide.

Acceptable FortiRecon use cases

When using FortiRecon, there are certain acceptable use case requirements that must be followed to properly leverage FortiRecon's capabilities. FortiRecon use case requirements include the following:

- The FortiRecon solution must only be used for the licensed entity and its brands. See Requirements on page 8 and Licensing on page 9.
- Domains that are added for scanning and monitoring must be owned by the licensed entity.
- The licensed entity may not add the domains and apps of its customers, partners, or vendors to *Profile Settings* > *Seeds* or the *EASM* module for monitoring. However, up to 25 of these assets may be added for vendor monitoring in the *Adversary Centric Intelligence* module. See Vendor Risk Assessment on page 120.
- Bank identification numbers (BINs) should only be added for the licensed entity and brand. See Card Fraud on page 98.

Customer monitoring

Organizations, such as MSSPs, that want to set up monitoring for their customers can reach out to our account and sales team for suitable options.

Licensing

FortiRecon requires a license. You can choose to purchase a license for one, two, or all three of the following FortiRecon modules:

- External Attack Surface Management (EASM)
- Brand Protection (BP)
- Adversary Centric Intelligence (ACI)

In addition to the desired modules, the license also indicates the maximum number of assets to be monitored by FortiRecon.

For details about the different modules and solution bundles, see the FortiRecon data sheet.

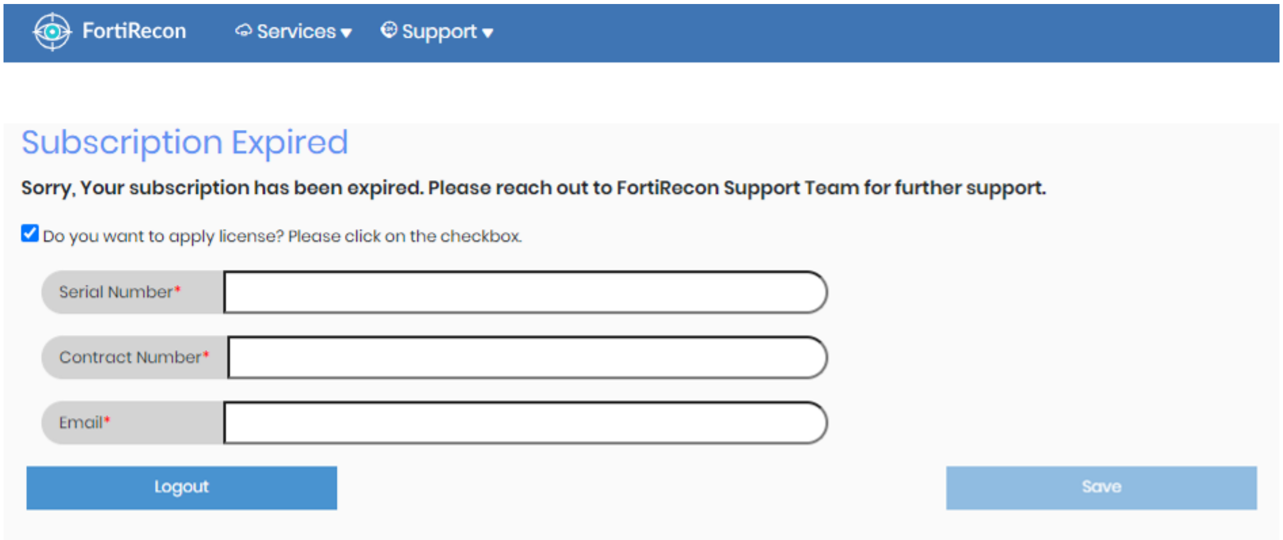
Trial Period

FortiRecon offers a 30-day trial period, allowing you to fully explore all the platform's features.

Upgrading Options

During the trial period, you have two options for upgrading:

1. **Purchasing a License**: You can purchase a license and add it to FortiRecon before the trial period expires. To add the purchased license, edit the serial and contract number fields in the *Profile Settings* page. See Subscription Details.
2. **Expired Trial Period**: If the trial period has already expired, attempting to log in will display an expiration page. In this case, you can purchase a license, select the *Do you want to apply license?* checkbox and enter the following information.
   - Serial Number.
   - Contract Number.
   - Email address used to purchase the license.



Subscription Expired

Sorry, Your subscription has been expired. Please reach out to FortiRecon Support Team for further support.

☑ Do you want to apply license? Please click on the checkbox.

Serial Number*

Contract Number*

Email*

Default alerts

FortiRecon automatically sends out default alerts if certain triggers are identified. Default alerts for each module include:

Module	Alert
External Attack Surface Management (EASM)	• New scan refresh • Leaked credentials present as part of a third party breach • Continuous monitoring refresh alert • Leaked credentials for new domain
Brand Protection (BP)	• Fraudulent domains identified, such as phishing and brand impersonation

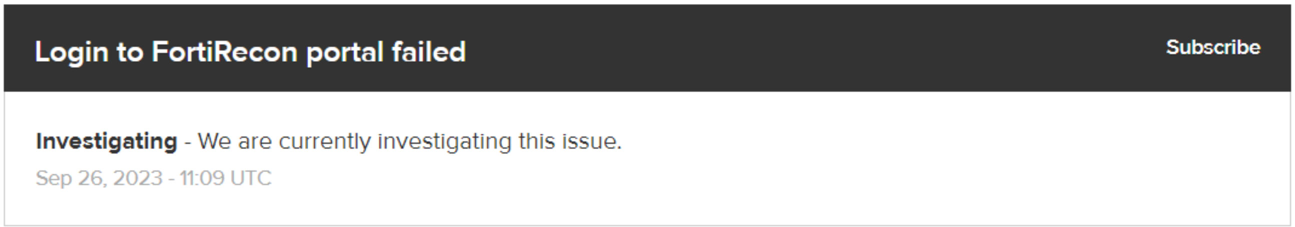
Module	Alert
	• New rogue mobile application identified • Social media impersonation identified • Exposed sensitive information on code repository • Files found in open cloud storage bucket • New threats to executives in executive monitoring
Adversary Centric Intelligence (ACI)	• Any published flash alert or report • Any high relevance report • Stealer infection identified • Credit or debit cards identified on card shops • Organization or vendor listed on a ransomware naming and shaming site • Intelligence collection lookup alert, if there is a match in the default system ICL query • Daily digest

Monitoring Service Status

The FortiRecon Status page provides an overview of the current and historical availability of the FortiRecon service. You can receive and track notifications for incidents and downtime affecting the FortiRecon GUI and Rest APIs.

To access the FortiRecon Status page, navigate to https://status.fortirecon.forticloud.com/.

The status page displays the real-time and historical incidents affecting the FortiRecon service. The real-time events affecting the infrastructure and usage of the service are displayed on the top of the page. Click *Subscribe To Updates* to receive notifications.

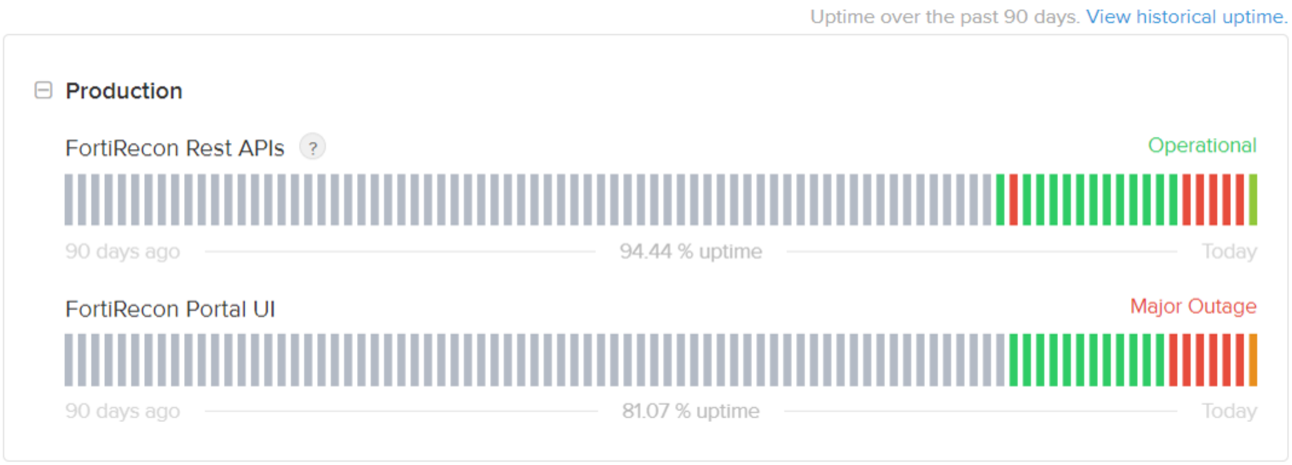


Login to FortiRecon portal failed

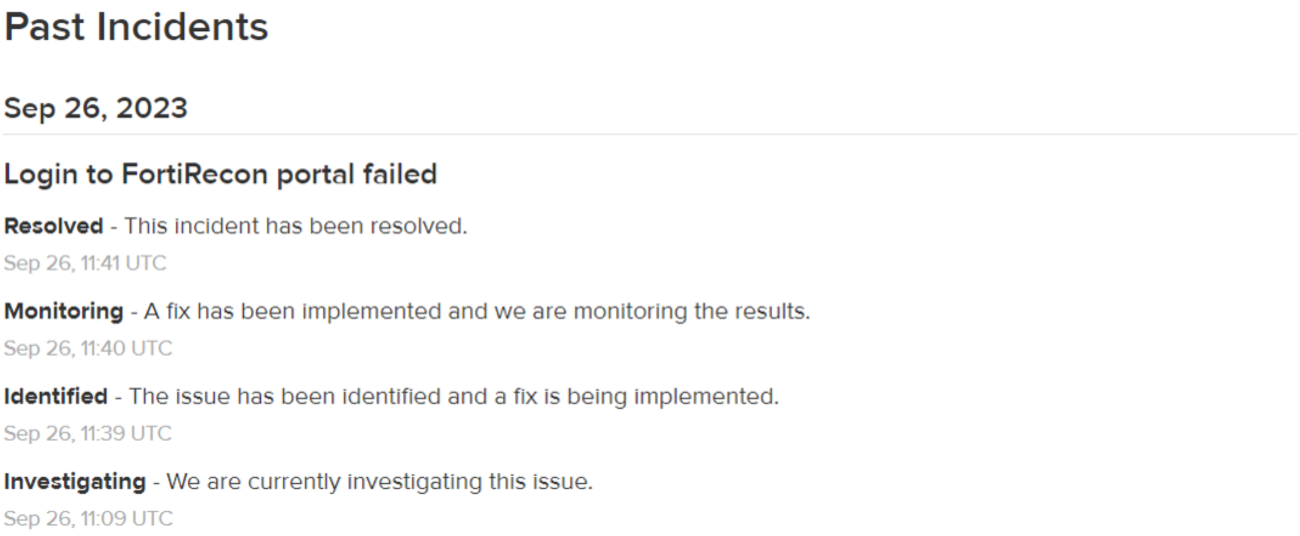
Investigating - We are currently investigating this issue.

Sep 26, 2023 - 11:09 UTC

The FortiRecon service uptime is displayed graphically for a period of 90 days. The downtime/outage events experienced by the service are indicated in colored bars; hover over each bar to view the details. Click *View historical uptime* to view the uptime/downtime experienced by the service in the past.



The historical incidents are listed in *Past Incidents* section.



Past Incidents

Sep 26, 2023

Login to FortiRecon portal failed

Resolved - This incident has been resolved.

Sep 26, 11:41 UTC

Monitoring - A fix has been implemented and we are monitoring the results.

Sep 26, 11:40 UTC

Identified - The issue has been identified and a fix is being implemented.

Sep 26, 11:39 UTC

Investigating - We are currently investigating this issue.

Sep 26, 11:09 UTC

Getting started

This section explains how to get started with FortiRecon.

When you first start with FortiRecon, you can:

- Register your FortiRecon license. See Registering the FortiRecon license on page 13.
- Subscribe to FortiRecon and start the service. See Subscribing to FortiRecon on page 14.

Registering the FortiRecon license

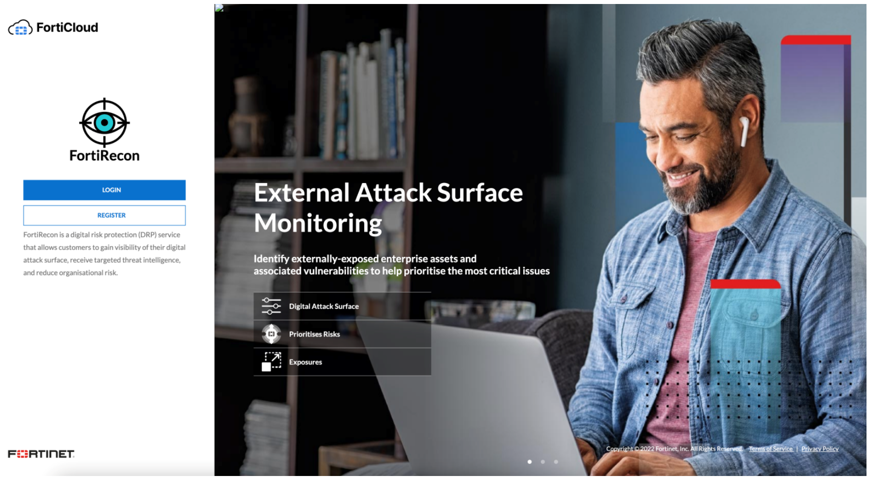
You must purchase and register a FortiRecon license before you can subscribe to FortiRecon. After you purchase the license, register the license using FortiCloud Account Services. For more information about registering products on FortiCloud, see the *FortiCloud Account Services > Registering products* documentation.

Subscribing to FortiRecon

This section describes how to subscribe to FortiRecon and start the service. Before you can subscribe to FortiRecon, you must register the license. See Registering the FortiRecon license on page 13.

To subscribe to FortiRecon:

1. After the license is registered on FortiCloud, go to FortiRecon at https://fortirecon.forticloud.com.



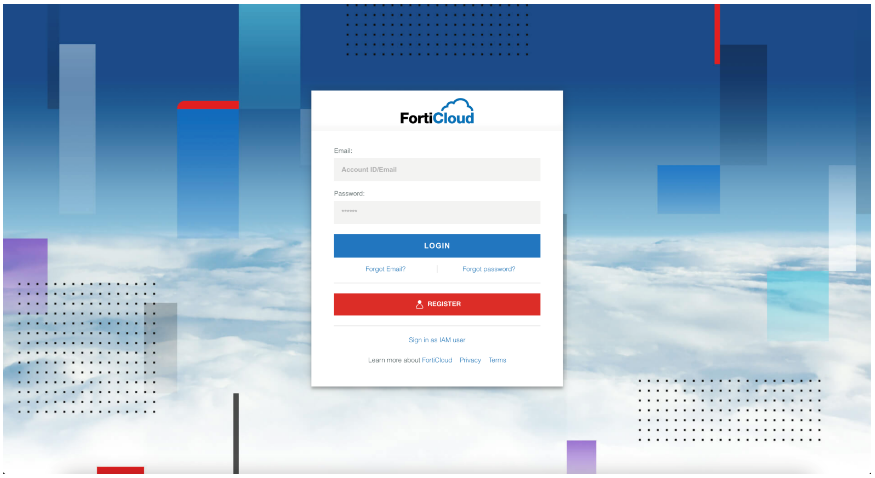
FortiRecon is a digital risk protection (DRP) service that allows customers to gain visibility of their digital attack surface, receive targeted threat intelligence, and reduce organisational risk.

External Attack Surface Monitoring

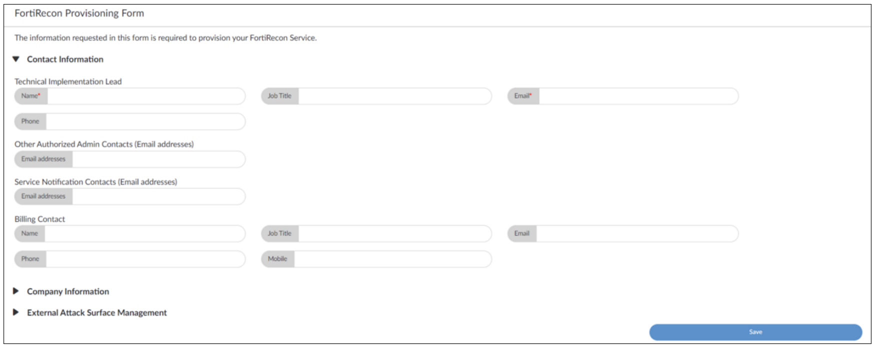
Identify externally-exposed enterprise assets and associated vulnerabilities to help prioritise the most critical issues

Copyright © 2022 Fortinet, Inc. All Rights Reserved.

2. Click *Login*. The FortiCloud login page is displayed.



3. Enter your FortiCloud credentials.
   After you log in to FortiRecon for the first time, the *FortiRecon Provisioning Form* is displayed.



FortiRecon Provisioning Form

The information requested in this form is required to provision your FortiRecon Service.

▼ Contact Information

Technical Implementation Lead

Name* | Job Title | Email*

Phone

Other Authorized Admin Contacts (Email addresses)

Email addresses

Service Notification Contacts (Email addresses)

Email addresses

Billing Contact

Name | Job Title | Email

Phone | Mobile

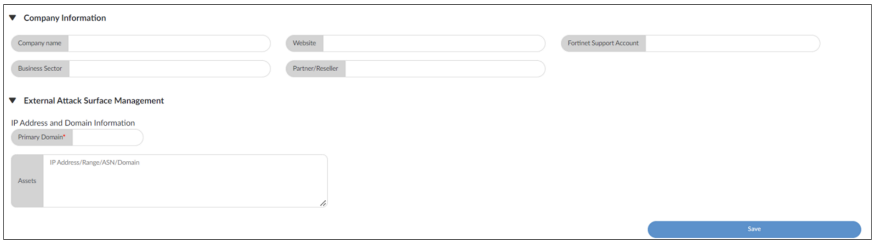
▶ Company Information

▶ External Attack Surface Management

4. Enter your contact information in the *Technical Implementation Lead* fields.

> Fields marked with a red asterisks are required information. Other fields are considered optional although it is suggested that you complete all of the fields provided to receive the most accurate service.

5. Enter the email addresses of members of your organization in the *Other Authorized Contacts* and *Service Notification Contacts* fields.
6. Enter the contact information of the billing contact in the *Billing Contact* fields.
7. Select the *Company Information* and *External Attack Surface Management* dropdowns. New information fields are displayed.



▼ Company Information

Company name | Website | Fortinet Support Account

Business Sector | Partner/Reseller

▼ External Attack Surface Management

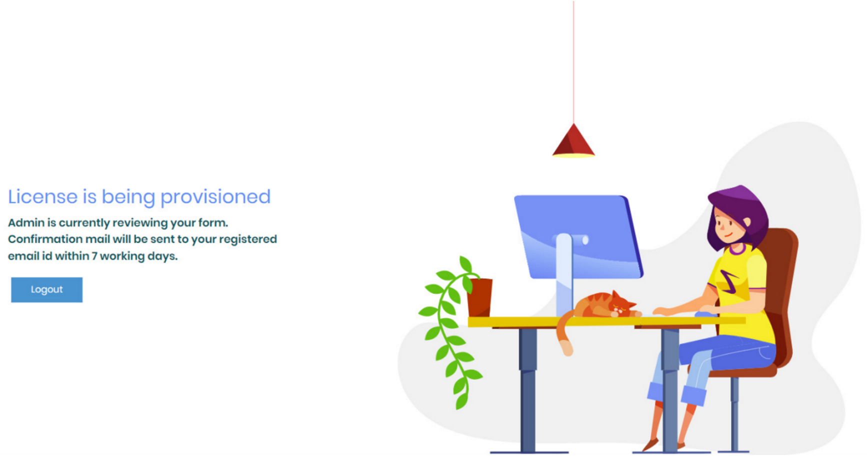
IP Address and Domain Information

Primary Domain*

Assets: IP Address/Range/ASN/Domain

8. Enter your organization's information in the *Company Information* fields.
9. Enter your organization's assets IP address and domain information in the *External Attack Surface Management* fields.
10. Click *Save*. Your information will be sent to the FortiRecon team for review and provisioning.

    A confirmation page is displayed.



License is being provisioned

Admin is currently reviewing your form. Confirmation mail will be sent to your registered email id within 7 working days.

11. Wait for the FortiRecon team to analyze your assets and populate the FortiRecon portal for you.

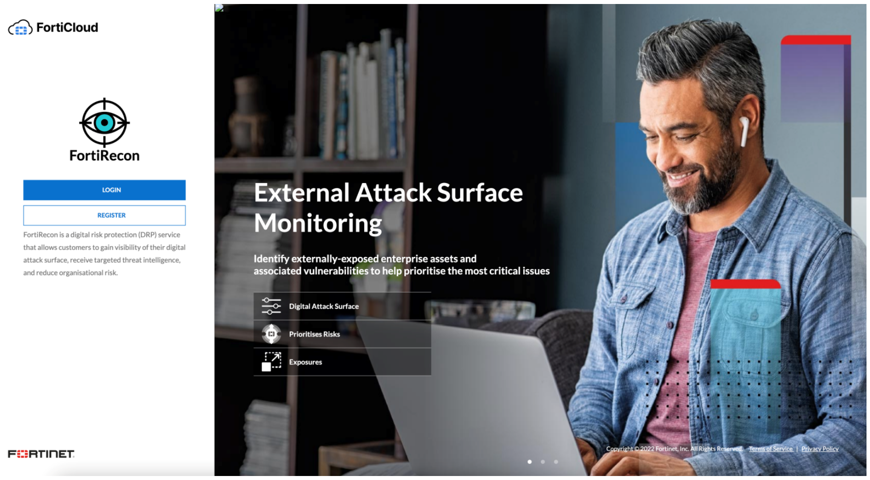
12. When you receive an email from the FortiRecon team, you can access the FortiRecon portal and review the analysis. See Accessing FortiRecon portal on page 17.

Accessing FortiRecon portal

After you have subscribed to FortiRecon and received an email from the FortiRecon team, you are ready to access the FortiRecon portal.

To access FortiRecon:

1. Go to FortiRecon at https://fortirecon.forticloud.com.



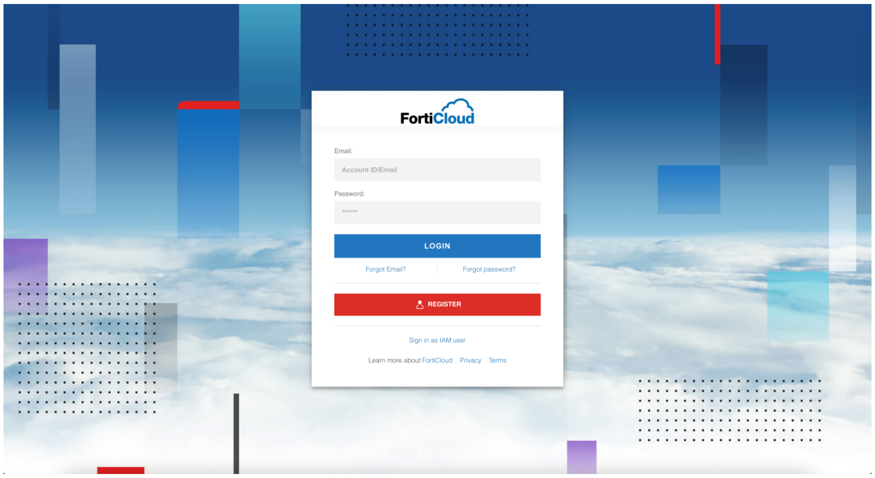
FortiRecon is a digital risk protection (DRP) service that allows customers to gain visibility of their digital attack surface, receive targeted threat intelligence, and reduce organisational risk.

External Attack Surface Monitoring

Identify externally-exposed enterprise assets and associated vulnerabilities to help prioritise the most critical issues

Copyright © 2022 Fortinet, Inc. All Rights Reserved. Terms of Service | Privacy Policy

2. Click *Login*. The FortiCloud login page is displayed.

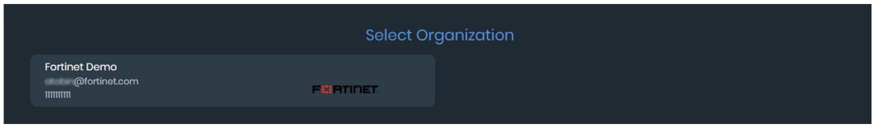


Email: Account ID/Email

Password: ******

Learn more about FortiCloud Privacy Terms

3. Enter your FortiCloud credentials.
4. Click *Login*. The FortiRecon *Select Organization* page is displayed.



Select Organization

Fortinet Demo
[redacted]@fortinet.com
[redacted]

5. Select the organization you want.
   The *EASM > Dashboard* page is displayed. See EASM on page 28.

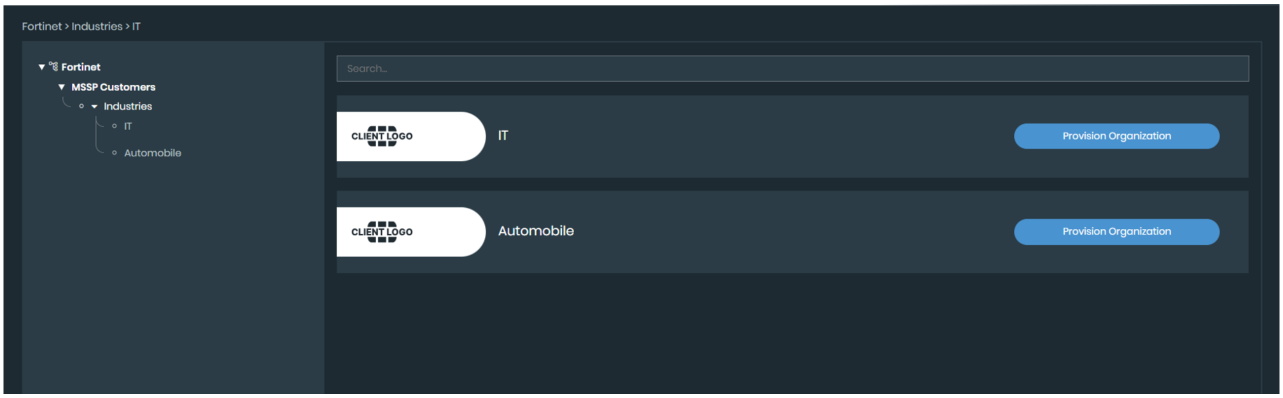
Organizations

FortiRecon supports *FortiCloud Organization*, enabling centralized account management, visibility, provisioning and hierarchical grouping of multiple FortiCare accounts with FortiRecon license through Organizational Units (OUs).

The Organization feature is primarily designed for Managed Security Service Providers (MSSPs).

Following is an overview of the process for creating and provisioning FortiRecon organization.

1. Create organization structure by setting up Organization and OUs. See Setup the Organization.
2. Invite accounts to join the Organization. See Invitations.
3. Create and manage IAM users. See Manage Users.
4. Login and provision FortiRecon OUs. See Provisioning FortiRecon Organization.



For more information about Organizations, view Organization Portal guide.

Setup the Organization

The first step for creating an Organization requires the root account user to create the Organization and define the Organization hierarchy with OUs.

When you create an Organization your account becomes the Root Account for the organization. Users with the proper permissions can add Organizational Units (OU) and invite members to join the organization.

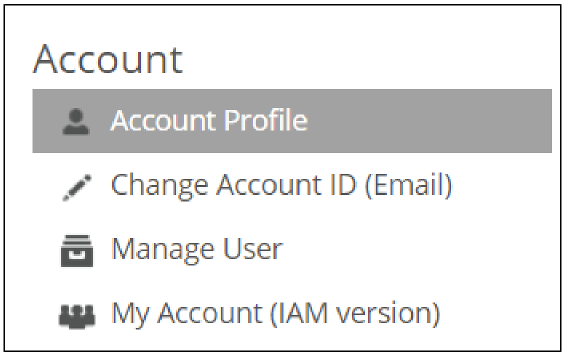
- Enabling Organization Portal
- Creating an Organization
- Adding and deleting OUs

> To create an organization in FortiCare, the FortiCare account must have a *FortiCloud Premium* subscription.

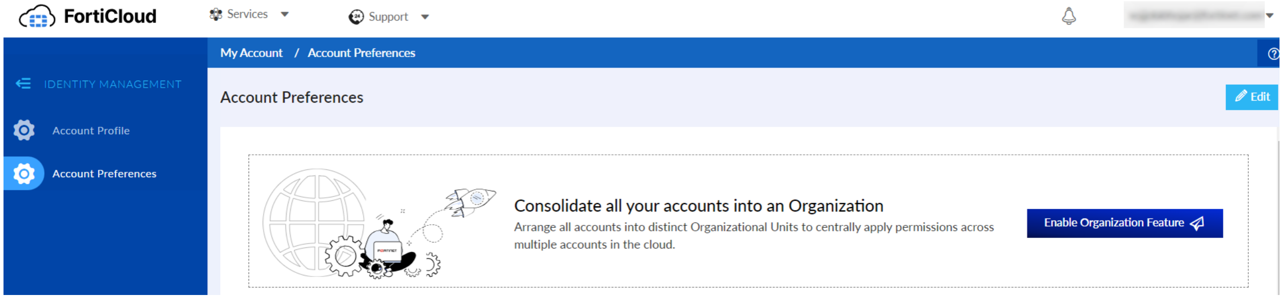
Enabling Organization Portal

To access Organization Portal in FortiCare, perform the following steps:

1. Log in to https://support.fortinet.com/ using your FortiCare account with a premium subscription.
2. From the profile menu, select *My Account.*
3. In the My Account page, click *My Account (IAM Version)*.



4. Navigate to *Account Preferences*.
5. Click *Enable Organization Feature*.



Account Preferences

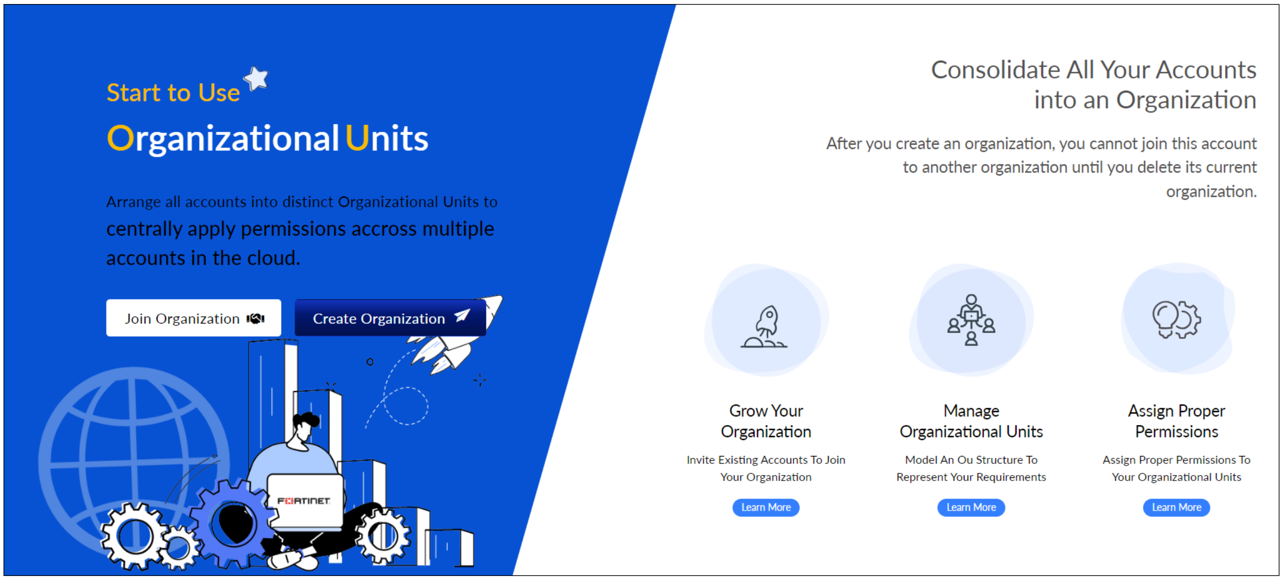
Consolidate all your accounts into an Organization

Arrange all accounts into distinct Organizational Units to centrally apply permissions across multiple accounts in the cloud.

Creating an Organization

To create an organization, perform the following steps:

1. Ensure that you have enabled Organization Portal in FortiCare. See Enabling Organization Portal.
2. In the Organization Portal, click *Create Organization*. The Master Account page opens.



Start to Use

Organizational Units

Arrange all accounts into distinct Organizational Units to centrally apply permissions accross multiple accounts in the cloud.

Consolidate All Your Accounts into an Organization

After you create an organization, you cannot join this account to another organization until you delete its current organization.

Grow Your Organization

Invite Existing Accounts To Join Your Organization

Manage Organizational Units

Model An Ou Structure To Represent Your Requirements

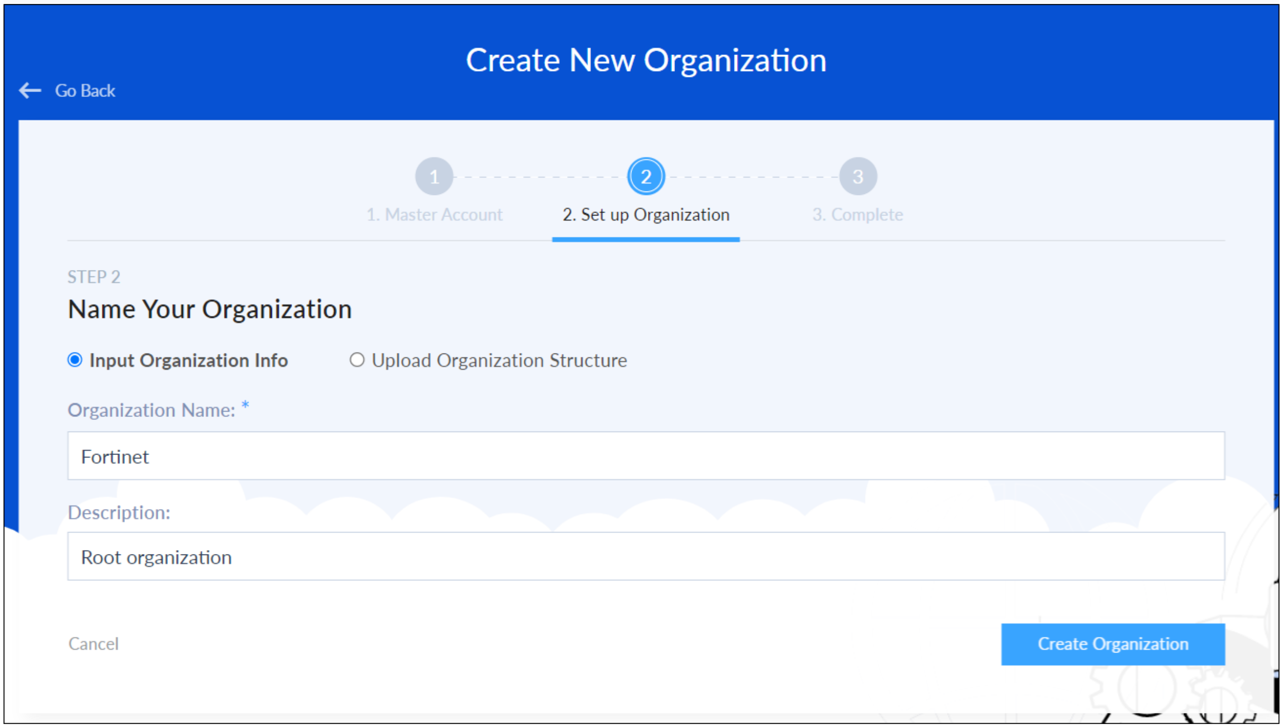
Assign Proper Permissions

Assign Proper Permissions To Your Organizational Units

3. Click *Next*. The Set up Organization page opens.

   Provide the required information:

Input Organization Info	Select this option to create your organization with the GUI.
Upload Organization Structure	Select this option to create the organization and Organizational Units with an Excel sheet. See To create an organization with the Bulk Import template.
Organization Name	Enter a name for the organization.
Description	Enter a brief description of the organization.



Create New Organization

STEP 2

Name Your Organization

● Input Organization Info ○ Upload Organization Structure

Organization Name: * Fortinet

Description: Root organization

4.

5. Click *Create Organization*. The Complete page opens.

6. Click *Close & Go To General*. The General page opens.

To create an organization with the Bulk Import template:

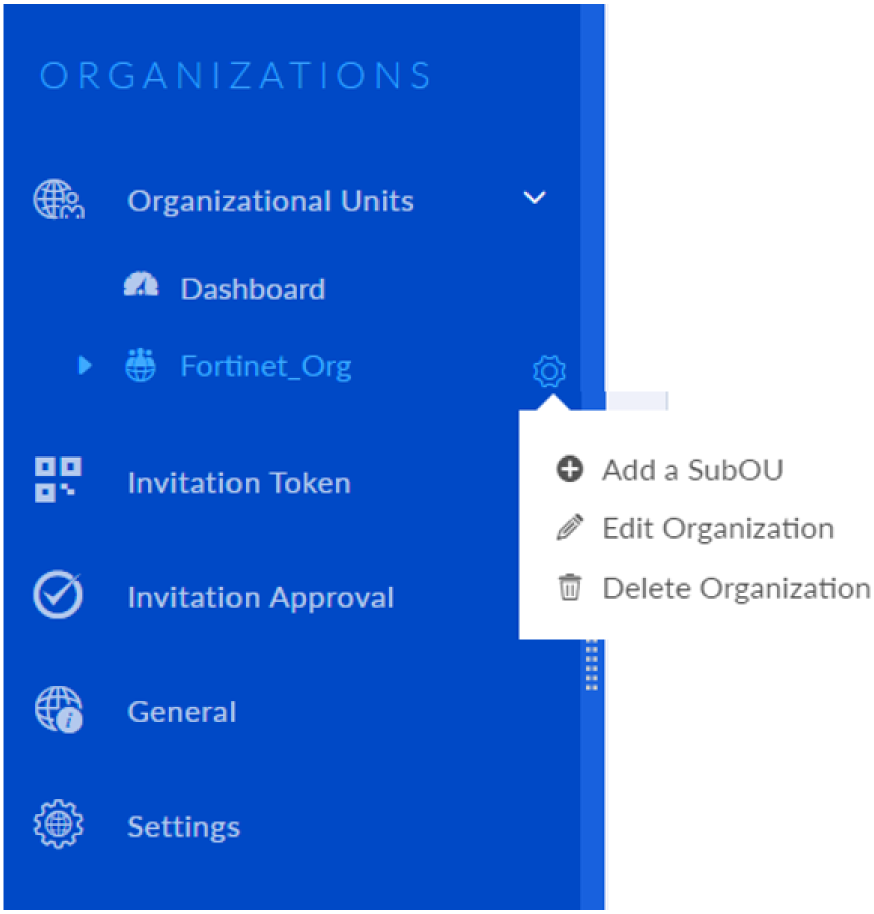
1. On the Set up Organization page, click *Upload Organization Structure*.
2. Download the Bulk Import template.
3. Use the template instructions to enter the OU information and create the organization hierarchy.
4. After you have completed the template, click *Organization Structure File Upload*, and upload the file.
5. Click *Confirm*.

Adding and deleting OUs

Organizational Units (OU) are folders for organizing your accounts. FortiRecon supports only one level of Organization Unit (OU) structure. After the OU is created, you can edit the organization details, or delete it.

To create an Organizational Unit:

1. In the navigation menu, hover over the Organization name and click the gear icon.
2. Click *Add a SubOU*. The *Add a SubOU to <org_name>* dialog opens.



3. Enter the *OU Name* and *OU Description*, then click *Confirm*. The unit is added to the organization.

To delete an Organizational Unit:

1. Hover over the OU name and click the gear icon.
2. Click *Delete OU*. The *Confirm to delete this organizational unit* dialog opens.
3. Accept the terms of the deletion and click *Confirm*.

To edit an Organization's details:

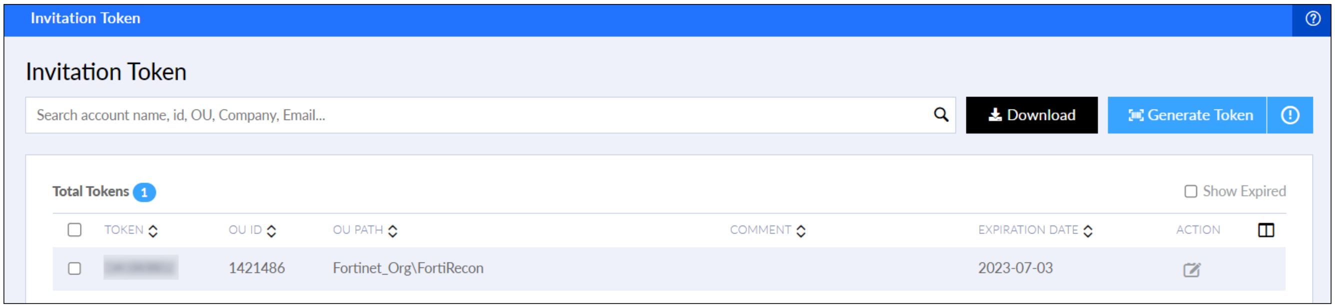
1. Hover over the Organization name and click the gear icon.
2. Click *Edit Organization* or *Edit OU*. The *Edit <OU_name>* dialog opens.
3. Update the *OU Name* and *OU Description*, and click *Confirm*.

Invitations

Once the Organization and OUs have been created, you can invite member accounts to join the Organization OUs using invitation tokens.

The process for inviting accounts is as follows:

1. The root account user generates the invitation token for each OU from the Invitation Token page. See Creating invitation tokens.
2. The root account user invites accounts to join the Organization OUs by sharing the assigned invitation token and Organization portal link (https://support.fortinet.com/organizations/) with member account users.
3. Member account users go to https://support.fortinet.com/organizations/.
4. Member account users select Join Organization and use the provided invitation token to request access.
5. The root account user approves member account requests from the Invitation Token page. See Invitation Approval.



□	TOKEN	OU ID	OU PATH	COMMENT	EXPIRATION DATE	ACTION
□	[redacted]	1421486	Fortinet_Org\FortiRecon		2023-07-03	

Creating invitation tokens

Create Invitation Tokens to invite Member Accounts via email.

To create an invitation token:

1. Go to the Invitation Token page and click *Generate Token*. The Generate Token dialog opens.
2. Configure the token settings:

Choose An Organization	Select the Organization or OU from the dropdown.

Token Expiry Date	Click the calender icon to select the token expiry date.
Comment (Optional)	Enter a description of the token.
Generate a separate token for each SubOU	Enable this option to create unique token for each OU in the organization.

3. Click *Generate Token*.

Invitation Approval

After the invitation token has been sent, the recipient can then use it to join the organization. When they request to join the organization, the request will appear on the Invitation Approval page, which displays the generated tokens and the accounts that received an invitation. Use the Invitation Approval page to approve the invitation response.

The Invitation Approval page displays the following information.

Token	The Invitation Token number.
OU ID	The Organizational Unit ID.
OU Path	The Organizational Unit name and the sub-OU.
Comment	Comments entered when the token was created.
# of Accounts Requested	Number of accounts submitted a joined orgnization request.
# of Accounts Pending Approval	The number of accounts that have not been approved.
Expiration Date	The token expiry date.

To approve an invitation:

1. Go to *Invitation Approval* and expand a token in the list.
2. Select an invitation and click *Approve.*
3. The *Confirm* to approve dialog opens.
4. Select the acknowledgment.
5. Click *Confirm.*

Manage Users

Once member accounts are added to the OUs, you can create an Organization administrative IAM user that can create and manage IAM users for the Organization OUs.

The process for creating an Organization administrative IAM user is as follows:

1. Go to the Services > IAM portal.
2. Create a new permission profile for the Organization administrative IAM user:
   a. Go to *Permission Profiles* and create a new profile.
   b. Set the type to *Organization*.

   c. Add the Asset Management, FortiCare and FortiRecon portals. Select either *Admin* or *ReadOnly* access for FortiRecon and FortiCare portals as per your requirement.
   d. Click *Submit.*

MSSP root admin/OU admins should have Admin access for Recon portal.

   See Permission profiles within Organizations in the Identity & Access Management guide for more information.

3. Create the Organization administrative IAM user:
   a. Click Add New > IAM User. The User Details pane opens.
   b. Enter the user's details and click *Next*.

Username	Type the username with no spaces. The username specified here will be used to login.
Full Name	Type the user's first and last name.
Email	Type the user's email address.
Phone	Select the country code from the dropdown, and type the user's phone number.
Description (Optional)	Type a description of the user.

   c. Set the type to Organization.
   d. Set the Permission Scope to the Organization.
   e. Select the permission profile created in the previous step.
   f. Verify the details and click *Confirm*.
   g. Generate an IAM user login password.
      i. Go to IAM Users, and click the full name of the user. The User Profile tab is displayed.
      ii. Go to the Security Credentials tab, and click Generate Password. Password reset link will be generated.

See Creating users, user groups, and roles within Organizations in the Identity & Access Management guide for more information.

Based on the access type and permission scope provided, the following roles are supported for FortiRecon:

Role	Description
pAdmin	The IAM user with *admin* access and *root organization* as permission scope will be the pAdmin. pAdmins have the ability to create and edit organizations within FortiRecon.
pUser	The IAM user with *read only* access and *root organization* as permission scope will be the pUsers. pUsers have a complete view of the organization/OU structure and read only access to FortiRecon portal. They cannot create or edit organizations.
OU Admin	The IAM user with *admin* access and any *OU* except root organization as permission scope will be the OU Admin. OU Admins will be admins for the respective organization provisioned under their OU.

Role	Description
OU User	The IAM user with *read only* access and any *OU* except root organization as permission scope will be the OU User. OU Users have read only access and can view the organization/OU structure but they will not be redirected to the FortiRecon portal unless their access is provisioned by pAdmin or OU admin.
Root account user	Only root account users will able to enable or disable other IAM users by updating user profiles in FortiCare.

The root account user must share the following details with IAM user:

- **Account ID** - the Account ID of the root account user where IAM is added
- **Username -** the IAM username provided during user creation
- **Password reset link**

If the IAM user is logging in for the first time, email verification is required.

Provisioning FortiRecon Organization

Once the organization structure is created and IAM user are added, you will be able to provision FortiRecon organizations.

Prerequisites

The following requirements must be met before provisioning a FortiRecon organization:

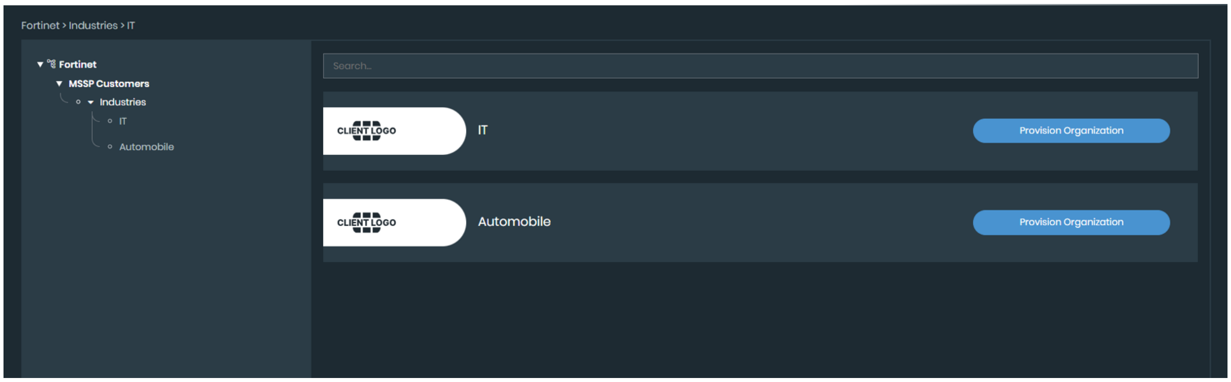
- A **pAdmin** IAM user account.
- An **OU Admin/ OU User** IAM user account. The member email account with FortiRecon license must be added as OU Admin/OU User.

See Manage Users.

To provision a FortiRecon OU:

1. Login to FortiRecon portal using pAdmin credentials.
   a. If logging in for the first time email verification must be completed.
   b. After verifying the email successfully, reload the FortiRecon portal. The FortiRecon Organization/OU structure

is displayed.



Fortinet > Industries > IT

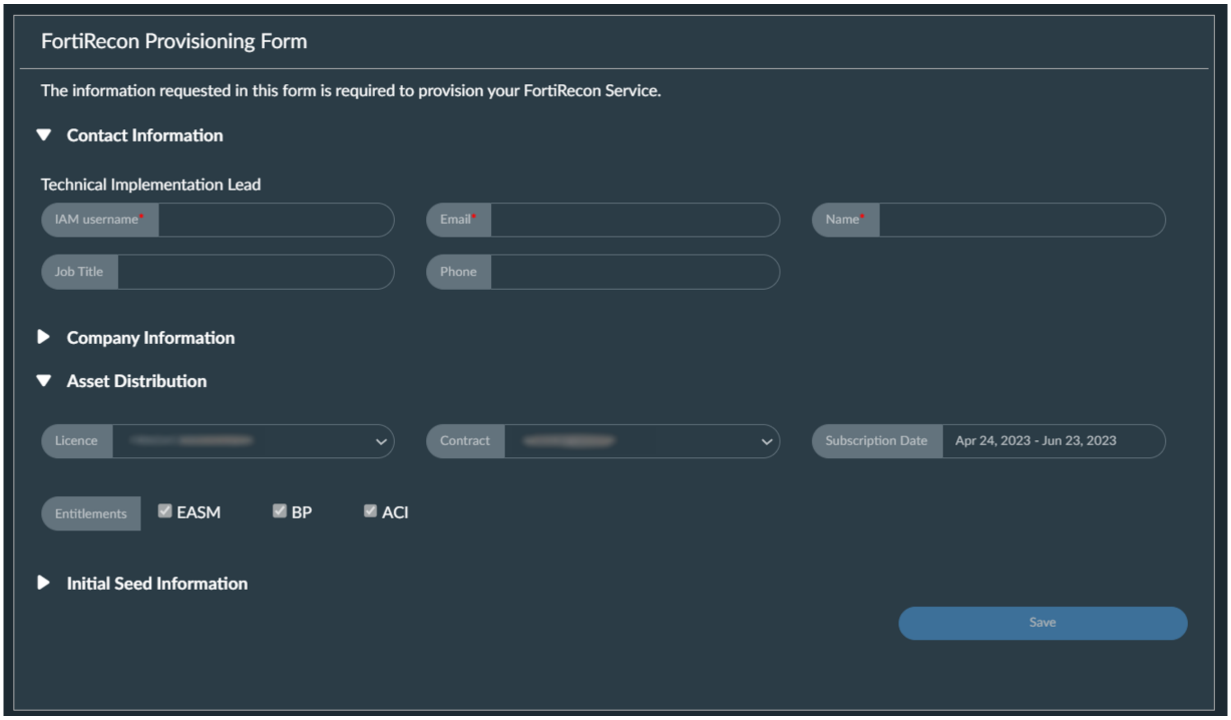
- Fortinet
  - MSSP Customers
    - Industries
      - IT
      - Automobile

Search...

