User Guide

FortiRecon 23.2.a

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

May 31, 2023
FortiRecon 23.2.a User Guide
75-232-918291-20230531

TABLE OF CONTENTS

Change Log

Date	Change Description
2023-05-31	Initial release.
2023-06-05	Updated Adding assets manually section.

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 16.
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 45.
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 73.
Profile Settings	The Profile Settings module allows you to personalize your FortiRecon account and provide information on your organization. See Profile settings on page 108.

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 11 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 102.
- Bank identification numbers (BINs) should only be added for the licensed entity and brand. See Card Fraud on page 83.

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.

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
Brand Protection (BP)	• Fraudulent domains identified, such as phishing and brand impersonation • New rogue mobile application identified • Social media impersonation identified • Exposed sensitive information on code repository • Files found in open cloud storage bucket
Adversary Centric Intelligence (ACI)	• Any published flash alert or report • Any high relevance report • Stealer infection identified • Organization or vendor listed on a ransomware naming and shaming site • Daily digest

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 11.
- Subscribe to FortiRecon and start the service. See Subscribing to FortiRecon on page 12.

Registering the FortiRecon license

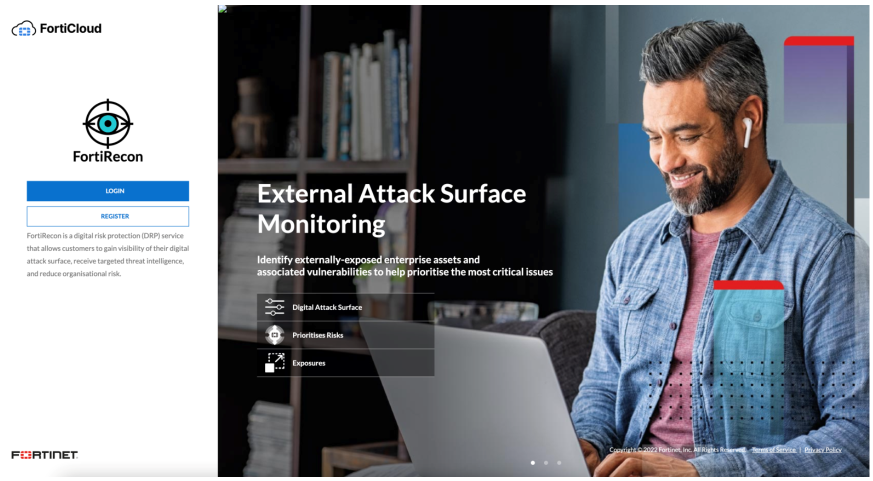
You must purchase and register a FortiRecon license before you can subscribe to FortiRecon. After you purchase the license, register the license using FortiCloud Account Services. For more information about registering products on FortiCloud, see the *FortiCloud Account Services > Registering products*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

Subscribing to FortiRecon

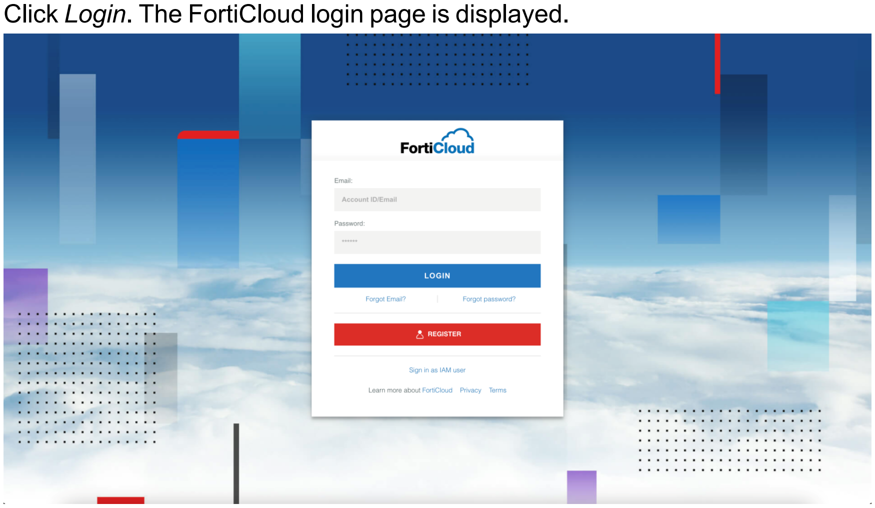
This section describes how to subscribe to FortiRecon and start the service. Before you can subscribe to FortiRecon, you must register the license. See Registering the FortiRecon license on page 11.