CLIENT LOGO IT — Provision Organization

CLIENT LOGO Automobile — Provision Organization

2. Click *Provision Organization* for the OU that you desire to provision.
3. Provide the necessary information in the FortiRecon Provisioning Form.
   a. In Contact Information section, enter the IAM username that belongs to the IAM user added to this OU, and upon entering the IAM username, other fields such as email and name will be automatically filled.
   b. In Asset Distribution section, the license and contract details will be retrieved from the email account associated with this OU. The subscription date and entitlements will be automatically filled based on the selected license and contract.
   c. Enter *Company Information* and *Initial Seed Information* details.



FortiRecon Provisioning Form

The information requested in this form is required to provision your FortiRecon Service.

▼ Contact Information

Technical Implementation Lead

IAM username* | Email* | Name*

Job Title | Phone

▶ Company Information

▼ Asset Distribution

Licence [redacted] | Contract [redacted] | Subscription Date Apr 24, 2023 - Jun 23, 2023

Entitlements ☑ EASM ☑ BP ☑ ACI

▶ Initial Seed Information

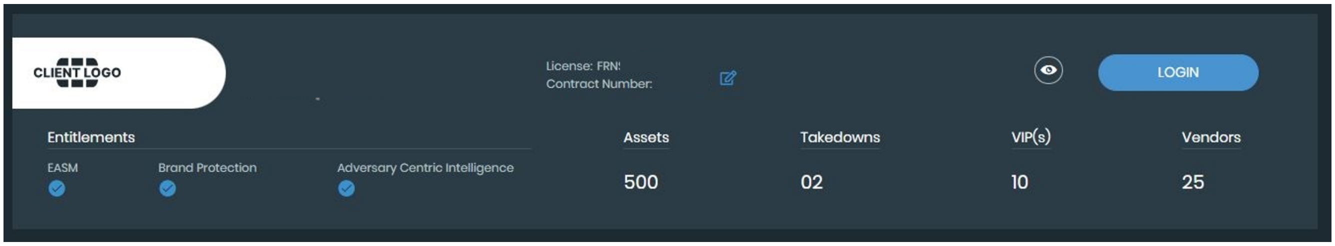
Save

4. Click *Save.*

Once the Organization is provisioned , the following information is displayed:

- License number
- Contract number
- Entitlements included (EASM/ Brand Protection/ Adversary Centric Intelligence)
- Assets count

- Takedown credits
- VIP profile count
- Vendors count

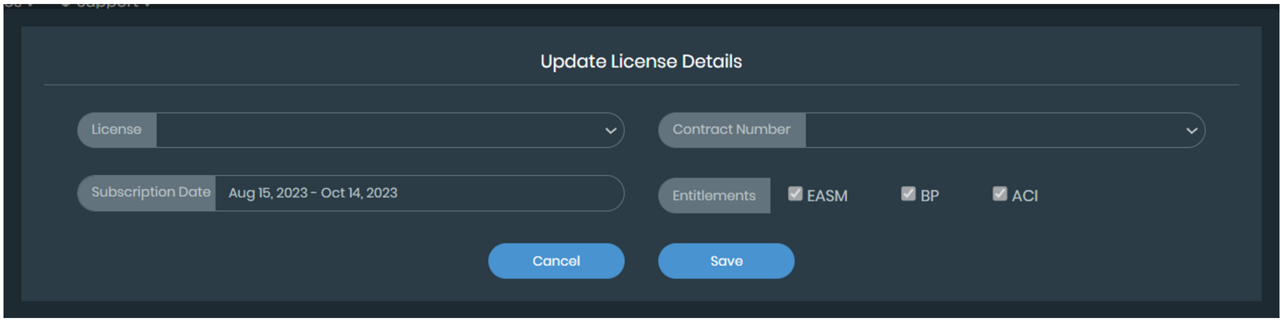


License: FRN:
Contract Number:

Entitlements			Assets	Takedowns	VIP(s)	Vendors
EASM ✓	Brand Protection ✓	Adversary Centric Intelligence ✓	500	02	10	25

To edit license details:

1. Click edit icon next to License field.
2. In *Update License Detail*s window, select the required license from the *License* drop down menu, if available.
3. *Subscription Date* and *Entitlements* are auto populated based on the selected license.


Update License Details

License:

Contract Number:

Subscription Date: Aug 15, 2023 - Oct 14, 2023

Entitlements: ☑ EASM ☑ BP ☑ ACI

To view the organization details, click view icon.

To log in to the FortiRecon portal for the provisioned organization, click *Login*.

When *OU User* logs in to the FortiRecon portal for the first time, *Your account is yet to be provisioned* message will be displayed. The *pAdmin* or *OU Admin* will receive a warning for the OU User under *Profile Settings* > *Users*, where they can provide access to the user by clicking on the edit button and assigning an access template to them. Once access is granted, the *OU User* will be notified and can subsequently access the FortiRecon portal.

EASM

The External Attack Surface Management (EASM) module provides information about your digital assets, potential security issues, and leaked credentials. You can use the EASM module to identify exposed known and unknown assets, learn about associated vulnerabilities, and prioritize the remediation of critical issues.

FortiRecon scans your digital assets and displays the results. There are two types of scans:

- **Scheduled Scan** - Full scan that consists of both *Passive* and *Active* scanners, performed weekly or monthly based on your subscription.
- **Continuous Scan** - Continuously scans all discovered assets to detect any updates such as new ports or services. The results are updated on refresh.

The *EASM* module displays scan results for your organization on the following pages :

Dashboard	Displays widgets that summarize your discovered assets and potential security issues related to your assets. You can click some widgets to display more details on the other tabs. See Dashboard on page 28.
Asset Discovery	Displays a summary of all discovered assets and details about each asset. You can mark assets as false positives, manually add assets, and manually remove assets. See Asset Discovery on page 31.
Security Issues	Displays a summary of all potential security issues and details about each issue. You can filter security issues and change the status of security issues to reflect action taken at your organization. See Security Issues on page 40.
Asset Management	Displays tags and groups used to filter and link assets. See Asset Management on page 46.
Leaked Credentials	Displays a summary of leaked credentials by year and details about each breached dataset or leaked credential incident. See Leaked Credentials on page 52.
Integrations	Displays Azure and AWS integration that are tracked in *Asset Discovery* and *Security Issues*. See Integrations on page 55.

Dashboard

The *EASM* > *Dashboard* page displays a number of widgets that summarize your discovered digital assets and potential security issues. From the *EASM* > *Dashboard* page, you can:

- View a summary of your discovered digital assets. See Viewing discovered assets summary on page 29.
- View a summary of potential security issues related to your organization. See Viewing security issues summary on page 29.
- View a global map of your assets and the number of potential security issues affecting your organization. See Viewing a map of assets on page 30.
- Download the dashboard content to your hard drive. See Downloading the EASM dashboard details on page 31.

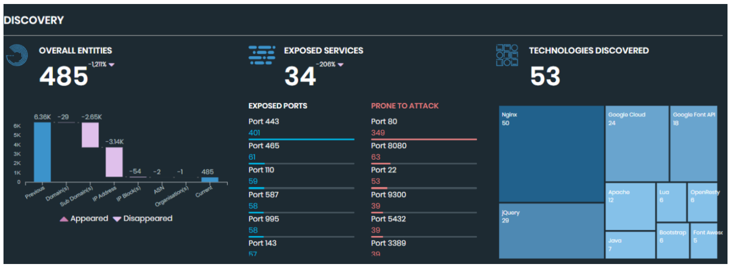
Viewing discovered assets summary

The *EASM* > *Dashboard* page displays the following widgets that summarize your discovered digital assets in the *Discovery* section:

- Overall Entities
- Exposed Services
- Technologies Discovered

To view discovered assets summary:

1. Go to the *EASM* > *Dashboard* page. The list of assets discovered by FortiRecon is displayed in the *Discovery* section.



2. Use the following widgets to review your discovered assets:

Overall Entities	Displays the number of following entities discovered by FortiRecon: • *Previous*: results of the previous FortiRecon scan. • *Domain*: number of domains found by the latest scan. • *Sub-domain*: number of sub-domains found by the latest scan. • *IP address*: number of IP addresses found by the latest scan. • *IP block*: number of IP blocks found by the latest scan. • *ASN* (Autonomous System Number): number of ASNs found by the latest scan. • *Org name*: number of organizations found by the latest scan. • *Current*: results of the current scan
Exposed Services	Displays all the exposed services discovered by FortiRecon, including exposed ports.
Technologies Discovered	Displays all the technologies discovered by FortiRecon.

3. Click the *Overall Entities* widget or the *Exposed Services* widget to display more details on the *Asset Discovery* page. See Asset Discovery on page 31.

Viewing security issues summary

The *EASM* > *Dashboard* page displays the following widgets that summarize potential security issues in the *Issues* section:

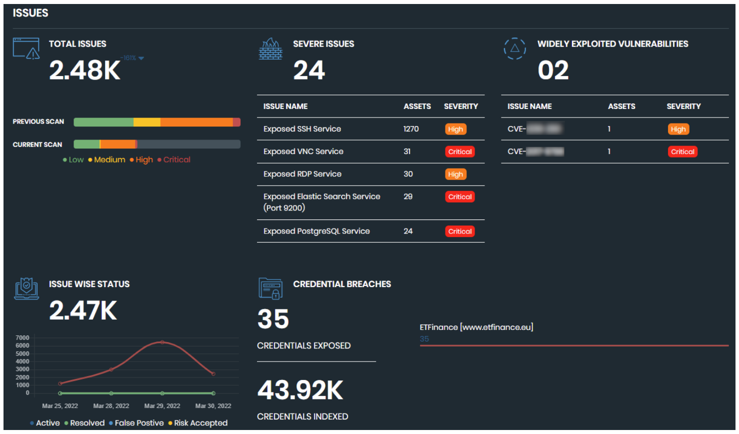
- Total Issues
- Severe Issues
- Widely Exploited Vulnerabilities

- Issue Wise Status
- Credential Breaches

Use the *Severe Issues* tooltip to review information on the count of unique *High* and *Critical* issues.

To view discovered assets summary:

1. Go to the *EASM* > *Dashboard* page, and scroll to the *Issues* section. The list of potential security issues is displayed.



ISSUES

TOTAL ISSUES

2.48K -161%

PREVIOUS SCAN

CURRENT SCAN

● Low ● Medium ● High ● Critical

SEVERE ISSUES

24

ISSUE NAME	ASSETS	SEVERITY
Exposed SSH Service	1270	High
Exposed VNC Service	31	Critical
Exposed RDP Service	30	High
Exposed Elastic Search Service (Port 9200)	29	Critical
Exposed PostgreSQL Service	24	Critical

WIDELY EXPLOITED VULNERABILITIES

02

ISSUE NAME	ASSETS	SEVERITY
CVE-[redacted]	1	High
CVE-[redacted]	1	Critical

ISSUE WISE STATUS

2.47K

CREDENTIAL BREACHES

35

CREDENTIALS EXPOSED

43.92K

CREDENTIALS INDEXED

ETFinance [www.etfinance.eu]

35

2. Use the following widgets to review your security issues:

Total Issues	Displays the total number of issues discovered by the latest scan compared to the results of the previous scan.
Severe Issues	Displays the number of severe issues, and then lists the name, affected assets, and severity rating of the issues.
Widely Exploited Vulnerabilities	Displays the number of widely exploited vulnerabilities discovered, and then lists the name, affected assets, and severity rating of the issues.
Credential Breaches	Displays the number of exposed credentials and the number of indexed credentials.

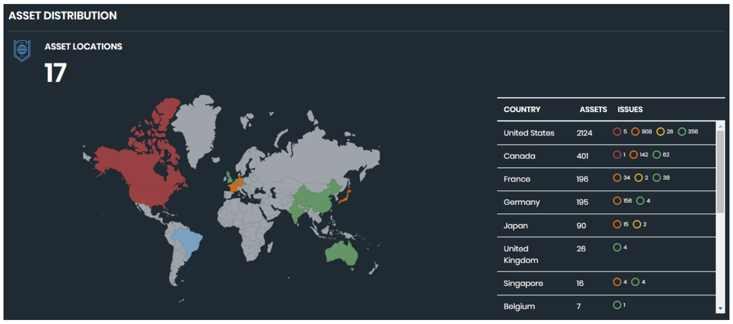
3. Click an issue or vulnerability to display more details on the *Security Issues* page. See Security Issues on page 40.

Viewing a map of assets

The *EASM* > *Dashboard* page displays a global map of your digital assets in the *Asset Distribution* section. The color of the country aligns with the highest severity level of potential issues. If the country is blue, no issues are recorded.

To view a map of assets:

1. Go to the *EASM* > *Dashboard* page, and scroll to the *Asset Distribution* section. A global map of your discovered assets is displayed.



ASSET DISTRIBUTION

ASSET LOCATIONS

17

COUNTRY	ASSETS	ISSUES
United States	2124	○ 5 ○ 908 ○ 26 ○ 356
Canada	401	○ 1 ○ 142 ○ 62
France	196	○ 34 ○ 2 ○ 38
Germany	195	○ 156 ○ 4
Japan	90	○ 15 ○ 2
United Kingdom	26	○ 4
Singapore	16	○ 4 ○ 4
Belgium	7	○ 1

2. Use the table to view the number of assets and potential security issues in each country.

Column	Description
Country	Lists countries where your digital assets were discovered.
Assets	Displays the number of assets discovered in each country.
Issues	Displays the number of potential security issues and indicates the severity rating of the issues by color: • Red indicates critical. • Orange indicates high. • Yellow indicates medium. • Green indicates low. The colors on the map align with the severity level of the issues.

3. Click a country or issue in the table to display more details on the *Security Issues* page. See Security Issues on page 40.

Downloading the EASM dashboard details

The EASM dashboard details can be downloaded to your hard drive. The process downloads a zip file named *EASM Dashboard.zip* that contains the following items:

- List of discovered assets in Microsoft Excel format
- List of issues in Microsoft Excel format
- An attack surface summary dashboard in PDF

To download the EASM dashboard:

1. Go to *EASM* > *Dashboard*, and click *Download*.
2. Retrieve the download from *Profile Settings*. See Retrieving downloads on page 145.

Asset Discovery

The *EASM* > *Asset Discovery* page provides a summary of all discovered assets and details about each asset. From the *Asset Discovery* page, you can:

- View a summary about and details of your assets. See Viewing asset details on page 32.
- Mark discovered assets as false positives to remove them from the next scheduled FortiRecon scan. See Marking assets as false positives on page 34.
- Manually add assets to FortiRecon to include them in the next scheduled scan. See Adding assets manually on page 35.
- Manually remove assets from the next scheduled FortiRecon scan. See Removing assets manually on page 35.
- Assign tags to assets for focused filtering. See Assigning tags on page 36.

> Tags are created in *EASM* > *Asset Management*. Assets can also be assigned to tags in bulk in the *Asset Management* page. See Asset Management on page 46.

- Perform a FortiDAST vulnerability scan on assets. See Performing a FortiDAST scan on page 37.
- View DNS health report for your domains. See DNS Health Report on page 38.
- Export a list of assets to an Excel file. See Exporting assets.

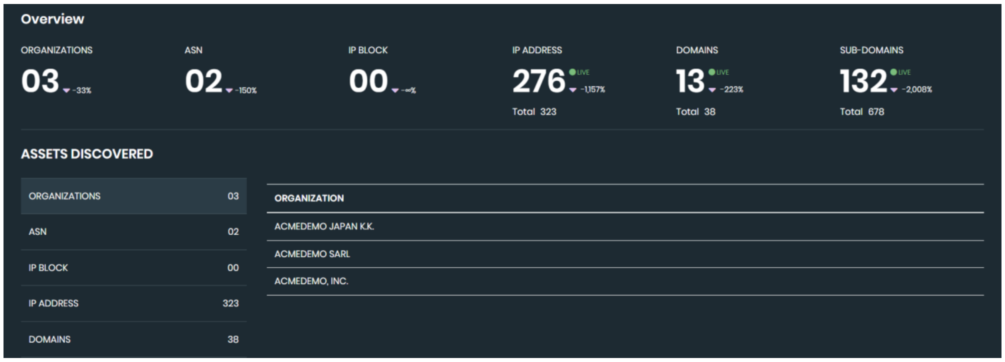
Viewing asset details

The *EASM* > *Asset Discovery* page displays the number of assets in an *Overview* section and in an *Assets Discovered* list.

You can display details about an asset by clicking a number in the *Overview* section or a category in the *Assets Discovered* list. When you are reviewing asset details, you can mark assets as *False Positive* as needed to remove them from future FortiRecon scans.

To view asset details:

1. Go to *EASM* > *Asset Discovery*. The number of discovered assets display in an *Overview* section across the top and in an *Assets Discovered* list on the left side of the page.



Overview

ORGANIZATIONS	ASN	IP BLOCK	IP ADDRESS	DOMAINS	SUB-DOMAINS
03 ▾ -33%	02 ▾ -150%	00 ▾ -∞%	276 ● LIVE ▾ -1,157%	13 ● LIVE ▾ -223%	132 ● LIVE ▾ -2,008%
			Total 323	Total 38	Total 678

ASSETS DISCOVERED

ORGANIZATIONS	03
ASN	02
IP BLOCK	00
IP ADDRESS	323
DOMAINS	38

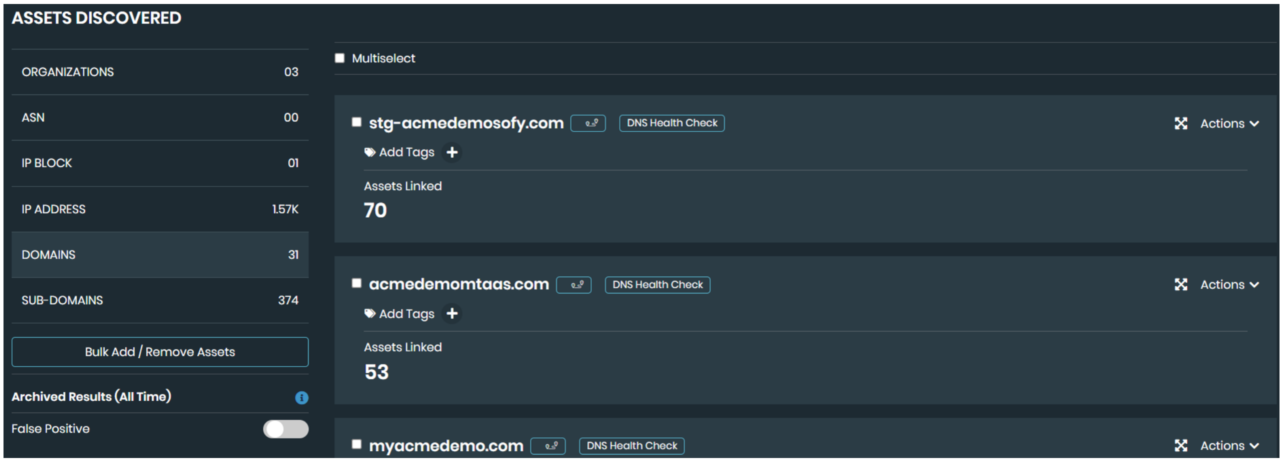
ORGANIZATION
ACMEDEMO JAPAN K.K.
ACMEDEMO SARL
ACMEDEMO, INC.

The following information is available:

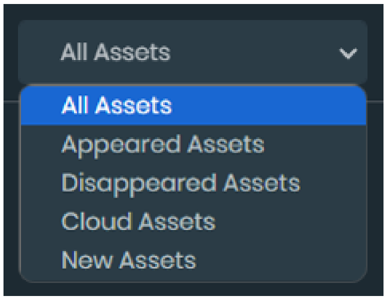
Organizations	The number of organizations that have been detected as belonging to you.
ASN	The number of autonomous system numbers (ASNs) that are linked to the detected organizations.
IP blocks	The number of IP blocks associated with the ASNs.

IP address	The number of IP addresses that are linked to the IP blocks.
Domains	The number of domains linked to your organization.
Sub-domains	The number of sub-domains linked to your organization.

2. In the *Overview* bar, click a number, or in the *Assets Discovered* list, click an asset category. Details about the selected item are displayed on the right side of the page.
   For example, click *Domains*. On the right side of the page, the names of the discovered domains are displayed.



3. Filter the assets from the dropdown menu:

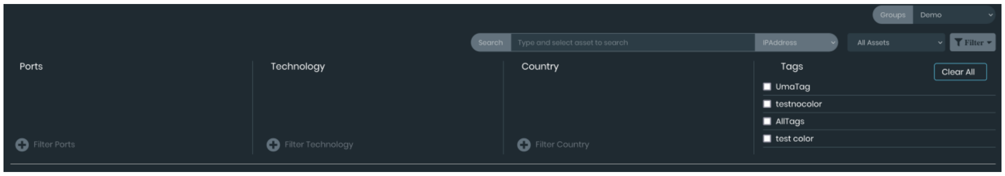


   a. Select *Appeared Assets* to show assets that appeared in the latest scan.
   b. Select *Disappeared Assets* to show assets that disappeared in the latest scan.
   c. Select *Cloud Assets* to show cloud-based assets.

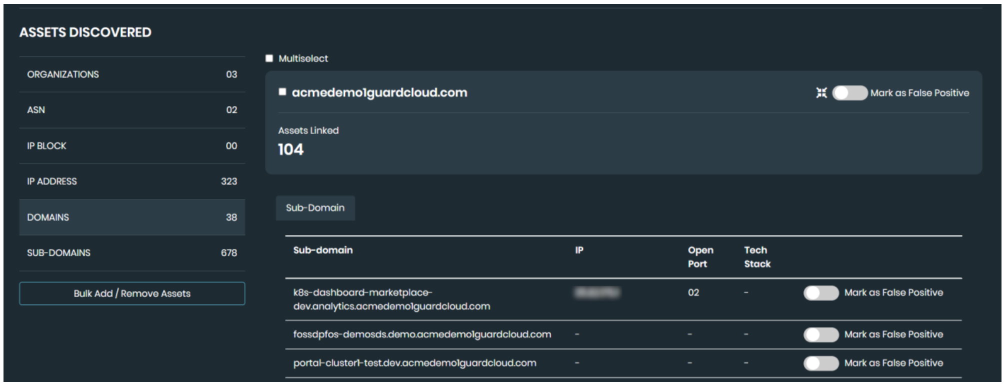
   Cloud assets can only be filtered if the AWS cloud environment has been integrated. See Integrations on page 55.

   d. Select *New Assets* to show new assets or assets that have updates.

4. Select *Filter* to define ports, technology, country, tag, and group filters.



5. Click the *Expand* icon. Details about the domain are displayed.



ASSETS DISCOVERED

ORGANIZATIONS	03
ASN	02
IP BLOCK	00
IP ADDRESS	323
DOMAINS	38
SUB-DOMAINS	678

□ acmedemo1guardcloud.com

Assets Linked
104

Sub-domain	IP	Open Port	Tech Stack	
k8s-dashboard-marketplace-dev.analytics.acmedemo1guardcloud.com	[redacted]	02	-	Mark as False Positive
fossdpfos-demosds.demo.acmedemo1guardcloud.com	-	-	-	Mark as False Positive
portal-cluster1-test.dev.acmedemo1guardcloud.com	-	-	-	Mark as False Positive

6. If an asset should be removed from the next scheduled FortiRecon scan, mark the asset as *False Positive*. See also Marking assets as false positives on page 34.

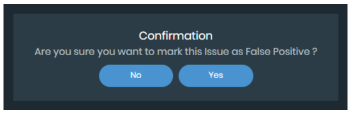
Marking assets as false positives

You can manually mark any of the following discovered assets as false positives to remove them from the next scheduled FortiRecon scan:

- ASN
- IP blocks
- IP addresses
- Domains
- Sub-domains

To mark false positives:

1. Go to *EASM* > *Asset Discovery*. The discovered assets are displayed.
2. Click one of the following assets to display its details:
   - ASN
   - IP Blocks
   - IP Address
   - Domains
   - Sub-domains
3. Select an asset, and toggle on *Mark as False Positive*.

   Confirmation
   Are you sure you want to mark this Issue as False Positive ?

   You can also select the *Multiselect* checkbox to select all or some assets, and then mark them as false positives.

   A confirmation dialog is displayed.
4. Click *Yes*.

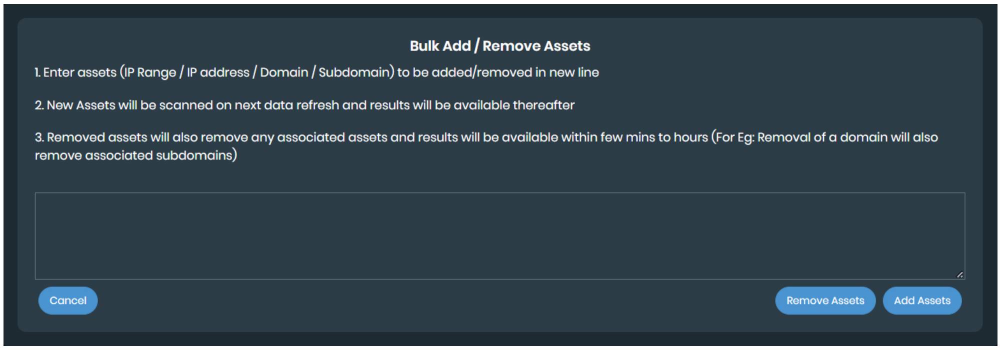
Adding assets manually

FortiRecon discovers assets for you. You can also manually add assets to FortiRecon scans.

When you manually add assets to FortiRecon, results for the assets are visible after the next scheduled FortiRecon scan.

To add assets:

1. Go to *EASM* > *Asset Discovery*. The discovered assets are displayed.
2. Click *Bulk Add / Remove Assets*. The *Bulk Add / Remove Assets* dialog is displayed.



Bulk Add / Remove Assets

1. Enter assets (IP Range / IP address / Domain / Subdomain) to be added/removed in new line

2. New Assets will be scanned on next data refresh and results will be available thereafter

3. Removed assets will also remove any associated assets and results will be available within few mins to hours (For Eg: Removal of a domain will also remove associated subdomains)

3. Enter the assets, and click *Add Assets*.

The scan results for the newly added assets will be available within 24 hours in FortiRecon portal.

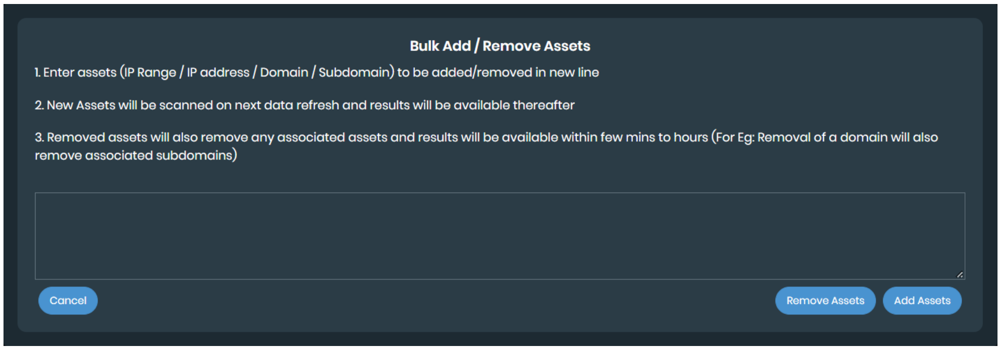
Removing assets manually

FortiRecon discovers assets for you. You can also manually remove assets from FortiRecon scans.

When you manually remove assets from FortiRecon, any associated assets are also removed. The changes are visible within minutes or hours, depending on the change.

To remove assets:

1. Go to *EASM* > *Asset Discovery*. The discovered assets are displayed.
2. Click *Bulk Add / Remove Assets*. The *Bulk Add / Remove Assets* dialog is displayed.



Bulk Add / Remove Assets

1. Enter assets (IP Range / IP address / Domain / Subdomain) to be added/removed in new line

2. New Assets will be scanned on next data refresh and results will be available thereafter

3. Removed assets will also remove any associated assets and results will be available within few mins to hours (For Eg: Removal of a domain will also remove associated subdomains)

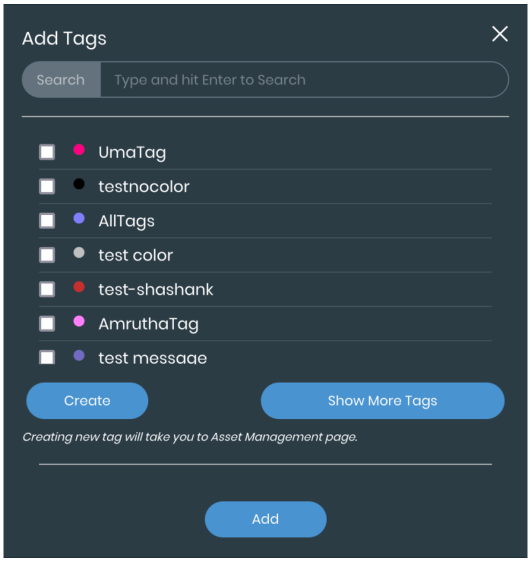
3. Enter the assets, and click *Remove Assets*.

Assigning tags

Tags can be assigned to assets for focused filtering in the *EASM* > *Asset Discovery* page. For more information on tags, see Asset Management on page 46.

To assign a tag to an asset:

1. Go to *EASM* > *Asset Discovery*.
2. Find the asset you want to tag and click the + icon. The *Add Tags* dialog is displayed.

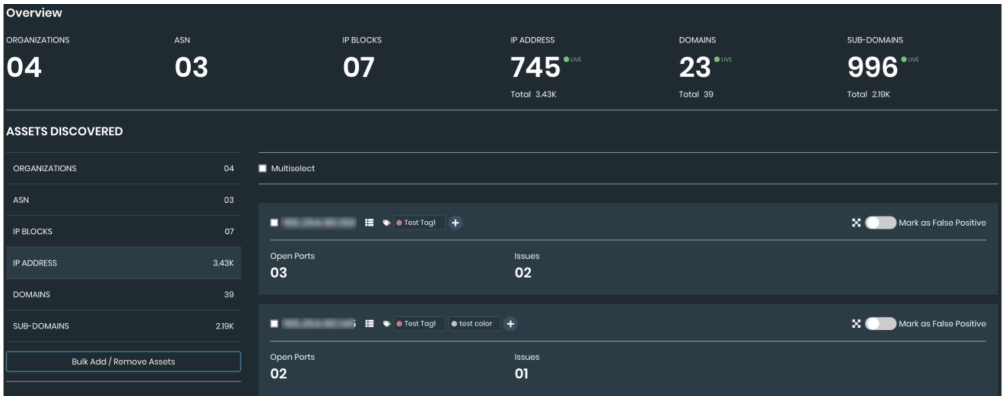


- ☐ ● UmaTag
- ☐ ● testnocolor
- ☐ ● AllTags
- ☐ ● test color
- ☐ ● test-shashank
- ☐ ● AmruthaTag
- ☐ ● test message

Creating new tag will take you to Asset Management page.

To create a new tag, click *Create* in the *Add Tags* dialog or go to *EASM* > *Asset Management* page. See Creating a tag on page 46.

3. Select the tags you would like to assign.
4. Click *Add*.

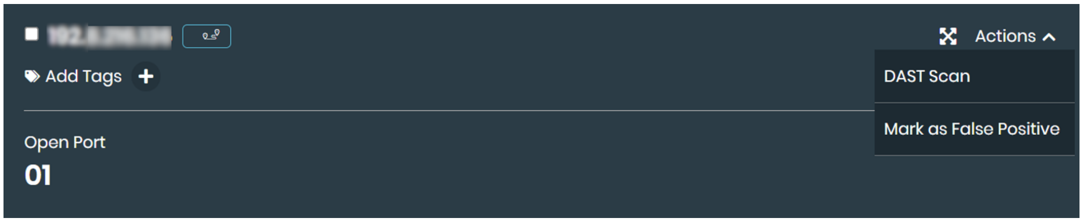


Performing a FortiDAST scan

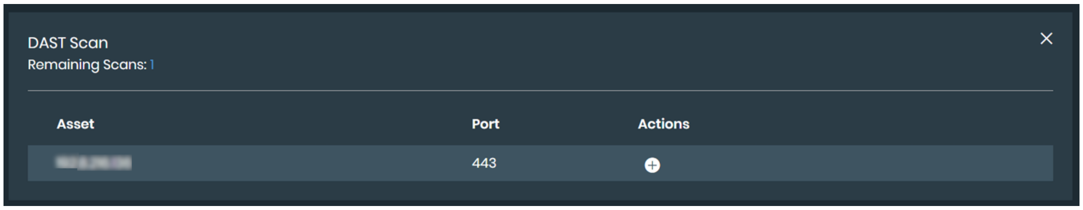
You can use FortiDAST to perform a vulnerability scan on your assets. By leveraging a FortiDAST integration with FortiRecon, you can identify vulnerabilities and security gaps within your assets. See the FortiDAST User Guide for more information on how the integration and scanning works.

To scan an asset with FortiDAST:

1. Add a FortiDAST integration to FortiRecon. See Adding integrations on page 55.
2. Go to *EASM* > *Asset Discovery*.
3. Navigate to the asset you want to scan.
4. Select *Actions* > *DAST Scan*.



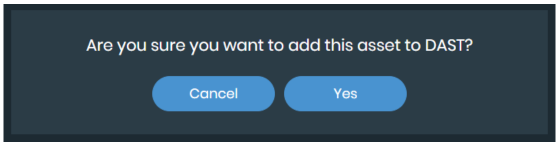
The *DAST Scan* dialog opens with number of *Remaining Scans* displayed.



DAST Scan
Remaining Scans: 1

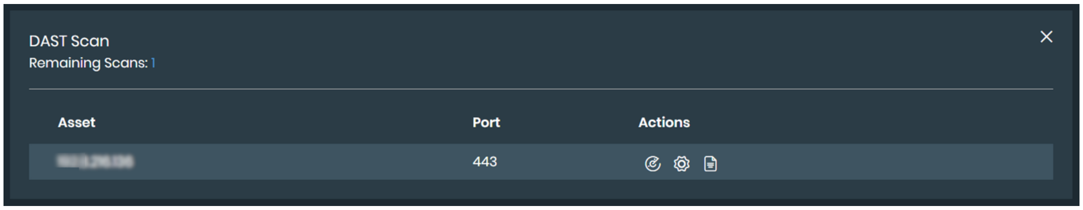
Asset	Port	Actions
[redacted]	443	⊕

5. Click *Add* beside the asset you want to add to DAST. A confirmation message is displayed.



Are you sure you want to add this asset to DAST?

6. Click *Yes*. The *Scan*, *Config Scan*, and *View Result* buttons become available for the asset.



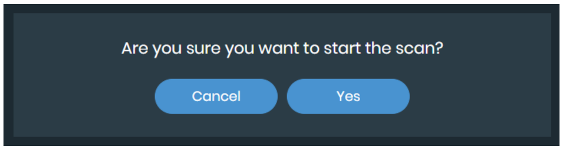
DAST Scan
Remaining Scans: 1

Asset	Port	Actions
[redacted]	443	◎ ⚙ 🗎

7. Click *Config Scan*. You will be redirected to FortiDAST.

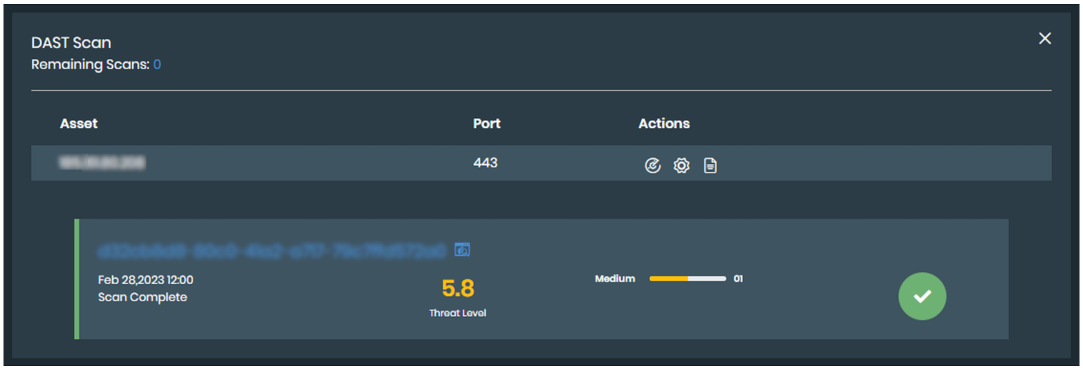
Only master or sub users will be redirected to FortiDAST to complete the configuration. Other users will be prompted with a dialog on how to proceed.

8. Configure the scanner. See the FortiDAST User Guide for more information.
9. Click *Scan*. A confirmation message is displayed.



Are you sure you want to start the scan?

10. Click *Yes*.
11. Once the scan has started, click *View Result* to view the status of the scan.



DAST Scan
Remaining Scans: 0

Asset	Port	Actions
[redacted]	443	

[redacted]

Feb 28,2023 12:00
Scan Complete

5.8
Threat Level

Medium 01

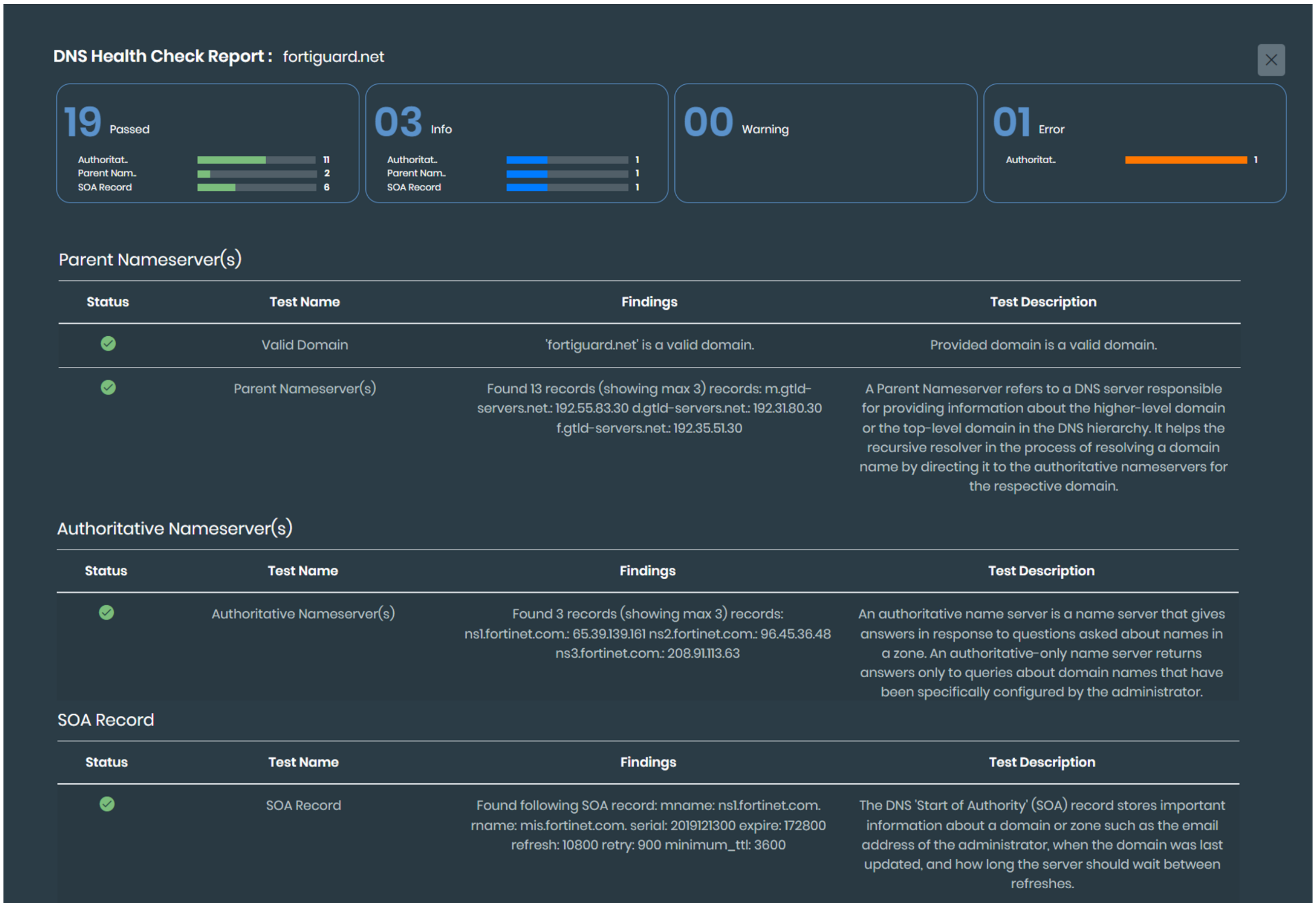
> You can scan the same asset again by selecting *ReScan*.

DNS Health Report

FortiRecon's DNS Health Report feature is a powerful tool that provides a comprehensive analysis of your domain's DNS health. This feature offers detailed information on passed, info, warning, and error counts, allowing you to quickly identify and address any potential issues. The report includes sections dedicated to the *Parent Nameserver(s)*, *Authoritative Nameserver(s)*, and *SOA Records*, offering valuable insights into the overall health and adherence to DNS standards of your domain.

To view DNS health report:

1. Go to *EASM* > *Asset Discovery* > *Domain*.
2. Navigate to the domain you want to view the report for.
3. Select *DNS Health Report*.



DNS Health Check Report : fortiguard.net

Parent Nameserver(s)

Status	Test Name	Findings	Test Description
✓	Valid Domain	'fortiguard.net' is a valid domain.	Provided domain is a valid domain.
✓	Parent Nameserver(s)	Found 13 records (showing max 3) records: m.gtld-servers.net.: 192.55.83.30 d.gtld-servers.net.: 192.31.80.30 f.gtld-servers.net.: 192.35.51.30	A Parent Nameserver refers to a DNS server responsible for providing information about the higher-level domain or the top-level domain in the DNS hierarchy. It helps the recursive resolver in the process of resolving a domain name by directing it to the authoritative nameservers for the respective domain.

Authoritative Nameserver(s)

Status	Test Name	Findings	Test Description
✓	Authoritative Nameserver(s)	Found 3 records (showing max 3) records: ns1.fortinet.com.: 65.39.139.161 ns2.fortinet.com.: 96.45.36.48 ns3.fortinet.com.: 208.91.113.63	An authoritative name server is a name server that gives answers in response to questions asked about names in a zone. An authoritative-only name server returns answers only to queries about domain names that have been specifically configured by the administrator.

SOA Record

Status	Test Name	Findings	Test Description
✓	SOA Record	Found following SOA record: mname: ns1.fortinet.com. rname: mis.fortinet.com. serial: 2019121300 expire: 172800 refresh: 10800 retry: 900 minimum_ttl: 3600	The DNS 'Start of Authority' (SOA) record stores important information about a domain or zone such as the email address of the administrator, when the domain was last updated, and how long the server should wait between refreshes.

Exporting assets

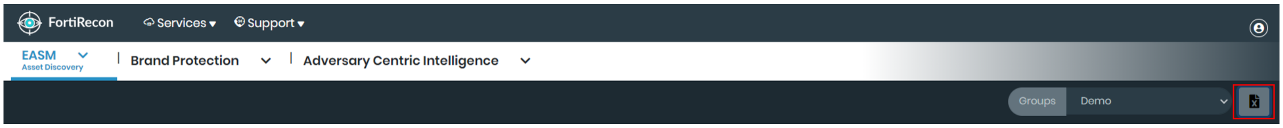
You can export a list of assets into an Excel file. The spreadsheet will include the information on:

- Asset
- Open Ports
- Linked Assets
- Total Issues
- Country
- Tags
- Groups
- Discovery
- Last Refreshed On

To export discovered assets:

1. Go to *EASM* > *Asset Discovery*.
2. Optionally, apply the required filters to export specific types of assets. See Viewing asset details.

3. Click *Download* icon. The file is downloaded to your computer.



Security Issues

The *EASM* > *Security Issues* page provides a summary of all potential security issues and details about each issue. From the *Security Issues* page, you can:

- View a summary about and details of all potential security issues related to your assets. See Viewing security issues on page 40.
- Apply filters to the list of security issues to hone in on specific issues. See Filtering security issues on page 42.
- Change the status of security issues to reflect changes made at your organization to address the issues. See Changing the status of security issues on page 43.
- Add a comment to explain status changes made to security issues. See Adding a comment to a security issue on page 44.
- Export security issues to an Excel file. See Exporting security issues.

Viewing security issues

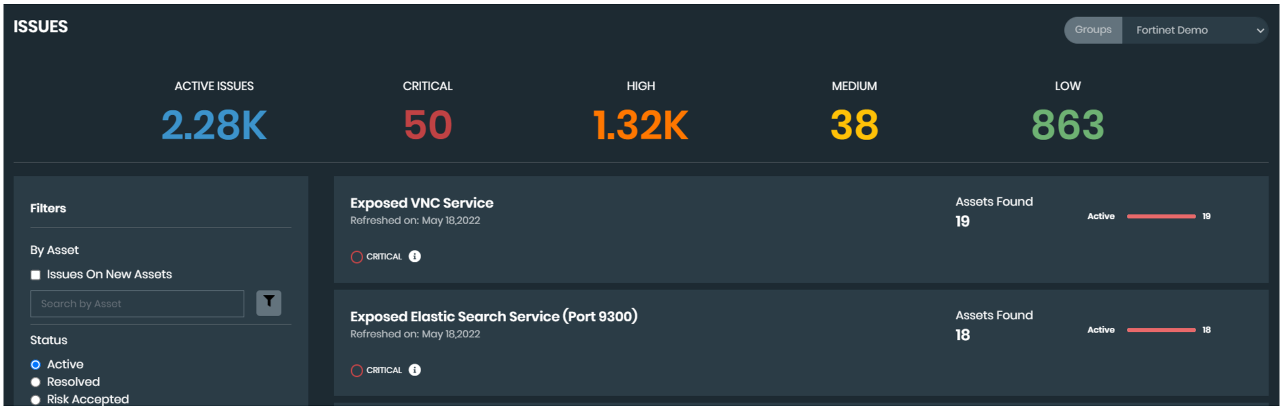
The *EASM* > *Security Issues* page displays the number of active security issues and how many of the active security issues are rated critical, high, medium, and low. Color indicates the severity of a security issue:

Critical	Security issues rated *Critical* are red.
High	Security issues rated *High* are orange.
Medium	Security issues rated *Medium* are yellow.
Low	Security issues rated *Low* are green.

You can use search and filters to change the list of reports that are displayed, and then click each report to display its details.

To view security issues:

1. Go to *EASM* > *Security Issues*. The security issues are displayed.
   The *Issues* bar across the top displays the number of active security issues and the number of active security issues that are rated critical, high, medium, and low security risk.
   For each report, the number of affected assets is also displayed.



ISSUES

Groups Fortinet Demo

ACTIVE ISSUES	CRITICAL	HIGH	MEDIUM	LOW
2.28K	50	1.32K	38	863

Filters

By Asset

□ Issues On New Assets

Search by Asset

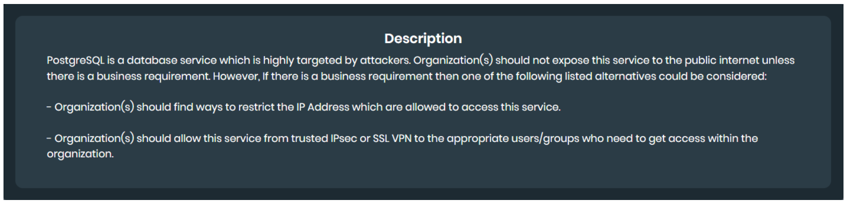
Status

● Active
● Resolved
● Risk Accepted

Exposed VNC Service
Refreshed on: May 18,2022
○ CRITICAL
Assets Found
19
Active 19

Exposed Elastic Search Service (Port 9300)
Refreshed on: May 18,2022
○ CRITICAL
Assets Found
18
Active 18

2. In the *Issues* section, click the number under *Critical*, *High*, *Medium*, or *Low*. The corresponding filter is selected and only those reports are displayed.
3. For each report, click the *i* icon to display a description of the issue and suggested remediation steps.



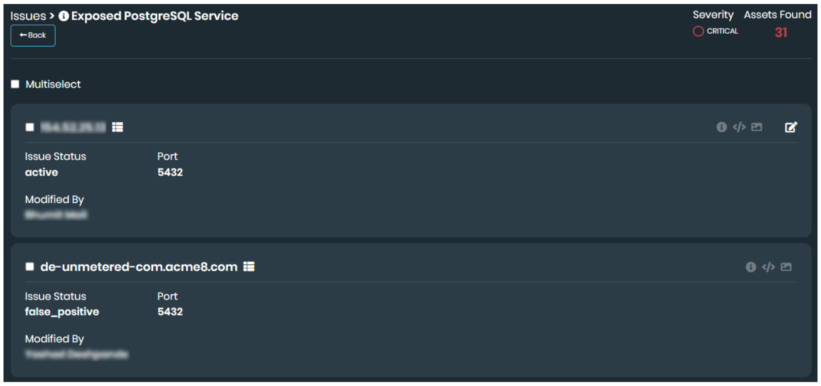
Description

PostgreSQL is a database service which is highly targeted by attackers. Organization(s) should not expose this service to the public internet unless there is a business requirement. However, If there is a business requirement then one of the following listed alternatives could be considered:

- Organization(s) should find ways to restrict the IP Address which are allowed to access this service.

- Organization(s) should allow this service from trusted IPsec or SSL VPN to the appropriate users/groups who need to get access within the organization.

4. Click the title of a report to display details about affected assets.



Issues > Exposed PostgreSQL Service
←Back

Severity: ○ CRITICAL
Assets Found: 31

□ Multiselect

□ [redacted]

Issue Status
active

Port
5432

Modified By
[redacted]

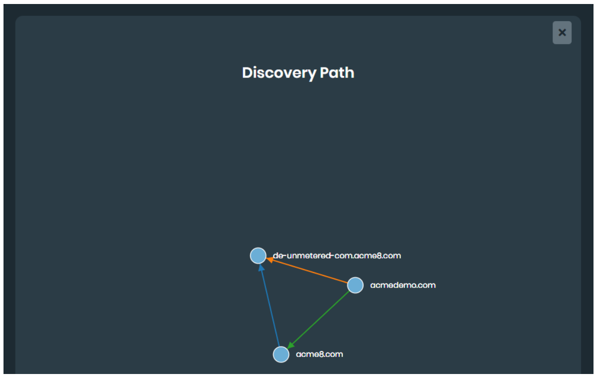
□ de-unmetered-com.acme8.com

Issue Status
false_positive

Port
5432

Modified By
[redacted]

5. If available, view the path used to discover the issue:
   a. Click the *Discovery Path* icon. The discovery path is displayed.