To subscribe to FortiRecon:

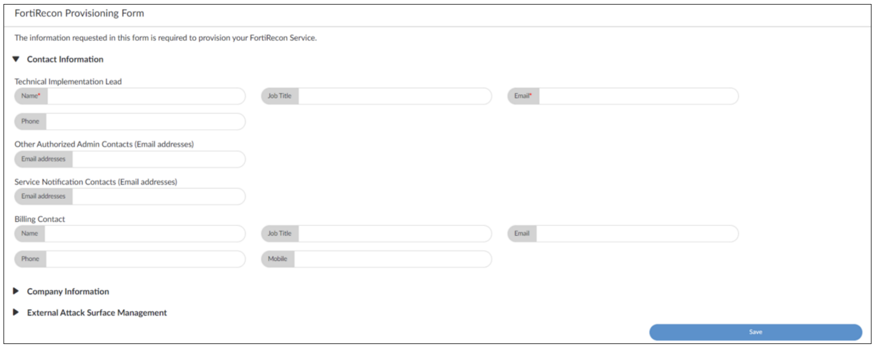
1. After the license is registered on FortiCloud, go to FortiRecon at https://fortirecon.forticloud.com.



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.



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

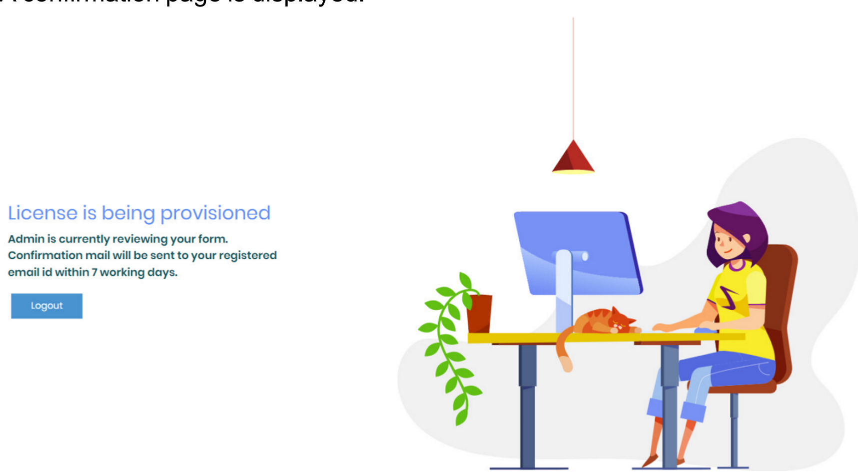
Fields marked with a red asterisks are required information. Other fields are considered optional although it is suggested that you complete all of the fields provided to receive the most accurate service.

---

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.

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.



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

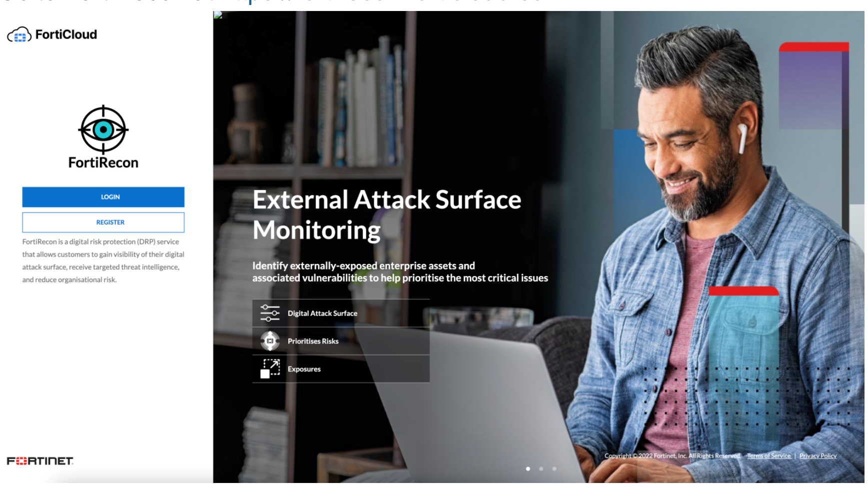
12. When you receive an email from the FortiRecon team, you can access the FortiRecon portal and review the analysis. See Accessing FortiRecon portal on page 15.