Discovery Path

   b. Click the *X* in the top-right corner to close the window.

6. When available, click the following icons:

Additional Information	Displays additional information about the security issue.
Raw Data	Displays raw data about the security issue.
Edit	Click to change the status of a security issue to reflect action taken by your organization to address the issue. See Changing the status of security issues on page 43.

7. Click the *Back* button.

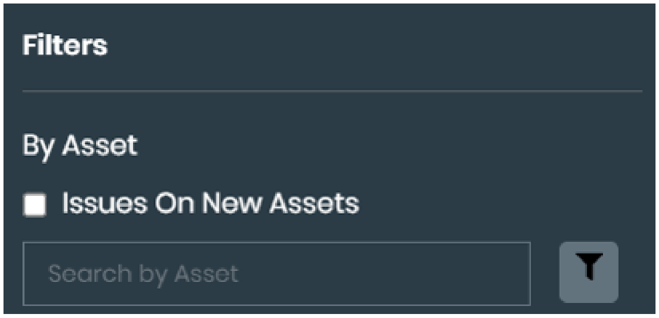
Filtering security issues

By default, the *EASM* > *Asset Discovery* page displays all potential security issues, starting with critical security issues. You can use filters to display specific types of issues.

You can search for specific security issues using the *Search by Asset* field. Enter IP address information, such as 192.168.10.10 or 192.168.12.0/24.

To filter security issues:

1. Go to *EASM* > *Security Issues*. The list of security issues is displayed.
2. Select the *Issues On New Assets* checkbox to filter security issues on newly discovered assets.



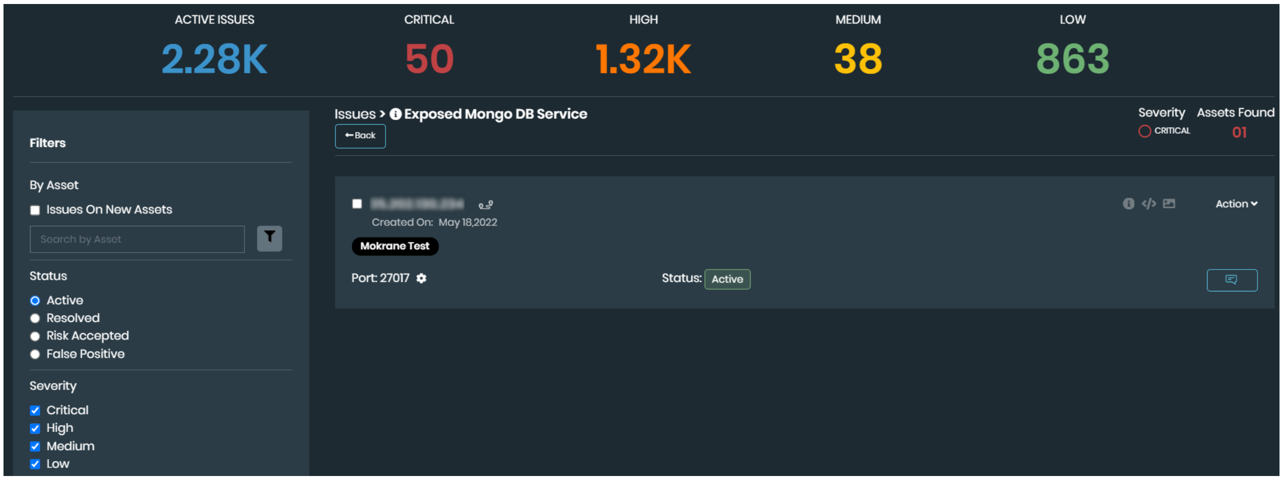
3. Add advanced search features:
   a. Click the filter icon. The advanced search fields are displayed.
   b. Select the *Search Type*.
   c. Click *Search*.
4. Select one or more filters, and click *Search*:

Filter	Options
Status	Select one of the following statuses: • Active • Resolved • Risk accepted • False positive
Severity	Select one or more of the following severity statuses:

Filter	Options
	• Critical • High • Medium • Low
Category	Select one or more of the categories. The list of categories changes based on the displayed security issues.
Country	Select one or more countries.

The list of filtered security issues is displayed.

5. (Optional) In the *Filters* list, toggle on *False Positive*. The list displays only issues marked with a status of *False Positive*.
6. Click an issue title to display its details.
   In the following example, the details for the *Exposed Mongo DB Service* issue are displayed:



□ [redacted]
Created On: May 18,2022
Port: 27017
Status: Active

7. Click *Edit* in the top-right corner to change the status by selecting one of the following options:
   - Mark as Resolved
   - Risk Accepted
   - False Positive
8. Click *Back* to display the list of issues again.
9. In the *Filters* list, click *Clear* to remove all filters.

Changing the status of security issues

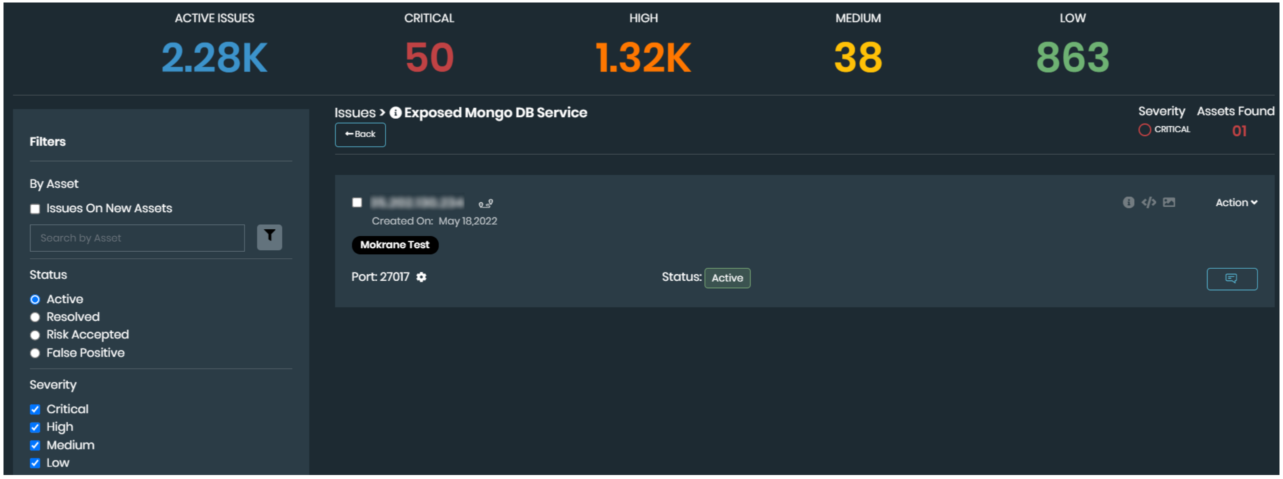
As you review and address security issues reported by FortiRecon, you can change the status of each issue to reflect your understanding and actions:

Mark as Active	Available only after you change the status of a security issue from active to another status. Select to move an issue back to the active status.

Mark as Resolved	Select to indicate actions taken at your organization have resolved the security issue.
Risk Accepted	Select to indicate actions taken at your organization have not fully resolved the security issue, but the current level of risk is acceptable.
False Positive	Select to indicate that the security issue is not an issue for your organization. The issue is considered a *False Positive* issue.

To change the status of security issues:

1. Go to *EASM* > *Security Issues*. The discovered assets are displayed.
2. If necessary, select one or more filters, and click *Search*.
   The list of filtered security issues is displayed.
3. Click an issue title to display its details.
   In the following example, the *Exposed Mongo DB Service* security issue is displayed:



4. Click *Edit* in the top-right corner to change the status by selecting one of the following options:
   - Mark as Resolved
   - Risk Accepted
   - False Positive
5. Click *Back* to display the list of issues again.

Adding a comment to a security issue

When editing a security issue on *EASM* > *Security Issues*, the client can leave a comment to describe the changes and why they were made.

Selecting the comment button will open all comments for that issue. This allows you to review all changes and discussions related to the issue.

To add a comment to a security issue:

1. Go to *EASM* > *Security Issues*.
2. Select a type of security issue.
3. Locate the issue you would like to make a change to.
4. Click the comment button. A list of previous comments and a text box is displayed.
5. Enter a comment related to the status change.
6. Click *Add*.

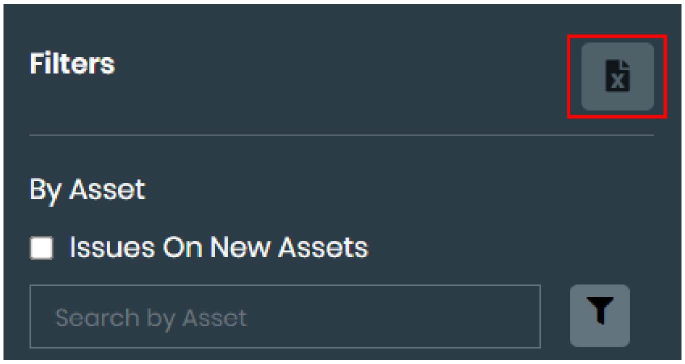
Exporting security issues

You can export a list of security issues into an Excel file. The spreadsheet will include the information on:

- Issue Category
- Issue Name
- Severity
- Asset
- Port
- Issue Status
- Tags
- Groups
- Last Refreshed On
- Additional Details
- Recommendations

To export the security issues:

1. Go to *EASM* > *Security Issues*.
2. Optionally, apply filters to export specific security issues. See Filtering security issues.
3. Click *Download* icon. The file is downloaded to your computer.



Asset Management

You can create and manage asset tags and groups in the *EASM* > *Asset Management* page. From the *Asset Management* page, you can:

- Create a new asset tag. See Creating a tag on page 46.
- Assign individual and bulk assets to an asset tag. See Adding assets to a tag on page 46.
- Manage, edit, and delete asset tags. See Managing tags on page 47.
- Create a new asset group. See Creating a group on page 48.
- Assign individual and bulk assets to an asset group. See Adding assets to a group on page 49.
- Manage, edit, and delete asset groups. See Managing groups on page 50.
- Filter *EASM* pages by group. See Filtering by group on page 51.
- Limit access to specific assets and security issues using groups and tags. See Limiting access to assets and issues on page 51.

Tags and groups are integrated throughout the *EASM* pages. You can filter by tags in the *Asset Discovery* and *Security Issues* pages; see Viewing asset details on page 32. Groups can be filtered in all *EASM* pages.

Creating a tag

Asset tags can be used to mark specific assets for focused filtering in the *Security Issues* and *Asset Discovery* pages. When creating a tag, a tag color is selected so that assets can be differentiated by tag. Tags must be configured in the *Tag Management* tab before assets can be assigned.

Some tags are automatically generated and cannot be edited or deleted.

To create a tag:

1. Go to *EASM* > *Asset Management*.
2. Select the *Tag Management* tab.
3. Click *Create*. The *Create Tag* dialog is displayed.
4. Enter a *Tag Name*.
5. Enter a *Tag Description*.
6. Select the *Theme Color* icon to assign the tag color.
7. Click *Submit*. The new group is added to the *Tag Management* tab.

Adding assets to a tag

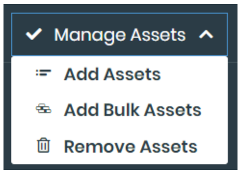
You can add individual or bulk assets to a tag from the *Tag Management* tab.

Assets must be included in *EASM > Asset Discovery* before they can be tagged. See Adding assets manually on page 35.

Tags can also be assigned to assets in *EASM > Asset Discovery*. See Assigning tags on page 36.

To add assets to a tag:

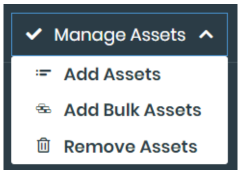
1. Go to *EASM > Asset Management*.
2. Select the *Tag Management* tab.
3. Locate the tag you want to add assets to and click *Manage Assets*. A dropdown menu is displayed.



4. Select *Add Assets*.
5. Select the assets to add from the *Validated Assets list*.
6. Click the right arrow. The selected assets will be moved into the tag field.
7. Select *Propagate the tag to asset* to apply tags to the asset associations. Select the *i* icon for more information.
8. Click *Save*.

To add bulk assets to a tag:

1. Go to *EASM > Asset Management*.
2. Select the *Tag Management* tab.
3. Locate the tag you want to add assets to and click *Manage Assets*. A dropdown menu is displayed.

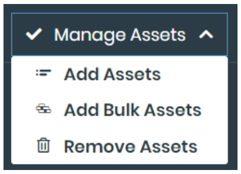


4. Select *Add Bulk Assets*.
5. Enter the asset information in the left field.
6. Select *Propagate the tag to asset* to apply tags to the asset associations. Select the *i* icon for more information.
7. Click *Validate*. Once validated, assets are displayed in the right field. Any assets that failed validation are listed.
8. Click *Save*.

Managing tags

Asset tags can be managed from the *Tag Management* tab. You can remove assets from a tag, edit a tag, or delete a tag.

To remove an asset from a tag:

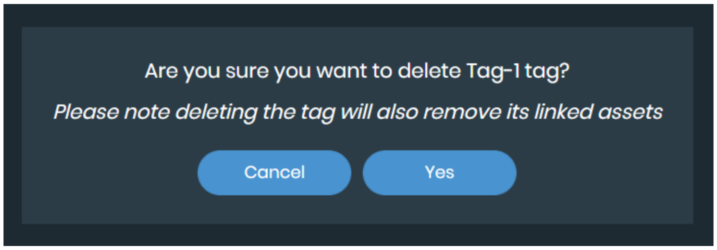
1. Go to *EASM* > *Asset Management*.
2. Select the *Tag Management* tab.
3. Locate the tag you want to remove assets from and click *Manage Assets*. A dropdown menu is displayed.
   

4. Select *Remove Assets*.
5. Select the assets you want to remove or click *Select All*.
6. Click *Remove Selected*.

To edit a tag:

1. Go to *EASM* > *Asset Management*.
2. Select the *Tag Management* tab.
3. Locate the tag you want to edit and click the *Edit* icon.
4. Edit the fields.
5. Click *Submit*.

To delete a tag:

1. Go to *EASM* > *Asset Management*.
2. Select the *Tag Management* tab.
3. Locate the tag you want to delete and click the *Delete* icon. A confirmation message is displayed.
   
   Are you sure you want to delete Tag-1 tag?

   Please note deleting the tag will also remove its linked assets

4. Click *Yes*.

Creating a group

Asset groups can be used to consolidate related assets. Groups can be viewed in the *Dashboard*, *Asset Discovery*, and *Security Issues* pages. An asset group must be created in the *Group Management* tab before assets can be assigned.

Assets can also be grouped based on subsidiary hierarchy. This allows for separate reporting and delegation of remediation responsibilities.

To create a group:

1. Go to *EASM* > *Asset Management*.
2. Select the *Group Management* tab.
3. Click *Create*. The *Create Group* dialog is displayed.
4. Enter a *Group Name*.
5. Enter a *Group Description*.
6. Click *Submit*. The new group is added to the *Group Management* tab.

Once a group has been created, you can assign assets to the group. See Adding assets to a group on page 49.

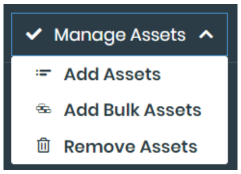
Adding assets to a group

You can add individual or bulk assets to a group from the *Group Management* tab.

Assets must be included in *Asset Discovery* before they can be tagged. See Adding assets manually on page 35.

To add assets to a group:

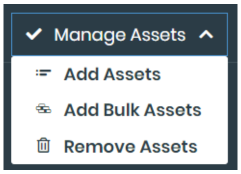
1. Go to *EASM* > *Asset Management*.
2. Select the *Group Management* tab.
3. Locate the group you want to add assets to and click *Manage Assets*. A dropdown menu is displayed.



4. Select *Add Assets*.
5. Select the assets to add from the *Validated Assets list*.
6. Click the right arrow. The selected assets will be moved into the tag field.
7. Select *Propagate the tag to asset* to apply tags to the asset associations. Select the *i* icon for more information.
8. Click *Save*.

To add bulk assets to a group:

1. Go to *EASM* > *Asset Management*.
2. Select the *Group Management* tab.
3. Locate the group you want to add assets to and click *Manage Assets*. A dropdown menu is displayed.



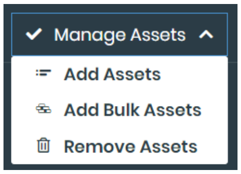
4. Select *Add Bulk Assets*.
5. Enter the asset information in the left field.
6. Select *Propagate the tag to asset* to apply tags to the asset associations. Select the *i* icon for more information.
7. Click *Validate*. Once validated, assets are displayed in the right field. Any assets that failed validation are listed.
8. Click *Save*.

Managing groups

Asset tags can be managed from the *Group Management* tab. You can remove assets from a group, edit a group, or delete a group.

To remove an asset from a group:

1. Go to *EASM* > *Asset Management*.
2. Select the *Group Management* tab.
3. Locate the group you want to remove assets from and click *Manage Assets*. A dropdown menu is displayed.



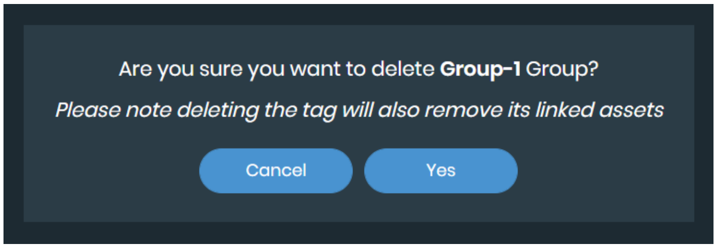
4. Select *Remove Assets*.
5. Select the assets you want to remove or click *Select All*.
6. Click *Remove Selected*.

To edit a group:

1. Go to *EASM* > *Asset Management*.
2. Select the *Group Management* tab.
3. Locate the group you want to edit and click the *Edit* icon.
4. Edit the fields.
5. Select *Assign Group To All Users* to make the assets visible to all users. See Limiting access to assets and issues on page 51.
6. Click *Submit*.

To delete a group:

1. Go to *EASM* > *Asset Management*.
2. Select the *Group Management* tab.
3. Locate the group you want to delete and click the *Delete* icon. A confirmation message is displayed.



Are you sure you want to delete **Group-1** Group?

Please note deleting the tag will also remove its linked assets

4. Click *Yes*.

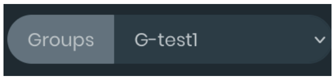
Filtering by group

Once a group has been created, you can filter by group in the *EASM* > *Security Issues* and *EASM* > *Asset Discovery* pages using the *Groups* dropdown menu. The Groups filter will be set to all assets of the organization by default.

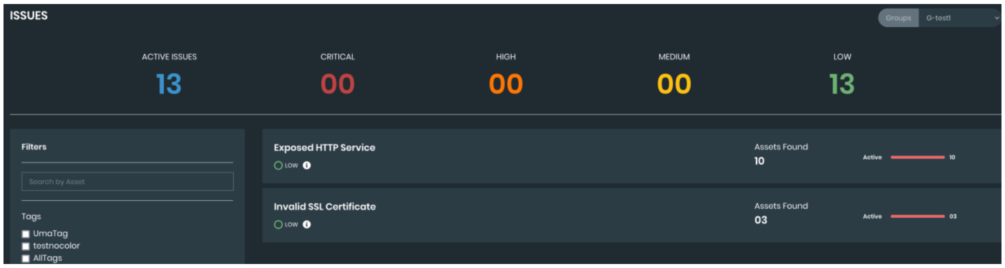
The following example demonstrates filtering by group in the *EASM* > *Security Issues* page.

To filter by group:

1. Go to *EASM* > *Security Issues*.
2. Click the *Groups* dropdown menu.



3. Select the group you want to filter by. The page will displayed information related to the selected group.



ISSUES

Groups: G-test1

ACTIVE ISSUES	CRITICAL	HIGH	MEDIUM	LOW
13	00	00	00	13

Filters

Search by Asset

Tags
- □ UmaTag
- □ testnocolor
- □ AllTags

Issue	Severity	Assets Found	Active
Exposed HTTP Service	○ LOW	10	10
Invalid SSL Certificate	○ LOW	03	03

Limiting access to assets and issues

User access to specific assets and security issues can be limited through the use of groups and tags. User asset and security issue visibility is limited to the groups they are assigned to and any tags associated with these group assets.

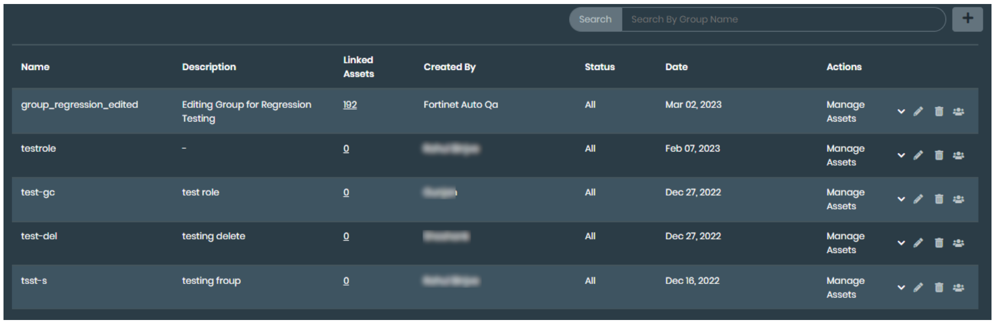
The following table presents examples of visible and hidden assets based on the groups that a user is assigned to:

User assigned to	Visible assets	Hidden assets
A single group with no tags assigned	• All assets that have been added to the group	• Assets that have not been added to the group
A single group with tags assigned to the assets	• Assets that have been added to the group that also have the tags assigned	• Assets that have not been added to the group • Any assets included in the

User assigned to	Visible assets	Hidden assets
		assigned group that do not have the tags assigned
Multiple groups with no tags assigned	• All assets that have been added to any of the assigned groups	• Assets that have not been added to any of the groups
Multiple groups with tags assigned to the assets	• Assets that have been added to any of the assigned groups that also have the tags assigned	• Assets that have not been added to any of the groups • Any assets included in the assigned groups that do not have the tags assigned

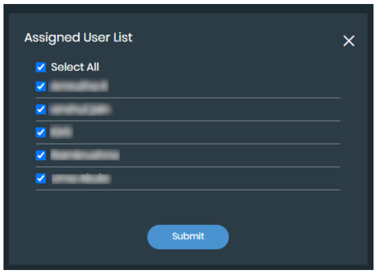
To assign users to a group:

1. Go to *EASM* > *Asset Management*.
2. Select the *Group Management* tab.



Name	Description	Linked Assets	Created By	Status	Date	Actions
group_regression_edited	Editing Group for Regression Testing	192	Fortinet Auto Qa	All	Mar 02, 2023	Manage Assets
testrole	-	0	[redacted]	All	Feb 07, 2023	Manage Assets
test-gc	test role	0	[redacted]	All	Dec 27, 2022	Manage Assets
test-del	testing delete	0	[redacted]	All	Dec 27, 2022	Manage Assets
tsst-s	testing froup	0	[redacted]	All	Dec 16, 2022	Manage Assets

3. Select *Assign User*. The *Assigned User List* dialog is displayed.



Assigned User List

- ☑ Select All
- ☑ [redacted]
- ☑ [redacted]
- ☑ [redacted]
- ☑ [redacted]
- ☑ [redacted]

4. Select the users you want to assign:
   - Select specific users to assign to the group.
   - Select *Select All* to make the group assets and security issues visible to all users.
5. Click *Submit*.

Leaked Credentials

The FortiRecon team continually monitors for credential leaks and provides alerts to you through the FortiRecon portal. If any leaked or breached credentials that involve email addresses of the organizations or the users of their systems are detected, the FortiRecon portal automatically displays the information.

As part of consolidated collection, the leaked credentials are gathered from multiple sources:

- Publicly leaked or breached databases
- Privately shared databases
- Paste sites
- Malware infections

Leaked credentials are the primary source of *Password Re-Use Attacks*. It is important for any organization to quickly neutralize leaked credentials.

On the *EASM* > *Leaked Credentials* page, you can:

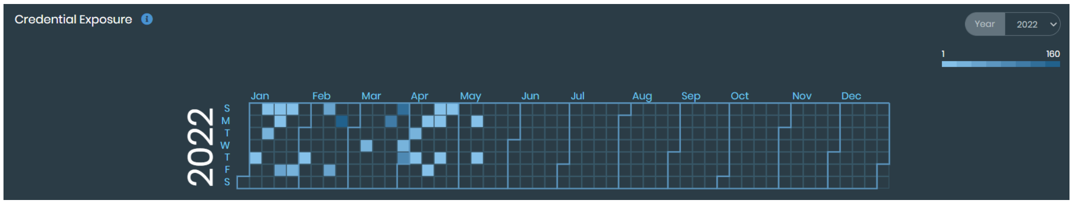
- View leaked credentials by year. See Viewing leaked credentials by year on page 53.
- View breached datasets. See Viewing breached datasets on page 53.
- View leaked credential details. See Viewing leaked credential details on page 54.
- Export a list of leaked accounts. See Exporting leaked accounts on page 55.

Viewing leaked credentials by year

The *EASM* > *Leaked Credentials* page provides a calendar year of all breaches. You can change the year to view previous year data.

To view leaked credentials by year:

1. Go to *EASM* > *Leaked Credentials*. The *Credential Exposure* year is displayed.
   Colored blocks indicate a breach. Light colored blocks indicate few affected credentials, and dark colored blocks indicate many affected credentials.



2. Hover over the block to display details about the breach.
3. From the *Year* menu, select a different year. The calendar changes to the selected year.
4. Click a color block to display details on the *Leaked Credentials* page. See Viewing leaked credential details on page 54.

Viewing breached datasets

On the *EASM* > *Leaked Credentials* page, you can click the *Breach Dataset* tab to view results displayed on the following tabs:

- The *Relevant* tab displays breach information that contains email addresses related to your organization's domains.
- The *Other* tab displays all breach information indexed in FortiRecon's database, including breach information related to third-parties that does not contain email addresses related to your organization's domains.

You can filter the list of breached datasets by date, and you can search for keywords.

To view breached datasets:

1. Go to *EASM* > *Leaked Credentials*. The *Breach Dataset* tab is displayed with the *Relevant* tab selected. The following columns of information are available:

Breach Name	Displays the name of the breach. A red *Includes passwords* is displayed when the breach includes passwords.
Breach Date	Displays the date that the breach occurred.
Added On	Displays the date that the information was made available to other malicious actors.
Compromised Accounts	Displays the number of known compromised accounts.

2. Click a breach to display more information about it.
3. On the *Breached Dataset* tab, filter reports by a date range:
   a. Click *Filter Report by Date Range*. Two calendars are displayed.
   b. In the left calendar, select a month, year, and day to specify the start date of the range.
   c. In the right calendar, select a month, year, and day to specify the end date of the range.
   Only reports from the date range are displayed.
   d. Click the *Filter Report by Date Range* box, and click *X* to remove the date range filter.
4. In the *Search* box, type a term, and press *Enter*.
   In the *Search* box, clear the term to remove it.
5. Click the *Other* tab. The most recent breaches added by FortiRecon are displayed.
   On the *Other* tab, you can filter the data by date and use the *Search* box.

Viewing leaked credential details

On the *EASM* > *Leaked Credentials* page, click the *Leaked Credentials* tab to view the results.

You can filter the list of leaked credentials by date and domain, and you can search for keywords.

To view leaked credential details:

1. Go to *EASM* > *Leaked Credentials*, and click *Leaked Credentials*.
2. Filter reports by a date range:
   a. Click *Filter Report by Date Range*. Two calendars are displayed.
   b. In the left calendar, select a month, year, and day to specify the start date of the range.
   c. In the right calendar, select a month, year, and day to specify the end date of the range.
   Only reports from the date range are displayed.
   d. Click the *Filter Report by Date Range* box, and click *X* to remove the date range filter.
3. In the *Domain* list, select one or more domains.
   In the *Domain* box, delete the selected domain names to remove the filter.
4. Click a domain name to display more details.
5. Click the *Other* tab.
6. In the *Search* box, type a term, and press *Enter*.
   In the *Search* box, delete the term to remove it.

Exporting leaked accounts

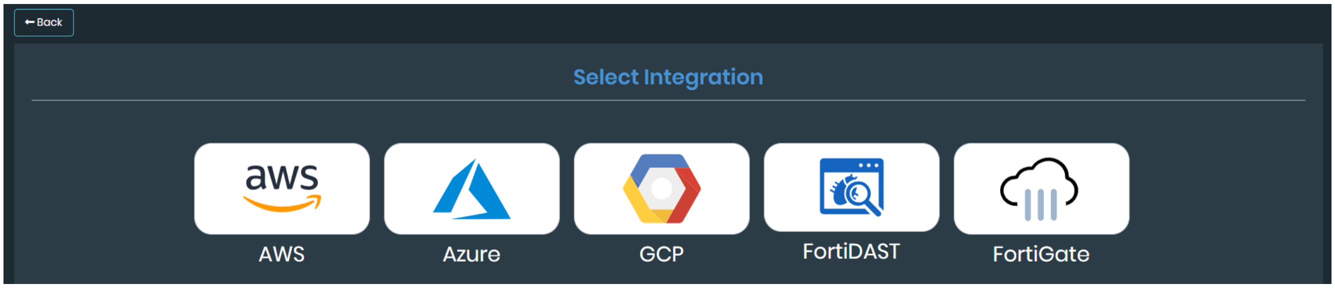
You can export a list of leaked accounts to Microsoft Excel format.

To export leaked accounts:

1. Go to *EASM* > *Leaked Credentials*, and click *Leaked Credentials*.
2. Click the *Export Leaked Accounts*. A file named *Leaked Accounts.xlsx* is exported to your computer.

Integrations

You can enable read only access to your environments and discover their cloud assets. Once assets are discovered, they are added to the *EASM* > *Asset Discovery* and *Security Issues* pages. Click the *i* on the *Integrations* page for more information.



On the *EASM* > *Integrations* page, you can:

- Add new integrations for AWS, Azure, Google Cloud Platform, FortiDAST, and FortiGate. See Adding integrations on page 55.
- Edit and delete existing integrations. See Editing integrations on page 58.

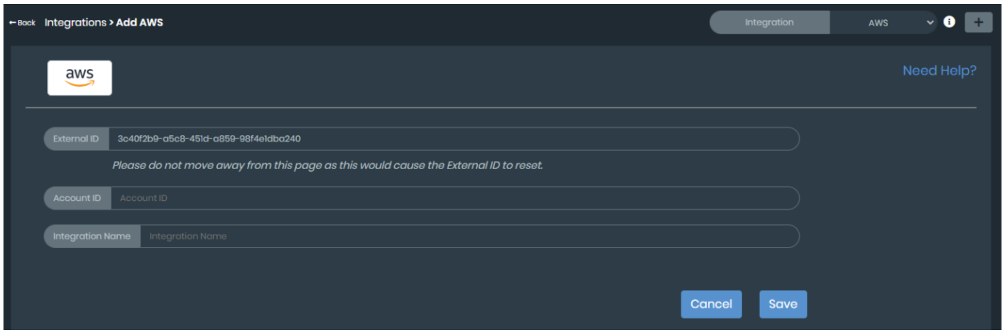
Adding integrations

The *EASM* > *Integrations* page displays all existing integrations. You can manually add new integrations as needed.

- AWS
- Azure
- Google Cloud Platform
- FortiDAST
- FortiGate

To add a new AWS integration:

1. Go to *EASM* > *Integrations*.
2. Click the + icon.
3. Select *AWS*. The *Add AWS* page is displayed.



External ID 3c40f2b9-a5c8-451d-a859-98f4e1dba240

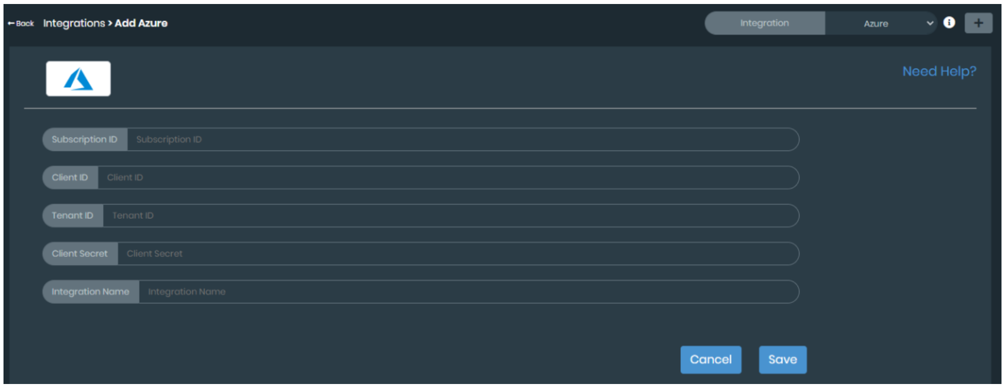
Please do not move away from this page as this would cause the External ID to reset.

For more information on creating an AWS IAM policy and role, click *Need Help?*.

4. Enter the account ID number in the *Account ID* field.
5. Enter a descriptive name in the *Integration Name* field.
6. Click *Save*.

To add a new Azure integration:

1. Go to *EASM* > *Integrations*.
2. Click the + icon.
3. Select *Azure*. The *Add Azure* page is displayed.



4. Enter the relevant values in the *Subscription ID*, *Client ID*, *Tenant ID*, and *Client Secret* fields.

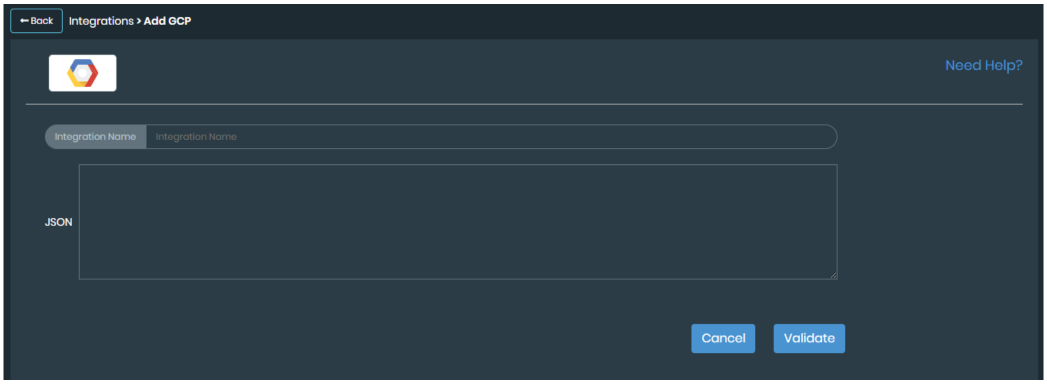
These four values are necessary to create read-only access for your Azure cloud account. For information on generating these values, click *Need Help?*.

5. Enter a descriptive name in the *Integration Name* field.
6. Click *Save*.

To add a new Google Cloud Platform integration:

1. Go to *EASM* > *Integrations*.
2. Click the + icon.

3. Select *GCP*. The *Add GCP* page is displayed.



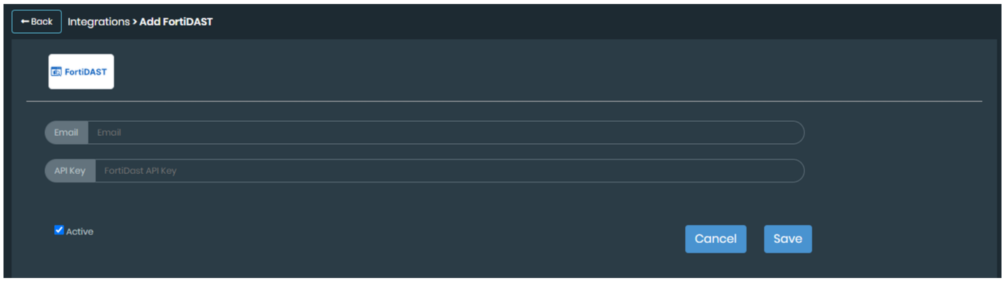
4. Enter a descriptive name in the *Integration Name* field.
5. Enter the *JSON* information from the GCP configuration file.

For information on generating the GCP key file and downloading JSON, click *Need Help?*.

6. Click *Validate*.

To add a new FortiDAST integration:

1. Go to *EASM* > *Integrations*.
2. Click the + icon.
3. Select *FortiDAST*. The *Add FortiDAST* page is displayed.



4. Enter the master email address in the *Email* field.
5. Enter the *API Key* from FortiDAST.
6. Click *Save* to verify the key.

Once the FortiDAST integration is verified, you can scan assets in the *EASM* > *Asset Discovery* page. See Performing a FortiDAST scan.

FortiGate Integration

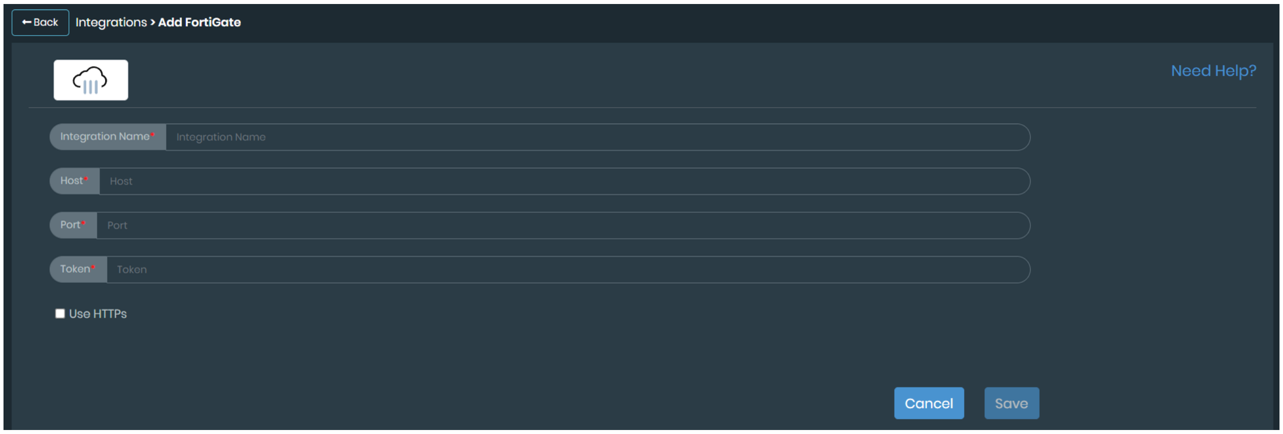
Integrating FortiGate with FortiRecon enhances the asset discovery capabilities of FortiRecon EASM. It does this by adding FortiGate Interface IPs and all IPs behind NAT to the *EASM* > *Asset Discovery* page. Once the integration is verified, all assets discovered via FortiGate will have additional metadata, including:

- Name of Virtual IP on FortiGate
- Mapped Internal IP
- MAC address of Internal IP
- Mapped External Port
- Mapped Internal Port
- Operating System

You can use this metadata to take action faster on security vulnerabilities and threats.

To add a new FortiGate integration:

1. Go to *EASM* > *Integrations*.
2. Click the + icon.
3. Select *FortiGate*. The *Add FortiGate* page is displayed.



4. Enter a name for the integration.
5. Enter FortiGate IP address in the *Host* field.
6. Enter the *Port* number.
7. Enter the FortiGate access *Token*.

For information on creating token, click *Need Help?*

8. Select *Use HTTPs* checkbox if required.
9. Click *Save*.

Editing integrations

You can edit and delete existing integrations from the *EASM* > *Integrations* page.

To edit an integration:

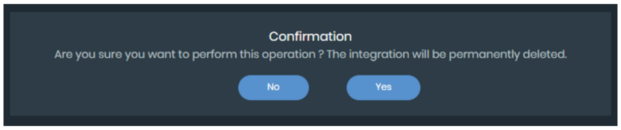
1. Go to *EASM* > *Integrations*.
2. Click *Edit*. The integration details are displayed.
3. Edit the fields you want to change.

   You cannot edit the *External ID* field for an AWS integration. You cannot edit the *Account ID*, *Subscription ID*, or *Tenant ID* for an Azure integration.

4. Click *Save*.

To delete an integration:

1. Go to *EASM* > *Integrations*.
2. Click *Delete*. The *Confirmation* message is displayed.



Confirmation

Are you sure you want to perform this operation ? The integration will be permanently deleted.

3. Select *Yes*.

Brand Protection

The Brand Protection (BP) module uses proprietary algorithms to detect common techniques used by cyber threat actors, such as web-based phishing attacks, typo-squatting, defacements, rogue apps, credential leaks, and brand impersonation in social media. You can use the Brand Protection module to detect activity early and take action, such as web site or application takedown, to protect your brand value, trust, integrity, and reputation.

The *Brand Protection* module contains the following pages:

Dashboard	Displays a summary of typo-squatting domains, flash alerts and reports, rogue apps, phishing campaigns, and takedown requests. See Dashboard on page 61.
Domain Threats	Displays a list of typo-squatted domains and phishing URLs. You can initiate domain takedown or the suspension of monitoring. See Domain Threats on page 63.
Social Media Threats	Displays all discovered profiles that may be impersonating your organization's social media pages. You can filter profiles, initiate profile takedown, and export a Microsoft Excel file containing profile details. See Social Media Threats on page 67.
Rogue Mobile Apps	Displays all discovered apps that may be impersonating your organization's assets. You can filter apps, assign status, initiate app takedown, and export a Microsoft Excel file with app details. See Rogue Mobile Apps on page 75.
VIP Monitoring	Displays threats targeted at high-profile individuals of your organization. You can filter threats and add VIP profiles for monitoring. See VIP Monitoring.
Code Repo Exposure	Displays a list of attributes exposed in code repositories. See Code Repo Exposure on page 83.
Open Bucket Exposure	Displays a list of files exposed in open buckets. See Open Bucket Exposure on page 85.
Take Down	Displays a list of takedown request tickets and their current status. See Take Down on page 86.

Brand Protection also includes *Logo Monitoring* feature which provides an additional method for identifying your brand on known phishing or malicious pages. This feature enhances the accuracy of identifying cases involving brand impersonation.

FortiRecon logo monitoring feature performs the following tasks:

- Analyzes all active typo-squatted domains to determine whether they host pages containing your organization's logo or logos that are resembling. When such domains are identified, a *Logo Detection* tag is assigned to the domain.
- Examines all domains and pages that are processed, which are obtained through phishing feeds to identify any instances where your organization might be impacted.
- Inspects all pages that are identified through the detection of the FortiRecon watermark.

Dashboard

The *Brand Protection* > *Dashboard* page provides information on threats to your organization's public facing assets, such as brand abuse, domain threats, and information exposure. From the *Brand Protection* > *Dashboard* page, you can:

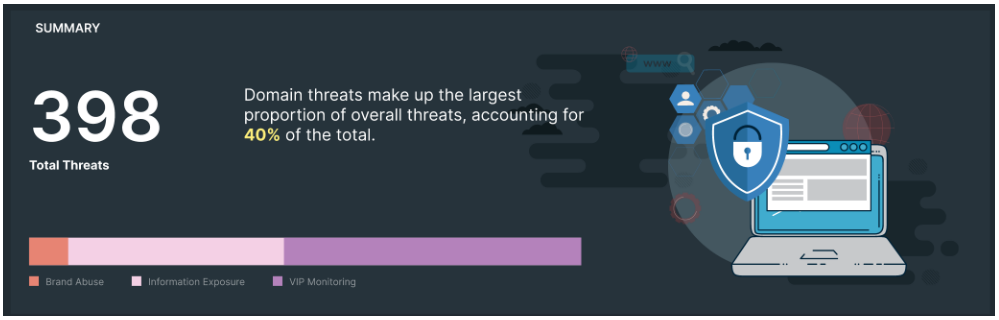
- View a summary of domain threats to your organization. See Viewing the domain threat summary on page 61.
- View a summary of brand abuse, such as rogue apps or social media threats. See Viewing the brand abuse summary on page 61.
- View a summary of information exposure, including code and file exposure. See Viewing the information exposure summary on page 62.
- View trends and important alerts of threats to your brand. See Viewing the alert summary on page 62.
- View total credits used and available for domain takedown. See Viewing the takedown credit summary on page 63.

Viewing the domain threat summary

The *Dashboard* displays a summary of domain threats in the *Summary* widget.

To view the domain threat summary:

1. Go to *Brand Protection* > *Dashboard*.
2. Scroll to the *Summary* widget. *Total Threats* and the distribution of threat type is displayed.



SUMMARY

398

Total Threats

Domain threats make up the largest proportion of overall threats, accounting for 40% of the total.

3. Hover over the threat type distribution bar to see the number of threats for each type.

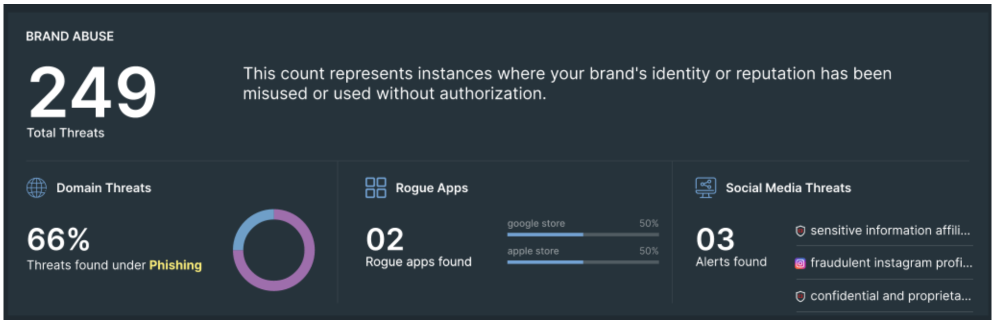
Viewing the brand abuse summary

The *Dashboard* displays information on domain phishing, rogue apps, and social media threats in the *Brand Abuse* widget.

To view the brand abuse summary:

1. Go to *Brand Protection* > *Dashboard*.
2. Scroll to the *Brand Abuse* widget. High level information on *Total Threats*, *Domain Threats*, *Rogue Apps*, and *Social*

Media Threats are displayed.



BRAND ABUSE

249

Total Threats

This count represents instances where your brand's identity or reputation has been misused or used without authorization.

Domain Threats

66%

Threats found under **Phishing**

Rogue Apps

02

Rogue apps found

Social Media Threats

03

Alerts found

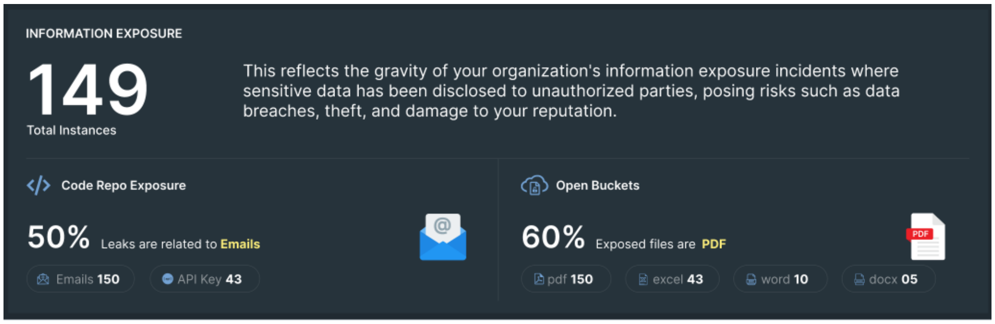
- sensitive information affili...
- fraudulent instagram profi...
- confidential and proprieta...

Viewing the information exposure summary

The *Dashboard* displays information on discovered, exposed information, such as code and file exposure in the *Information Exposure* widget.

To view the information exposure summary:

1. Go to *Brand Protection* > *Dashboard*.
2. Scroll to the *Information Exposure* widget. High level information about code and file exposure is displayed.



INFORMATION EXPOSURE

149

Total Instances

This reflects the gravity of your organization's information exposure incidents where sensitive data has been disclosed to unauthorized parties, posing risks such as data breaches, theft, and damage to your reputation.

Code Repo Exposure

50% Leaks are related to **Emails**

Emails **150** | API Key **43**

Open Buckets

60% Exposed files are **PDF**

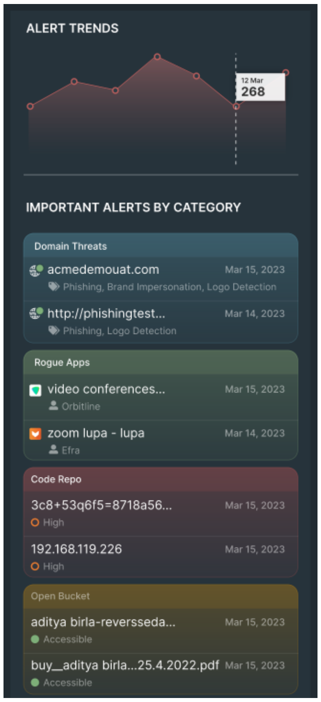
pdf **150** | excel **43** | word **10** | docx **05**

Viewing the alert summary

The *Dashboard* displays high level information on alerts in the *Alert Trends* widget.

To view the alert summary:

1. Go to *Brand Protection* > *Dashboard*.
2. Scroll to the *Alert Trends* widget. Trends are displayed in a graph and important alert highlights are organized by category.



IMPORTANT ALERTS BY CATEGORY

Domain Threats

acmedemouat.com Mar 15, 2023
Phishing, Brand Impersonation, Logo Detection

http://phishingtest... Mar 14, 2023
Phishing, Logo Detection

Rogue Apps

video conferences... Mar 15, 2023
Orbitline

zoom lupa - lupa Mar 14, 2023
Efra

Code Repo

3c8+53q6f5=8718a56... Mar 15, 2023
High

192.168.119.226 Mar 15, 2023
High

Open Bucket

aditya birla-reversseda... Mar 15, 2023
Accessible

buy_aditya birla...25.4.2022.pdf Mar 15, 2023
Accessible

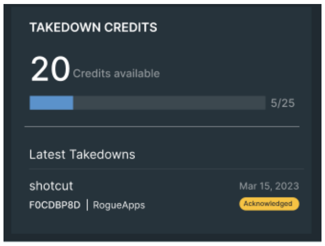
3. Hover over the graph for more information on daily alerts.

Viewing the takedown credit summary

The *Dashboard* displays information on available and used takedown credits and the most recent domain takedowns in the *Takedown Credits* widget.

To view the takedown credit summary:

1. Go to *Brand Protection > Dashboard*.
2. Scroll to the *Takedown Credits* widget. The number of used, total, and available credits is displayed.



TAKEDOWN CREDITS

20 Credits available

5/25

Latest Takedowns

shotcut Mar 15, 2023
F0CDBP8D | RogueApps Acknowledged

Domain Threats

The *Domain Threats* page displays a list of domains impersonating your organization's domain, such as typo-squatted domains and phishing URLs.

From the *Brand Protection > Domain Threats* page, you can:

- Review discovered domain threats and high level threat information. See Reviewing domain threats on page 64.
- Take action against impersonating domains, such as requesting domain takedown. See Managing domain threats on page 64.
- Filter the list of domains. See Filtering domains on page 64.
- Create a digital watermark. See Digital watermark on page 65.

Reviewing domain threats

You can review information about domain threats in the *Brand Protection* > *Domain Threats* page. Information displayed about domain threats includes:

- Domain name and URL
- Registration date
- Threat type tags
- Threat status
- Original domain

To review exposed attributes:

1. Go to *Brand Protection* > *Domain Threats*.
2. Review the high level threat information:
   - Review the distribution of threat types and the total number of discovered threats in the *Summary*.
   - Review the distribution of threat statuses in *Domain Status*.
   - Review the number of takedown credits available in *Takedown Credits*.
3. Select a threat to review detailed threat information.

Managing domain threats

You can interact with discovered domain threats, such as marking the files as resolved or request domain takedown.

To manage a threat:

1. Go to *Brand Protection* > *Domain Threats*
2. Find the threat you want to manage.
3. Change the status:
   - Select *Action* > *Mark as Resolved* to indicate that the domain threat has been resolved.
   - Select *Action* > *Take Down* to initiate the domain takedown process.
4. Click *Comment* to add a comment to the threat history.

Filtering domains

You can filter threats by date, status, threat type tags, or original domain.

To filter domain threats:

1. Go to *Brand Protection* > *Domain Threats*
2. Filter threats by a date range:
   1. Click *Filter By Date Range*. Two calendars are displayed.
   2. In the left calendar, select a month, year, and day to specify the start date of the range.
   3. Select a month, year, and day to specify the end date of the range.
      Only threats from the date range are displayed.
   4. Click the *Filter By Date Range* box, and click *X* to remove the date range filter.
3. Search for keywords:
   1. In the *Type and hit Enter to Search* box, type a keyword, and press *Enter*.

      The threats are filtered to display only threats with the keyword.
   2. Click the *X* beside the keyword to remove the filter.
4. Filter by status in the *By Status* section:
   - Select *Online*, *Offline*, or *Non Functional* to filter threats by their assigned status.
5. Select the threat type in the *By Tags* section.
6. Click *Search*. The files with the matching filters are displayed.

Digital watermark

FortiRecon uses digital watermarks on official login and sensitive pages to track cloning and re-hosting of the web pages as phishing sites on another IP address. A small script that helps the FortiRecon research team track the cloning or re-hosting of the site is provided for you to embed into your website. This process also helps you identify whether any of your customers have been victims of phishing on any cloned pages, and then take remedial actions.

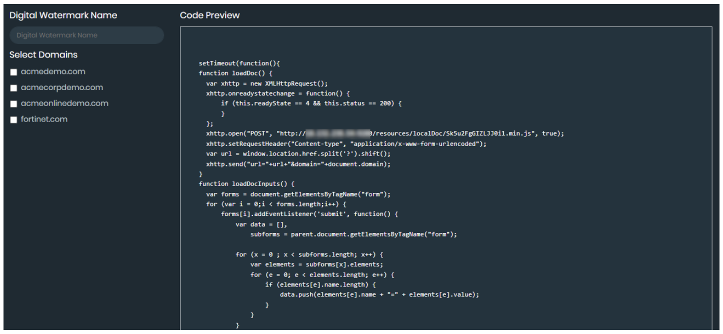
Adding watermarks

You can create a digital watermark to be embedded into your website on the *Domain Threats* page. You can download the digital watermark in two formats:

- CDN Link: The JavaScript code is hosted on Fortinet's server, and you must embed the link into the index or login page of your web application using the `<script>` tag.
- JavaScript file: The code is hosted on your own server, and you must embed the file using the `<script>` tag, or paste the code into the index or login page of your web application.

To create a digital watermark:

1. Go to *Brand Protection* > *Phishing* and select *Digital Watermark*. A list of current watermarks are displayed.
2. Click *Add Watermark*. The *Code Preview* pane is displayed.



Digital Watermark Name

Digital Watermark Name

Select Domains

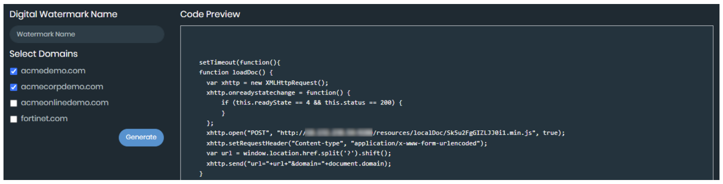
- □ acmedemo.com
- □ acmecorpdemo.com
- □ acmeonlinedemo.com
- □ fortinet.com

Code Preview

```
setTimeout(function(){
function loadDoc() {
  var xhttp = new XMLHttpRequest();
  xhttp.onreadystatechange = function() {
      if (this.readyState == 4 && this.status == 200) {
      }
  };
  xhttp.open("POST", "http://[redacted]/resources/localDoc/Sk5u2FgGIZLJJ0i1.min.js", true);
  xhttp.setRequestHeader("Content-type", "application/x-www-form-urlencoded");
  var url = window.location.href.split('?').shift();
  xhttp.send("url="+url+"&domain="+document.domain);
}
function loadDocInputs() {
  var forms = document.getElementsByTagName("form");
  for (var i = 0;i < forms.length;i++) {
      forms[i].addEventListener('submit', function() {
          var data = [],
              subforms = parent.document.getElementsByTagName("form");

          for (x = 0 ; x < subforms.length; x++) {
              var elements = subforms[x].elements;
              for (e = 0; e < elements.length; e++) {
                  if (elements[e].name.length) {
                      data.push(elements[e].name + "=" + elements[e].value);
                  }
              }
          }
```

3. Enter a name for the watermark in the *Digital Watermark Name* text box.
4. Under *Select Domains*, select the domains you want to include. The *Generate* button is displayed.



Digital Watermark Name

Watermark Name

Select Domains

- ☑ acmedemo.com
- ☑ acmecorpdemo.com
- □ acmeonlinedemo.com
- □ fortinet.com

Code Preview

```
setTimeout(function(){
function loadDoc() {
  var xhttp = new XMLHttpRequest();
  xhttp.onreadystatechange = function() {
      if (this.readyState == 4 && this.status == 200) {
      }
  };
  xhttp.open("POST", "http://[redacted]/resources/localDoc/Sk5u2FgGIZLJJ0i1.min.js", true);
  xhttp.setRequestHeader("Content-type", "application/x-www-form-urlencoded");
  var url = window.location.href.split('?').shift();
  xhttp.send("url="+url+"&domain="+document.domain);
}
```

5. Review the code in *Code Preview* and click *Generate*. The list of watermarks is displayed after the new watermark is generated.
6. Download the watermark:
   a. Click *Copy CDN Link* to copy the CDN Link to your computer's clipboard.
   b. Click *Download Digital Watermark* to download the JavaScript file to your computer.

   The digital watermark can be added to your website.

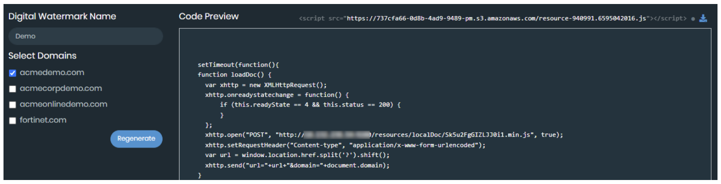
A maximum of 10 domains can be added to a digital watermark when choosing domains in *Select Domains*.

Editing watermarks

You can edit digital watermarks through the *Brand Protection* > *Phishing* page.

To edit a digital watermark:

1. Go to *Brand Protection* > *Domain Threats* and select *Digital Watermark*. A list of current watermarks is displayed.
2. Find the watermark you want to edit and select *View & Regenerate*. The *Code Preview* is displayed.



Digital Watermark Name

Demo

Select Domains

- ☑ acmedemo.com
- □ acmecorpdemo.com
- □ acmeonlinedemo.com
- □ fortinet.com

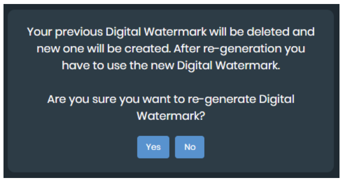
Code Preview

```
<script src="https://737cfa66-0d8b-4ad9-9489-pm.s3.amazonaws.com/resource-940991.6595042016.js"></script>
```

```
setTimeout(function(){
function loadDoc() {
  var xhttp = new XMLHttpRequest();
  xhttp.onreadystatechange = function() {
      if (this.readyState == 4 && this.status == 200) {
      }
  };
  xhttp.open("POST", "http://[redacted]/resources/localDoc/Sk5u2FgGIZLJJ0i1.min.js", true);
  xhttp.setRequestHeader("Content-type", "application/x-www-form-urlencoded");
  var url = window.location.href.split('?').shift();
  xhttp.send("url="+url+"&domain="+document.domain);
}
```

3. Make changes to *Digital Watermark Name* and *Select Domains* as needed.

   Review the changed code in *Code Preview* and select *Regenerate*. A confirmation message is displayed.



Your previous Digital Watermark will be deleted and new one will be created. After re-generation you have to use the new Digital Watermark.

Are you sure you want to re-generate Digital Watermark?

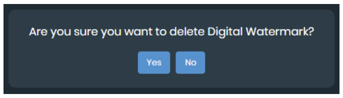
4. Click *Yes*.

Deleting watermarks

You can delete digital watermarks through the *Brand Protection* > *Phishing* page.

To delete a digital watermark:

1. Go to *Brand Protection* > *Domain Threats* and select *Digital Watermark*. A list of current watermarks is displayed.
2. Find the watermark you want to remove and click *Delete*. A confirmation message is displayed.



Are you sure you want to delete Digital Watermark?

3. Click *Yes*.

Social Media Threats

The *Social Media Threats* page displays a list of profiles impersonating your organization's social media profiles. This feature is supported for **Twitter**, **LinkedIn**, **Facebook** and **Instagram** social media platforms.

From the *Brand Protection* > *Social Media Threats* page, you can:

- View the list of profiles that are social media threats. See Reviewing social media threats on page 67.
- Take action against impersonating profiles, such as requesting profile takedown. See Managing social media threats on page 68.
- Filter the list of profiles. See Filtering social media threats on page 68.
- Add official social media profiles. See Adding official profiles on page 69.
- Export information on discovered profiles. See Exporting impersonating profiles.
- View archived alerts. See Alerts on page 70.

Reviewing social media threats

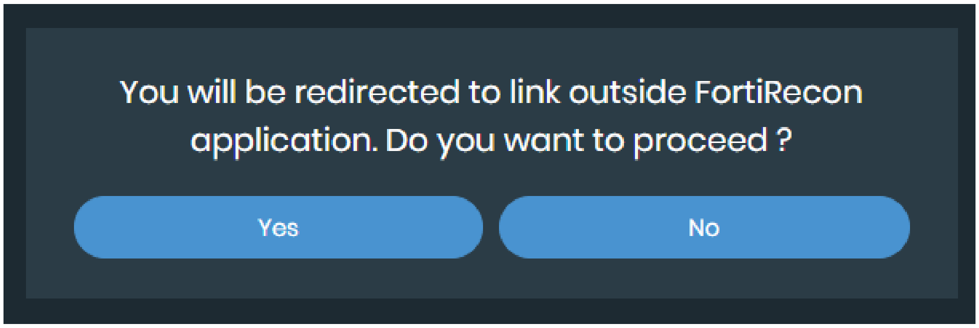
You can review information about social media threats in the *Brand Protection* > *Social Media Threats* page. Information displayed about social media threats includes:

- Profile name
- Handle name
- Location
- Friends count

- Followers count
- Posts count

To review social media threats:

1. Go to *Brand Protection > Social Media Threats*.
2. Review the high level threat information:
    - Review the distribution of profile types and the total number of discovered profiles in the *Alert Summary*.
    - Review the distribution of threat profiles based on the social media platforms in *Threats by Social Media*.
    - Review the number of takedown credits available in *Takedown Credits*.
3. Click ↗ icon next to a discovered threat profile to open the profile in a new tab. A warning message is displayed.



You will be redirected to link outside FortiRecon application. Do you want to proceed ?

4. Click *Yes*.

Managing social media threats

You can interact with discovered social media threats, such as marking the profile as false positive or request profile takedown.

To manage a threat:

1. Go to *Brand Protection > Social MediaThreats*
2. Find the threat you want to manage.
3. Change the status:
    - Select *Action > Mark as False Positive* to indicate that the social media threat has been falsely identified.
    - Select *Action > Take Down* to initiate the profile takedown process.
4. Click *Comment* to add a comment to the threat history.

Filtering social media threats

You can filter threats by date, status, threat type tags, or original domain.

To filter domain threats:

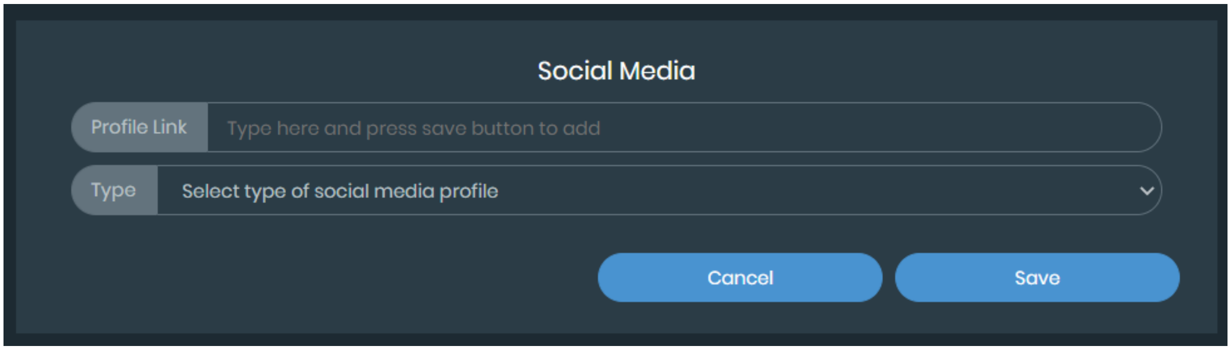
1. Go to *Brand Protection > Social Media Threats*
2. Filter threats by a date range:
   a. Click *Filter By Date Range*. Two calendars are displayed.
   b. In the left calendar, select a month, year, and day to specify the start date of the range.
   c. Select a month, year, and day to specify the end date of the range.
      Only threats from the date range are displayed.
   d. Click the *Filter By Date Range* box, and click *X* to remove the date range filter.
3. Search for keywords:
   a. In the *Type and hit Enter to Search* box, type a keyword, and press *Enter*.
      The threats are filtered to display only threats with the keyword.
   b. Click the *X* beside the keyword to remove the filter.
4. Filter by status in the *By Alert Status* section:
   - Select *Active*, *False Positive*, or *Active Takedown* to filter threats by their assigned status.
5. Select the social media platform in the *By Social Media* section.
6. Click *Search*. The profiles with the matching filters are displayed.

Adding official profiles

You can add official social media profile of your organization from *Brand Protection > Social Media Threats* page to differentiate between legitimate and impersonating profiles.

To add official profiles:

1. Go to *Brand Protection > Social Media Threats*
2. Click *Official Profiles* on the top right corner.
3. Click add icon.
4. Provide the required information:
   a. Enter the profile URL.
   b. Select the social media platform.



Social Media

Profile Link: Type here and press save button to add

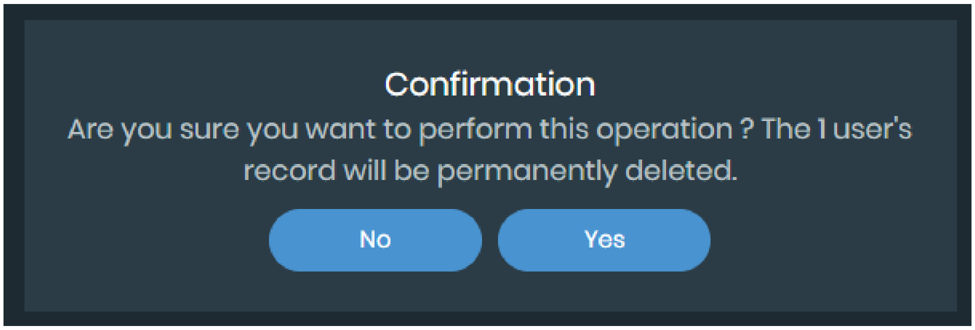
Type: Select type of social media profile

5. You can also add official social media profiles in bulk by uploading excel (XLS) file containing profile information including profile URL and type.
   a. Click Upload XLS icon.
   b. Browse and select the file. Click *Open*.

Note: Ensure that the format in which the profiles data is stored matches with the required format. To view the required format click Download Sample XLS icon.

To delete an official profile:

1. Go to *Brand Protection* > *Social Media Threats*
2. Click *Official Profiles* on the top right corner.
3. Select the required profile.
4. Click Delete icon.
5. A confirmation message is displayed. Click *Yes*.



Confirmation

Are you sure you want to perform this operation ? The 1 user's record will be permanently deleted.

Alerts

FortiRecon lists flash reports prior to version 23.2.0 on the *Brand Protection* > *Social Media Threats* > *Show Archived* page.

From the *Archived Alerts* page, you can:

- View flash reports. See Viewing flash reports on page 70.
- Filter through all flash reports available. See Filtering reports on page 71.
- Download flash reports as threat intelligence reports in PDF or as an observable Microsoft Excel file. See Downloading reports on page 71.
- Email and share links to flash reports with others. SeeSharing reports on page 73
- Rate flash reports for relevance. See Rating reports on page 74.
- Review reports and send queries to FortiRecon. See Reviewing reports on page 74.

Viewing flash reports

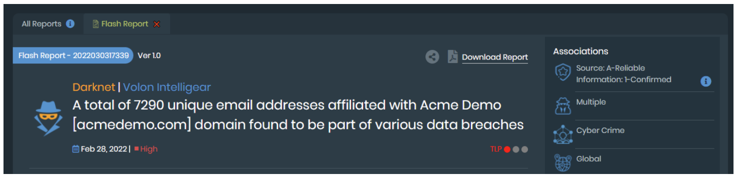
The *Brand Protection* > *Social Media Threats* > *Show Archived* page displays all the flash reports archived to you. By default all reports are displayed, starting with the latest report. Reports include in depth information, such as:

- Threat summary
- Threat detail
- Assessment

A *Takedown* button is included in the report details of reports related to brand abuse. Select the button to begin the takedown process.

To view flash reports:

1. Go to *Brand Protection* > *Social Media Threats* > *Show Archived*. The *All Reports* tab displays all flash reports.
2. Click a report title to open the report details.



Flash Report - 2022030317339 Ver 1.0

Darknet | Volon Intelligear

A total of 7290 unique email addresses affiliated with Acme Demo [acmedemo.com] domain found to be part of various data breaches

Feb 28, 2022 | High TLP

Source: A-Reliable
Information: 1-Confirmed

Multiple

Cyber Crime

Global

Filtering reports

You can adjust the reports that display on the *Alerts* page.

To filter reports:

1. Go to *Brand Protection* > *Alerts*.
2. Filter reports by a date range:
   a. Click *Filter Report by Date Range*. Two calendars are displayed.
   b. In the left calendar, select a month, year, and day to specify the start date of the range.
   c. In the right calendar, select a month, year, and day to specify the end date of the range. Only reports from the date range are displayed.
   d. Click the *Filter Report by Date Range* box, and click *X* to remove the date range filter.
3. Search for keywords:
   a. In the *Type and hit Enter to Search* box, type a keyword, and press *Enter*.

      The reports are filtered to display only reports with the keyword.
   b. Click the *X* beside the keyword to remove the filter.

   The reports that match the set filters display.

Downloading reports

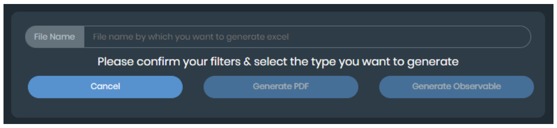
You can download reports from the *Alerts* tab as brand protection alerts in PDF or as an observable Microsoft Excel file. Brand protection alerts provide information from a flash report whereas observables outline any Indicators of Compromise (IOCs) highlighted in the flash report.

Downloaded reports can be set to include:

- All reports available
- Several, specific reports
- Single reports

To download all reports available:

1. Go to *Brand Protection* > *Social Media Threats* > *Show Archived*, and select *Downloads*. A confirmation dialog is displayed.

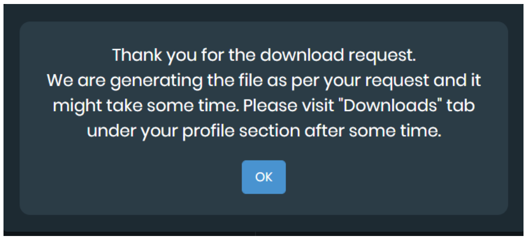
   

   File name by which you want to generate excel

   Please confirm your filters & select the type you want to generate

2. Enter a name for the downloaded file in the *File Name* text box.
3. Select the format of the downloaded file:
   - Select *Generate PDF* to download a brand protection alert in PDF.
   - Select *Generate Observable* to download details in Microsoft Excel format.

   The following message is displayed:

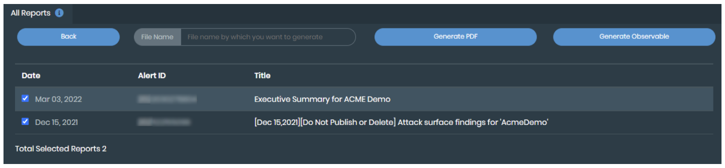
   

   Thank you for the download request.
   We are generating the file as per your request and it might take some time. Please visit "Downloads" tab under your profile section after some time.

4. Click *OK*.
5. Retrieve the report. See Retrieving downloads on page 145.

To download specific reports:

1. Go to *Brand Protection* > *Social Media Threats* > *Show Archived*.
2. Click the filter icon and set the desired report filters. See Filtering reports on page 71
3. Select *Download Specific Reports*, and select the reports to include in the report.
4. Select *Downloads*. A list of the selected reports is displayed with download options.

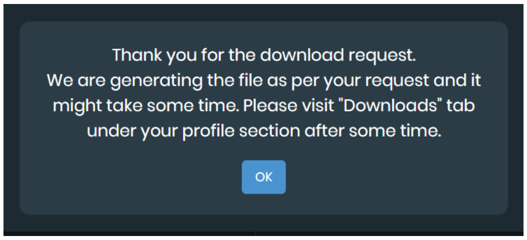
   File name by which you want to generate

Date	Alert ID	Title
☑ Mar 03, 2022	[redacted]	Executive Summary for ACME Demo
☑ Dec 15, 2021	[redacted]	[Dec 15,2021][Do Not Publish or Delete] Attack surface findings for 'AcmeDemo'

   Total Selected Reports 2

5. Enter a name for the downloaded file in the *File Name* text box.
6. Select the format of the downloaded file:
   - Select *Generate PDF* to download a brand protection alert in PDF.
   - Select *Generate Observable* to download details in Microsoft Excel format.

   The following message is displayed:

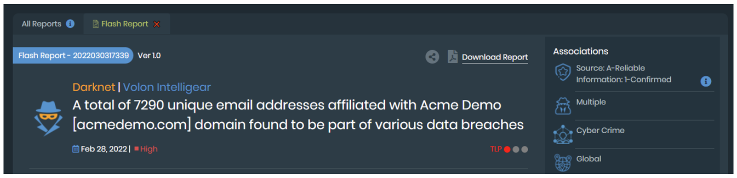
   

   Thank you for the download request.
   We are generating the file as per your request and it might take some time. Please visit "Downloads" tab under your profile section after some time.

7. Click *OK*.
8. Retrieve the report. See Retrieving downloads on page 145.

To download a single report:

1. Go to *Brand Protection* > *Social Media Threats* > *Show Archived* and click the desired report. The report details open in a new tab.



A total of 7290 unique email addresses affiliated with Acme Demo [acmedemo.com] domain found to be part of various data breaches

2. Click *Download Report*.

   The report downloads to your computer in PDF.

Sharing reports

You can share a link so that other users can access details of the report without needing to download a file. You can email the link or copy the link to share in a format of your choice.

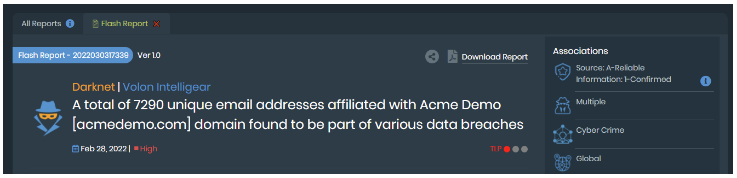
Only recipients who have a FortiRecon account can access reports through a shared link.

The Traffic Light Protocol (TLP) level dictates who you can share a report with:

- *TLP Red*: The report cannot be shared outside of your organization and should be restricted only to personnel who need to know.
- *TLP Amber*: The report can only be shared with members of your organization and clients who need to know the information to protect themselves.
- *TLP Green*: The report can be shared with peers and partner organizations but cannot be shared on publicly accessible channels.
- *TLP White*: The report can be shared without restriction.

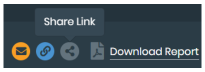
To share a link to a report:

1. Go to *Brand Protection* > *Social Media Threats* > *Show Archived* and select the report you want to share. The report details are displayed in a new tab.



A total of 7290 unique email addresses affiliated with Acme Demo [acmedemo.com] domain found to be part of various data breaches

2. Hover your mouse over *Share Link*. *Copy Link* and *Email* display.



3. Select how you would like to share the link:
   a. Click *Copy Link* to share the link in a format of your choice.
      The link is copied to your computer clipboard, and you can paste it into a message as needed.
   b. Click *Email* to email the link.
      Your personal email opens with a draft that includes the report link.

You cannot share Executive Summaries.

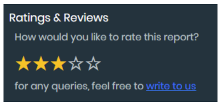
Rating reports

You can rate reports in a five star scale. The collection of ratings helps the FortiRecon team provide more relevant reports.

The rating scale is based on five stars. The rating can range from one to five by moving left to right along the stars, with the leftmost star representing one.

To rate a report:

1. Go to *Brand Protection* > *Social Media Threats* > *Show Archived* and select the report you want to rate.
   The report details are displayed in a new tab.
2. Hover your mouse over the stars in *Ratings & Reviews*.
   The stars turn yellow as you move the mouse across them.



Ratings & Reviews

How would you like to rate this report?

★★★☆☆

for any queries, feel free to write to us

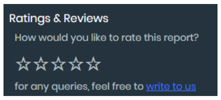
3. Click the star that corresponds to your rating out of five.
   Your rating is saved, and you can change it at any time by selecting a different star.

Reviewing reports

You can send reviews and queries to the FortiRecon team. Any questions or reviews on reports can be sent using the *write to us* feature.

To review a report:

1. Go to *Brand Protection* > *Social Media Threats* > *Show Archived* and select the report you want to review.
   The report details are displayed in a new tab.
2. In *Ratings & Reviews*, select *write to us*.



Ratings & Reviews

How would you like to rate this report?

☆☆☆☆☆

for any queries, feel free to write to us

Your personal email opens with a draft that is ready to be sent to the FortiRecon team.

Rogue Mobile Apps

On the *Brand Protection > Rogue Mobile Apps* page, the FortiRecon research team continuously monitors a number of application stores to identify newly created applications that appear similar to your organization's official application.

From the *Brand Protection > Rogue Mobile Apps* page, you can:

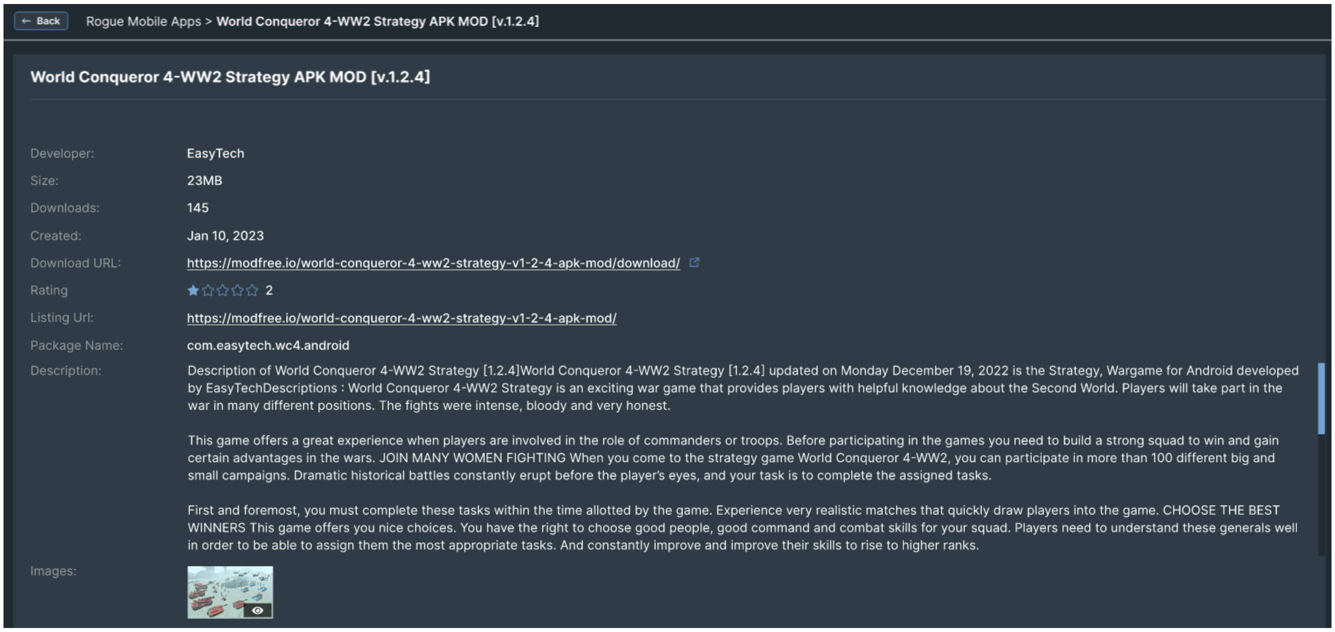
- View information on monitored applications. See Reviewing rogue applications on page 75.
- Filter for specific mobile applications. See Filtering rogue applications on page 76.
- Add official applications. See Adding official applications on page 76.
- Assign an app status. See Assigning application status on page 78.
- Initiate takedown of a rogue application. See Taking down rogue apps on page 78.
- Export information on applications. See Exporting rogue applications on page 79.

Reviewing rogue applications

You can view more information on monitored applications on the *Rogue Mobile Apps* page.

To review rogue applications:

1. Go to *Brand Protection > Rogue Mobile Apps*.
2. Review the high level threat information:
   - Review the distribution of application types and the total number of discovered rogue applications in the *Rogue App Summary*.
   - Review the distribution of applications based on the app stores in *By App Stores*.
   - Review the number of takedown credits available in *Takedown Credits*.
3. Filter for the application you want to review. See Filtering rogue applications on page 76.
4. Select the application you want to review. The app information is displayed in a new tab.


← Back
Rogue Mobile Apps > World Conqueror 4-WW2 Strategy APK MOD [v.1.2.4]

World Conqueror 4-WW2 Strategy APK MOD [v.1.2.4]

Developer:	EasyTech
Size:	23MB
Downloads:	145
Created:	Jan 10, 2023
Download URL:	https://modfree.io/world-conqueror-4-ww2-strategy-v1-2-4-apk-mod/download/
Rating	★☆☆☆☆ 2
Listing Url:	https://modfree.io/world-conqueror-4-ww2-strategy-v1-2-4-apk-mod/
Package Name:	com.easytech.wc4.android
Description:	Description of World Conqueror 4-WW2 Strategy [1.2.4]World Conqueror 4-WW2 Strategy [1.2.4] updated on Monday December 19, 2022 is the Strategy, Wargame for Android developed by EasyTechDescriptions : World Conqueror 4-WW2 Strategy is an exciting war game that provides players with helpful knowledge about the Second World. Players will take part in the war in many different positions. The fights were intense, bloody and very honest. This game offers a great experience when players are involved in the role of commanders or troops. Before participating in the games you need to build a strong squad to win and gain certain advantages in the wars. JOIN MANY WOMEN FIGHTING When you come to the strategy game World Conqueror 4-WW2, you can participate in more than 100 different big and small campaigns. Dramatic historical battles constantly erupt before the player's eyes, and your task is to complete the assigned tasks. First and foremost, you must complete these tasks within the time allotted by the game. Experience very realistic matches that quickly draw players into the game. CHOOSE THE BEST WINNERS This game offers you nice choices. You have the right to choose good people, good command and combat skills for your squad. Players need to understand these generals well in order to be able to assign them the most appropriate tasks. And constantly improve and improve their skills to rise to higher ranks.
Images:	

Filtering rogue applications

You can filter the apps that appear on the *Rogue Mobile Apps* page by *App Status*, *App Stores* and *Start & End Date*.

To filter apps:

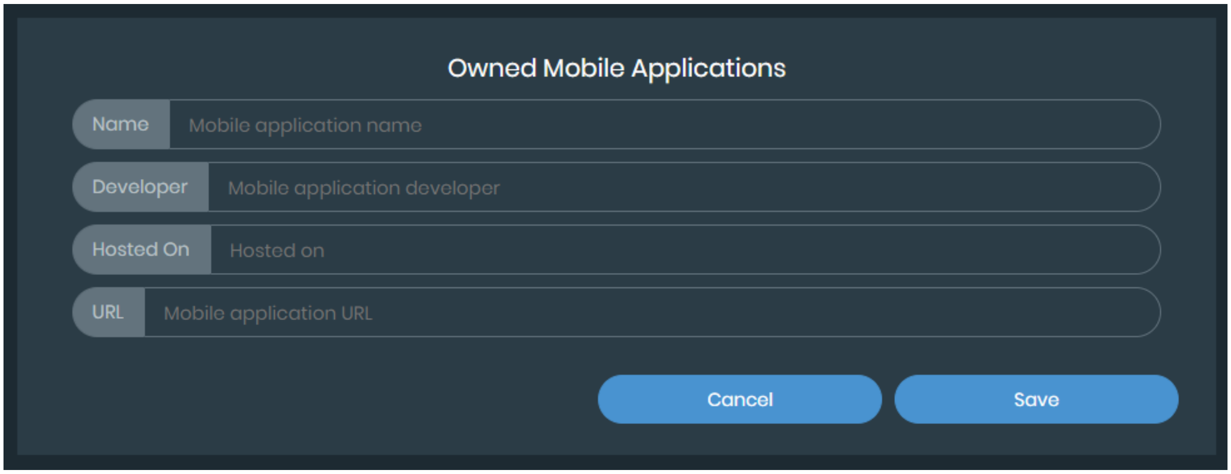
1. Go to *Brand Protection* > *Rogue Mobile Apps*.
2. Filter reports by a date range:
   a. Click *Filter By Date Range*. Two calendars are displayed.
   b. In the left calendar, select a month, year, and day to specify the start date of the range.
   c. In the right calendar, select a month, year, and day to specify the end date of the range.
      Only apps from the date range are displayed.
   d. Click the *Filter By Date Range* box, and click *X* to remove the date range filter.
3. Search for keywords:
   a. In the *Type and hit Enter to Search* box, type a keyword, and press *Enter*.
      The apps are filtered to display only apps with the keyword.
   b. Click the *X* beside the keyword to remove the filter.
4. Select the *App Status*, either *Unofficial* or *Rogue*.
5. Select the *App Stores*.
6. Click *Search*. The applications with the matching filters are displayed.

Adding official applications

You can add officia lapplications of your organization from *Brand Protection* > *Rogue Mobile Apps* page to differentiate between legitimate and rogue applications.

To add official applications:

1. Go to *Brand Protection* > *Rogue Mobile Apps*
2. Click *Official Apps* on the top right corner.
3. Click add icon.
4. Enter the following information in the confirmation pop-up:
   a. Application name.
   b. Developer
   c. Hosted on
   d. URL

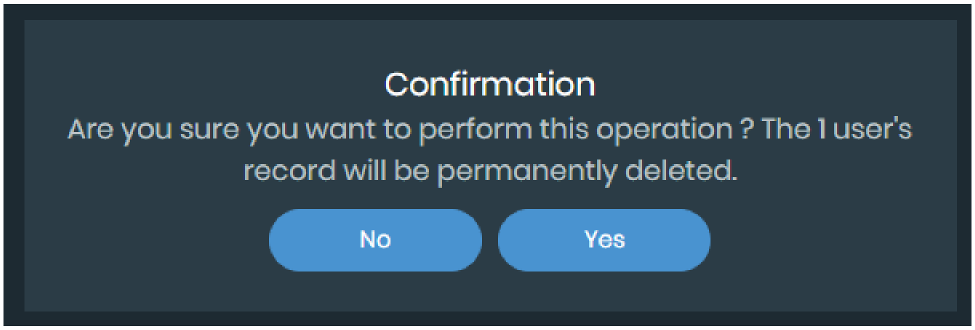


5. You can also add official applications in bulk by uploading excel (XLS) file containing application information including application name, mobile app developer, hosted on and app URL.
   a. Click Upload XLS icon.
   b. Browse and select the file. Click *Open*.

   Note: Ensure that the format in which the profiles data is stored matches with the required format. To view the required format click Download Sample XLS icon.

To delete an official application:

1. Go to *Brand Protection* > *Rogue Mobile Apps*
2. Click *Official Profiles* on the top right corner.
3. Select the required application.
4. Click Delete icon.
5. A confirmation message is displayed. Click *Yes*.


Confirmation

Are you sure you want to perform this operation ? The 1 user's record will be permanently deleted.

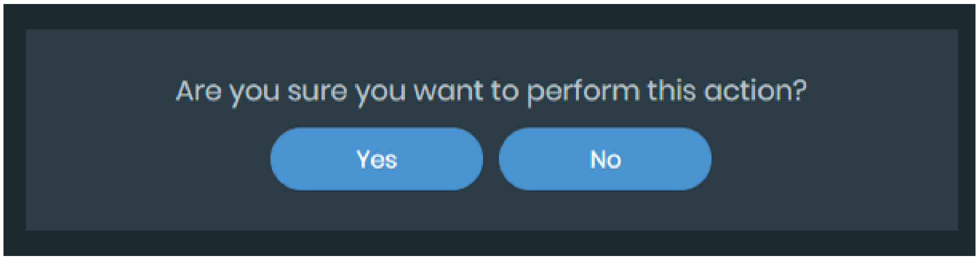
Assigning application status

You can use the following status designations to define app status on the *Rogue Mobile Apps* page:

- *Unofficial*: The app is not published by officially recognized users.
- *Rogue*: The app is unofficial and potentially malicious. If an application is marked as *Rogue*, the *Takedown* function becomes available.

To assign a new application status:

1. Go to *Brand Protection* > *Rogue Mobile Apps* and find the app.
2. Click Actions and select the new application status. A confirmation message is displayed.

   Are you sure you want to perform this action?

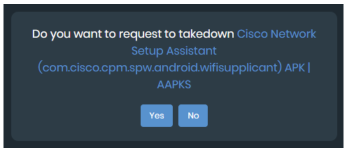
3. Click *Yes*.

Taking down rogue apps

If an app is determined to be malicious and rogue, you can initiate the takedown process in the *Rogue Mobile Apps* page.

To initiate takedown of a malicious application:

1. Go to *Brand Protection* > *Rogue Mobile Apps* and find the app.
2. If the application is assigned to *Unofficial*, change the application status to *Rogue*. See Assigning application status on page 78.
3. Click *Takedown*. A confirmation message is displayed.

   Do you want to request to takedown Cisco Network Setup Assistant (com.cisco.cpm.spw.android.wifisupplicant) APK | AAPKS

4. Click *Yes*. A tracking *Ticket* appears.
5. Go to *Brand Protection* > *Take Down* to review the status of the application takedown.

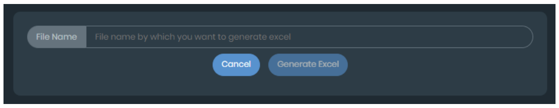
Exporting rogue applications

You can export details on potentially rogue mobile applications in the *Rogue Mobile Apps* page. Information included in exported file includes:

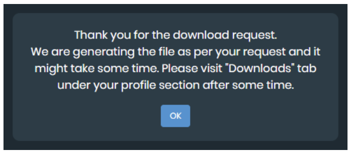
- App name and size
- Description
- Developer name and URL
- Download count and URL
- Date the app was discovered
- Listing URL
- Package name
- Source name
- Status

To export rogue application details:

1. Go to *Brand Protection* > *Rogue Mobile Apps*.
2. Set the desired filters. See Filtering rogue applications on page 76
3. Click *Download* icon next to the Filters title. A confirmation dialog is displayed.



4. Enter a name for the export file in the *File Name* text box.
5. Select *Generate Excel*. A confirmation message is displayed.



Thank you for the download request.
We are generating the file as per your request and it might take some time. Please visit "Downloads" tab under your profile section after some time.

6. Click the menu in the top-right corner and select *Profile Settings*.
7. Go to the *Downloads* tab. The list of available downloads are displayed.
8. Click the download. A file with the name you set is downloaded to your computer in Microsoft Excel format.

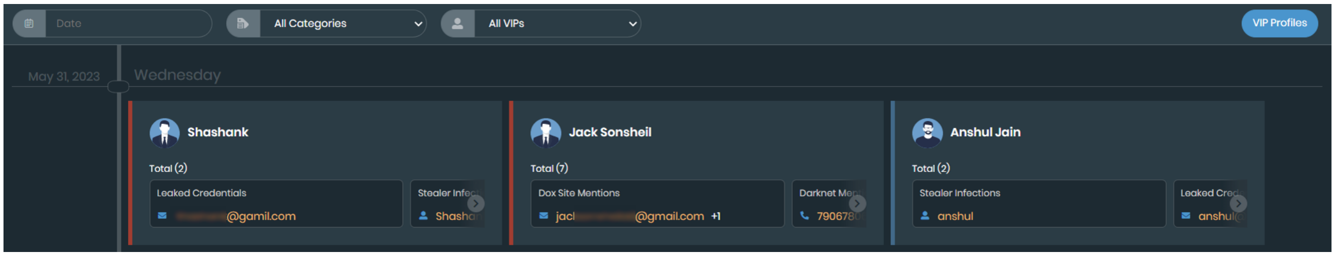
VIP Monitoring

The *Brand Protection* > *VIP Monitoring* page provides enhanced visibility and proactive threat detection, enabling you to monitor high-profile individuals for any malicious activity, providing real-time alerts and actionable insights to mitigate potential security risks.

From the *Brand Protection* > *VIP Monitoring* page, you can:

- View the timeline of threats for the official VIP profiles added. See Reviewing VIP profile threats on page 80.
- Filter the list of VIP profile threats. See Filtering VIP profile threats on page 81.
- Add official VIP profiles. See Adding VIP profiles on page 81.

A maximum of 10 VIP profiles can be added for monitoring.



May 31, 2023 Wednesday

Shashank
Total (2)
Leaked Credentials
[redacted]@gamil.com
Stealer Infec
Shasha

Jack Sonsheil
Total (7)
Dox Site Mentions
jacl[redacted]@gmail.com +1
Darknet Me
79067

Anshul Jain
Total (2)
Stealer Infections
anshul
Leaked Cred
anshul

Reviewing VIP profile threats

You can review information about VIP profile threats in the *Brand Protection* > *VIP Monitoring* page. Information includes comprehensive overview of identified threats categorized into various types, including leaked credentials, Telegram mentions, Dox site mentions, Darknet mentions, social media threats, stealer infections, and leaked documents.

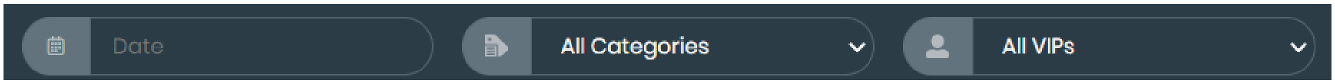
Threat Category	Description
Leaked credentials	Instances where the VIP's credentials have been exposed or compromised.
Telegram Mentions	References or discussions related to the VIP on the Telegram messaging platform.
Dox Site Mentions	Mentions or references of the VIP on websites known for sharing personal or private information.
Darknet Mentions	References or discussions related to the VIP on the darknet.
Social Media Threats	Threats posed to the VIP's security or reputation on social media platforms (*LinkedIn, Facebook, Instagram* and *Twitter*).
Stealer Infections	Indications of malware or malicious software infecting the VIP's devices with the intent of stealing sensitive information.
Leaked documents	Instances where documents or files associated with the VIP have been leaked or made publicly accessible without authorization

To review VIP profile threats:

1. Go to *Brand Protection* > *VIP Monitoring.*
2. Select the desired report.
3. Review the identified threats.

Filtering VIP profile threats

You can filter threats by date, threat category, or VIP profile.



To filter domain threats:

1. Go to *Brand Protection* > *VIP Monitoring*
2. Filter threats by a date range:
   a. Click *Date* . Two calendars are displayed.
   b. In the left calendar, select a month, year, and day to specify the start date of the range.
   c. Select a month, year, and day to specify the end date of the range.
   Only threats from the date range are displayed.
   d. Click the *Date* box, and click *X* to remove the date range filter.
3. Filter by threat category:
   - Click *All Categories* and select the desired category from the dropdown, to filter threats by their categories.
4. Filter by VIP profiles:
   - Click *All VIPs* and select the desired profile from the dropdown, to filter threats by profile.

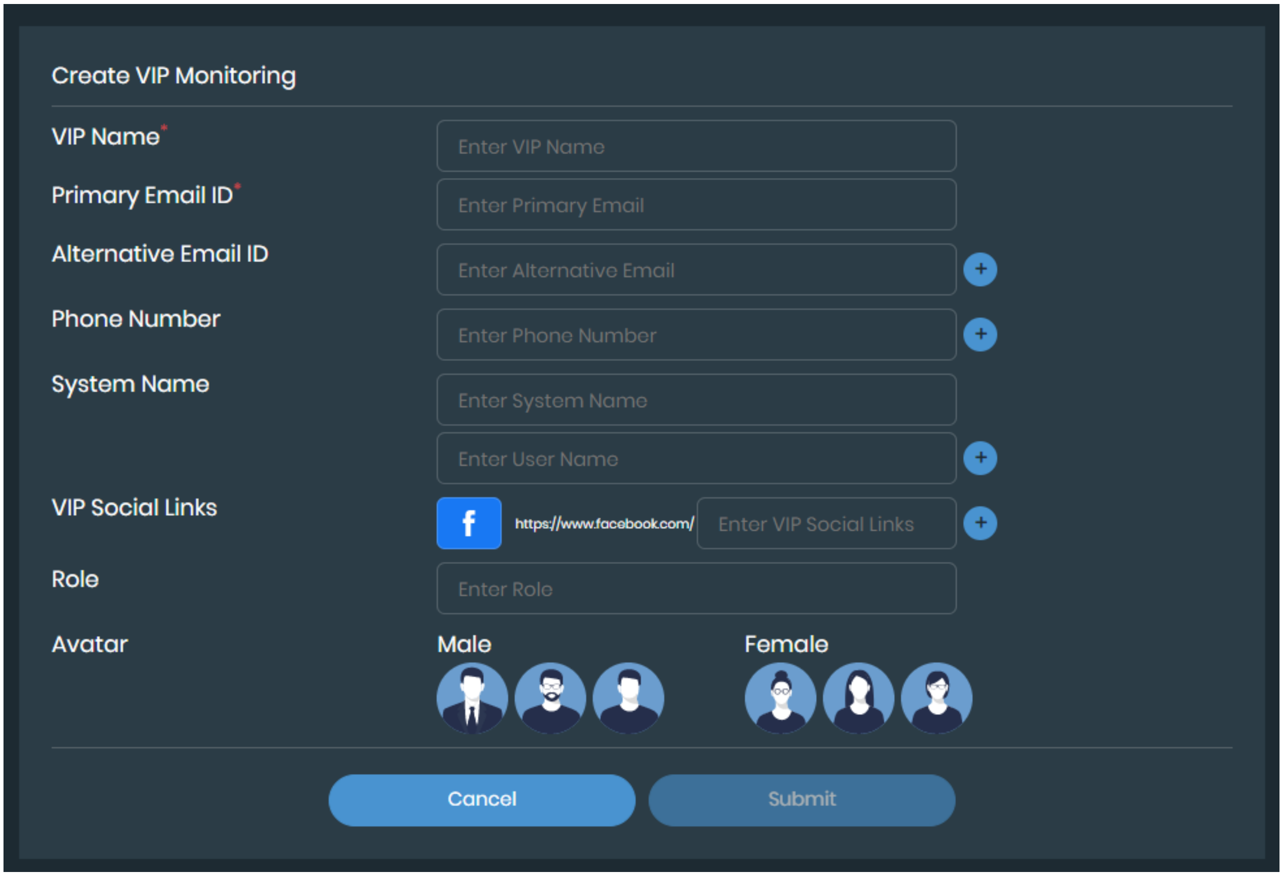
Adding VIP profiles

You can add official VIP profiles of your organization from *Brand Protection* > *VIP Monitoring* page.

To add official profiles:

1. Go to *Brand Protection* > *VIP Monitoring*.
2. Click *VIP Profiles* on the top right corner.
3. Click *+Add Profiles.*
4. Provide the required information, including:
   a. *VIP Name* - Enter the name of the high-profile individual.
   b. *Primary Email ID* - Enter the main email address associated with the VIP.
   c. *Alternative Email ID* - Enter an additional email address.
   d. *Phone Number* - Enter the contact number.
   e. *System Name* - Enter the system and user name.
   f. *VIP Social Links* - Enter the social media profile links. Select the social media platform by clicking the social media icon and selecting desired platform. Click + icon to add more than one social media profile link.
   g. *Role* - Enter the role of the VIP.
   h. *Avatar* - Choose the avatar from the available options.

5. Click *Submit*.



Create VIP Monitoring

VIP Name* Enter VIP Name

Primary Email ID* Enter Primary Email

Alternative Email ID Enter Alternative Email +

Phone Number Enter Phone Number +

System Name Enter System Name

Enter User Name +

VIP Social Links f https://www.facebook.com/ Enter VIP Social Links +

Role Enter Role

Avatar Male Female

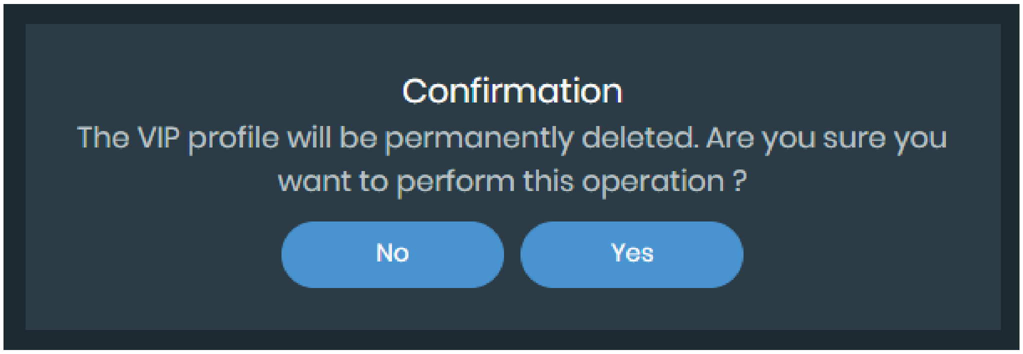
Cancel Submit

To edit a VIP profile:

1. Go to *Brand Protection* > *VIP Monitoring.*
2. Click *VIP Profiles* on the top right corner.
3. Click Edit icon on the desired VIP profile.
4. Make the necessary changes and click *Submit.*

To delete a VIP profile:

1. Go to *Brand Protection* > *VIP Monitoring.*
2. Click *VIP Profiles* on the top right corner.
3. Click Delete icon on the desired VIP profile.
4. A confirmation message is displayed. Click *Yes*.



Confirmation

The VIP profile will be permanently deleted. Are you sure you want to perform this operation ?

Code Repo Exposure

The *Code Repo Exposure* page displays a list of attributes that have been exposed in code repositories.

From the *Brand Protection > Code Repo Exposure* page, you can:

- Review attribute information. See Reviewing attributes on page 83.
- Take action against the discovered attributes. See Managing attributes on page 83.
- Filter attributes. See Filtering attributes on page 84.

Reviewing attributes

You can review information about exposed code attributes in the *Brand Protection > Code Repo Exposure* page. Information displayed about discovered exposed code includes:

- Attributes and values
- Matched domains identified with the exposure
- Raw information about the exposure
- Discovery date
- Risk status

To review exposed attributes:

1. Go to *Brand Protection > Code Repo Exposure*.
2. Review the high level attribute information:
   - Review the risk level and total number of the alerts in the *Alert Summary*.
   - Review the attribute types in *Top 5 Attributes*.
3. Select an alert to view the attribute type, domain, and raw information.

Managing attributes

You can interact with discovered exposed code, such as marking the attribute as resolved or ignored, or adding a comment to the attribute history. Archived attributes can be viewed by selecting *Show Archived*.

To manage an attribute:

1. Go to *Brand Protection* > *Code Repo Exposure*.
2. Find the attribute you want to adjust.
3. Change the status:
    - Select *Action* > *Mark as Resolved* to indicate that the exposed code risk has been resolved.
    - Select *Action* > *Mark as False Positive* if the discovered code is not a risk.
4. Click *Comment* to add a comment to the attribute history.

To manage multiple attributes at once:

1. Go to *Brand Protection* > *Code Repo Exposure*.
2. Select the attributes you want to adjust. The *Action* dropdown menu is displayed.
3. Adjust the status or comment history of all of the attributes:
    - Select *Action* > *Mark as Resolved* to indicate that the exposed code risk has been resolved for all of the selected attributes.
    - Select *Action* > *Mark as False Positive* if the discovered code is not a risk.
    - Click *Action* > *Comment* to add a global comment to the attribute history of the selected attributes.

Filtering attributes

You can filter attributes by date, status, risk level, or attribute.

To filter attributes:

1. Go to *Brand Protection* > *Code Repo Exposure*
2. Filter attributes by a date range:
    a. Click *Filter By Date Range*. Two calendars are displayed.
    b. In the left calendar, select a month, year, and day to specify the start date of the range.
    c. Select a month, year, and day to specify the end date of the range.
    Only attributes from the date range are displayed.
    d. Click the *Filter By Date Range* box, and click *X* to remove the date range filter.
3. Search for keywords:
    a. In the *Type and hit Enter to Search* box, type a keyword, and press *Enter*.

    The attributes are filtered to display only attributes with the keyword.

    b. Click the *X* beside the keyword to remove the filter.
4. Filter by status in the *By Alert Status* section:
    - Select *Active*, *Resolved*, or *Ignored* to filter attributes by their assigned status.
5. Filter by risk level in the *By Risk Level* section:
    - Select *High*, *Medium*, or *Low* to filter by risk level.
6. Select the domain from the *By Matched Domain* section.
7. Select the attribute type in the *By Attributes* section to filter by type.
8. Click *Search*. The attributes with the matching filters are displayed.

Open Bucket Exposure

The *Open Bucket Exposure* page displays a list of files exposed in open buckets.

From the *Brand Protection > Open Bucket Exposure* page, you can:

- Review files exposed on open buckets. See Reviewing files on page 85.
- Take action against discovered files. See Managing files on page 85.
- Filter files. See Filtering files on page 86.

Reviewing files

You can review information about exposed files in the *Brand Protection > Open Bucket Exposure* page. Information displayed about discovered exposed files includes:

- File name
- File type
- Bucket source
- Bucket name
- Discovery date
- File accessibility

To review exposed attributes:

1. Go to *Brand Protection > Open Bucket Exposure*.
2. Review the high level file information:
   - Review the distribution of bucket sources and the total number of discovered files in the *Alert Summary*.
   - Review the distribution of file types in *Top 5 File Types*.
3. Select a file to review detailed file information.

Managing files

You can interact with discovered exposed files, such as marking the files as resolved or ignored, or adding a comment to the attribute history. Archived files can be viewed by selecting *Show Archived*.

To manage a file:

1. Go to *Brand Protection > Open Bucket Exposure*
2. Find the file you want to adjust.
3. Change the status:
   - Select *Action > Mark as Resolved* to indicate that the exposed risk has been resolved.
   - Select *Action > Mark as Ignored* to indicate that the identified exposure can be ignored.
4. Click *Comment* to add a comment to the file history.

To manage multiple files at once:

1. Go to *Brand Protection* > *Open Bucket Exposure*
2. Select the files you want to adjust. The *Action* dropdown menu is displayed.
3. Adjust the status or comment history of all of the file:
   - Select *Action* > *Mark as Resolved* to indicate that the exposure risk has been resolved for all of the selected files.
   - Select *Action* > *Mark as Ignored* to indicate that the identified exposures can be ignored.
   - Click *Action* > *Comment* to add a global comment to the file history of the selected files.

Filtering files

You can filter files by date, status, risk level, or attribute.

To filter files:

1. Go to *Brand Protection* > *Open Bucket Exposure*
2. Filter files by a date range:
   a. Click *Filter By Date Range*. Two calendars are displayed.
   b. In the left calendar, select a month, year, and day to specify the start date of the range.
   c. Select a month, year, and day to specify the end date of the range.
   Only files from the date range are displayed.
   d. Click the *Filter By Date Range* box, and click *X* to remove the date range filter.
3. Search for keywords:
   a. In the *Type and hit Enter to Search* box, type a keyword, and press *Enter*.

      The files are filtered to display only files with the keyword.
   b. Click the *X* beside the keyword to remove the filter.
4. Filter by status in the *By Alert Status* section:
   - Select *Active*, *Resolved*, or *Ignored* to filter files by their assigned status.
5. Filter by accessibility in the *By File Status* section.
6. Select the open bucket source from the *By Bucket* section.
7. Select the file type in the *By Type* section.
8. Click *Search*. The files with the matching filters are displayed.

Take Down

The FortiRecon team uses a proprietary Digital Millennium Copyright Act (DMCA) process to execute the takedown. During the takedown process, notices are sent to the offending parties, hosting providers, and registrars with provisions of local and international laws to demand that the account be taken down on account of impersonation, phishing, and so on.

You can review the current status of takedown requests in the *Brand Protection* > *Take Down* page.

From the *Brand Protection* > *Take Down* page, you can:

- Filter for specific takedown requests by date, category, status, and ticket number. See Filtering takedown requests on page 87.

Filtering takedown requests

You can filter the takedown requests or search for specific *Ticket* numbers on the *Take Down* page.

To filter requests by category and status:

1. Go to *Brand Protection* > *Take Down*.
2. Filter requests by a date range:
   1. Click *Filter By Date Range*. Two calendars are displayed.
   2. In the left calendar, select a month, year, and day to specify the start date of the range.
   3. In the right calendar, select a month, year, and day to specify the end date of the range.
      Only requests from the date range are displayed.
   4. Click the *Filter By Date Range* box, and click *X* to remove the date range filter.
3. Search for keywords:
   1. In the *Type and hit Enter to Search* box, type a *Ticket* number, and press *Enter*.

      The requests are filtered to display only requests with the keyword.
   2. Click the *X* beside the keyword to remove the filter.
4. Select the request category in the *Category* dropdown.
5. Select the current status of the request from the *Status* dropdown:
   1. *Requested*: You have requested that the fraudulent product be taken down.
   2. *Acknowledged*: The FortiRecon team has acknowledged that they have received the request for takedown.
   3. *Work In Progress*: The FortiRecon team is currently working on taking down the fraudulent product.
   4. *Closed*: The fraudulent product has been taken down and the ticket has been closed.

   The tickets that match the set filters are displayed.

Adversary Centric Intelligence

The Adversary Centric Intelligence (ACI) module leverages FortiGuard Threat Analysts to provide comprehensive coverage of dark web, open source, and technical threat intelligence, including threat actor insights. This information enables administrators to proactively assess risks, respond faster to incidents, better understand their attackers, and protect assets

The *Adversary Centric Intelligence* module contains the following pages:

Dashboard	Displays a summary of your organization's risk exposure to overall global threats. See Dashboard on page 88.
Reports	Displays all the intelligence reports available to you. See Reports on page 92.
Card Fraud	Displays information about credit or debit cards that are for sale on darknet marketplaces. See Card Fraud on page 98.
Stealer Infections	Displays information about possible infected systems that are affiliated with your employees or end-users and are for sale on darknet market places. See Stealer Infections on page 100.
OSINT - Cyber Threats	Displays OSINT-based intelligence reports about threat events. See OSINT Cyber Threats on page 105.
Vulnerability Intelligence	Displays information on monitored CVEs. See Vulnerability Intelligence on page 110.
Ransomware Intelligence	Displays information on total and potential ransomware incidents. See Ransomware Intelligence on page 114.
Vendor Risk Assessment	Displays information on a vendor watchlist and the vendor's security hygiene. See Vendor Risk Assessment on page 120.
Intelligence Collection Lookup	Displays threat intelligence from various sources to let you search for a specific posts or messages using a simple search query. See Intelligence Collection Lookup.
Investigation	Displays tabs to let you search for and investigate the reputation of an IPv4 address, domain, file hash, or CVE. See Investigation on page 131.

Dashboard

The *Adversary Centric Intelligence* > *Dashboard* page provides a summary of your organization's risk exposure to global threats. From the *Adversary Centric Intelligence* > *Dashboard* page, you can:

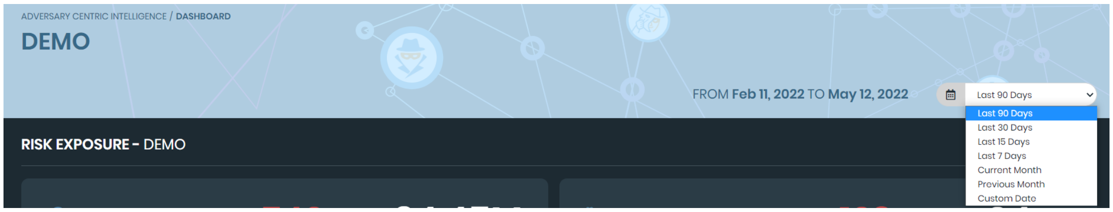
- Change the date range for the dashboard content. See Changing the dashboard date range on page 89.
- View your organization's risk exposure. See Viewing risk exposure summary on page 89.
- View global threat reports. See Viewing global threat report summary on page 91.

Changing the dashboard date range

By default, the *Adversary Centric Intelligence > Dashboard* page displays information for the last 90 days. You can change the date range.

To change the dashboard date range:

1. Go to the *Adversary Centric Intelligence > Dashboard* page.
   The banner identifies the date range for the displayed information. In the following example, the date range is *From Feb 11, 2022 to May 12, 2022*.



FROM **Feb 11, 2022** TO **May 12, 2022**

2. From the calendar dropdown list, select a different date range.

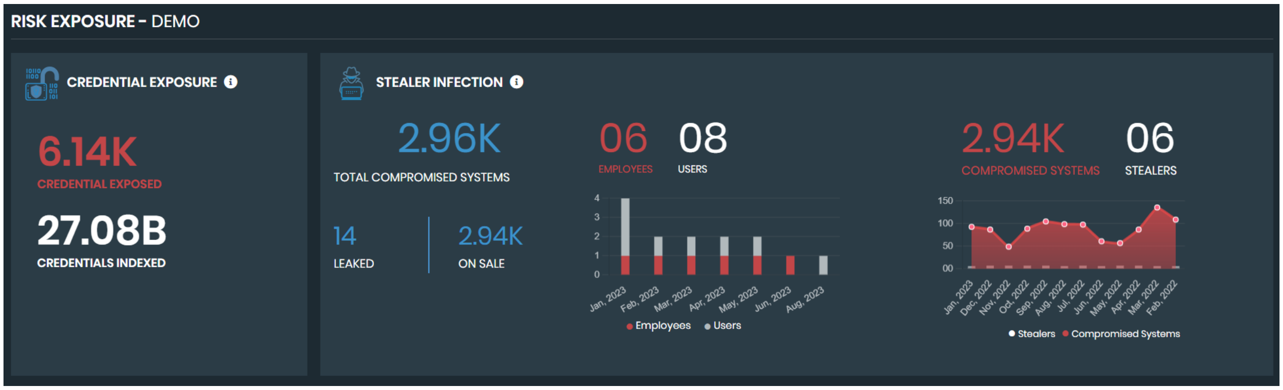
Viewing risk exposure summary

The *Adversary Centric Intelligence > Dashboard* page displays the following widgets in the *Risk Exposure* section that summarize the risk exposure of your organization to global threats:

- Credential Exposure
- Stealer Infection
- Associated Threats
- Global Event Exposure
- Card Fraud

To view risk exposure summary:

1. Go to the *Adversary Centric Intelligence > Dashboard* page, and scroll to the *Risk Exposure* section. A summary of your organization's risk exposure is displayed.



2. Use the following widgets to review your exposure to risk:

Credential Exposure	Displays the number of email addresses related to your organization's domains that are part of third-party credential breaches. The number of exposed credentials and the number of indexed credentials are displayed.
Stealer Infection	Displays data from potentially infected systems that are affiliated with your employees or end-users and are leaked or for sale on credential stealer marketplaces on the darknet. The total number of compromised systems along with number of leaked and on sale compromised systems are displayed. Hover your mouse over on the *Employees/Users* chart to view the number of affected employees and users on a specific date. Hover your mouse over on the *Compromised Systems/Stealers* chart to view the number of compromised systems and stealers on a specific date.
Associated Threats	Displays information about threats reported against your industry and geographical area. The number of reported threats that are specific to your industry and the number of reported threats in your geographic area are displayed. Click the widget to display more details on the *Adversary Centric Intelligence > Reports* page.
High Relevance Reports	Displays the reports that are flagged as highly relevant to your organization. Reports must meet certain criteria to be considered relevant. The newest reports are displayed at the top. Click a report to display more details on the *Adversary Centric Intelligence > Reports* page.
Global Event Exposure	Displays the latest, published intelligence reports related to notable cyber events from around the globe. Automatically scrolls through the reports, or click the blue bars at the bottom of the widget to view specific reports.
Card Fraud This widget is only displayed for banking organizations that issue credit or debit cards.	Displays statistics related to credit or debit cards that are listed for sale on darknet marketplaces.

	The number of cards for sale is displayed as well as how many of the cards are credit cards and how many are debit cards. Click the *Cards for Sale* number to display more details on the *Adversary Centric Intelligence* > *Card Fraud* page. Hover your mouse over the bars in the chart to view the number of card frauds on a specific date. The top card bin numbers are also displayed.

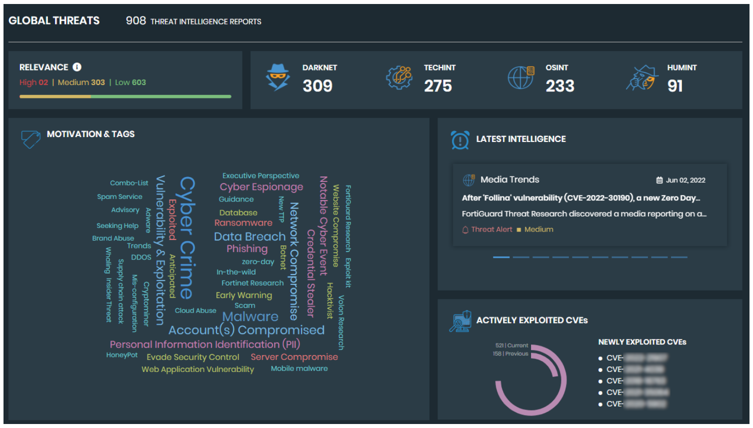
Viewing global threat report summary

The *Adversary Centric Intelligence* > *Dashboard* page displays the following widgets in the *Global Threats* section that summarize latest intelligence reports related to ongoing, notable, global cyber events:

- Relevance
- Categories
- Motivational Tags
- Latest Intelligence
- Actively Exploited CVEs
- Top Actors
- Notable Category Reporting

To view global threat report summary:

1. Go to the *Adversary Centric Intelligence* > *Dashboard* page, and scroll to the *Global Threats* section. The number of global threat reports is displayed as well as several widgets.



GLOBAL THREATS 908 THREAT INTELLIGENCE REPORTS

RELEVANCE ⓘ
High 02 | Medium 303 | Low 603

DARKNET 309
TECHINT 275
OSINT 233
HUMINT 91

MOTIVATION & TAGS

LATEST INTELLIGENCE

Media Trends Jun 02, 2022
After 'Follina' vulnerability (CVE-2022-30190), a new Zero Day...
FortiGuard Threat Research discovered a media reporting on a...
Threat Alert ■ Medium

ACTIVELY EXPLOITED CVEs

521 | Current
158 | Previous

NEWLY EXPLOITED CVEs
- CVE-[redacted]
- CVE-[redacted]
- CVE-[redacted]
- CVE-[redacted]
- CVE-[redacted]

2. Use the following widgets to review the global threat intelligence reports:

Relevance	Displays the number of reports that are relevant to your organization and are rated high, medium, or low risk. Reports must meet certain criteria to be considered high, medium, or low risk. Click the widget to display more details on the *Adversary Centric Intelligence* > *Reports* page.
Categories	Displays the number of reports for each category, such as Darknet, TechINT, OSINT, and HUMINT.

	Click a category to display more details on the *Adversary Centric Intelligence* > *Reports* page.
Motivational Tags	Displays the available motivational tag filters for reports. Click a tag to display the *Adversary Centric Intelligence* > *Reports* page filtered on the tag.
Latest Intelligence	Displays the latest, published intelligence reports organized into the following categories: • Flash Alert • Flash Report • Threat Alert • Threat Report Automatically scrolls through the reports, or you can click the blue bars at the bottom of the widget to view specific reports.
Actively Exploited CVEs	Displays the number of currently and previously exploited CVEs and identifies a list of newly exploited CVEs. Click the widget to display more details on the *Adversary Centric Intelligence* > *Investigation* page.
Top Actors	Displays the number of actors being tracked as well as the number of reports on the actors. Displays a summary of top actors. Click the name of a top actor to display more details on the *Adversary Centric Intelligence* > *Reports* page.
Notable Category Reporting	Click a report to display more details on the *Adversary Centric Intelligence* > *Reports* page.

Reports

The *Adversary Centric Intelligence* > *Reports* page displays all the intelligence reports available to you. By default all reports are displayed, starting with the latest report. From the *Adversary Centric Intelligence* > *Reports* page, you can:

- View the details of each report. See Viewing reports on page 92.
- Apply filters to the list of reports to hone in on specific reports. See Filtering reports on page 94.
- Download a PDF of reports. See Downloading reports and observables on page 95.
- Share reports. See Sharing reports on page 96.
- Export observables to Microsoft Excel format. See Exporting observables on page 97.

Viewing reports

The *Adversary Centric Intelligence* > *Reports* page displays all the reports available to you on the *All Reports* tab. By default all reports are displayed, starting with the latest report.

You can filter the list of reports, and search the list of reports using a keyword. See Filtering reports on page 94.

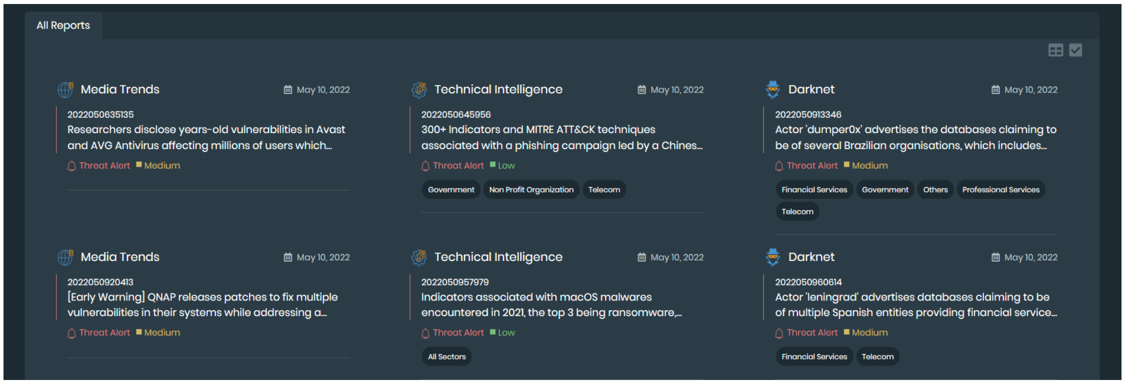
When you open a report, its details are displayed on a separate tab, and you can download a PDF of the report, share the report with another person, and access related reports. When the report contains associated observables, you can download them in Microsoft Excel format.

From an open report, you can also click associated tags to filter the list of reports on the *All Reports* tab, and then access additional related reports.

See also Rating reports on page 74.

To view reports:

1. Go to *Adversary Centric Intelligence* > *Reports*. All reports are displayed in the *All Reports* tab.



Media Trends — May 10, 2022
2022050635135
Researchers disclose years-old vulnerabilities in Avast and AVG Antivirus affecting millions of users which...
Threat Alert ■ Medium

Technical Intelligence — May 10, 2022
2022050645956
300+ Indicators and MITRE ATT&CK techniques associated with a phishing campaign led by a Chines...
Threat Alert ■ Low
Government | Non Profit Organization | Telecom

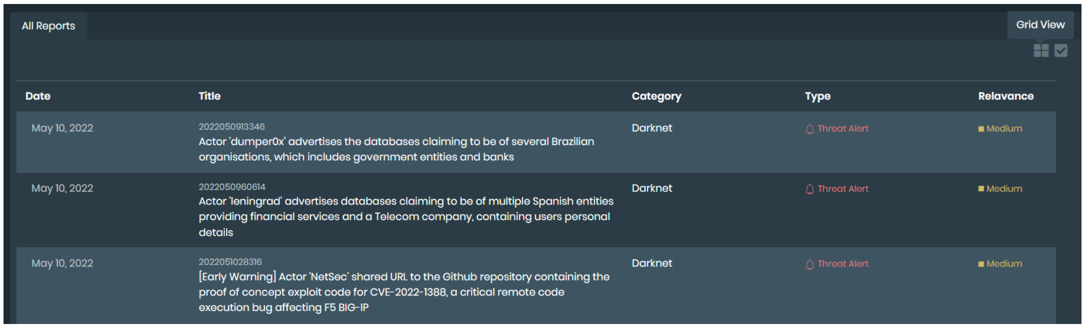
Darknet — May 10, 2022
2022050913346
Actor 'dumper0x' advertises the databases claiming to be of several Brazilian organisations, which includes...
Threat Alert ■ Medium
Financial Services | Government | Others | Professional Services | Telecom

Media Trends — May 10, 2022
2022050920413
[Early Warning] QNAP releases patches to fix multiple vulnerabilities in their systems while addressing a...
Threat Alert ■ Medium

Technical Intelligence — May 10, 2022
2022050957979
Indicators associated with macOS malwares encountered in 2021, the top 3 being ransomware,...
Threat Alert ■ Low
All Sectors

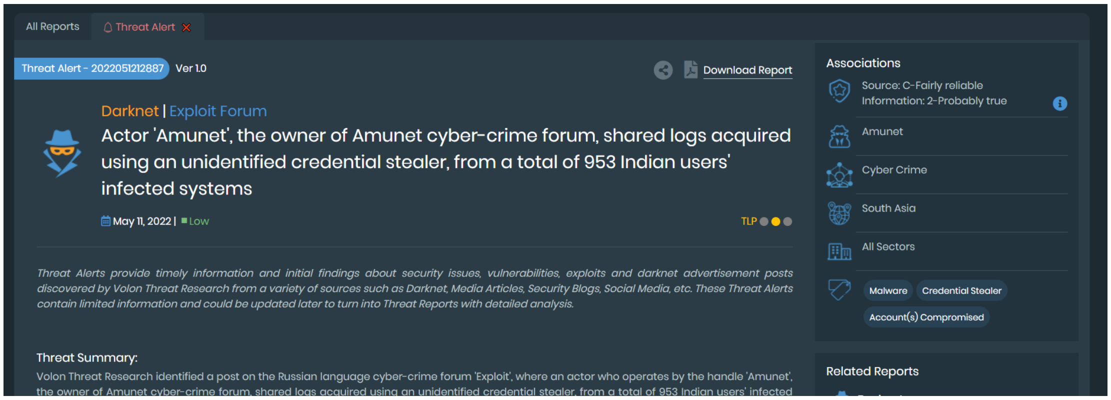
Darknet — May 10, 2022
2022050960614
Actor 'leningrad' advertises databases claiming to be of multiple Spanish entities providing financial service...
Threat Alert ■ Medium
Financial Services | Telecom

2. On the *All Reports* tab, toggle between *Grid View* and *Table View*.
In the following example, *Table View* is selected, and you can click the *Grid View* button to change to *Grid View*.



Date	Title	Category	Type	Relavance
May 10, 2022	2022050913346 Actor 'dumper0x' advertises the databases claiming to be of several Brazilian organisations, which includes government entities and banks	Darknet	Threat Alert	■ Medium
May 10, 2022	2022050960614 Actor 'leningrad' advertises databases claiming to be of multiple Spanish entities providing financial services and a Telecom company, containing users personal details	Darknet	Threat Alert	■ Medium
May 10, 2022	2022051028316 [Early Warning] Actor 'NetSec' shared URL to the Github repository containing the proof of concept exploit code for CVE-2022-1388, a critical remote code execution bug affecting F5 BIG-IP	Darknet	Threat Alert	■ Medium

3. Click a report title to display the report details in a new tab.



Darknet | Exploit Forum

Actor 'Amunet', the owner of Amunet cyber-crime forum, shared logs acquired using an unidentified credential stealer, from a total of 953 Indian users' infected systems

May 11, 2022 | ■ Low

Threat Alerts provide timely information and initial findings about security issues, vulnerabilities, exploits and darknet advertisement posts discovered by Volon Threat Research from a variety of sources such as Darknet, Media Articles, Security Blogs, Social Media, etc. These Threat Alerts contain limited information and could be updated later to turn into Threat Reports with detailed analysis.

Threat Summary:
Volon Threat Research identified a post on the Russian language cyber-crime forum 'Exploit', where an actor who operates by the handle 'Amunet', the owner of Amunet cyber-crime forum, shared logs acquired using an unidentified credential stealer, from a total of 953 Indian users' infected

Associations
Source: C-Fairly reliable
Information: 2-Probably true
Amunet
Cyber Crime
South Asia
All Sectors
Malware | Credential Stealer | Account(s) Compromised

Related Reports

From the report details page, you can:

- Hover over various icons and words to view tooltips of information.
- Click some words to display more information. For example, click *TLP* (traffic light protocol) to display definitions of the different TLPs and rules around sharing the information.
- Click the *Share Link* button to share a link to the report with another person who has a FortiRecon account.
- Click the *Download Report* link to download a PDF of the report to your computer.
- View and search associated observables as well as click *Export Observables* to download the list of observables in Microsoft Excel format.

From *Associations* area on the right, you can:

- View what is associated with the report, such as the reliability rating, adversary, motivation, tags, and so on.
- Click the *i* icon to view information about reliability ratings.
- Click a tag to return to the *All Reports* tab to view the list of reports filtered on the selected tag.

From *Related Reports* area on the right, you can:

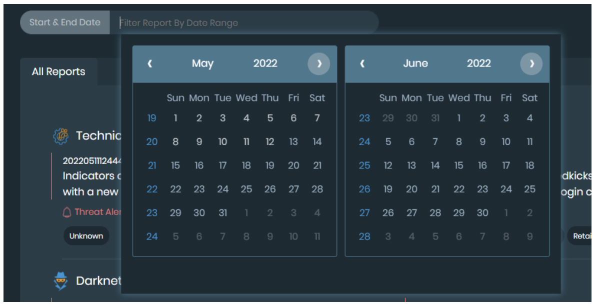
- View a list of reports related to the open report.
- Click a related report to open it in a new tab.
- Click a tag to return to the *All Reports* tab to view the list of reports filtered on the selected tag.

Filtering reports

Reports can by filtered by date range, keywords, categories of filters, and relevance to your organization.

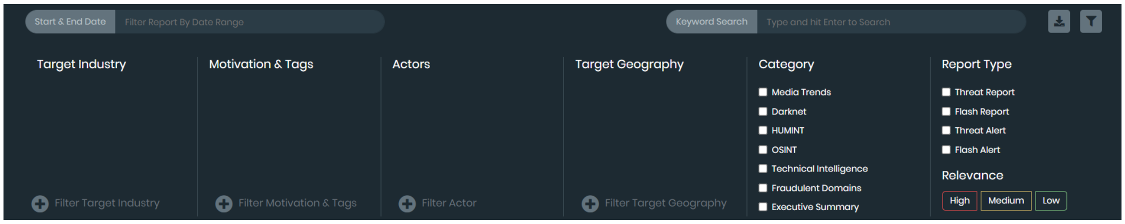
To filter reports:

1. Go to *Adversary Centric Intelligence* > *Reports*.
2. Filter reports by a date range:
   a. Click *Filter Report by Date Range*. Two calendars are displayed.



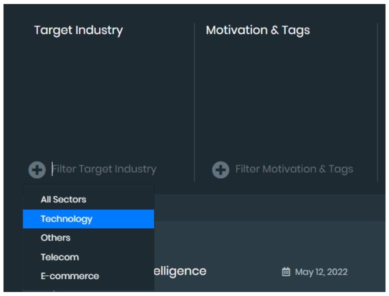
   b. In the left calendar, select a month, year, and day to specify the start date of the range.
   c. In the right calendar, select a month, year, and day to specify the end date of the range. Only reports from the date range are displayed.
   d. Click the *Filter Report by Date Range* box, and click *X* to remove the date range filter.
3. Search for keywords:
   a. In the *Type and hit Enter to Search* box, type a keyword, and press *Enter*. The reports are filtered to display only reports with the keyword.
   b. Click the *X* beside the keyword to remove the filter.

4. Filter reports by categories:
   a. On the right side, click the *Filters* button. The following filter categories are displayed:



- *Target Industry*
- *Motivation & Tags*
- *Actors*
- *Target Geography*
- *Category*
- *Report Type*

   b. Under the *Target Industry*, *Motivation & Tags*, *Actors*, and *Target Geography* categories, click *Filter <category name>*, and select one or more filters.



   c. Under *Category* and *Report Types*, select checkboxes to enable the filters, and clear checkboxes to disable filters.
   d. Under *Report Type* > *Relevance*, click *High*, *Medium*, and/or *Low* to enable the filters, and clear the filters to disable them.

Downloading reports and observables

You can download a PDF of the reports displayed on the *Adversary Centric Intelligence* > *Reports* page to your hard drive. A maximum of 300 reports can be downloaded at one time.

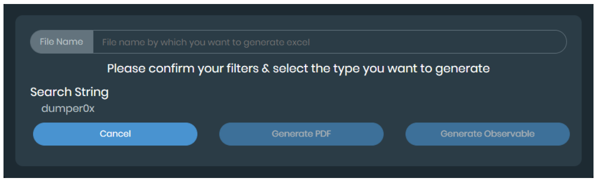
When the report includes Indicators of Compromise (IOCs), you can click the *Generate Observable* button to download the IOCs in Microsoft Excel format.

When you open a report, you can download a PDF of the open report.

To download reports:

1. Go to *Adversary Centric Intelligence* > *Reports*.
2. Filter the reports. See Filtering reports on page 94.
   The filtered list of reports is displayed.
3. (Optional) Select which of the filtered reports to download:
   a. Click the *Download Specific Reports* button. Checkboxes are displayed beside each report title.
   b. Select the checkbox beside each report you want to download.

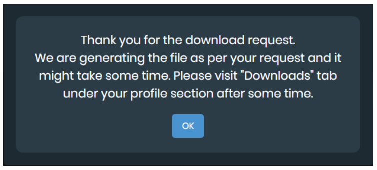
4. Click the *Downloads* button. A confirmation dialog is displayed.



Please confirm your filters & select the type you want to generate

Search String
dumper0x

5. In the *File Name* box, type a name.
6. (Optional) If the report contains IOC information, you can click *Generate Observable* to download IOC information in Microsoft Excel format.
7. Click *Generate PDF*.
   A dialog is displayed.

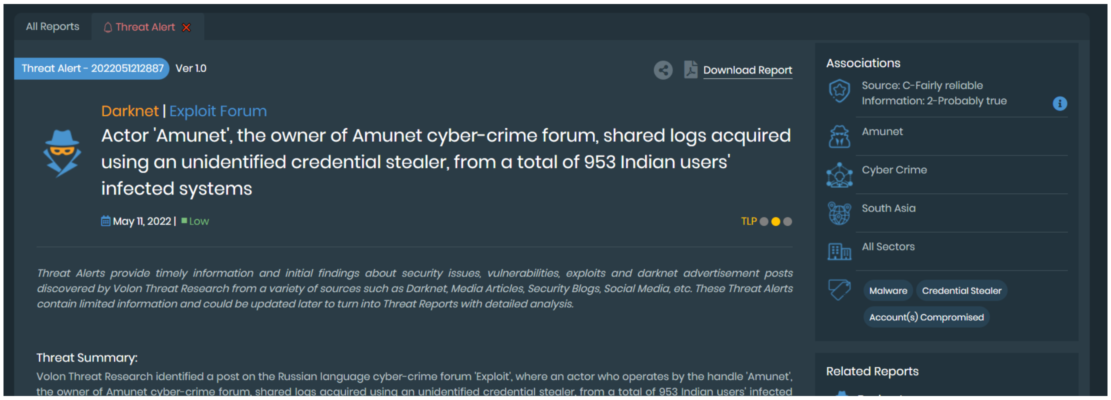


Thank you for the download request.
We are generating the file as per your request and it might take some time. Please visit "Downloads" tab under your profile section after some time.

8. Click *OK*.
9. Retrieve the download. See Retrieving downloads on page 145.

To download a PDF from an open report:

1. Go to *Adversary Centric Intelligence* > *Reports*.
2. Click a report to display its details.



Actor 'Amunet', the owner of Amunet cyber-crime forum, shared logs acquired using an unidentified credential stealer, from a total of 953 Indian users' infected systems

Source: C-Fairly reliable
Information: 2-Probably true

Threat Alerts provide timely information and initial findings about security issues, vulnerabilities, exploits and darknet advertisement posts discovered by Volon Threat Research from a variety of sources such as Darknet, Media Articles, Security Blogs, Social Media, etc. These Threat Alerts contain limited information and could be updated later to turn into Threat Reports with detailed analysis.

Threat Summary:
Volon Threat Research identified a post on the Russian language cyber-crime forum 'Exploit', where an actor who operates by the handle 'Amunet', the owner of Amunet cyber-crime forum, shared logs acquired using an unidentified credential stealer, from a total of 953 Indian users' infected

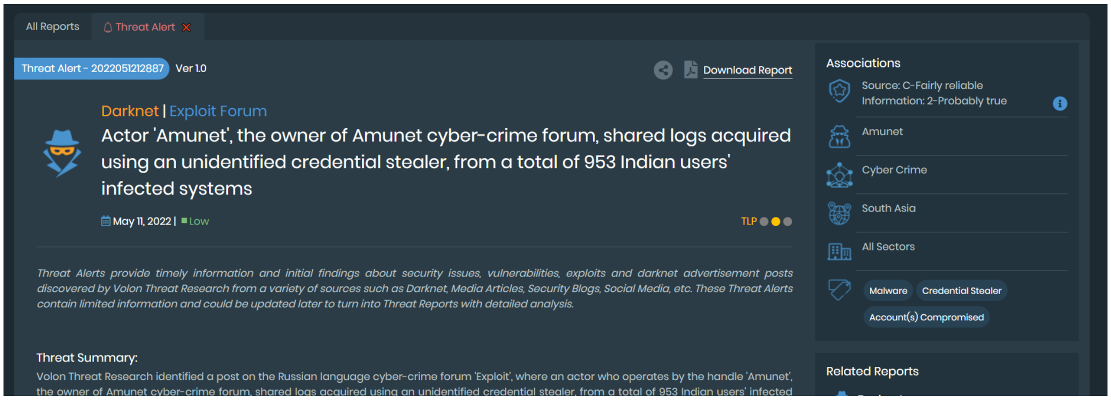
3. Click the *Download Report* button.
   A PDF of the report is downloaded to your computer.

Sharing reports

You can share reports by using a link or an email.

To share a report:

1. Go to *Adversary Centric Intelligence* > *Reports*.
2. Click a report to display its details.



Darknet | Exploit Forum

Actor 'Amunet', the owner of Amunet cyber-crime forum, shared logs acquired using an unidentified credential stealer, from a total of 953 Indian users' infected systems

May 11, 2022 | Low   TLP

Threat Alerts provide timely information and initial findings about security issues, vulnerabilities, exploits and darknet advertisement posts discovered by Volon Threat Research from a variety of sources such as Darknet, Media Articles, Security Blogs, Social Media, etc. These Threat Alerts contain limited information and could be updated later to turn into Threat Reports with detailed analysis.

Threat Summary:

Volon Threat Research identified a post on the Russian language cyber-crime forum 'Exploit', where an actor who operates by the handle 'Amunet', the owner of Amunet cyber-crime forum, shared logs acquired using an unidentified credential stealer, from a total of 953 Indian users' infected

Associations

Source: C-Fairly reliable
Information: 2-Probably true

Amunet

Cyber Crime

South Asia

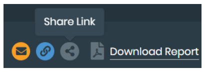
All Sectors

Malware · Credential Stealer · Account(s) Compromised

Related Reports

3. Click the *Share Link* button.

   The *Email* and *Copy Link* buttons are displayed.



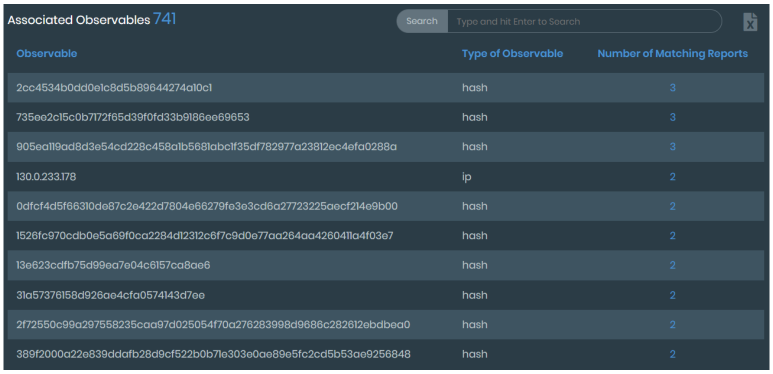
Exporting observables

When a report has associated observables, they are displayed at the bottom of the report in the *Associated Observables* section.

You can download the list of observables in Microsoft Excel format. The downloaded file is password protected. FortiRecon provides the password you need to open the file in Microsoft Excel.

To export observables:

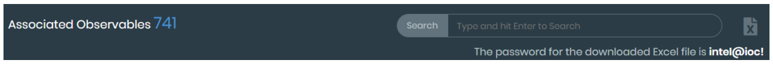
1. View a report. See Viewing reports on page 92.
2. Scroll down to the *Associated Observables* section.
   In the following example, the report has 741 associated observables:



Observable	Type of Observable	Number of Matching Reports
2cc4534b0dd0e1c8d5b89644274a10c1	hash	3
735ee2c15c0b7172f65d39f0fd33b9186ee69653	hash	3
905ea119ad8d3e54cd228c458a1b5681abc1f35df782977a23812ec4efa0288a	hash	3
130.0.233.178	ip	2
0dfcf4d5f66310de87c2e422d7804e66279fe3e3cd6a27723225aecf214e9b00	hash	2
1526fc970cdb0e5a69f0ca2284d12312c6f7c9d0e77aa264aa4260411a4f03e7	hash	2
13e623cdfb75d99ea7e04c6157ca8ae6	hash	2
31a57376158d926ae4cfa0574143d7ee	hash	2
2f72550c99a297558235caa97d025054f70a276283998d9686c282612ebdbea0	hash	2
389f2000a22e839ddafb28d9cf522b0b71e303e0ae89e5fc2cd5b53ae9256848	hash	2

3. On the right, click the *Download Observables* button.

   The password for the download is displayed. In the following example, the password is *intel@ioc!*.



The password for the downloaded Excel file is **intel@ioc!**

The excel file is downloaded to your computer.

4. Open the Excel file.

   You are prompted for the password.

5. Type the password from FortiRecon, and click *OK*. The Excel file opens.

Card Fraud

> The *Adversary Centric Intelligence* > *Card Fraud* page widget is only displayed for banking organizations that issue credit or debit cards.

The *Adversary Centric Intelligence* > *Card Fraud* page displays information about credit or debit cards that are for sale on darknet marketplaces. From the *Card Fraud* page, you can:

- View a summary of the total number of leaked cards as well as information about each leaked card. See Viewing leaked card information on page 98.
- Filter the information. See Filtering leaked card information on page 99.
- Download the list of leaked cards to Microsoft Excel format. See Exporting a list of leaked cards on page 99.

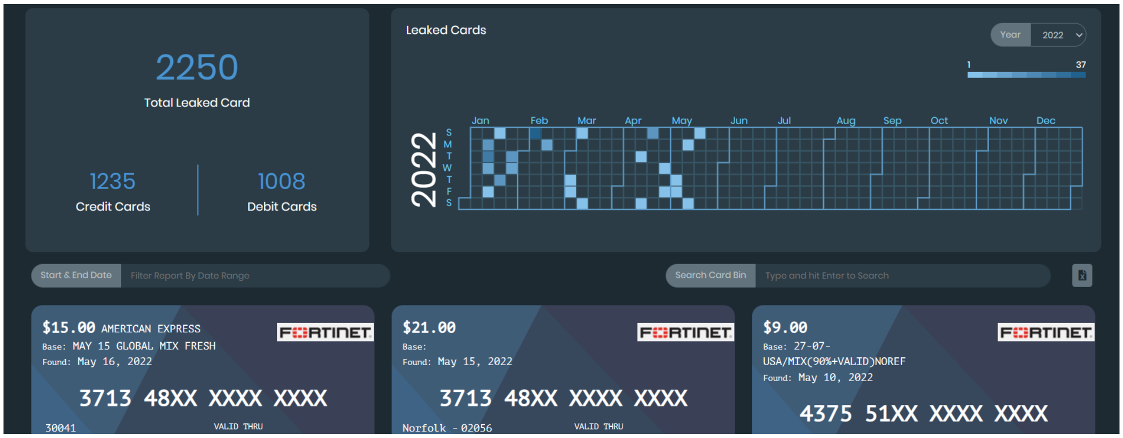
Viewing leaked card information

The *Adversary Centric Intelligence* > *Card Fraud* page displays information about the number of leaked cards as well as details about the leaked cards for a specific date range.

To view leaked card information:

1. Go to *Adversary Centric Intelligence* > *Card Fraud*. The *Card Fraud* page is displayed.

   The *Total Leaked Card*, *Credit Cards*, and *Debit Cards* numbers are for the default date range. Details about the leaked cards are displayed below.



2250 Total Leaked Card

1235 Credit Cards

1008 Debit Cards

$15.00 AMERICAN EXPRESS
Base: MAY 15 GLOBAL MIX FRESH
Found: May 16, 2022
3713 48XX XXXX XXXX
30041 VALID THRU

$21.00
Base:
Found: May 15, 2022
3713 48XX XXXX XXXX
Norfolk - 02056 VALID THRU

$9.00
Base: 27-07-USA/MIX(90%+VALID)NOREF
Found: May 10, 2022
4375 51XX XXXX XXXX

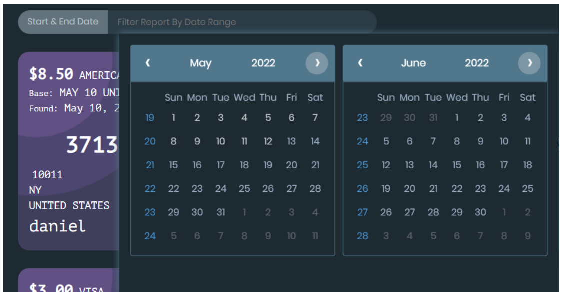
2. You can filter the displayed information. See Filtering leaked card information on page 99.

Filtering leaked card information

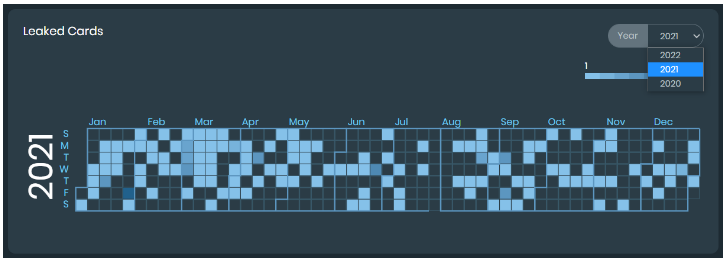
You can filter information about leaked cards by year, date range, and bank identification number (BIN).

To filter leaked card information:

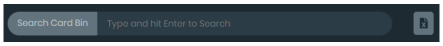
1. Go to *Adversary Centric Intelligence* > *Card Fraud*.
2. Filter reports by a date range:
   a. Click *Filter Report by Date Range*. Two calendars are displayed.



   b. In the left calendar, select a month, year, and day to specify the start date of the range.
   c. In the right calendar, select a month, year, and day to specify the end date of the range. Only reports from the date range are displayed.
   d. Click the *Filter Report by Date Range* box, and click *X* to remove the date range filter.
3. Filter by year:
   a. In the *Leaked Cards* widget, select a year from the dropdown list.



4. Filter by card BIN:
   a. In the *Search Card Bin* box, type a BIN, and press *Enter*.

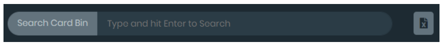


Exporting a list of leaked cards

You can download the list of leaked cards to a Microsoft Excel file.

To export leaked cards:

1. Go to *Adversary Centric Intelligence* > *Card Fraud*.
2. Beside the *Search Card Bin* box, click the *Export Leaked Cards* button.

   The *Leaked Card.xlsx* file is downloaded.
3. Open the file in Microsoft Excel.

Stealer Infections

The *Adversary Centric Intelligence* > *Stealer Infection* page includes information about possible infected systems that are affiliated with your employees or end-users that are listed for sale on credential stealer darknet marketplaces. The compromised system information is organized into two tabs:

1. **Leaked** - The *Compromised Systems(Leaked)* tab displays the stolen data that has been shared over Darknet forums, Telegram channels, Tor sites or any other medium where the threat actor operates. See Viewing leaked compromised systems.
2. **On Sale** - The *Compromised Systems(On Sale)* tab displays the stolen data that is currently being offered for sale on various Darknet marketplaces. See Viewing on sale compromised systems.

On the *Stealer Infection* page, you can:

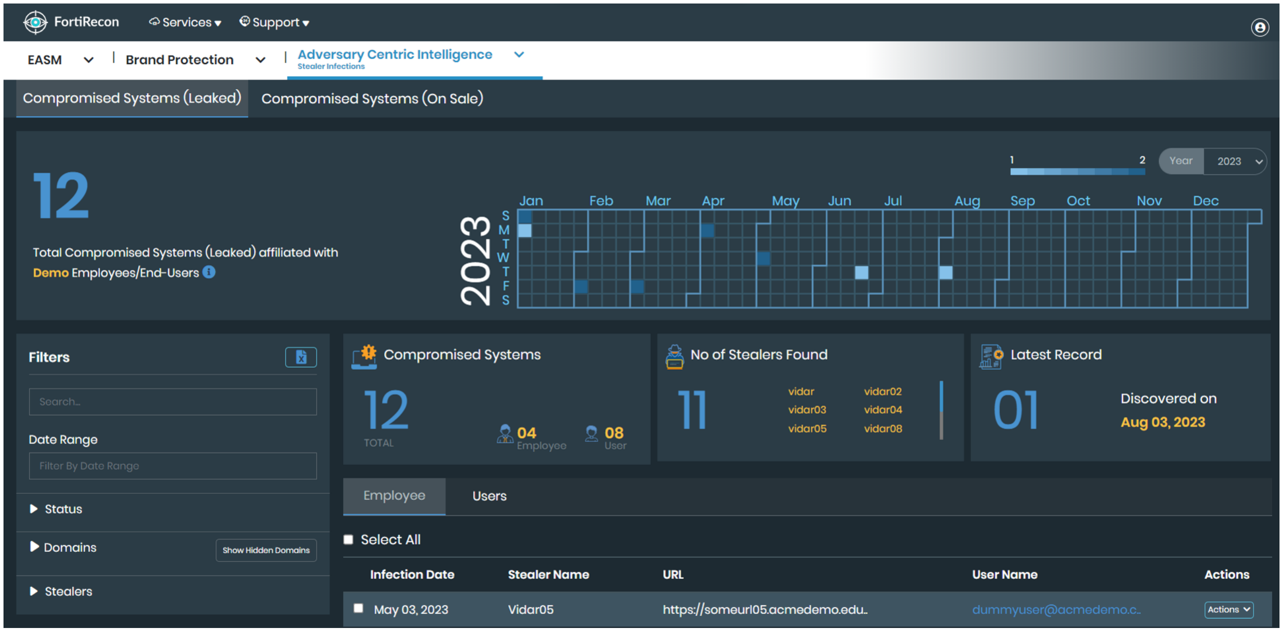
- Filter stealer infection information. See Filtering stealer infection information on page 103.
- Export market place data. See Exporting stealer infections data on page 105.

Viewing leaked compromised systems

The *Adversary Centric Intelligence* > *Stealer Infections* > *Compromised Systems(Leaked)* page displays information about possible infected systems that are affiliated with your employees or end-users that has been shared over Darknet forums, Telegram channels, Tor sites or any other medium where the threat actor operates.

To view leaked compromised systems information:

1. Go to *Adversary Centric Intelligence* > *Stealer Infections* > *Compromised Systems(Leaked)*.



	Infection Date	Stealer Name	URL	User Name	Actions
□	May 03, 2023	Vidar05	https://someurl05.acmedemo.edu..	dummyuser@acmedemo.c..	Actions

2. Use the following widgets to review information about leaked compromised systems:

Total Compromised Systems (Leaked) affiliated with <organization name>	Displays the total number of compromised systems leaked affiliated with your organization. The calendar displays a summary of the leaked stealer events in the selected calendar year. Colored blocked indicate a stealer event. Light colors blocks indicate few affected credentials, and dark colored blocks indicate many affected credentials. Hover your mouse over each block to view the discovery date and the number of affected credentials.
Compromised Systems	Displays the total number of compromised systems including affected employees and end-users count.
No of Stealers Found	Displays the number of stealers found and the names of the stealers.
Latest Record	Displays the latest number of stealer events and the date that the event was discovered.
Employee	Displays a list of affected employees information.
Users	Displays a list of affected end-users information.

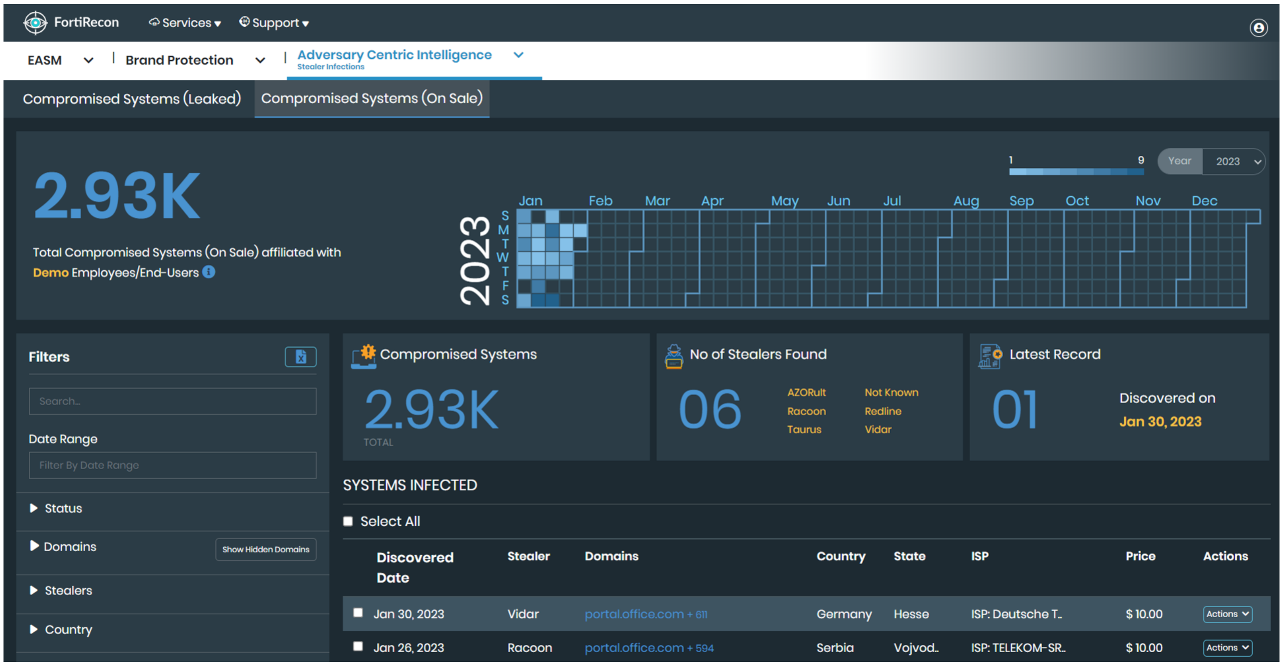
The values in all widgets are updated based on the filters applied, except for *Total Compromised Systems(Leaked) affiliated with <organization name>* value.

Viewing on sale compromised systems

The *Adversary Centric Intelligence > Stealer Infections > Compromised Systems(On Sale)* page displays information about possible infected systems that are affiliated with your employees or end-users and are for sale on darknet market places.

To view on sale compromised systems information:

1. Go to *Adversary Centric Intelligence > Stealer Infections > Compromised Systems(On Sale)*.



SYSTEMS INFECTED

□ Select All

	Discovered Date	Stealer	Domains	Country	State	ISP	Price	Actions
□	Jan 30, 2023	Vidar	portal.office.com + 611	Germany	Hesse	ISP: Deutsche T..	$ 10.00	Actions
□	Jan 26, 2023	Racoon	portal.office.com + 594	Serbia	Vojvod..	ISP: TELEKOM-SR..	$ 10.00	Actions

2. Use the following widgets to review information about on sale compromised systems:

Total Compromised Systems (On Sale) affiliated with <organization name>	Displays the total number of compromised systems on sale affiliated with your organization. The calendar displays a summary of the on sale stealer events in the selected calendar year. Colored blocked indicate a stealer event. Light colors blocks indicate few affected credentials, and dark colored blocks indicate many affected credentials. Hover your mouse over each block to view the discovery date and the number of affected credentials.
Compromised Systems	Displays the total number of compromised systems.
No of Stealers Found	Displays the number of stealers found and the names of the stealers.
Latest Record	Displays the latest number of stealer events and the date that the event was discovered.
Systems Infected	Displays a list of infected systems.

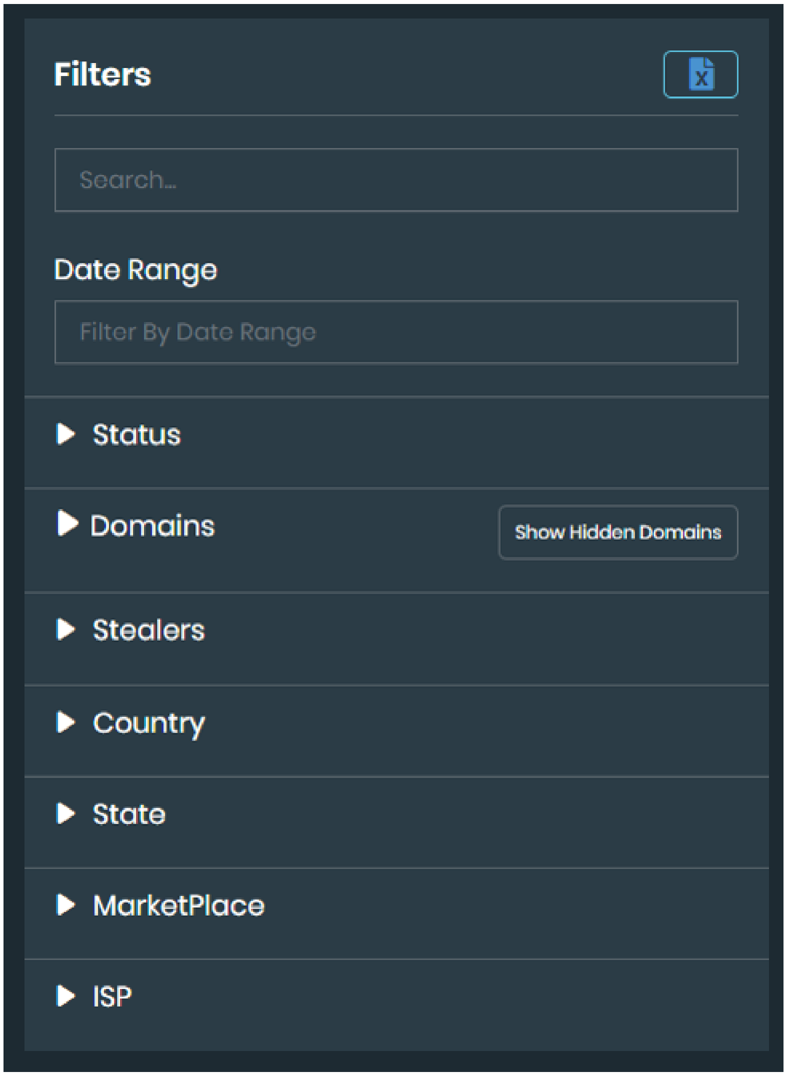
The values in all widgets are updated based on the filters applied, except for *Total Compromised Systems(On Sale) affiliated with <organization name>* value.

Filtering stealer infection information

You can use several methods to filter information in the *Stealer Infections* .

To filter stealer infection information:

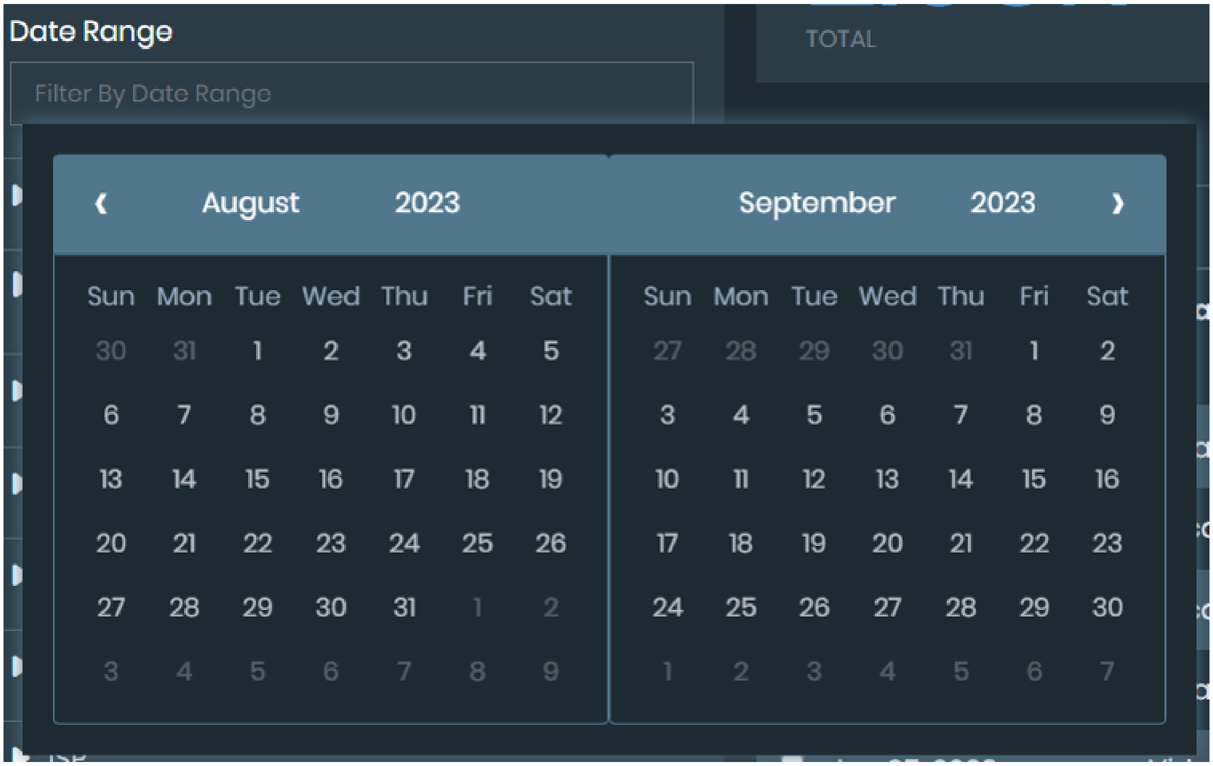
1. Go to *Adversary Centric Intelligence* > *Stealer Infections*.
2. Select the desired tab *Compromised Systems(Leaked)* or *Compromised Systems(On Sale)*.
3. In the *Filters* pane on the left hand side select the filters.



4. Search for keywords:
   a. In the *Type and hit Enter to Search* box, type a keyword, and press *Enter*.
      The information is filtered.

   b. Clear the keyword and press *Enter* to remove the filter.

5. Filter information by a date range:
   a. Click *Filter Report by Date Range*. Two calendars are displayed.



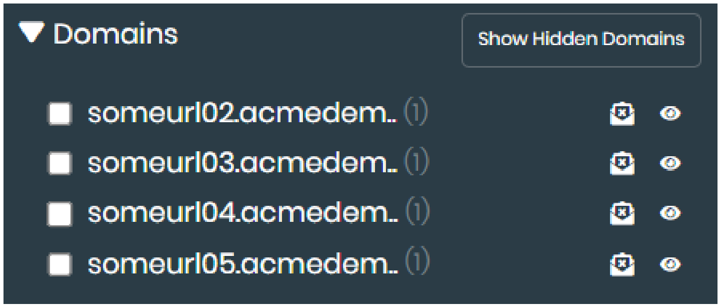
August			2023			
Sun	Mon	Tue	Wed	Thu	Fri	Sat
30	31	1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31	1	2
3	4	5	6	7	8	9

September			2023			
Sun	Mon	Tue	Wed	Thu	Fri	Sat
27	28	29	30	31	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
1	2	3	4	5	6	7

   b. In the left calendar, select a month, year, and day to specify the start date of the range.
   c. In the right calendar, select a month, year, and day to specify the end date of the range.
      Only information from the date range is displayed.
   d. Click the *X* in the *Start & End Date* box to remove the date range filter.

6. Click *Active* or *Resolved* to filter by status.

7. Filter by domains.

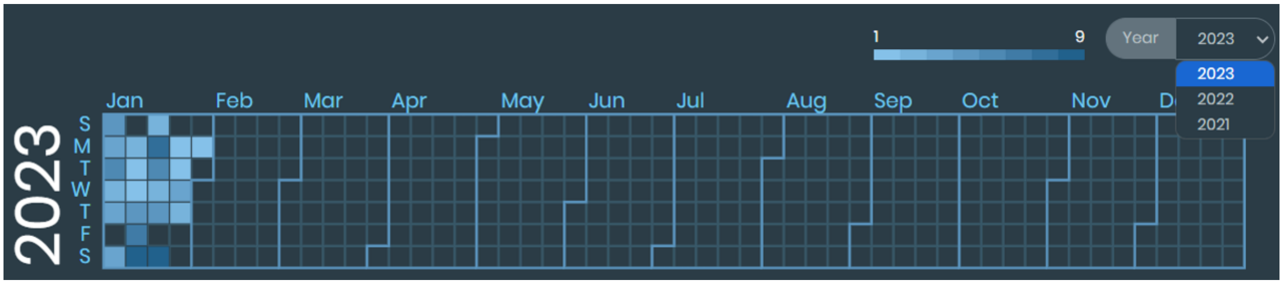


□ someurl02.acmedem.. (1)
□ someurl03.acmedem.. (1)
□ someurl04.acmedem.. (1)
□ someurl05.acmedem.. (1)

   a. Click desired domains to filter.
   b. Click ⊠ icon next to desired domain to unsubscribe and stop email notifications.
   c. Click 👁 icon next to desired domain to hide the domain.
   d. Click *Show Hidden Domains* to view hidden domains. Click ⊘ icon next to the desired hidden domain to unhide.

8. Click stealers to filter the data based on a specific stealers.

9. The following additional filters are available for *Compromised Systems(On Sale)* page. Click desired values to filter.
   - *Country*
   - *State*
   - *Marketplace*
   - *ISP*
10. Filter the events by year using *Calendar* widget:

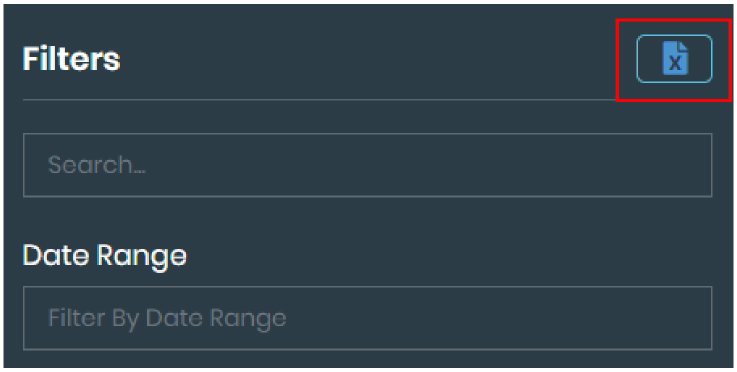


Exporting stealer infections data

You can download the stealer infections information to an *All Market Place.xlsx* file in Microsoft Excel format.

To export stealer infections information:

1. Go to *Adversary Centric Intelligence* > *Stealer Infections*.
2. Select the desired tab *Compromised Systems(Leaked)* or *Compromised Systems(On Sale)*.
3. (Optional) Filter the data. See Filtering stealer infection information on page 103.
4. In the Filters pane on the left hand side, click the *Download* icon.



5. An *All Market Place.xlsx* file is downloaded.

OSINT Cyber Threats

Open Source Intelligence (OSINT) is method of gathering threat intelligence from publicly available sources. Over time, OSINT coverage has changed to a great extent. Previously, it only covered sources such as Blogs, news, business websites, social networks, and so on.

The *Adversary Centric Intelligence* > *OSINT - Cyber Threats* page provides you the ability to stay up to date with information published in open source platforms, such as social media, GitHub repositories, and so on. Information for review is based on specific criteria, including:

- Exploited vulnerabilities
- Zero day vulnerabilities
- Global events

On the *OSINT - Cyber Threats* page, you can:

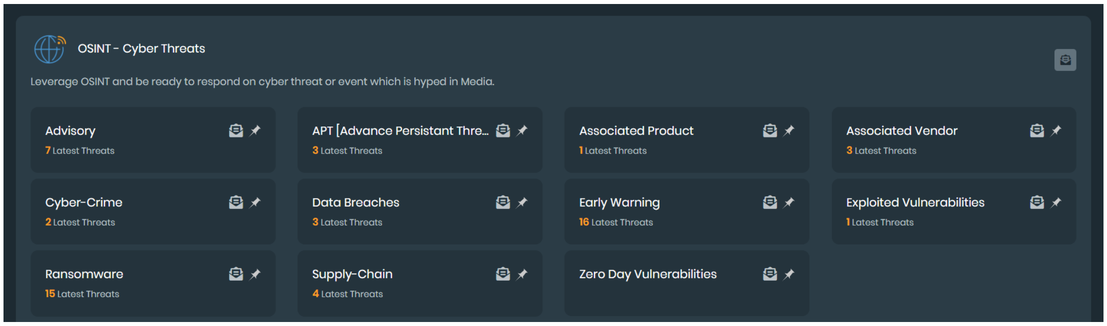
- Review threat events. See Reviewing threats on page 106.
- Pin threat events to the top of the list. See Pinning events on page 107.
- Subscribe to threat event notifications. See Subscribing to event notifications on page 107.
- Subscribe other FortiRecon users to event notifications. See Adding subscriptions on page 109.

Reviewing threats

You can view more information about each threat.

To review threats:

1. Go to *Adversary Centric Intelligence* > *OSINT - Cyber Threats*. The list of events is displayed.



OSINT - Cyber Threats

Leverage OSINT and be ready to respond on cyber threat or event which is hyped in Media.

Advisory
7 Latest Threats

APT [Advance Persistant Thre...
3 Latest Threats

Associated Product
1 Latest Threats

Associated Vendor
3 Latest Threats

Cyber-Crime
2 Latest Threats

Data Breaches
3 Latest Threats

Early Warning
16 Latest Threats

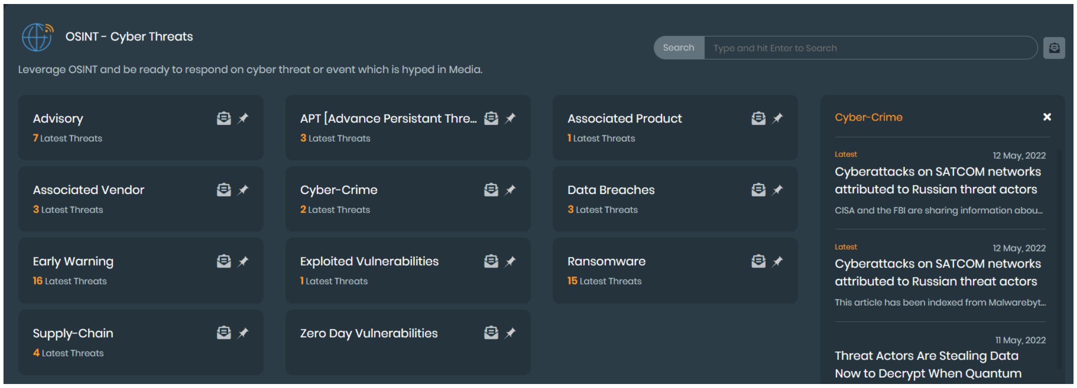
Exploited Vulnerabilities
1 Latest Threats

Ransomware
15 Latest Threats

Supply-Chain
4 Latest Threats

Zero Day Vulnerabilities

2. Click an event title, such as *Cyber-Crime*. The list of events is displayed on the right side.
   In the following example, *Cyber-Crime* is selected:



OSINT - Cyber Threats

Search: Type and hit Enter to Search

Leverage OSINT and be ready to respond on cyber threat or event which is hyped in Media.

Advisory
7 Latest Threats

APT [Advance Persistant Thre...
3 Latest Threats

Associated Product
1 Latest Threats

Associated Vendor
3 Latest Threats

Cyber-Crime
2 Latest Threats

Data Breaches
3 Latest Threats

Early Warning
16 Latest Threats

Exploited Vulnerabilities
1 Latest Threats

Ransomware
15 Latest Threats

Supply-Chain
4 Latest Threats

Zero Day Vulnerabilities

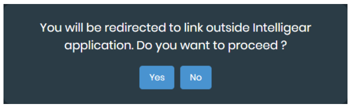
Cyber-Crime ×

Latest 12 May, 2022
Cyberattacks on SATCOM networks attributed to Russian threat actors
CISA and the FBI are sharing information abou...

Latest 12 May, 2022
Cyberattacks on SATCOM networks attributed to Russian threat actors
This article has been indexed from Malwarebyt...

11 May, 2022
Threat Actors Are Stealing Data Now to Decrypt When Quantum

3. On the right, click the event to display more information about it outside the FortiRecon portal.
   A confirmation dialog is displayed.



You will be redirected to link outside Intelligear application. Do you want to proceed ?

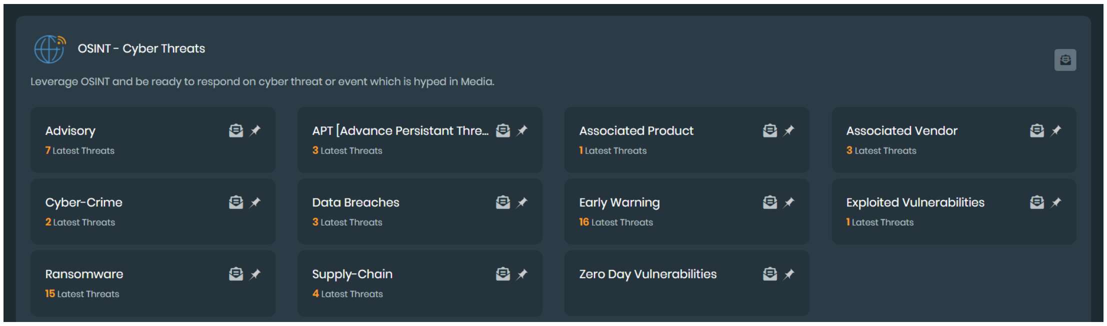
4. Click *Yes* to open the link in a new tab in your browser.

Pinning events

You can pin events to the top of the list. Pinned events have an orange *Pin* icon. Unpinned events have a white *Pin* icon.

To pin events:

1. Go to *Adversary Centric Intelligence* > *OSINT - Cyber Threats*. The list of events is displayed.

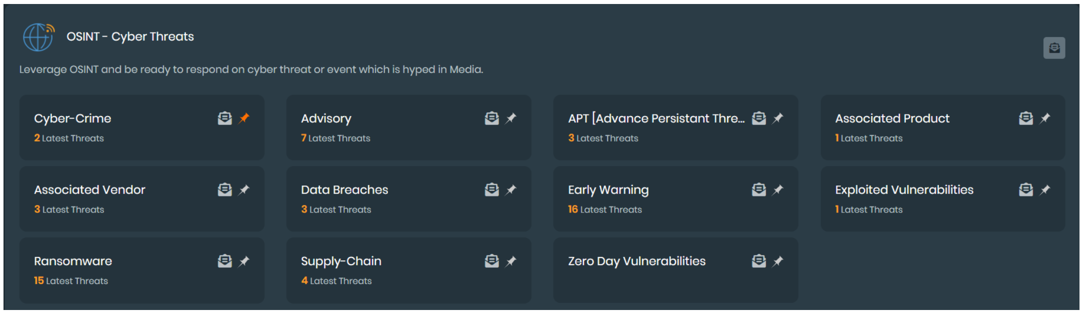


OSINT - Cyber Threats

Leverage OSINT and be ready to respond on cyber threat or event which is hyped in Media.

Advisory — 7 Latest Threats
APT [Advance Persistant Thre... — 3 Latest Threats
Associated Product — 1 Latest Threats
Associated Vendor — 3 Latest Threats
Cyber-Crime — 2 Latest Threats
Data Breaches — 3 Latest Threats
Early Warning — 16 Latest Threats
Exploited Vulnerabilities — 1 Latest Threats
Ransomware — 15 Latest Threats
Supply-Chain — 4 Latest Threats
Zero Day Vulnerabilities

2. Click the *Pin* icon beside an event to turn the pin orange and pin the event to the top of the list.
   In the following example, *Cyber-Crime* is pinned to the top of the list.



OSINT - Cyber Threats

Leverage OSINT and be ready to respond on cyber threat or event which is hyped in Media.

Cyber-Crime — 2 Latest Threats
Advisory — 7 Latest Threats
APT [Advance Persistant Thre... — 3 Latest Threats
Associated Product — 1 Latest Threats
Associated Vendor — 3 Latest Threats
Data Breaches — 3 Latest Threats
Early Warning — 16 Latest Threats
Exploited Vulnerabilities — 1 Latest Threats
Ransomware — 15 Latest Threats
Supply-Chain — 4 Latest Threats
Zero Day Vulnerabilities

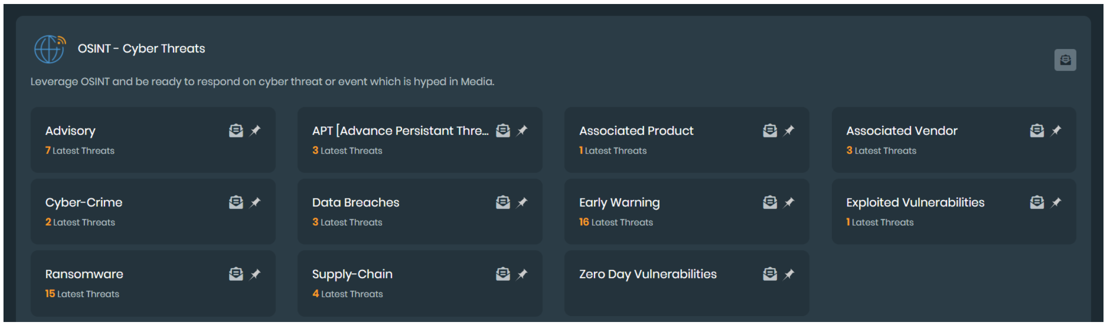
Click the *Pin* icon again to turn the pin white and unpin the event from the top of the list.

Subscribing to event notifications

You can enable subscriptions to receive notifications for one or more threat events. You can also change subscriptions and unsubscribe.

To subscribe to event notifications:

1. Go to *Adversary Centric Intelligence* > *OSINT - Cyber Threats*. The list of events is displayed.



OSINT - Cyber Threats

Leverage OSINT and be ready to respond on cyber threat or event which is hyped in Media.

Advisory
7 Latest Threats

APT [Advance Persistant Thre...
3 Latest Threats

Associated Product
1 Latest Threats

Associated Vendor
3 Latest Threats

Cyber-Crime
2 Latest Threats

Data Breaches
3 Latest Threats

Early Warning
16 Latest Threats

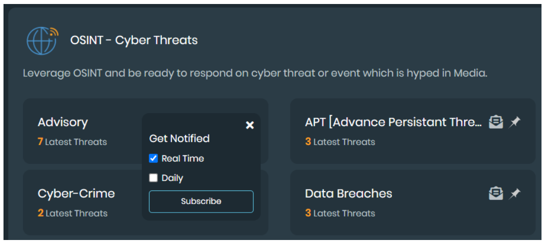
Exploited Vulnerabilities
1 Latest Threats

Ransomware
15 Latest Threats

Supply-Chain
4 Latest Threats

Zero Day Vulnerabilities

2. For an event, click the *Subscribe* icon. The subscription options are displayed for the event.
   In the following example, subscription options are displayed for the *Advisory* event:



OSINT - Cyber Threats

Leverage OSINT and be ready to respond on cyber threat or event which is hyped in Media.

Advisory
7 Latest Threats

Get Notified ×
☑ Real Time
□ Daily
Subscribe

APT [Advance Persistant Thre...
3 Latest Threats

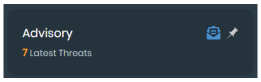
Cyber-Crime
2 Latest Threats

Data Breaches
3 Latest Threats

3. Select one of the following options to specify when to receive the notification:

Real time	Select to receive a notification when a new threat event is published.
Daily	Select to specify the time each day to receive a notification about new threat events.

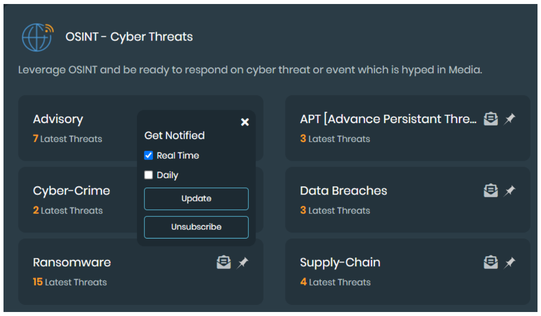
4. Click *Subscribe*.
   The *Subscribe* icon turns blue.



Advisory
7 Latest Threats

To change event notifications:

1. Go to *Adversary Centric Intelligence* > *OSINT - Cyber Threats*. The list of events is displayed.
2. Click a blue *Subscribe* icon. The subscription options are displayed.



OSINT - Cyber Threats

Leverage OSINT and be ready to respond on cyber threat or event which is hyped in Media.

Advisory
7 Latest Threats

Get Notified ×
☑ Real Time
□ Daily
Update
Unsubscribe

APT [Advance Persistant Thre...
3 Latest Threats

Cyber-Crime
2 Latest Threats

Data Breaches
3 Latest Threats

Ransomware
15 Latest Threats

Supply-Chain
4 Latest Threats

3. Change when you get notified, and click *Update*.

To unsubscribe from event notifications:

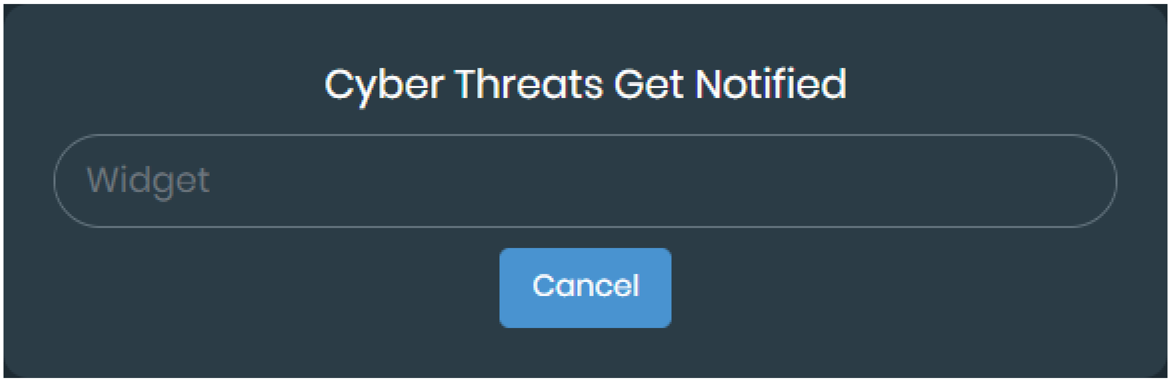
1. Go to *Adversary Centric Intelligence* > *OSINT - Cyber Threats*. The list of events is displayed.
2. Click a blue *Subscribe* icon. The subscription options are displayed.
3. Click *Unsubscribe*.
   The *Subscribe* icon turns white, and notifications are turned off.

Adding subscriptions

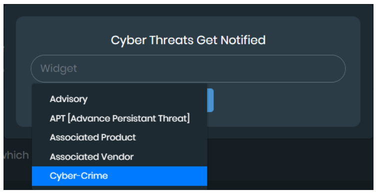
FortiRecon users with Admin privilege can set up subscriptions for other FortiRecon users to receive notifications about events.

To add subscriptions:

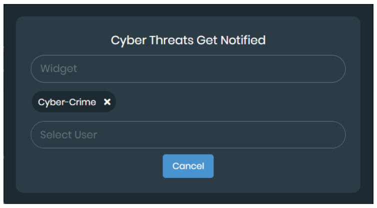
1. Go to *Adversary Centric Intelligence* > *OSINT - Cyber Threats*, and click the *Add Subscription* button. The *Cyber Threats Get Notified* dialog is displayed.



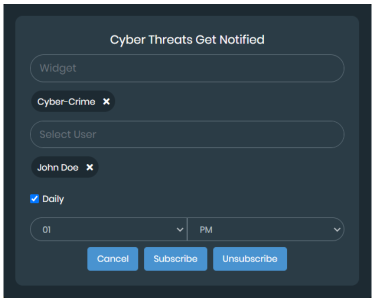
2. Click the *Widget* box, and select the threat events.
   In the following example, *Cyber-Crime* is selected.



   The *Select User* box is displayed.



3. In the *Select User* box, select a user.



Cyber Threats Get Notified

Widget

Cyber-Crime ×

Select User

John Doe ×

☑ Daily

01 | PM

The *Daily* check box is displayed. By default users receive notifications in real-time as events occur.

4. Select *Daily* specify what time each day the user should receive the notification.
   Clear the *Daily* check box to receive notifications in real time.
5. Click *Subscribe*.

Vulnerability Intelligence

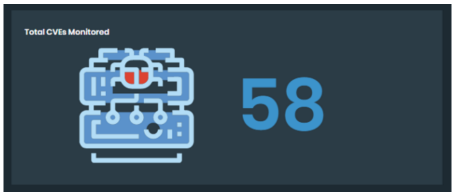
The *Adversary Centric Intelligence* > *Vulnerability Intelligence* page displays information on vulnerability exposure to help prioritize vulnerability patching. From the *Vulnerability Intelligence* page, you can:

- Review known CVEs. See Vulnerability exposure on page 110.
- Review the notable global CVEs. See Global notable vulnerabilities on page 111.
- View specific CVE reports. See Viewing and filtering CVE reports on page 112.
- Export a list of CVEs. See Exporting CVEs on page 113.
- Bulk add CVEs to monitor. See Manually adding CVEs on page 114.

Vulnerability exposure

Monitored CVEs can be reviewed at a high level from the *Adversary Centric Intelligence* > *Vulnerability Intelligence* page in the *Vulnerability exposure* section:

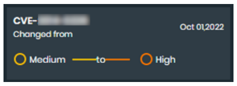
- *Total CVEs Monitored*: This tile displays the total count of monitored CVEs.

  Total CVEs Monitored

  58

  When the severity status of a CVE is changed, a flash tile will appear to show the updates.

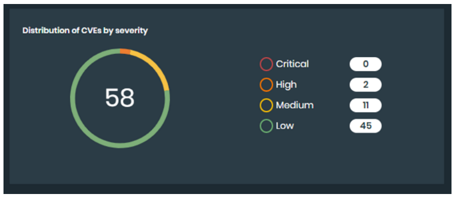
  CVE-[redacted]

  Changed from

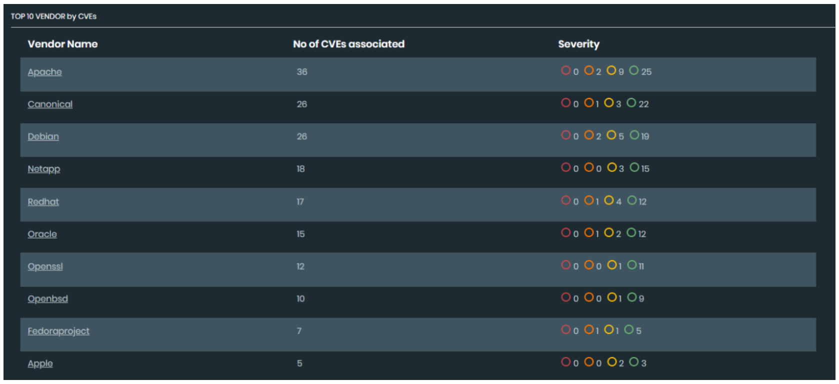
  Oct 01,2022

  ○ Medium —to— ○ High

- *Distribution of CVEs by severity*: This tile displays a graph of CVEs to show the total count of CVEs per rating, from *Low* to *Critical*.



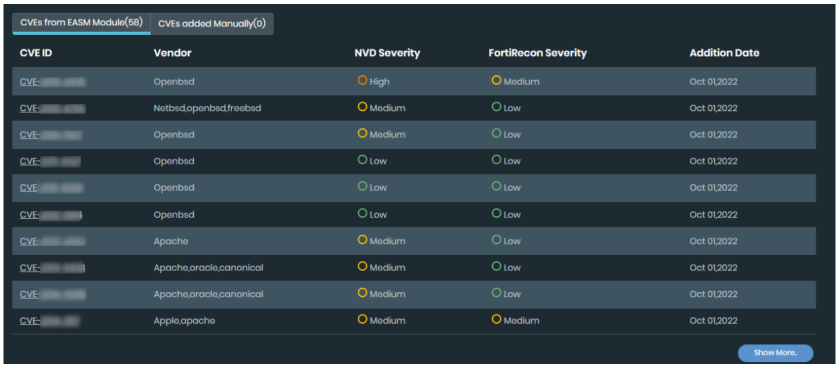
- *Top 10 vendors by CVEs*: Displays a list of the vendors with the most CVEs monitored and the severity range from *Low* to *Critical*. Select a *Vendor Name* or *Severity* to view more information.



TOP 10 VENDOR by CVEs

Vendor Name	No of CVEs associated	Severity
Apache	36	○ 0 ○ 2 ○ 9 ○ 25
Canonical	26	○ 0 ○ 1 ○ 3 ○ 22
Debian	26	○ 0 ○ 2 ○ 5 ○ 19
Netapp	18	○ 0 ○ 0 ○ 3 ○ 15
Redhat	17	○ 0 ○ 1 ○ 4 ○ 12
Oracle	15	○ 0 ○ 1 ○ 2 ○ 12
Openssl	12	○ 0 ○ 0 ○ 1 ○ 11
Openbsd	10	○ 0 ○ 0 ○ 1 ○ 9
Fedoraproject	7	○ 0 ○ 1 ○ 1 ○ 5
Apple	5	○ 0 ○ 0 ○ 2 ○ 3

- *CVEs from EASM Module*: Displays a list of automatically monitored CVEs. Select the *CVE ID* or *Show More* button to view more information.



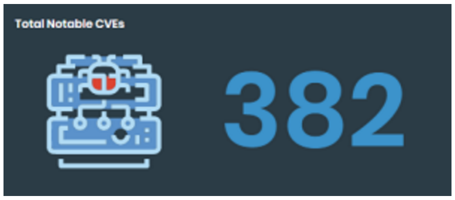
CVE ID	Vendor	NVD Severity	FortiRecon Severity	Addition Date
CVE-[redacted]	Openbsd	○ High	○ Medium	Oct 01,2022
CVE-[redacted]	Netbsd,openbsd,freebsd	○ Medium	○ Low	Oct 01,2022
CVE-[redacted]	Openbsd	○ Medium	○ Low	Oct 01,2022
CVE-[redacted]	Openbsd	○ Low	○ Low	Oct 01,2022
CVE-[redacted]	Openbsd	○ Low	○ Low	Oct 01,2022
CVE-[redacted]	Openbsd	○ Low	○ Low	Oct 01,2022
CVE-[redacted]	Apache	○ Medium	○ Low	Oct 01,2022
CVE-[redacted]	Apache,oracle,canonical	○ Medium	○ Low	Oct 01,2022
CVE-[redacted]	Apache,oracle,canonical	○ Medium	○ Low	Oct 01,2022
CVE-[redacted]	Apple,apache	○ Medium	○ Medium	Oct 01,2022

- *CVEs added Manually*: Displays a list of CVEs added by the user.

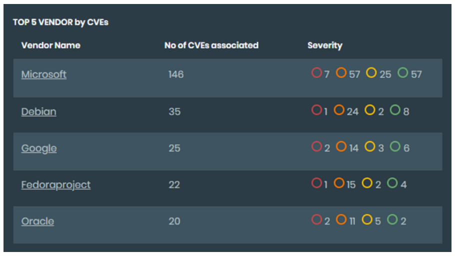
Global notable vulnerabilities

Monitored CVEs can be reviewed at a high level from the *Adversary Centric Intelligence* > *Vulnerability Intelligence* page in the *Global notable vulnerabilities* section:

- *Total Notable CVEs*: This tile displays the total count of notable CVEs.



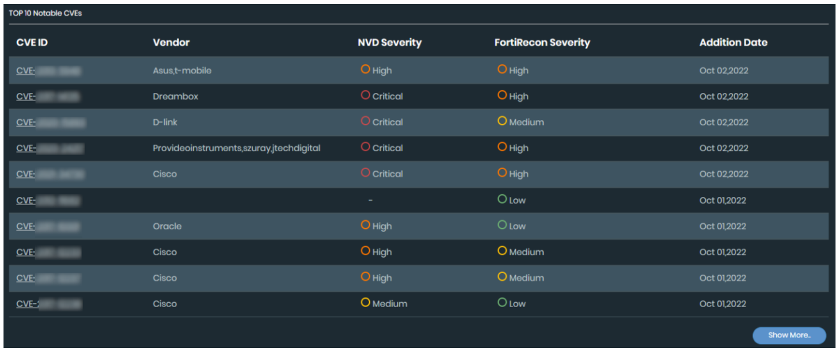
- *Top 5 vendors by CVEs*: Displays a list of the vendors with the most notable CVEs monitored and the severity range from *Low* to *Critical*. Select a *Vendor Name* to view more information.



TOP 5 VENDOR by CVEs

Vendor Name	No of CVEs associated	Severity
Microsoft	146	○ 7 ○ 57 ○ 25 ○ 57
Debian	35	○ 1 ○ 24 ○ 2 ○ 8
Google	25	○ 2 ○ 14 ○ 3 ○ 6
Fedoraproject	22	○ 1 ○ 15 ○ 2 ○ 4
Oracle	20	○ 2 ○ 11 ○ 5 ○ 2

- *Top 10 Notable CVEs*: Displays a list of the notable CVE monitored and the severity range from *Low* to *Critical*. Select the *CVE ID* or *Show More* button to view more information.



TOP 10 Notable CVEs

CVE ID	Vendor	NVD Severity	FortiRecon Severity	Addition Date
CVE-[redacted]	Asus,t-mobile	○ High	○ High	Oct 02,2022
CVE-[redacted]	Dreambox	○ Critical	○ High	Oct 02,2022
CVE-[redacted]	D-link	○ Critical	○ Medium	Oct 02,2022
CVE-[redacted]	Provideoinstruments,szuray,jtechdigital	○ Critical	○ High	Oct 02,2022
CVE-[redacted]	Cisco	○ Critical	○ High	Oct 02,2022
CVE-[redacted]		-	○ Low	Oct 01,2022
CVE-[redacted]	Oracle	○ High	○ Low	Oct 01,2022
CVE-[redacted]	Cisco	○ High	○ Medium	Oct 01,2022
CVE-[redacted]	Cisco	○ High	○ Medium	Oct 01,2022
CVE-[redacted]	Cisco	○ Medium	○ Low	Oct 01,2022

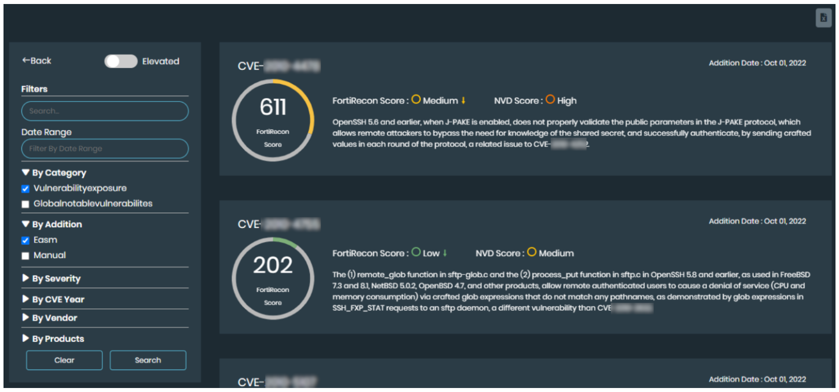
Viewing and filtering CVE reports

You can review detailed CVE reports in the *Adversary Centric Intelligence* > *Vulnerability Intelligence* page by:

- Selecting the CVE ID from the *Vulnerability exposure* > *CVEs from EASM Module* and *CVEs added Manually* tabs.
- Selecting the CVE ID from the *Global notable vulnerabilities* > *Top 10 Notable CVEs*.
- Filtering the vendor reports from *Vulnerability exposure* > *Top 10 vendor by CVEs* or *Global notable vulnerabilities* > *Top 5 vendor by CVEs*.
- Filtering all reports with the *Show More* button.

To filter reports:

1. Go to *Adversary Centric Intelligence* > *Vulnerability Intelligence*.
2. Select a *Vendor Name* or the *Show More* button. The CVE cards page is displayed.



CVE-[redacted]

Addition Date : Oct 01, 2022

611 FortiRecon Score

FortiRecon Score : ○ Medium ↓ NVD Score : ○ High

OpenSSH 5.6 and earlier, when J-PAKE is enabled, does not properly validate the public parameters in the J-PAKE protocol, which allows remote attackers to bypass the need for knowledge of the shared secret, and successfully authenticate, by sending crafted values in each round of the protocol, a related issue to CVE-[redacted].

CVE-[redacted]

Addition Date : Oct 01, 2022

202 FortiRecon Score

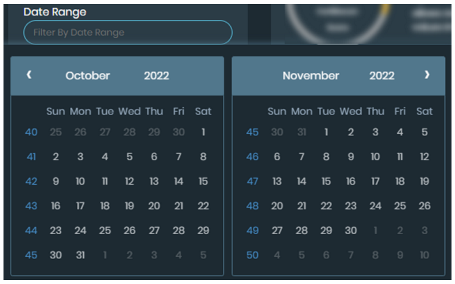
FortiRecon Score : ○ Low ↓ NVD Score : ○ Medium

The (1) remote_glob function in sftp-glob.c and the (2) process_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH_FXP_STAT requests to an sftp daemon, a different vulnerability than CVE[redacted]

CVE-[redacted]

Addition Date : Oct 01, 2022

3. Filter information by a date range:
   a. Click *Date Range*. Two calendars are displayed.



	Sun	Mon	Tue	Wed	Thu	Fri	Sat
40	25	26	27	28	29	30	1
41	2	3	4	5	6	7	8
42	9	10	11	12	13	14	15
43	16	17	18	19	20	21	22
44	23	24	25	26	27	28	29
45	30	31	1	2	3	4	5

	Sun	Mon	Tue	Wed	Thu	Fri	Sat
45	30	31	1	2	3	4	5
46	6	7	8	9	10	11	12
47	13	14	15	16	17	18	19
48	20	21	22	23	24	25	26
49	27	28	29	30	1	2	3
50	4	5	6	7	8	9	10

   b. In the left calendar, select a month, year, and day to specify the start date of the range.
   c. In the right calendar, select a month, year, and day to specify the end date of the range.
   d. Click the *X* to remove the date range filter.
4. Search for keywords:
   a. In the *Search* box, type a keyword.
5. Enable *Elevated* to search for CVEs that have had the severity increased.
6. Filter reports by information:
   a. Select the information dropdown menus:
      - *By Category*
      - *By Addition*
      - *By Severity*
      - *By CVE Year*
      - *By Vendor*
      - *By Products*
   b. Select one or more filters.
7. Click *Search*. The CVE reports that match the filters are displayed.
8. Select the CVE ID to view the full, detailed report.

Exporting CVEs

You can export a list of all or specific CVEs from the CVE cards page to an Excel file. Information in the file includes:

- CVE ID
- Truview Score
- Truview Severity
- NVD Severity
- Description
- Published date

To export CVEs:

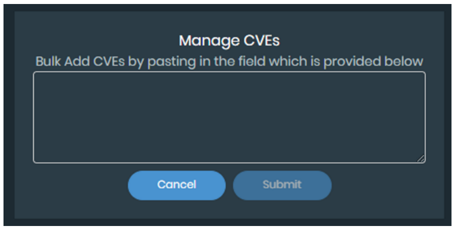
1. Go to *Adversary Centric Intelligence* > *Vulnerability Intelligence*.
2. Select a *Vendor Name* or the *Show More* button. The CVE cards page is displayed.
3. Filter for the reports you want included in the Excel file. See Viewing and filtering CVE reports on page 112.
4. Click *Export CVE List*. An Excel file is downloaded to your device.

Manually adding CVEs

You can bulk add CVEs to monitor in the *Vulnerability Exposure > CVEs added Manually* tab on the *Adversary Centric Intelligence > Vulnerability Intelligence* page.

To manually add CVEs:

1. Go to *Adversary Centric Intelligence > Vulnerability Intelligence*.
2. Click *Manage CVEs Watchlist*. The *Manage CVEs* dialog is displayed.



Manage CVEs

Bulk Add CVEs by pasting in the field which is provided below

3. Enter the CVE IDs in the text field.
4. Click *Submit*.

Ransomware Intelligence

The *Adversary Centric Intelligence > Ransomware Intelligence* page helps with supply chain monitoring and displays information on past and potential ransomware incidents. The information in this module is captured from blogs and sites operated by ransomware operators. The names of victims or potential victims mentioned in this section are purely based on information provided on these sites and blogs. The authenticity of these claims must be validated by your organization.

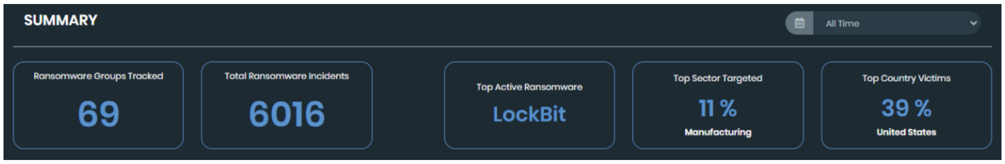
From the *Ransomware Intelligence* page, you can:

- View past and potential ransomware incidents. See Viewing ransomware intelligence on page 114.
- Filter ransomware incident information. See Filtering ransomware intelligence on page 116.
- Export information on ransomware incidents to an Excel file. See Exporting ransomware information on page 117.
- Create, edit, and monitor a ransomware watchlist. See Managing My Watchlist on page 118.

Viewing ransomware intelligence

The *Ransomware Intelligence* page contains multiple sections that display high level information on the ransomware threat landscape. Sections include:

- *Summary*: A summary to total incidents, groups currently being tracked, and the top sector, country, and active ransomware. Select a card to view more information in the *Ransomware Trends*.



SUMMARY

All Time

Ransomware Groups Tracked 69

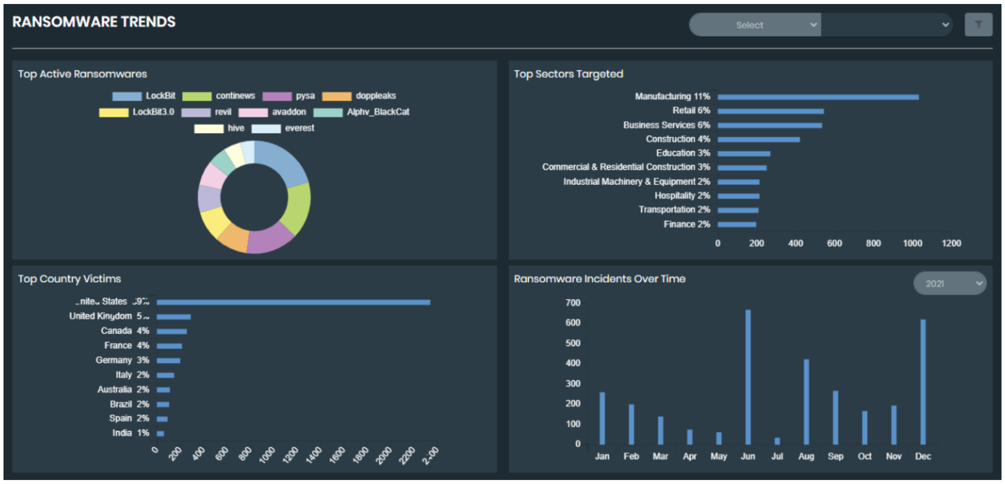
Total Ransomware Incidents 6016

Top Active Ransomware LockBit

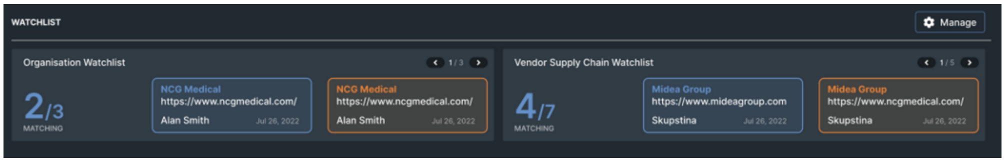
Top Sector Targeted 11 % Manufacturing

Top Country Victims 39 % United States

- *Ransomware Trends*: Graphical representations of ransomware trends, including top targeted sectors and victimized countries. The trends will adjust to reflect a particular trend if a card is selected in the *Summary*.



- *Watchlist*: A list of monitored organization and vendors. If an asset matches a monitor, an alert will be triggered. Add or edit your watchlist by selecting *Manage*.



NCG Medical
https://www.ncgmedical.com/
Alan Smith Jul 26, 2022

NCG Medical
https://www.ncgmedical.com/
Alan Smith Jul 26, 2022

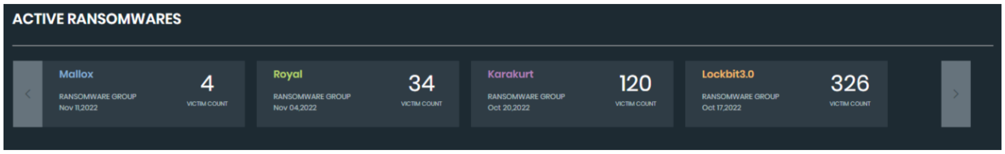
Midea Group
https://www.mideagroup.com
Skupstina Jul 26, 2022

Midea Group
https://www.ncgmedical.com/
Skupstina Jul 26, 2022

The color of the watchlist match depicts the following:

- *Blue*: The name of this entity has been identified as a target on ransomware blogs/sites.
- *Orange*: This entity has been targeted by a threat actor operating in the darknet, and there is a possibility that their network/system access is being offered for sale. Therefore, this entity is a potential candidate for a ransomware attack. You can find the associated report about this entity in the *ACI > Reports* section.

- *Active Ransomware*: A list of known, active ransomware and the current victim count for each.



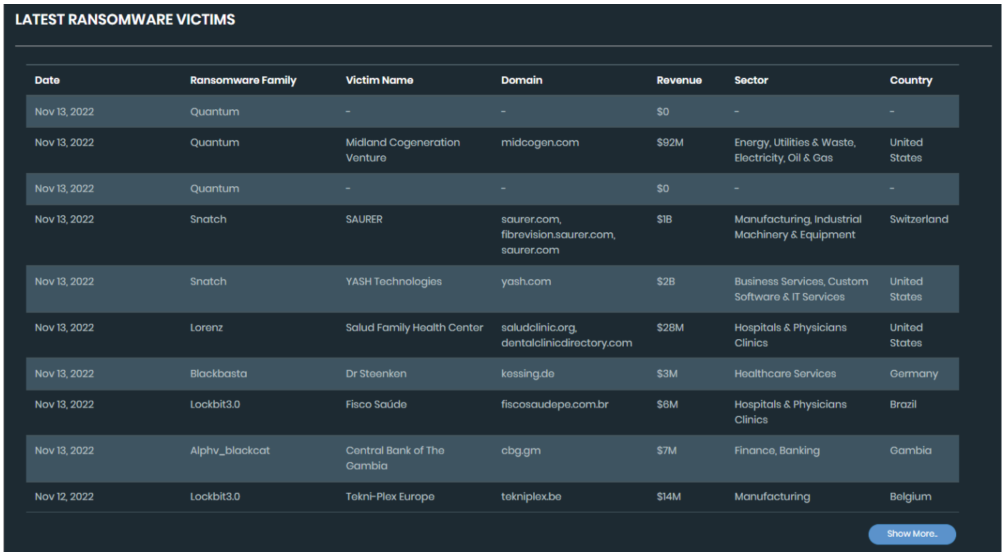
Mallox
RANSOMWARE GROUP
Nov 11,2022
4
VICTIM COUNT

Royal
RANSOMWARE GROUP
Nov 04,2022
34
VICTIM COUNT

Karakurt
RANSOMWARE GROUP
Oct 20,2022
120
VICTIM COUNT

Lockbit3.0
RANSOMWARE GROUP
Oct 17,2022
326
VICTIM COUNT

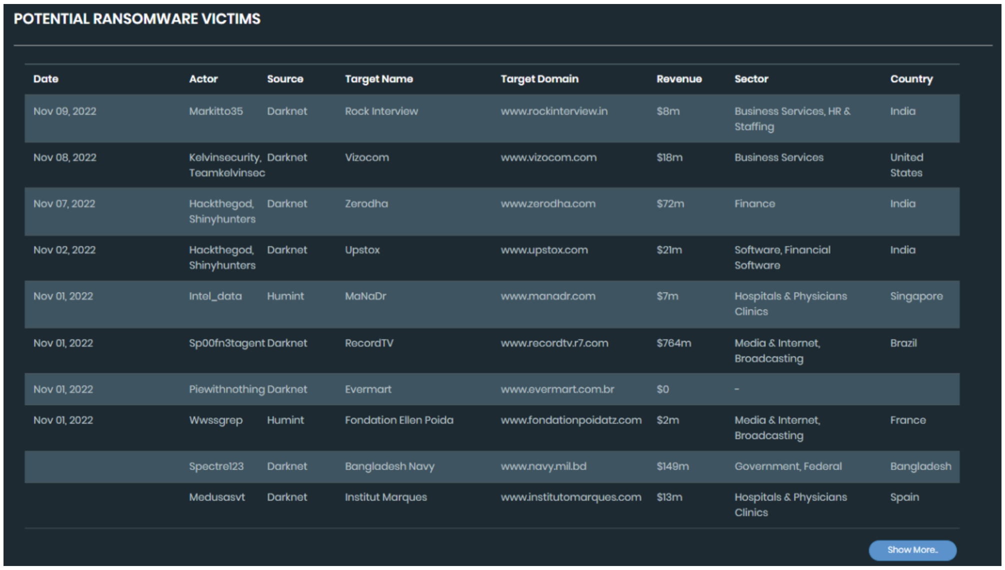
- *Latest Ransomware Victims*: A list of the most recent victims of ransomware victims, including information on the victim revenue, sector, and country. Select an entry for more information on a specific victim. Click *Show More* to view more victims.



LATEST RANSOMWARE VICTIMS

Date	Ransomware Family	Victim Name	Domain	Revenue	Sector	Country
Nov 13, 2022	Quantum	-	-	$0	-	-
Nov 13, 2022	Quantum	Midland Cogeneration Venture	midcogen.com	$92M	Energy, Utilities & Waste, Electricity, Oil & Gas	United States
Nov 13, 2022	Quantum	-	-	$0	-	-
Nov 13, 2022	Snatch	SAURER	saurer.com, fibrevision.saurer.com, saurer.com	$1B	Manufacturing, Industrial Machinery & Equipment	Switzerland
Nov 13, 2022	Snatch	YASH Technologies	yash.com	$2B	Business Services, Custom Software & IT Services	United States
Nov 13, 2022	Lorenz	Salud Family Health Center	saludclinic.org, dentalclinicdirectory.com	$28M	Hospitals & Physicians Clinics	United States
Nov 13, 2022	Blackbasta	Dr Steenken	kessing.de	$3M	Healthcare Services	Germany
Nov 13, 2022	Lockbit3.0	Fisco Saúde	fiscosaudepe.com.br	$6M	Hospitals & Physicians Clinics	Brazil
Nov 13, 2022	Alphv_blackcat	Central Bank of The Gambia	cbg.gm	$7M	Finance, Banking	Gambia
Nov 12, 2022	Lockbit3.0	Tekni-Plex Europe	tekniplex.be	$14M	Manufacturing	Belgium

- *Potential Ransomware Victims*: A list of targets identified as potential victims of ransomware, including information on revenue, sector, and country. Select an entry for more information on a specific target. Click *Show More* to view more potential targets.



POTENTIAL RANSOMWARE VICTIMS

Date	Actor	Source	Target Name	Target Domain	Revenue	Sector	Country
Nov 09, 2022	Markitto35	Darknet	Rock Interview	www.rockinterview.in	$8m	Business Services, HR & Staffing	India
Nov 08, 2022	Kelvinsecurity, Teamkelvinsec	Darknet	Vizocom	www.vizocom.com	$18m	Business Services	United States
Nov 07, 2022	Hackthegod, Shinyhunters	Darknet	Zerodha	www.zerodha.com	$72m	Finance	India
Nov 02, 2022	Hackthegod, Shinyhunters	Darknet	Upstox	www.upstox.com	$21m	Software, Financial Software	India
Nov 01, 2022	Intel_data	Humint	MaNaDr	www.manadr.com	$7m	Hospitals & Physicians Clinics	Singapore
Nov 01, 2022	Sp00fn3tagent	Darknet	RecordTV	www.recordtv.r7.com	$764m	Media & Internet, Broadcasting	Brazil
Nov 01, 2022	Piewithnothing	Darknet	Evermart	www.evermart.com.br	$0	-	
Nov 01, 2022	Wwssgrep	Humint	Fondation Ellen Poida	www.fondationpoidatz.com	$2m	Media & Internet, Broadcasting	France
	Spectre123	Darknet	Bangladesh Navy	www.navy.mil.bd	$149m	Government, Federal	Bangladesh
	Medusasvt	Darknet	Institut Marques	www.institutomarques.com	$13m	Hospitals & Physicians Clinics	Spain

Filtering ransomware intelligence

You can filter the information displayed on the *Ransomware Intelligence*, *Ransomware Intelligence* > *Latest Ransomware Victims*, *Ransomware Intelligence* > *Potential Ransomware Victims*, and *My Watchlist* pages.

To filter the high level ransomware information:

1. Go to *Adversary Centric Intelligence* > *Ransomware Intelligence*.
2. Specify your filters:

- Select a card from the *Summary* section.
- Select the filter icon and select the filter fields you want to include.

The *Ransomware Trends* section will update.

To filter information on the latest ransomware victims:

1. Go to *Adversary Centric Intelligence* > *Ransomware Intelligence*.
2. In the *Latest Ransomware Victims* section, click *Show More*. The *Latest Ransomware Victims* page is displayed.
3. Specify your filters:
   - Enter a keyword in the *Search* field.
   - Select a start and end range from the *Date Range* field.
   - Select specific filters from the list of categories.
4. Click *Search*. The list of victims that match your filters are displayed.

To filter information on potential ransomware victims:

1. Go to *Adversary Centric Intelligence* > *Ransomware Intelligence*.
2. In the *Potential Ransomware Victims* section, click *Show More*. The *Potential Ransomware Victims* page is displayed.
3. Specify your filters:
   - Enter a keyword in the *Search* field.
   - Select a start and end range from the *Date Range* field.
   - Select specific filters from the list of categories.
4. Click *Search*. The list of victims that match your filters are displayed.

To filter your watchlist:

1. Go to *Adversary Centric Intelligence* > *Ransomware Intelligence*.
2. In the *Watchlist* section, click *Manage*. The *My Watchlist* page is displayed.
3. Select a watchlist to filter:
   - *Organization Watchlist*
   - *Vendor Watchlist*
4. In *Organization Watchlist* tab, click the desired radio button to filter the results:
   - *All*: Show all the assets.
   - *EASM*: Show only assets that were automatically added to the watchlist by EASM.
   - *Manual*: Show only assets that were manually added to the watchlist.

   The watchlist will display any assets that match the set filters.

Exporting ransomware information

You can export a list of recent ransomware victims into an Excel file. The spreadsheet will include information on:

- Victim Name
- Affected Domains
- Revenue

- Sector
- Country
- Date
- Description

To export all of the ransomware victims:

1. Go to *Adversary Centric Intelligence* > *Ransomware Intelligence*.
2. Scroll to the victim list you want to export:
   - *Latest Ransomware Victims*
   - *Potential Ransomware Victims*
3. Click *Show More*. The list of victims is displayed.
4. Click the *Export List* icon. The file is downloaded to your computer.

To export specific ransomware victims:

1. Go to *Adversary Centric Intelligence* > *Ransomware Intelligence*.
2. Scroll to the victim list you want to export:
   - *Latest Ransomware Victims*
   - *Potential Ransomware Victims*
3. Click *Show More*. The list of victims is displayed.
4. Specify your filters. See Filtering ransomware intelligence on page 116.
5. Click the *Export List* icon. The file is downloaded to your computer.

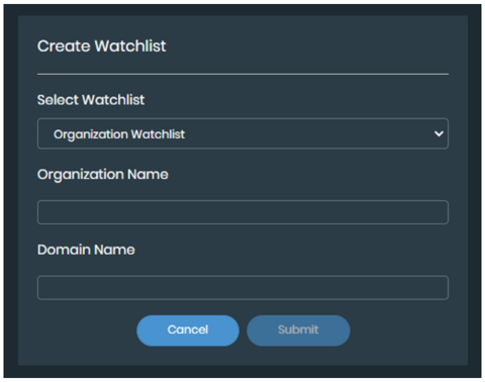
Managing My Watchlist

Users can monitor certain vendor and organization names in the *My Watchlist* page in the *Vendor Watchlist* and *Organization Watchlist*, respectively. If a match for a monitored asset appears, it triggers an alert. Vendors and organizations can be added to the watchlist manually by users or automatically by EASM.

To filter the monitored assets, see Filtering ransomware intelligence on page 116.

To create a new asset to manage:

1. Go to *Adversary Centric Intelligence* > *Ransomware Intelligence*.
2. In the *Watchlist* section, click *Manage*. The *My Watchlist* page is displayed.
3. Click + icon. The *Create Watchlist* dialog is displayed.



Create Watchlist

Select Watchlist: Organization Watchlist

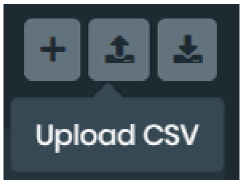
Organization Name

Domain Name

4. Select the watchlist to add to from the *Select Watchlist* dropdown.
5. Enter a name for the monitored asset.
6. Enter the domain name of the monitored asset.
7. Click *Submit*. The asset is displayed on the assigned watchlist.

To add vendors in bulk:

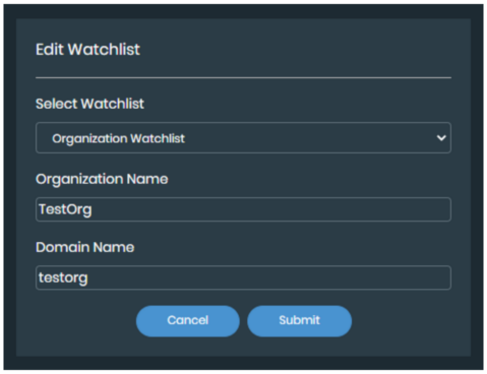
1. Go to *Adversary Centric Intelligence* > *Ransomware Intelligence*.
2. In the *Watchlist* section, click *Manage*. The *My Watchlist* page is displayed.
3. Click *Upload CSV* icon to upload the .csv files containing the vendors list. Browse and select the file. Click **Open**.



Note: Ensure that the format in which the vendors data is stored matches with the required format. To view the required format click *Download Sample CSV* icon, select the watchlist type from the drop down and click *Download*.

To edit a monitored asset:

1. Go to *Adversary Centric Intelligence* > *Ransomware Intelligence*.
2. In the *Watchlist* section, click *Manage*. The *My Watchlist* page is displayed.
3. Find the asset you want to edit and click *Edit icon*. The Edit Watchlist dialog is displayed.



Edit Watchlist

Select Watchlist: Organization Watchlist

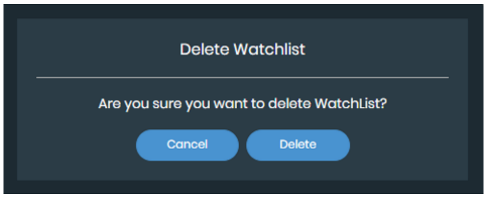
Organization Name: TestOrg

Domain Name: testorg

4. Edit the asset details and click *Submit*.

To delete a monitored asset:

1. Go to *Adversary Centric Intelligence* > *Ransomware Intelligence*.
2. In the *Watchlist* section, click *Manage*. The *My Watchlist* page is displayed.
3. Click *Delete icon*. A confirmation dialog is displayed.



Delete Watchlist

Are you sure you want to delete WatchList?

4. Select *Delete*.

Vendor Risk Assessment

The *Adversary Centric Intelligence* > *Vendor Risk Assessment* page is designed to create a watchlist of vendors that allows you to assess the security hygiene level of each vendor. From the *Vendor Risk Assessment* page, you can:

- Add new vendors to the watchlist. See Adding a new vendor to the watchlist on page 120.
- View the security hygiene assessment of a vendor. See Viewing the vendor risk assessment on page 121.

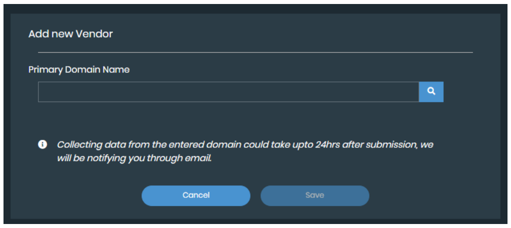
Adding a new vendor to the watchlist

You can add new vendors to the watchlist to generate a risk assessment report and identify the overall estimate risk exposure rating. Vendors can be added to the watchlist using the primary domain. Once the domain name has been submitted, collecting data and generating the risk assessment can take up to 24 hours.

If the overall estimated risk exposure rating of a vendor changes to *High*, an alert notification will be sent.

To add a new vendor to the watchlist:

1. Go to *Adversary Centric Intelligence* > *Vendor Risk Assessment*.
2. Click *Add Vendor*. The *Add new Vendor* dialog is displayed.



Add new Vendor

Primary Domain Name

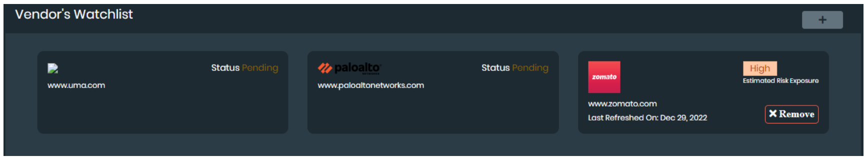
Collecting data from the entered domain could take upto 24hrs after submission, we will be notifying you through email.

3. Enter the vendor domain in the *Primary Domain Name* field.

4. Click the search icon. Vendor information will be displayed.
5. Click *Save*. The vendor risk assessment will begin to generate.

Removing a vendor from the watchlist

You can have a maximum of 25 individual vendors in the watchlist. To remove a vendor from the watchlist, click *Remove* on its watchlist card.



Vendor's Watchlist

Status Pending
www.uma.com

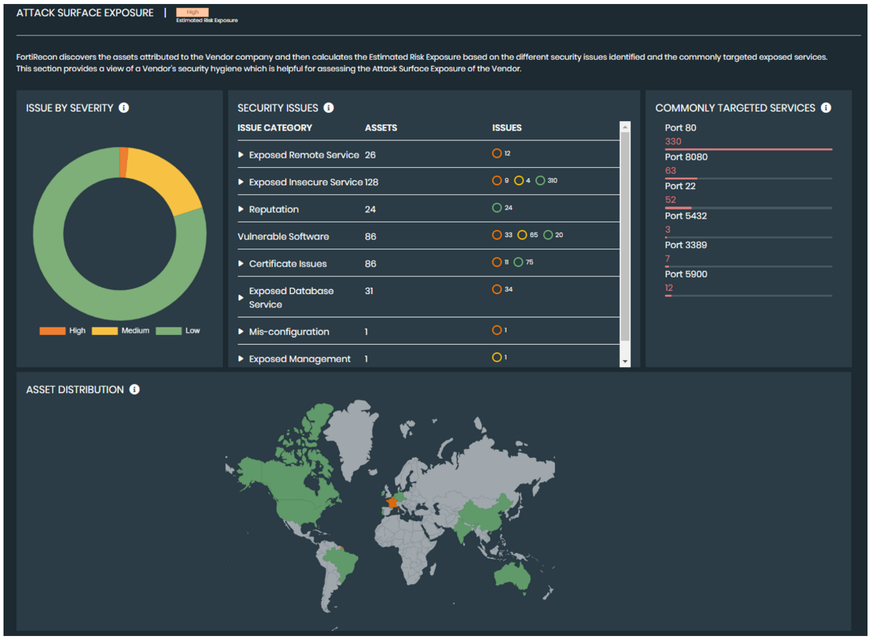
Status Pending
www.paloaltonetworks.com

High
Estimated Risk Exposure
www.zomato.com
Last Refreshed On: Dec 29, 2022

Viewing the vendor risk assessment

The vendor risk assessment organizes the generated vendors data into:

- *Attack Surface Exposure*: Provides an overview of the vendor company's assets and current security hygiene to assess the estimated risk exposure.



ATTACK SURFACE EXPOSURE | High Estimated Risk Exposure

FortiRecon discovers the assets attributed to the Vendor company and then calculates the Estimated Risk Exposure based on the different security issues identified and the commonly targeted exposed services. This section provides a view of a Vendor's security hygiene which is helpful for assessing the Attack Surface Exposure of the Vendor.

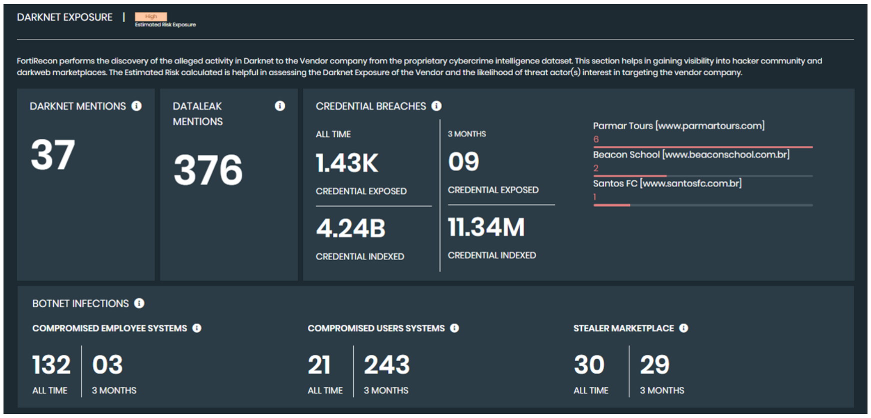
SECURITY ISSUES

ISSUE CATEGORY	ASSETS	ISSUES
▸ Exposed Remote Service	26	○ 12
▸ Exposed Insecure Service	128	○ 9 ○ 4 ○ 310
▸ Reputation	24	○ 24
Vulnerable Software	86	○ 33 ○ 65 ○ 20
▸ Certificate Issues	86	○ 11 ○ 75
▸ Exposed Database Service	31	○ 34
▸ Mis-configuration	1	○ 1
▸ Exposed Management	1	○ 1

COMMONLY TARGETED SERVICES

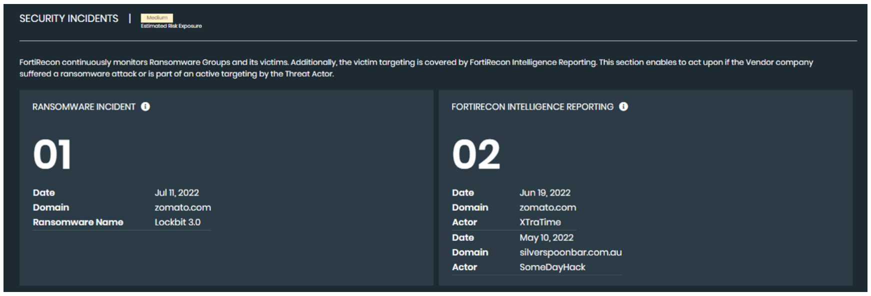
Port 80	330
Port 8080	63
Port 22	52
Port 5432	3
Port 3389	7
Port 5900	12

- *Darknet Exposure*: Provides an overview of potential activity in hacker communities and darkweb marketplaces toward the vendor company. The estimated risk can be used to assess the likelihood of threat actors' interest in targeting the vendor company.



FortiRecon performs the discovery of the alleged activity in Darknet to the Vendor company from the proprietary cybercrime intelligence dataset. This section helps in gaining visibility into hacker community and darkweb marketplaces. The Estimated Risk calculated is helpful in assessing the Darknet Exposure of the Vendor and the likelihood of threat actor(s) interest in targeting the vendor company.

- *Security Incidents*: Provides an overview of ransomware incidences and intelligence reporting so that action can be taken if the vendor company suffers a ransomware attack or is targeted by a threat actor.



FortiRecon continuously monitors Ransomware Groups and its victims. Additionally, the victim targeting is covered by FortiRecon Intelligence Reporting. This section enables to act upon if the Vendor company suffered a ransomware attack or is part of an active targeting by the Threat Actor.

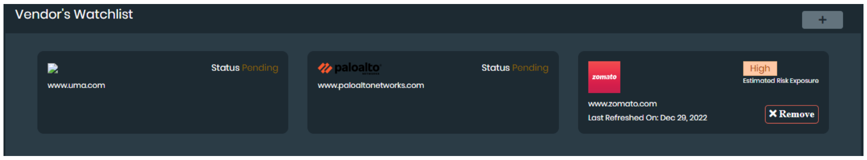
Date	Jul 11, 2022
Domain	zomato.com
Ransomware Name	Lockbit 3.0

Date	Jun 19, 2022
Domain	zomato.com
Actor	XTraTime
Date	May 10, 2022
Domain	silverspoonbar.com.au
Actor	SomeDayHack

Each of these sections is further divided into widgets that allow you to review detailed risk data in order to make informed decisions.

To view a vendor risk assessment:

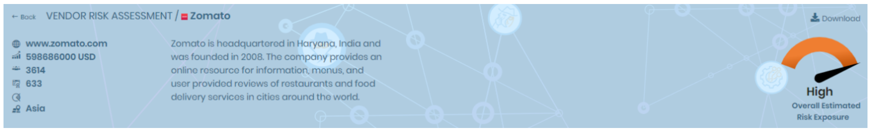
1. Go to *Adversary Centric Intelligence* > *Vendor Risk Assessment*.



2. Select the vendor that you want to review. The *Vendor Risk Assessment* opens.

You cannot review vendor information while the *Status* is *Pending*.

3. Review the banner for high-level information on the vendor and the *Overall Estimated Risk Exposure*.


← Back
VENDOR RISK ASSESSMENT / Zomato
Download
www.zomato.com
598686000 USD
3614
633
Asia
High
Overall Estimated Risk Exposure

Zomato is headquartered in Haryana, India and was founded in 2008. The company provides an online resource for information, menus, and user provided reviews of restaurants and food delivery services in cities around the world.

4. Review the *Attack Surface Exposure*:

Issue by Severity	The distribution of security issues by severity on the vendor's attack surface.
Security Issues	The type of security issues identified and the assets affected, distributed by severity. Select a dropdown arrow in the *Issue Category* for further breakdown of the assets.
Commonly Targeted Services	The services on the vendor's attack surface that are commonly targeted and the number of assets exposing the service.
Asset Distribution	A geographical distribution of the vendor's assets.

5. Review the *Darknet Exposure*:

Darknet Mentions	The number of mentions of the vendor's name or domain on platforms where threat actors perform active discussions.
Dataleak Mentions	The number of mentions of the vendors name or domain on datasets leaked by threat actors.
Credential Breaches	An overview of credentials affiliated with the vendor's domain that have been identified in third party data breaches.
Botnet Infections	An overview of botnet campaigns used to steal credentials from end users: • *Compromised Employee Systems*: The number of usernames from the shared infected system logs containing the email address domain affiliated with the vendor. • *Compromised Users Systems*: The number of credentials shared from the infected system logs containing the URL or application visited on the infected system matching the vendor's domain. These systems can be end users or employees. • *Stealer Marketplace*: The number of credentials stolen by threat actors containing the URL or application visited on the infected system matching the vendor's domain. These logs are being listed for sale on prominent stealer marketplaces.

6. Review the *Security Incidents*:

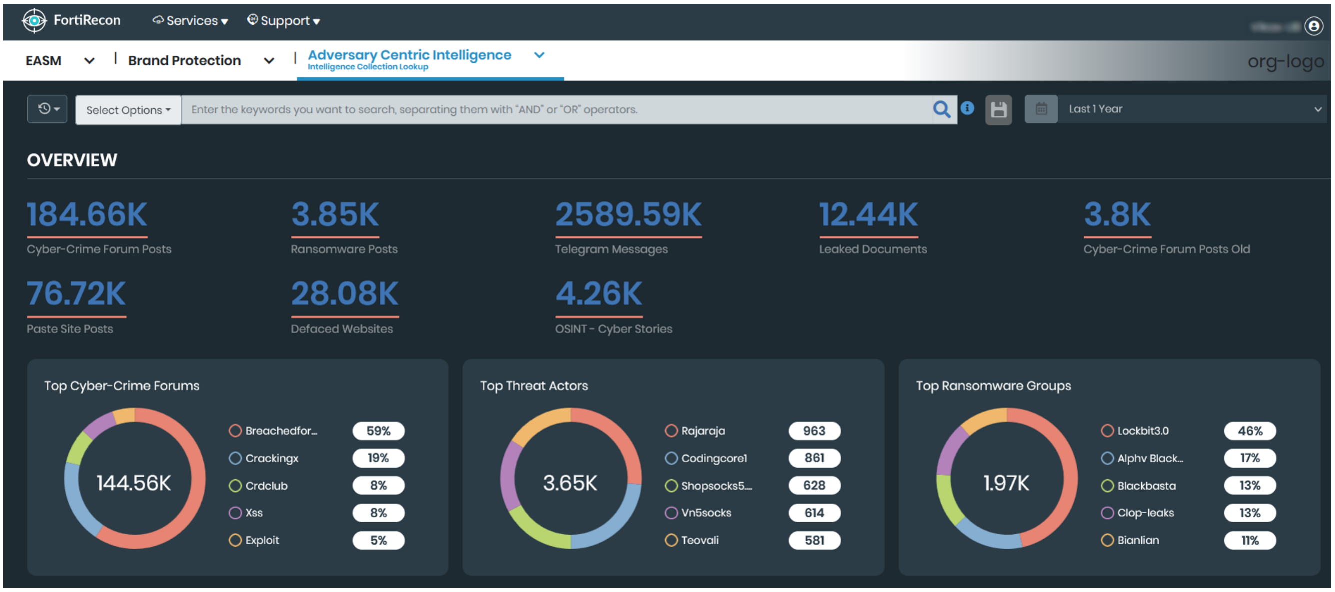
Ransomware Incident	The vendor name or domain appeared on the victim list by a ransomware group.
FortiRecon Intelligence Reporting	FortiRecon ACI reporting contains mention of the vendor's name or domain.

Intelligence Collection Lookup

The *Adversary Centric Intelligence* > *Intelligence Collection Lookup* page allows you to search the comprehensive intelligence collection, including cyber-crime forums, ransomware posts, Telegram messages, leaked documents, and more using a simple query syntax. From the *Intelligence Collection Lookup* page, you can:

Create and save search queries. See Search Query.

Review the search results. See Search Results.


FortiRecon
Services
Support
EASM
Brand Protection
Adversary Centric Intelligence
Intelligence Collection Lookup
org-logo
Select Options
Enter the keywords you want to search, separating them with "AND" or "OR" operators.
Last 1 Year

OVERVIEW

184.66K Cyber-Crime Forum Posts
3.85K Ransomware Posts
2589.59K Telegram Messages
12.44K Leaked Documents
3.8K Cyber-Crime Forum Posts Old
76.72K Paste Site Posts
28.08K Defaced Websites
4.26K OSINT - Cyber Stories

Top Cyber-Crime Forums (144.56K)

Breachedfor...	59%
Crackingx	19%
Crdclub	8%
Xss	8%
Exploit	5%

Top Threat Actors (3.65K)

Rajaraja	963
Codingcorel	861
Shopsocks5...	628
Vn5socks	614
Teovali	581

Top Ransomware Groups (1.97K)

Lockbit3.0	46%
Alphv Black...	17%
Blackbasta	13%
Clop-leaks	13%
Bianlian	11%

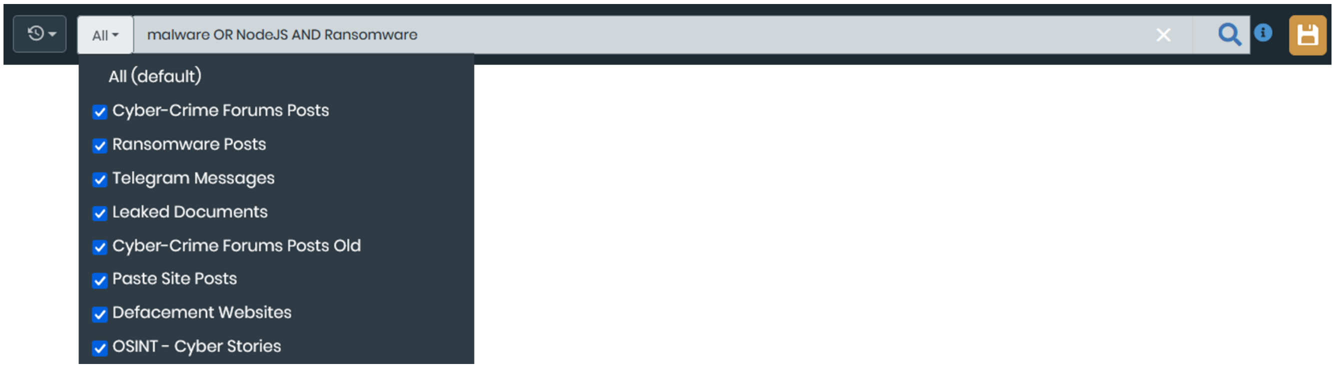
Search Query

You will able to search from the available intelligence sources using search query including keywords and operators.

Creating and running a search query

To create and run a search query:

1. Navigate to *Adversary Centric Intelligence* > *Investigation* page.
2. Enter the search query using keywords and operators you want to search in the search box. For supported query syntax, see Search Query Syntax.
3. Select the required sources, from the list. Supported sources include the following:
   - *All(default)*
   - *Cyber-Crime Forums Posts*
   - *Ransomware Posts*
   - *Telegram Messages*
   - *Leaked Documents*
   - *Cyber-Crime Forums Posts Old*
   - *Paste Site Posts*
   - *Defacement Websites*
   - *OSINT- Cyber Stores*
4. Click search icon.



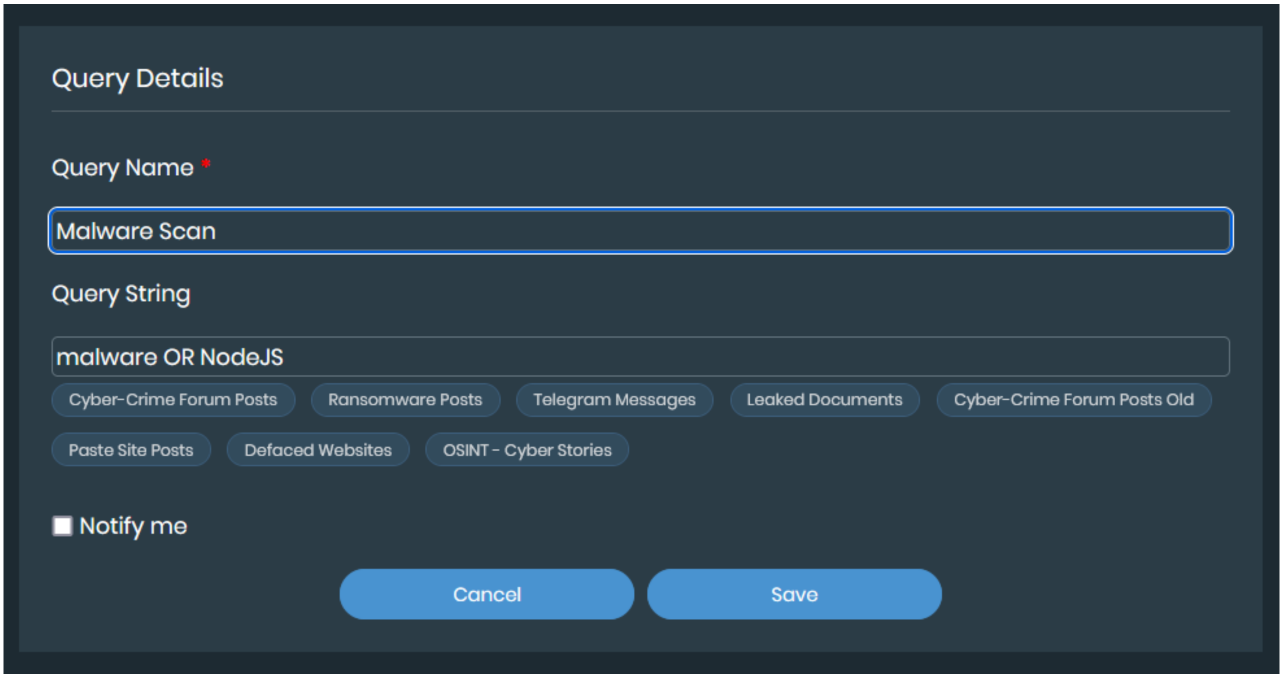
Saving a search query

You will be able to save your custom search queries for future use and to get notified. There are two types of saved queries:

- **System queries** - These queries are automatically generated for each organization based on their organization name, brand names, and primary domain. System queries cannot be edited.
- **User queries** - You can save custom search queries that are specific to your requirements.

To save a user search query:

1. Navigate to *Adversary Centric Intelligence* > *Investigation* page.
2. Enter and run the search query.
3. Click *Save* icon.
4. In the Query Details window, provide the *Query Name*.
5. Select *Notify* checkbox, if you want to enable notifications for the query.
6. Click *Save*.



Query Details

Query Name *

Malware Scan

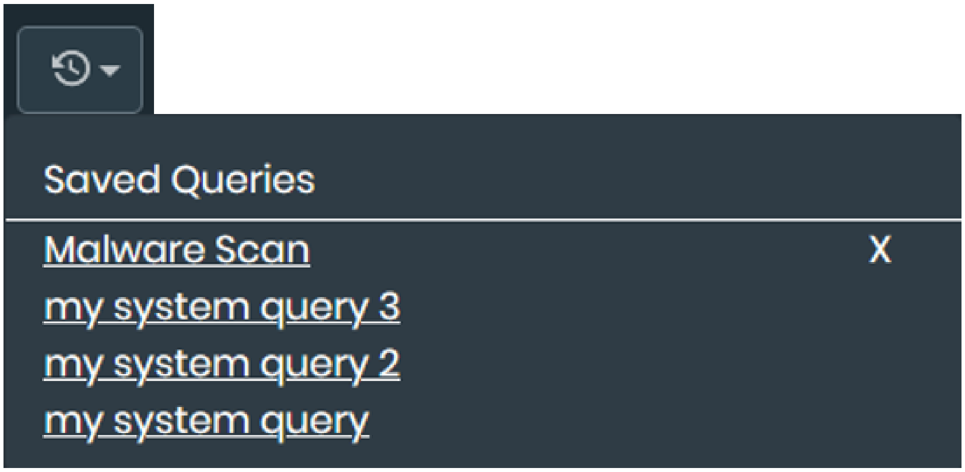
Query String

malware OR NodeJS

☐ Notify me

To run a saved search query:

1. Navigate to *Adversary Centric Intelligence* > *Investigation* page.
2. Click Saved Queries icon.
3. Select the required saved search query.



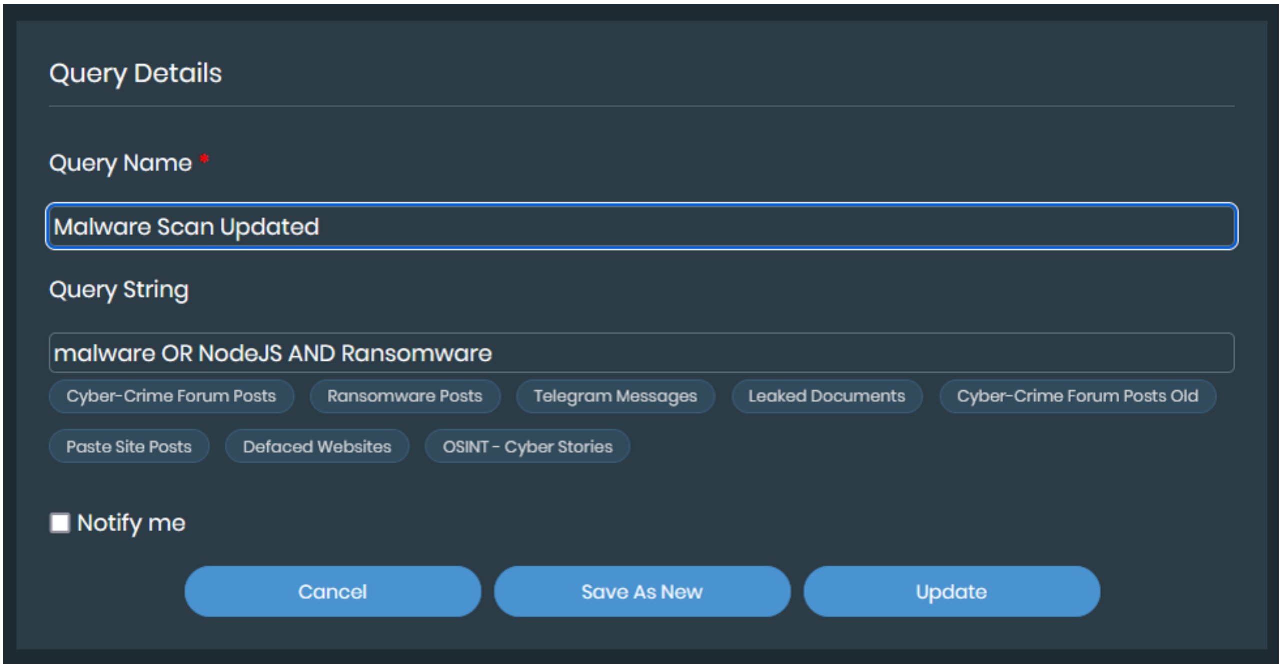
To delete a saved search query:

1. Navigate to *Adversary Centric Intelligence* > *Investigation* page.
2. Click Saved Queries icon.
3. Click *X* icon.

To update a saved search query:

1. Select the saved search query.
2. Update the search query in the search box if required.
3. Click *Save* icon.
4. Update the *Query Name* if required.

5. Click *Update* to update the existing search query or click *Save As New* to save as a new search query.



Query Details

Query Name *

Malware Scan Updated

Query String

malware OR NodeJS AND Ransomware

Search Query Syntax

Lucene query language is used to search for specific posts/messages. Following are the examples for using the query language.

Use Case	Query
To filter messages for exact domain match.	"knowbe4.com"
To filter messages for wildcard match containing the domain name.	*google.com
To filter messages for specific keyword with exact match.	"Cyber"
To filter messages for keyword with wildcard match.	*Cyber*
To find matches for multiple keywords.	("bank" OR "banco" OR "ATM malware")
To find matches for multiple keywords with AND condition	("stealer" OR "worm" OR "malware") AND ("bank")
To find matches for multiple keywords while excluding some keywords.	(healthcare OR medical*) NOT ("healthy" OR "Medical Cannabis")

Following operators and modifiers are supported.

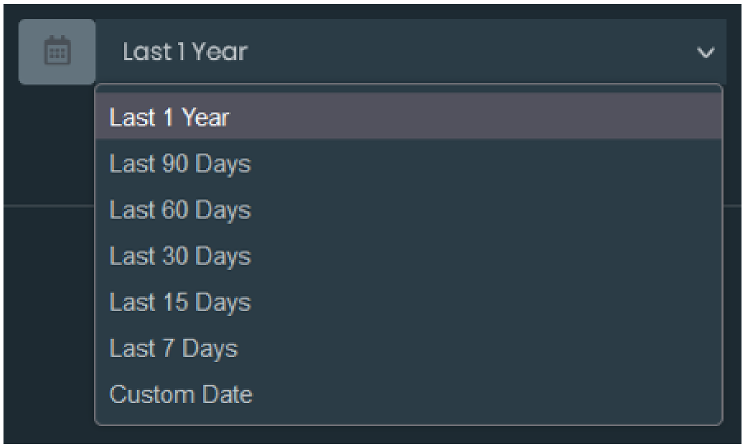
Operators and Modifier	Description
AND	Use this option to find both terms that exist in the text.
OR	Use this option to find at least one term that exists in the text.
NOT	Use this option to exclude that exists in the text.
*	Use this option to perform wildcard search.

Search Results

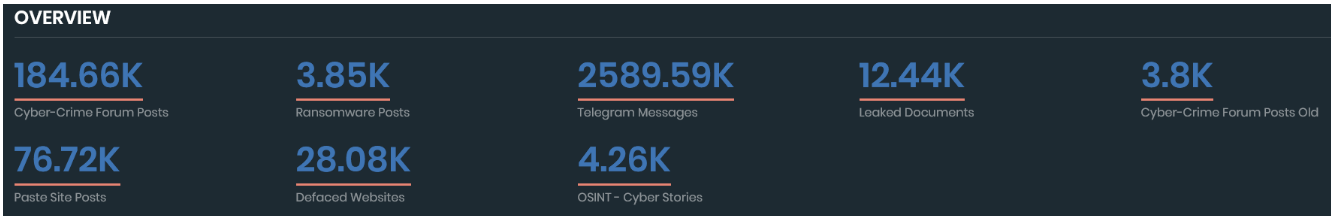
Once you run either a system or a custom search query, the filtered results are displayed. The default display period for the results is *1 year*. There are two sections available for viewing search results.

- Overview
- Detailed Results

To modify the result period, click date drop-down menu and choose the desired time period.



Overview


OVERVIEW

184.66K Cyber-Crime Forum Posts

3.85K Ransomware Posts

2589.59K Telegram Messages

12.44K Leaked Documents

3.8K Cyber-Crime Forum Posts Old

76.72K Paste Site Posts

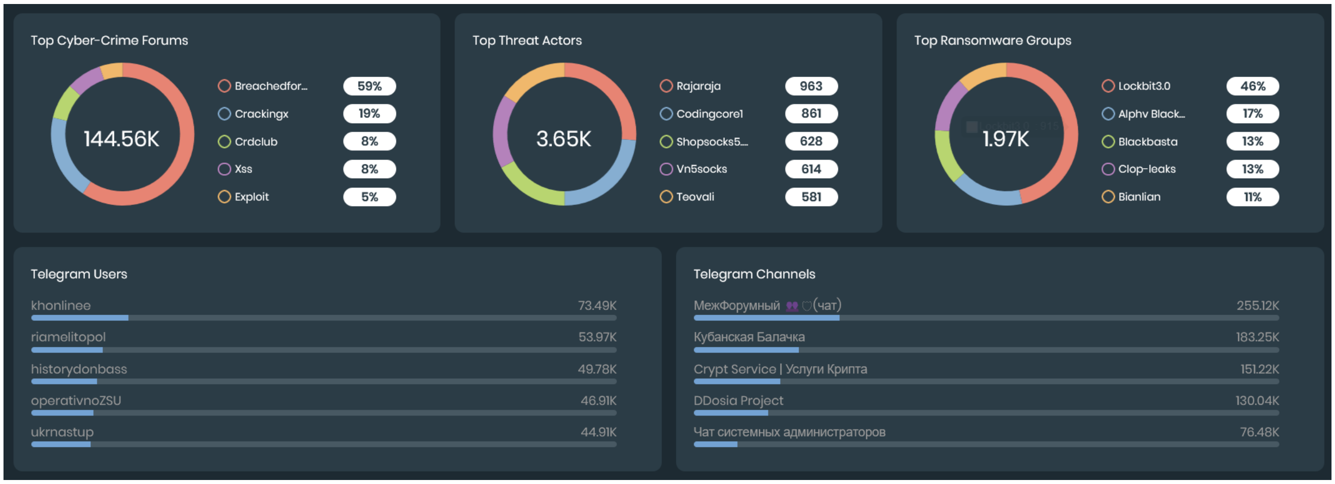
28.08K Defaced Websites

4.26K OSINT - Cyber Stories

The overview section provides the cumulative count of the following fields discovered in the search.

- *Cyber-Crime Forums Posts*
- *Ransomware Posts*

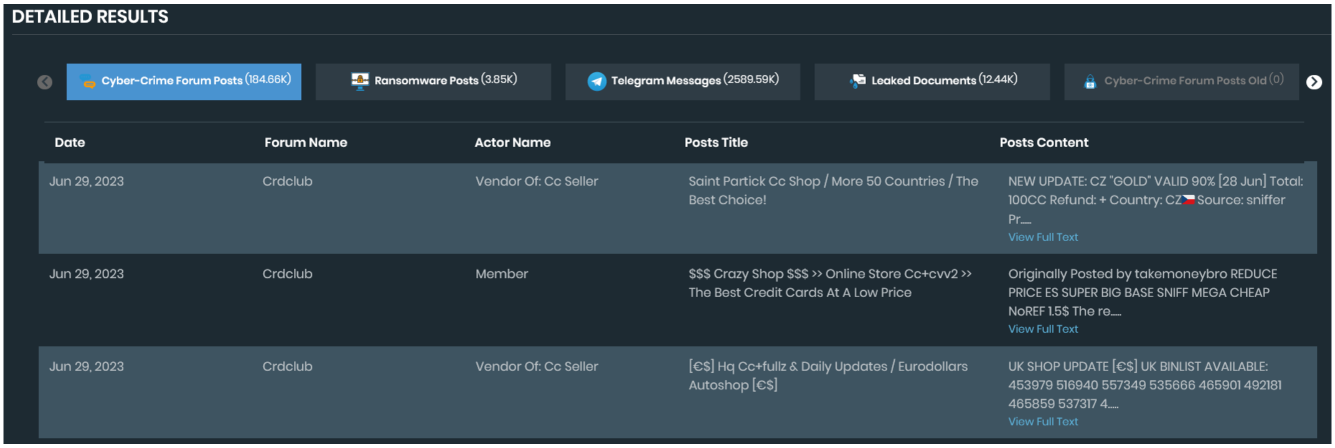
- *Telegram Messages*
- *Leaked Documents*
- *Cyber-Crime Forums Posts Old*
- *Paste Site Posts*
- *Defacement Websites*
- *OSINT- Cyber Stores*



The overview section also includes the following chart widgets:

- *Top Cyber-Crime Forums*: Displays the top 5 forums from Darknet posts.
- *Top Threat Actors*: Displays the top 5 threat actors contributing to Darknet posts.
- *Top Ransomware Groups*: Displays the top 5 groups from Ransomware posts.
- *Telegram Users*: Displays the top 10 users with Telegram posts.
- *Telegram Channels*: Displays the top 10 channels with Telegram posts.

Detailed Results


DETAILED RESULTS
Cyber-Crime Forum Posts (184.66K)
Ransomware Posts (3.85K)
Telegram Messages (2589.59K)
Leaked Documents (12.44K)
Cyber-Crime Forum Posts Old (0)

Date	Forum Name	Actor Name	Posts Title	Posts Content
Jun 29, 2023	Crdclub	Vendor Of: Cc Seller	Saint Partick Cc Shop / More 50 Countries / The Best Choice!	NEW UPDATE: CZ "GOLD" VALID 90% [28 Jun] Total: 100CC Refund: + Country: CZ 🇨🇿 Source: sniffer Pr.... View Full Text
Jun 29, 2023	Crdclub	Member	$$$ Crazy Shop $$$ >> Online Store Cc+cvv2 >> The Best Credit Cards At A Low Price	Originally Posted by takemoneybro REDUCE PRICE ES SUPER BIG BASE SNIFF MEGA CHEAP NoREF 1.5$ The re.... View Full Text
Jun 29, 2023	Crdclub	Vendor Of: Cc Seller	[€$] Hq Cc+fullz & Daily Updates / Eurodollars Autoshop [€$]	UK SHOP UPDATE [€$] UK BINLIST AVAILABLE: 453979 516940 557349 535666 465901 492181 465859 537317 4.... View Full Text

The detailed results section displays the detailed information of the discovered search results. The following data is displayed for each source.

Intelligence Source	Fields Displayed
Cyber-Crime Forum Posts	• Date • Forum • Name • Actor Name • Posts Title • Posts Content Click *View Full Text* to view the full content.
Ransomware Posts	• Date • Ransomware • Name • Title • Victim Company • Victim Country • Victim Sector • Posts Content Click *View Full Text* to view the full content.
Telegram Messages	• Date • Username • Channel • Message
Leaked Documents	• Date • Leak Name • File Name • File Data Click *View Full Text* to view the full content.
Cyber-Crime Forum Posts Old	• Date • Forum • Name • Actor Name • Posts Title • Posts Content Click *View Full Text* to view the full content.
Paste Site Posts	• Date • Author Name • Title • Content Click link icon to view the site posts in detail.
Defaced Websites	• Date

Intelligence Source	Fields Displayed
	• Source • Notifier • Domain Click link icon to view the website.
OSINT - Cyber Stories	• Date • Title • Content Click link icon to read the full article.

Investigation

The *Adversary Centric Intelligence* > *Investigation* page displays information about investigations into security events. From the *Investigation* page, you can:

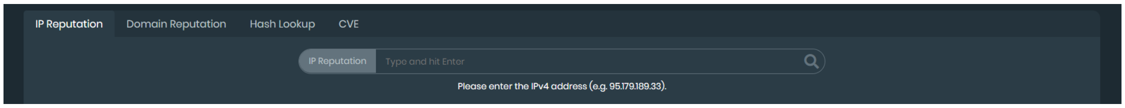
- Review the reputation of IPv4 addresses. See Reviewing IP address reputation on page 131.
- Review the reputation of a domain. See Reviewing domain reputation on page 131.
- Review a file hash. See Reviewing a file hash on page 132.
- Review a CVE. See Reviewing a CVE on page 132.

Reviewing IP address reputation

You can use the *IP Reputation* search bar to search for IPv4 addresses.

To review IP address reputation:

1. Go to *Adversary Centric Intelligence* > *Investigation* > *IP Reputation*. The *IP Reputation* tab is displayed.



Please enter the IPv4 address (e.g. 95.179.189.33).

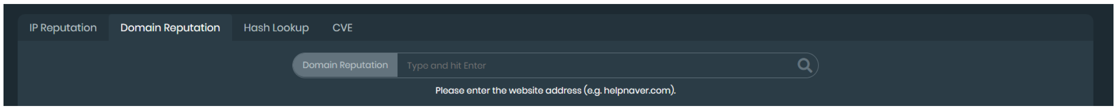
2. Type the IPv4 address, and press *Enter*.

Reviewing domain reputation

You can use the *Domain Reputation* search bar to search for domains.

To review domain reputation:

1. Go to *Adversary Centric Intelligence* > *Investigation* > *Domain Reputation*. The *Domain Reputation* tab is displayed.



Please enter the website address (e.g. helpnaver.com).

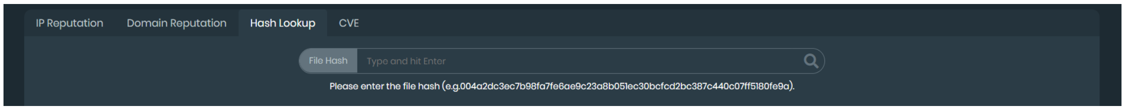
2. Type the domain name, and press *Enter*.

Reviewing a file hash

You can use the *File Hash* search bar to search for a file hash.

To review a file hash:

1. Go to *Adversary Centric Intelligence* > *Investigation* > *Hash Lookup*. The *Hash Lookup* tab is displayed.



Please enter the file hash (e.g.004a2dc3ec7b98fa7fe6ae9c23a8b051ec30bcfcd2bc387c440c07ff5180fe9a).

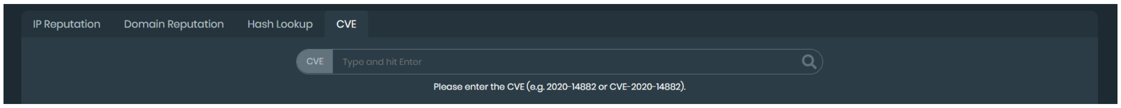
2. Type the file hash, and press *Enter*. The results are displayed.

Reviewing a CVE

You can use the *CVE* search bar to search for a CVE.

To review a CVE:

1. Go to *Adversary Centric Intelligence* > *Investigation* > *CVE*. The *CVE* tab is displayed.



Please enter the CVE (e.g. 2020-14882 or CVE-2020-14882).

2. Type the CVE, and press *Enter*. Information about the CVE is displayed.

Profile settings

The *Profile Settings* page allows you to personalize your FortiRecon account and provide information on your organization.

You can access *Profile Settings* from the menu in the top-right corner of FortiRecon. See Accessing profile settings on page 133. The menu appears as three vertical dots:

From the menu, you can also change the color theme of the FortiRecon pages. See Changing the GUI theme.

The *Profile Settings* module contains the following pages:

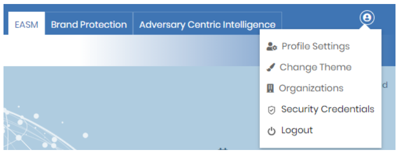
Profile	Displays information about your personal FortiRecon account. You can edit details of your account, configure daily digest reports, and enable custom email alerts. See Profile on page 134.
Users	Displays account information for members of your organization. Administrators can add, edit, and delete user accounts. See Users on page 138
Access Templates	Allows the creation and editing of access templates. Access templates control the modules and sub modules available to users on FortiRecon. See Access templates on page 140.
Audit Logs	Displays logs of all user actions performed within FortiRecon. See Audit Logs.
Downloads	Displays a list of all the files downloaded from FortiRecon in that last 30 days. You can download the files to your computer or delete unnecessary files. See Downloads on page 145.
Integrations	Displays the webhook integrations with Microsoft Teams and Slack. You can create, edit, disable, and delete integrations. See Integrations on page 146.
Seeds	Displays the domains, card BINs, and mobile applications of your organization that are being monitored by FortiRecon. See Seeds on page 149.

Accessing profile settings

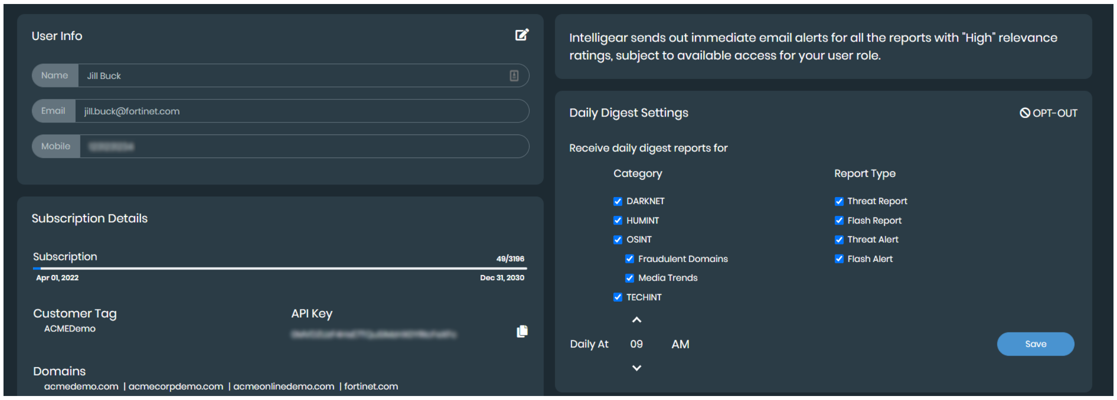
You can access the *Profile Settings* from any page by selecting the menu in the top-right corner.

To access profile settings:

1. Hover over the profile menu in the top-right corner, and select *Profile Settings*.



The *Profile* page is displayed.



User Info

Name: Jill Buck

Email: jill.buck@fortinet.com

Mobile: [redacted]

Intelligear sends out immediate email alerts for all the reports with "High" relevance ratings, subject to available access for your user role.

Daily Digest Settings

Receive daily digest reports for

Category	Report Type
☑ DARKNET	☑ Threat Report
☑ HUMINT	☑ Flash Report
☑ OSINT	☑ Threat Alert
☑ Fraudulent Domains	☑ Flash Alert
☑ Media Trends	
☑ TECHINT	

Daily At 09 AM

Subscription Details

Subscription 49/3196

Apr 01, 2022 Dec 31, 2030

Customer Tag: ACMEDemo

API Key: [redacted]

Domains: acmedemo.com | acmecorpdemo.com | acmeonlinedemo.com | fortinet.com

Profile

The *Profile* page provides information on your personal account information and allows you to customize settings. From the *Profile Settings* > *Profile* tab, you can:

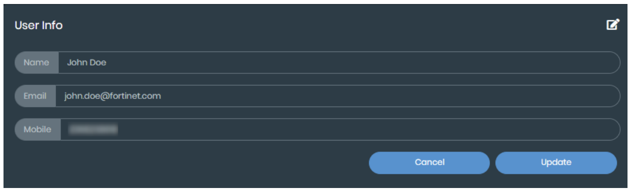
- Edit personal account information. See Editing user information on page 134.
- Configure daily reports on recent FortiRecon activity. See Opting in to daily digest reports on page 135.
- Opt-out of daily reports on recent FortiRecon activity. See Opting out of daily digest reports on page 135.
- View information about your subscription, such as registered domains, target industries and geography, keywords, and your API key. See Subscription Details on page 135.
- Copy your API key for sharing. See Sharing the API key on page 137.
- Configure personalized email notifications when specific keywords occur in FortiRecon reports. See Receiving custom email alerts on page 137.

Editing user information

You can edit your personal user information on the *Profile* page. To edit other FortiRecon account users, see Editing users on page 139.

To edit personal user information:

1. Go to *Profile Settings* > *Profile*.
2. Click the edit icon in *User Info*. The *Cancel* and *Update* buttons display.



User Info

Name: John Doe

Email: john.doe@fortinet.com

Mobile: [redacted]

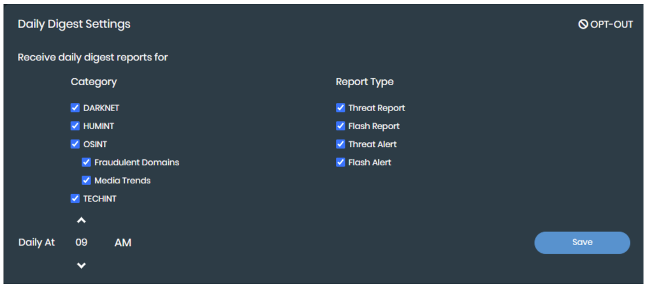
3. Enter new information into *Name*, *Email*, and *Mobile* as needed.
4. Click *Update*. Your personal user information is updated.

Opting in to daily digest reports

You can receive emailed daily digest reports that include important information and highlights on reports and alerts that occurred in the past 24 hours.

To opt-in to daily digest reports:

1. Go to *Profile Settings* > *Profile*.
2. Click *Opt-in* in *Daily Digest Settings*. The *Category* and *Report Type* fields become active.



Daily Digest Settings

Receive daily digest reports for

Category	Report Type
☑ DARKNET	☑ Threat Report
☑ HUMINT	☑ Flash Report
☑ OSINT	☑ Threat Alert
☑ Fraudulent Domains	☑ Flash Alert
☑ Media Trends	
☑ TECHINT	

Daily At 09 AM

3. Select the options to include, and clear the options to exclude from the daily digest report.
4. Use the up and down *Daily At* arrows, or manually enter the hour you want to receive the daily digest report.
5. Toggle *AM* and *PM* to decide the hour in the 12-hour time convention.
6. Click *Save*. The daily digest report is sent to your email each day at the time specified.

The *Daily At* feature uses the 12-hour time convention by default. If you enter a time in 24-hour format, the time is automatically adjusted to the 12-hour format. For example, if you enter 15 AM, the time is adjusted to 3 PM.

Opting out of daily digest reports

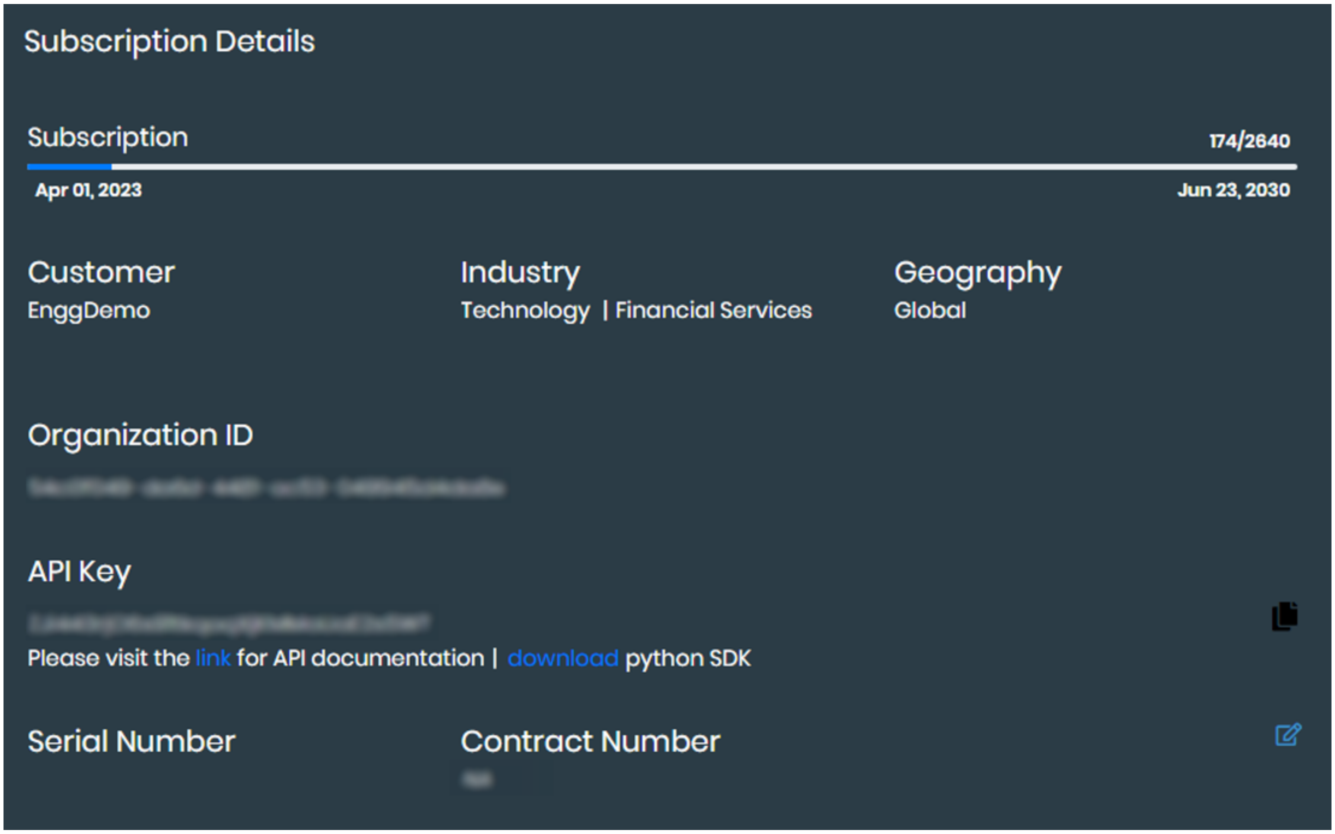
Daily digest reports are enabled by default, but you can stop the emails by opting-out in the *Profile* page.

To opt-out of daily digest reports:

1. Go to *Profile Settings* > *Profile*.
2. Click *Opt-out* in *Daily Digest Settings*. You will no longer receive daily digest reports.

Subscription Details

Subscription Details provides information on your subscription, including organization ID, license serial number, contract information, and your API key.



Subscription Details

Subscription 174/2640

Apr 01, 2023 Jun 23, 2030

Customer: EnggDemo

Industry: Technology | Financial Services

Geography: Global

Organization ID: [redacted]

API Key: [redacted]

Please visit the link for API documentation | download python SDK

Serial Number

Contract Number: [redacted]

To view subscription details:

1. Go to *Profile Settings* > *Profile*.
2. Scroll to *Subscription Details* to view information on your:
   - Subscription
   - Customer
   - Industry
   - Geography
   - Organization ID
   - API Key

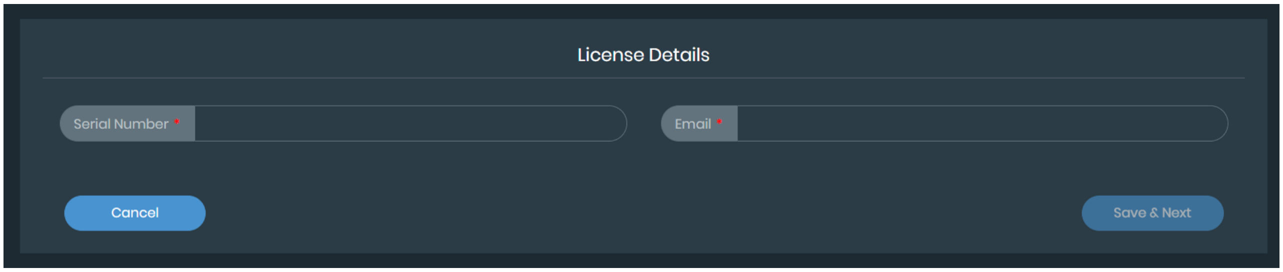
     > To access the API documentation or download the Python SDK package, click on the links below the API key.

   - Serial Number
   - Contract Number

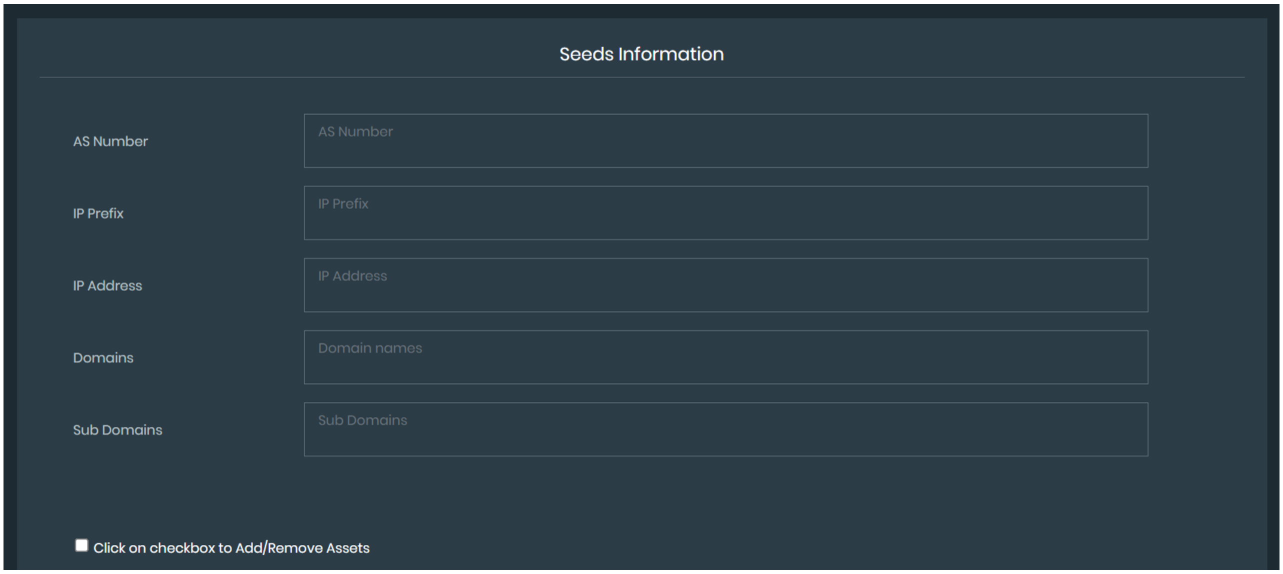
To add a new license:

1. Go to *Profile Settings* > *Profile*.
2. Scroll to *Subscription Details*

3. Click edit icon next to *Contract Number*.
4. Enter license serial number and email address used to purchase the license.



5. Click *Save & Next*.
6. Enter seed information. Based on the license purchased you will be able to add an additional domain or modify existing domain details. Select the *Add/Remove Assets* checkbox to add or remove assets.



Sharing the API key

You can copy your API key to your clipboard to share with others or use in other software.

To copy your API key:

1. Go to *Profile Settings* > *Profile*.
2. Click *Copy* in *Subscription Details*. The API key is copied to your clipboard.

Receiving custom email alerts

You can configure custom email alerts so that you receive email notifications whenever there is a report that relates to the categories you set.

To configure custom email alerts:

1. Go to *Profile Settings* > *Profile*.
2. In *Custom Email Alerts*, select alert inputs by clicking and choosing from:
   - *Target Industry*
   - *Motivation & Tags*
   - *Actors*
   - *Target Geography*
3. Click *Save*. Email alerts are configured and are sent when a set input occurs in a report.

Users

Multiple FortiRecon accounts can be created for an organization in the *Users* pages. The following roles are available for FortiRecon accounts:

- User: Has access limited to what is included in the assigned access template.
- Admin: Has administrative access over other accounts.

Only administrators can add and make changes to other accounts.

From the *Profile Settings* > *Users* page, you can:

- View all user accounts for your organization. See Viewing user accounts on page 138.
- Add new users. See Adding users on page 139.
- Edit existing users. See Editing users on page 139.
- Delete users. See Deleting users on page 140.

Viewing user accounts

You can view all of the current users for your organization on the *Users* page. User information listed for all users includes:

- Name
- Role
- Email
- Phone Number

To view user accounts:

1. Go to *Profile Settings* > *Users*.
2. Search for keywords:
   a. In the *Type and hit Enter to Search* box, type a name or email, and press *Enter*.

The user accounts are filtered to display only accounts with the keyword.

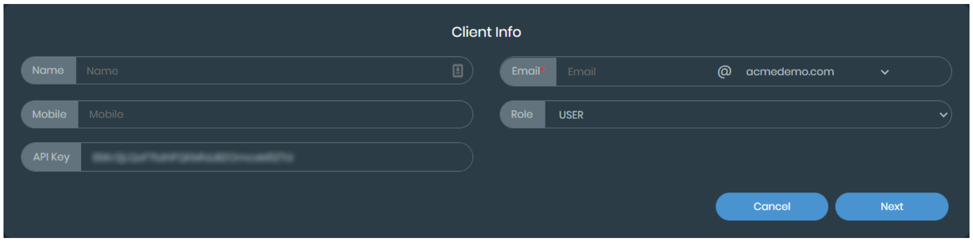
b. Click the *X* beside the keyword to remove the filter.

Adding users

Administrators can add new user accounts. Before you add new users, define access templates to select in the user accounts. See Access templates on page 140.

To add a user account:

1. Access *Profile Settings*, and click the *Users* page. The users are displayed.
2. Click the *Add User* button. The *Client Info* page is displayed.



Client Info

Name: Name

Email*: Email @ acmedemo.com

Mobile: Mobile

Role: USER

API Key: [redacted]

3. On the *Client Info* page, complete the following options, and click *Next*.

Name	Type a name for the user.
Mobile	Type the mobile phone number for the user.
API Key	Displays the automatically generated API key for the user.
Email	Type the email address, and select the domain for the user.
Role	Select one of the following roles: • User: gives the user access to the modules defined to their account. • Admin: gives the user access to the modules defined to their account and administrative access over other accounts.

The *Permissions* page is displayed

4. Select a *User Template* from the dropdown. The *Main Modules*, *Sub Modules*, and *Access* are adjusted to the template's settings.
5. Click *Save*. The user is created.

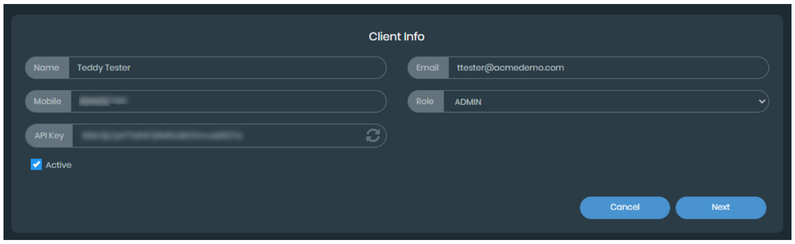
Editing users

All organization members with FortiRecon accounts are listed on the *Users* page. Administrators can edit the information of other members.

You cannot edit an email address.

To edit a user account:

1. Go to *Profile Settings* > *Users* and find the account you want to edit.
2. Click *Edit*. The *Client Info* page is displayed.



Client Info

Name: Teddy Tester

Email: ttester@acmedemo.com

Mobile: [redacted]

Role: ADMIN

API Key: [redacted]

☑ Active

3. On the *Client Info* page, complete any of the following options as needed, and click *Next*.

Name	Type a new name for the user.
Mobile	Type a new mobile phone number for the user.
API Key	Select *Re-generate API* to create a new *API Key*. This can be done when it is suspected that the API Key has been compromised or leaked.
Role	Select a new role from the *Role* dropdown.

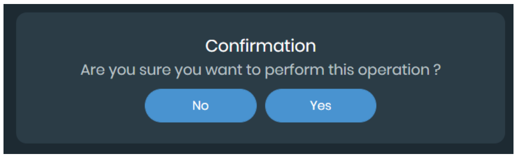
   The *Permissions* page is displayed.
4. Select a new *User Template* from the dropdown, if needed. The *Main Modules*, *Sub Modules*, and *Access* are adjusted to the template's settings.
5. Click *Save*. The user information and access permissions are updated.

Deleting users

Administrators can delete the account of another member on the *Users* page.

To delete a user account:

1. Go to *Profile Settings* > *Users* and find the account you want to delete.
2. Click *Delete*. A confirmation message is displayed.



Confirmation

Are you sure you want to perform this operation ?

3. Click *Yes*. The account is deleted.

Access templates

Access templates are used for controlling user accounts. When you create an access template, you can define what modules and sub modules a user can access, and then you can assign the access template to user accounts. See Adding users on page 139

From the *Profile Settings* > *Access Template* page, you can:

- View available access templates. See Viewing access templates on page 141.
- Add a new access template. See Adding a template on page 141.
- Edit an existing access template. See Editing a template on page 142.

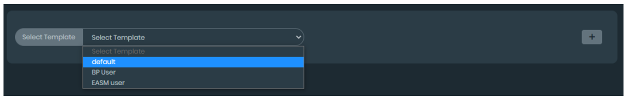
Viewing access templates

You can view the settings assigned to an access template in the *Access Templates* page. Assigned *Main Modules*, *Sub Modules*, and *Access* settings appear in the following formats:

- Grey: The Sub Module is a default setting that is always included if the Main Module is selected.
- Blue: The feature has been intentionally selected from the optional features.

To view an access template:

1. Go to *Profile Settings* > *Access Templates*.
2. Click the *Select Template* dropdown. A list of existing access templates is displayed.



3. Select the template you want to view. The template is displayed.

Adding a template

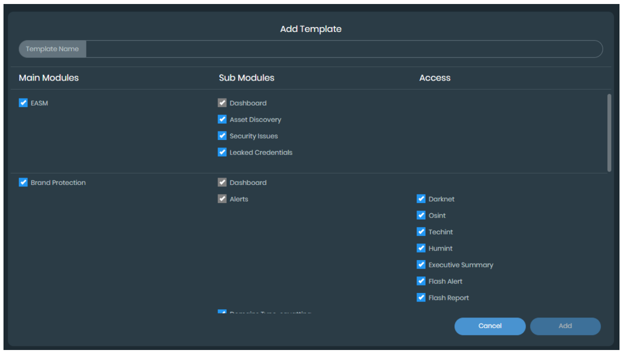
You can create new templates in the *Access Templates* page, and they can include any of the *Main Modules*, specific *Sub Modules*, and *Access* settings.

While all *Access* settings are optional, the following *Sub Modules* are mandatory when the associated *Main Module* has been selected:

Main Module	Mandatory Sub Modules
EASM	Dashboard
Brand Protection	Dashboard and Alerts
Adversary Centric Intelligence	Dashboard and Reports

To create an access template:

1. Go to *Profile Settings* > *Access Templates*.
2. Click *Add Template*. The *Add Template* page is displayed.



Add Template

Template Name

Main Modules	Sub Modules	Access
☑ EASM	☑ Dashboard ☑ Asset Discovery ☑ Security Issues ☑ Leaked Credentials	
☑ Brand Protection	☑ Dashboard	
	☑ Alerts	☑ Darknet ☑ Osint ☑ Techint ☑ Humint ☑ Executive Summary ☑ Flash Alert ☑ Flash Report

3. Enter a name in the *Template Name* text box.
4. Select the *Main Modules*, *Sub Modules*, and *Access* fields to enable user access to them.
5. Clear the *Main Modules*, *Sub Modules*, and *Access* fields to disable user access to them.
6. Click *Add*. The template is created.

Editing a template

You can edit a template that has previously been created to add or remove *Modules*, *Sub Modules*, and *Access* settings.

To edit an access template:

1. Go to *Profile Settings* > *Access Templates*.
2. From the *Select Template* dropdown, select the template you want to edit . The template is displayed.
3. Enter a new name in the *Template Name* text box, if needed.
4. Select the new *Main Modules*, *Sub Modules*, and *Access* fields to enable access to them.
5. Clear the *Main Modules*, *Sub Modules*, and *Access* fields to disable access to them.
6. Click *Save*. The template is updated.

Audit Logs

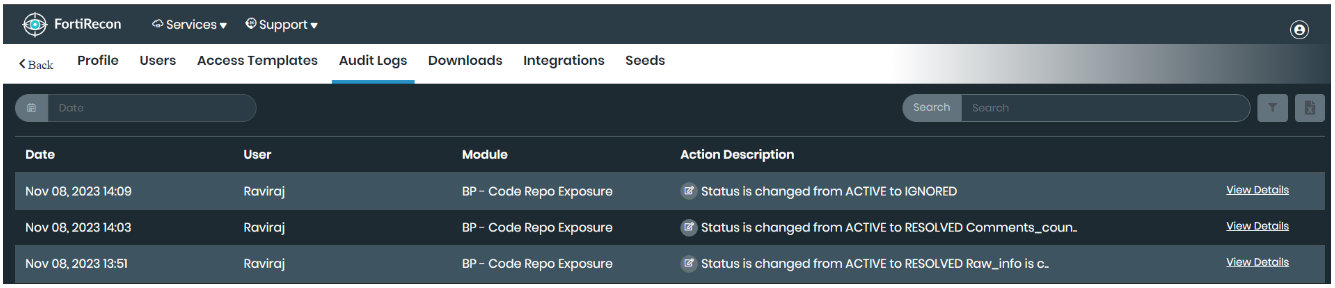
The Audit Logs page provides a comprehensive overview of all activities performed within FortiRecon, allowing you to track user actions, monitor changes made to your organization's data, and maintain compliance with security regulations.

From *Profile Settings* > *Audit Logs* tab, you can:

- View the audit logs. See Viewing the audit logs.
- Apply filters to the list of audit logs to view specific logs. See Filtering audit logs.
- Export audit logs to an Excel file. See Exporting audit logs.

Viewing audit logs

Audit logs capture detailed information about every action taken within FortiRecon, including the date and time of the action, the user responsible, FortiRecon module, and the action description.



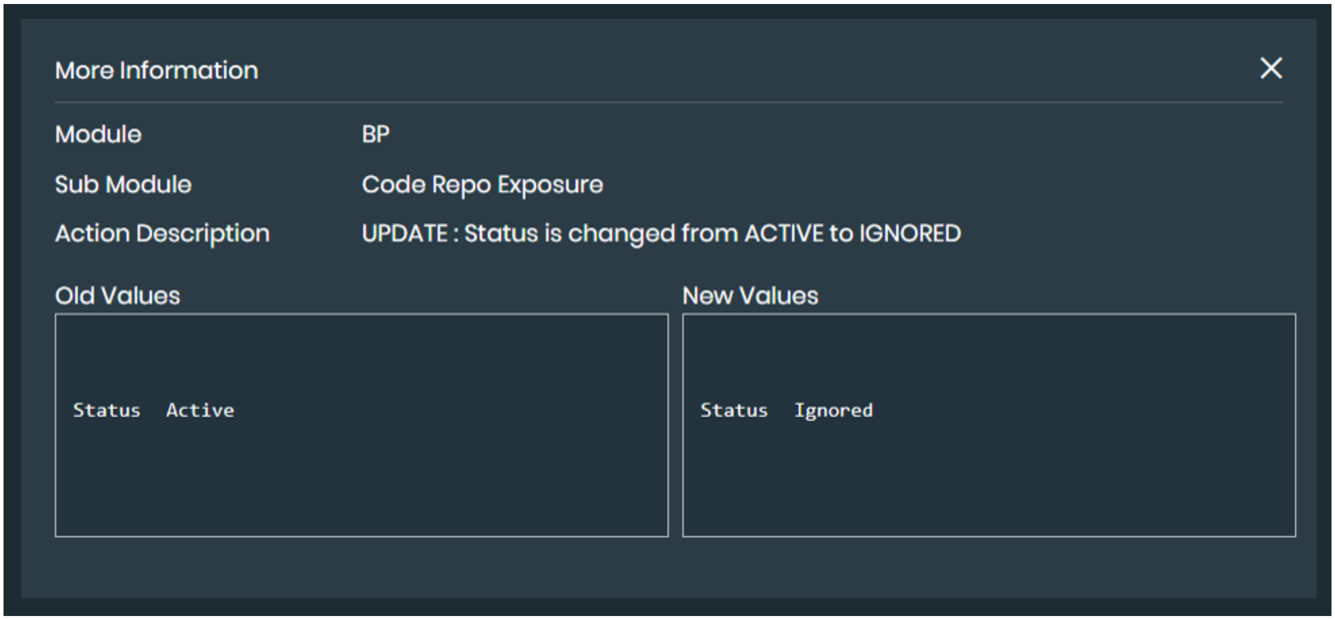
Date	User	Module	Action Description	
Nov 08, 2023 14:09	Raviraj	BP - Code Repo Exposure	Status is changed from ACTIVE to IGNORED	View Details
Nov 08, 2023 14:03	Raviraj	BP - Code Repo Exposure	Status is changed from ACTIVE to RESOLVED Comments_coun..	View Details
Nov 08, 2023 13:51	Raviraj	BP - Code Repo Exposure	Status is changed from ACTIVE to RESOLVED Raw_info is c..	View Details

To view audit logs:

1. Go to *Profile Settings* > *Audit Logs*.
2. Apply the required filters. See Filtering audit logs.
3. Click *View Details* next to a desired audit log to view detailed information.

More Information window displays detailed audit log information including:

- *Module*
- *Sub Module*
- *Action Description*
- *Old Values*
- *New Values*



More Information

Module	BP
Sub Module	Code Repo Exposure
Action Description	UPDATE : Status is changed from ACTIVE to IGNORED

Old Values

```
Status   Active
```

New Values

```
Status   Ignored
```

Filtering audit logs

By default, the *Profile Settings* > *Audit Logs* page displays all audit logs, starting with most recent log. You can use filters to display specific logs.

To filter audit logs:

1. Go to *Profile Settings* > *Audit Logs*.
    a. Filter audit logs by a date range:
    b. Click *Date* field. Two calendars are displayed.
    c. In the left calendar, select a month, year, and day to specify the start date of the range.
    d. Select a month, year, and day to specify the end date of the range.
    e. Only audit logs from the date range are displayed.
    f. Click the *Date* field, and click *X* to remove the date range filter.
2. Search for keywords:
    a. In the *Type and hit Enter to Search* box, type a keyword, and press *Enter*.
    b. The audit logs are filtered to display only logs with the keyword.
    c. Click the *X* beside the keyword to remove the filter.
3. To filter the audit logs by *Module, Sub Module*, or *User*, click the *Filter* icon, select the desired filters, and then click *Apply Filters*. To clear the applied filters, click the *Filter* icon and deselect the filters.

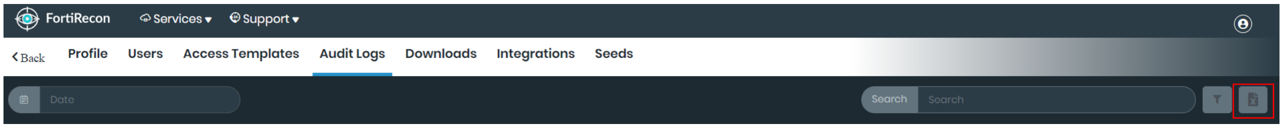
Exporting audit logs

You can export a list of audit logs into an Excel file. The spreadsheet will include the information on:

- Date
- User
- Module
- Sub Module
- Action Description

To export the audit logs:

1. Go to *Profile Settings* > *Audit Logs*.
2. Optionally, apply the required filters to export specific logs. See Filtering audit logs.
3. Click *Download* icon. The file is downloaded to your computer.



Downloads

Files downloaded from *EASM*, *Brand Protection*, and *Adversary Centric Intelligence* are saved in the *Downloads* page. Files are saved in a list with the most recently downloaded files at the top.

From the *Profile Settings* > *Downloads* page, you can:

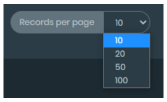
- View all downloads from the past 30 days. See Viewing downloads on page 145.
- Retrieve downloads from the past 30 days. See Retrieving downloads on page 145.
- Delete downloads. See Deleting downloads on page 145.

Viewing downloads

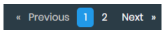
You can view all of your downloads from the past 30 days.

To view downloads:

1. Go to *Profile Settings* > *Downloads*. The most recent downloads are displayed.
2. From the *Records per page* dropdown list, select the number of downloads to display on the page.



3. Navigate between pages by selecting *Previous* and *Next*.



Retrieving downloads

You can retrieve downloaded files in the *Downloads* page.

To retrieve a downloaded file:

1. Go to *Profile Settings* > *Downloads* and find the file you want.
2. Click the file in the *Download* column. The file is downloaded to your computer.

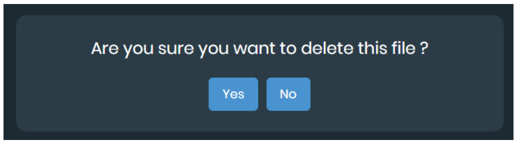
If a file is not finished downloading, an update message is displayed when you hover your mouse over the file. You cannot click the file until it is finished downloading.

Deleting downloads

Downloaded files are automatically deleted after 30 days. However, you can manually delete files if needed.

To delete downloaded files:

1. Go to *Profile Settings* > *Downloads* and find the file.
2. Click the delete icon in the *Actions* column. A confirmation message is displayed.



Are you sure you want to delete this file ?

3. Click *Yes*. The file is deleted.

Integrations

You can use webhook integration to receive automated alert and report notifications over Microsoft Teams and Slack. For example, if you have flash reports configured for a Slack integration, when a flash report appears on FortiRecon, you receive an automated notification on your Slack account.

From the *Profile Settings* > *Integrations* page, you can:

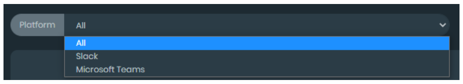
- View the details of existing integrations. See Viewing integration details on page 146.
- Create new integrations. See Adding integrations on page 147.
- Edit existing integrations. See Editing integrations on page 147.
- Disable integrations. See Disabling integrations on page 148.
- Delete integrations. See Deleting and disabling integrations on page 148.

Viewing integration details

You can view the details of an integration in the *Integrations* page.

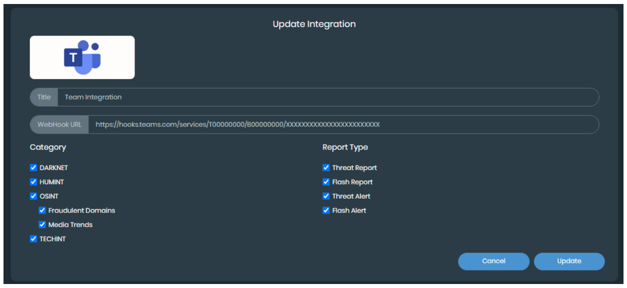
To view the details of an integration:

1. Go to *Profile Settings* > *Integrations*.
2. Find the integration you want to view:
   a. Search for keywords:
      i. In the *Type and hit Enter to Search* box, type a keyword, and press *Enter*.
         The integrations are filtered to display only integrations with the keyword.
      ii. Click the *X* beside the keyword to remove the filter.
   b. Search by platform:
      i. Select the *Platform* dropdown. A list of available integration platforms is displayed.



      ii. Select the platform you want to view.
         The integrations are filtered to display only integrations for that platform.

3. Click the name or icon of the integration. The *Update Integration* page displays the integration details.



Update Integration

Title: Team Integration

WebHook URL: https://hooks.teams.com/services/T00000000/B00000000/XXXXXXXXXXXXXXXXXXXXXXXX

Category
- ☑ DARKNET
- ☑ HUMINT
- ☑ OSINT
  - ☑ Fraudulent Domains
  - ☑ Media Trends
- ☑ TECHINT

Report Type
- ☑ Threat Report
- ☑ Flash Report
- ☑ Threat Alert
- ☑ Flash Alert

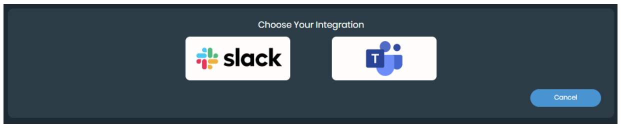
Adding integrations

You can add multiple webhook integrations to your account in FortiRecon.

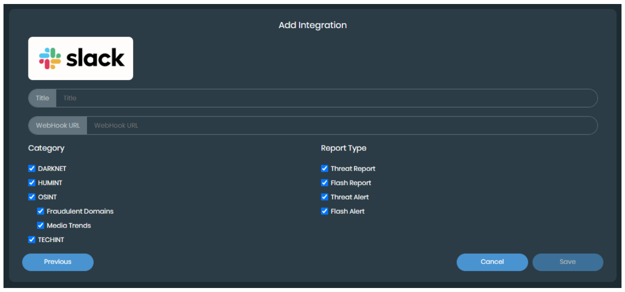
You must retrieve the webhook URL from Microsoft Teams and Slack before adding an integration to FortiRecon. See Microsoft Teams Webhooks and Connectors and Slack API Sending messages using Incoming Webhooks for more information.

To add an integration:

1. Go to *Profile Settings* > *Integrations*.
2. Click *Add Integrations*. The *Choose Your Integration* page is displayed.



3. Select the software you want to integrate with. The *Add Integration* page is displayed.



Add Integration

Title: Title

WebHook URL: WebHook URL

Category
- ☑ DARKNET
- ☑ HUMINT
- ☑ OSINT
  - ☑ Fraudulent Domains
  - ☑ Media Trends
- ☑ TECHINT

Report Type
- ☑ Threat Report
- ☑ Flash Report
- ☑ Threat Alert
- ☑ Flash Alert

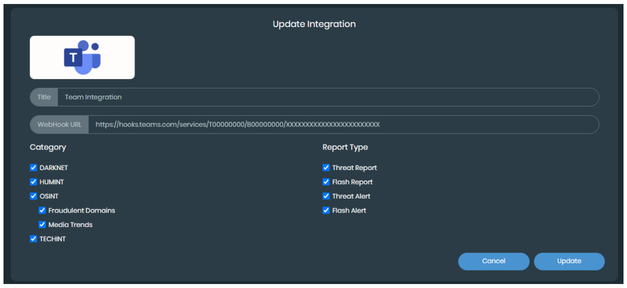
4. Enter the name of the integration in the *Title* text box.
5. Paste the webhook URL from the software into the *WebHook URL* text box.
6. Select the *Category* and *Report Type* fields that you want to include in the integration.
7. Clear any fields that you want to exclude from the integration.
8. Click *Save*. The integration is added.

Editing integrations

You can change the features and details of a webhook integration from the *Integrations* page.

To edit an integration:

1. Go to *Profile Settings* > *Integrations* and locate the integration.
2. Click the name or icon of the integration. The *Update Integration* page is displayed.



Update Integration

Title: Team Integration

WebHook URL: https://hooks.teams.com/services/T00000000/B00000000/XXXXXXXXXXXXXXXXXXXXXXXX

Category
- ☑ DARKNET
- ☑ HUMINT
- ☑ OSINT
  - ☑ Fraudulent Domains
  - ☑ Media Trends
- ☑ TECHINT

Report Type
- ☑ Threat Report
- ☑ Flash Report
- ☑ Threat Alert
- ☑ Flash Alert

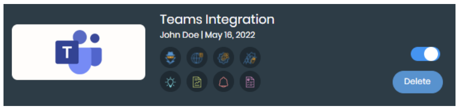
3. Edit the *Title* and *WebHook URL* text boxes, as needed.
4. Select the *Category* and *Report Type* fields that you want to include in the integration.
5. Clear any fields that you want to exclude from the integration.
6. Click *Update*. The webhook integration is updated.

Disabling integrations

You can temporarily disable unused integrations, and then enable them again in the future. The integration toggle allows you to enable and disable an integration as needed.

To disable an integration:

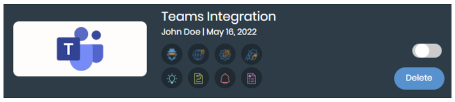
1. Go to *Profile Settings* > *Integrations* and find the integration.



Teams Integration

John Doe | May 16, 2022

2. Select the toggle to disable the integration. The notifications are no longer sent to the software.



Teams Integration

John Doe | May 16, 2022

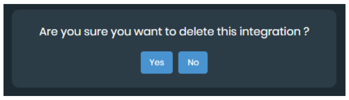
3. Select the toggle again to enable the integration.

Deleting and disabling integrations

You can delete unneeded webhook integrations.

To delete an integration:

1. Go to *Profile Settings* > *Integrations* and find the integration.
2. Click *Delete*. A confirmation message is displayed.



Are you sure you want to delete this integration ?

3. Click *Yes*. The integration is deleted.

Seeds

You can view your organization information in *Profile Settings* > *Seeds* page. *Seeds* page displays the information captured by FortiRecon during the following scenarios:

- Information you provide during onboarding.
- Any assets you add from *EASM* > *Asset Discovery* > *Bulk Add/Remove Assets*.

The Seeds section is read-only. If you want to remove an asset (ASN /IP address /IP range/ domain/ sub domain) from Seeds, you must remove it from *EASM* > *Asset Discovery* > *Bulk Add/Remove Assets*.

Because Seeds is your initial input, the EASM module uses it to discover additional assets and populate them in *EASM* > *Asset Discovery*. The assets in *EASM* > *Asset Discovery* are then used to populate the data in Brand Protection and ACI modules.

From the *Profile Settings* > *Seeds* page, you can:

- View your organization's registered assets. See Viewing your assets on page 149.

Viewing your assets

On the *Seeds* page, you can view the domain names, ASN, IP prefix, sub domains, card BINs, mobile apps, and social media profiles of your organization that are being monitored by FortiRecon. You can toggle between the following pages to view your organization's assets:

- Domains
- ASN
- IP Prefix
- IP Address
- Sub Domain
- Card BIN
- Owned Mobile Applications
- Social Media

To view your organization's assets:

1. Go to *Profile Settings* > *Seeds*.
2. Navigate between asset types by selecting desired tab.
3. Search for assets:

- Navigate to one of the tabs, and search for a keyword in the *Search* box to look for entries specific to that asset type.

www.fortinet.com