Accessing FortiRecon portal

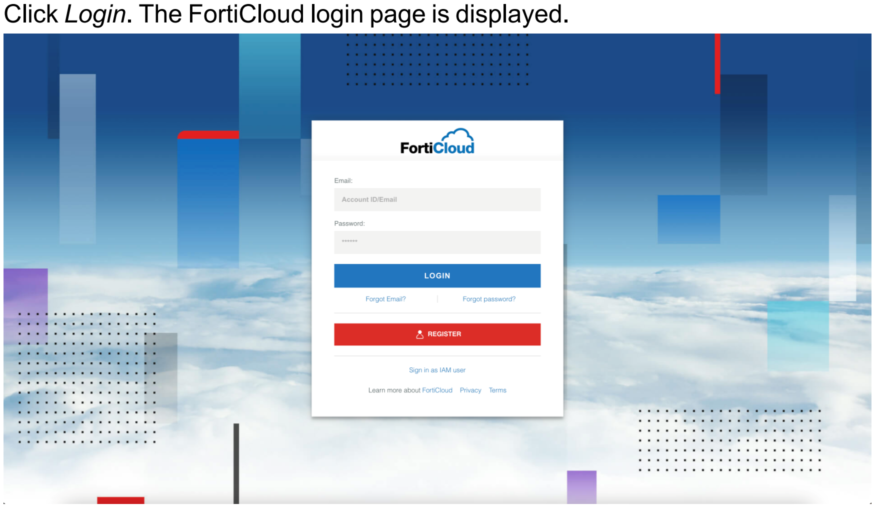
After you have subscribed to FortiRecon and received an email from the FortiRecon team, you are ready to access the FortiRecon portal.

To access FortiRecon:

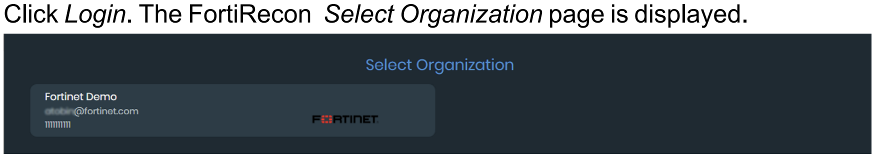
1. Go to FortiRecon at https://fortirecon.forticloud.com.



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



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



5. Select the organization you want.
   The *EASM* > *Dashboard* page is displayed. See EASM on page 16.

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 on a schedule and displays the results.

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 16.
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 19.
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 27.
Asset Management	Displays tags and groups used to filter and link assets. See Asset Management on page 32.
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 39.
Integrations	Displays Azure and AWS integration that are tracked in *Asset Discovery* and *Security Issues*. See Integrations on page 41.

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 17.
- View a summary of potential security issues related to your organization. See Viewing security issues summary on page 17.
- 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 18.
- Download the dashboard content to your hard drive. See Downloading the EASM dashboard details on page 19.

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 19.

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.

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.

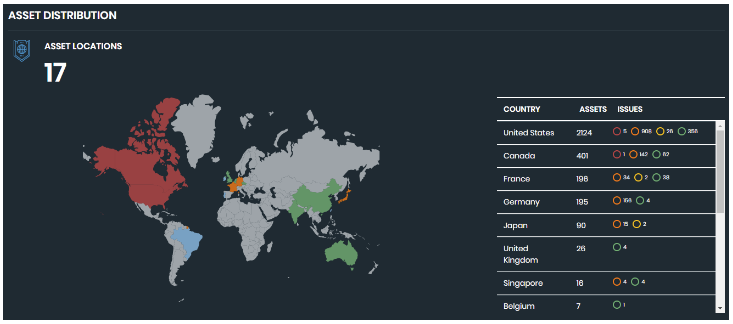
3. Click an issue or vulnerability to display more details on the *Security Issues* page. See Security Issues on page 27.

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.



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 27.

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 117.

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 20.
- Mark discovered assets as false positives to remove them from the next scheduled FortiRecon scan. See Marking assets as false positives on page 22.
- Manually add assets to FortiRecon to include them in the next scheduled scan. See Adding assets manually on page 23.
- Manually remove assets from the next scheduled FortiRecon scan. See Removing assets manually on page 23.
- Assign tags to assets for focused filtering. See Assigning tags on page 24.

> 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 32.

- Perform a FortiDAST vulnerability scan on assets. See Performing a FortiDAST scan on page 25.
- View DNS health report for your domains. See DNS Health Report on page 26.

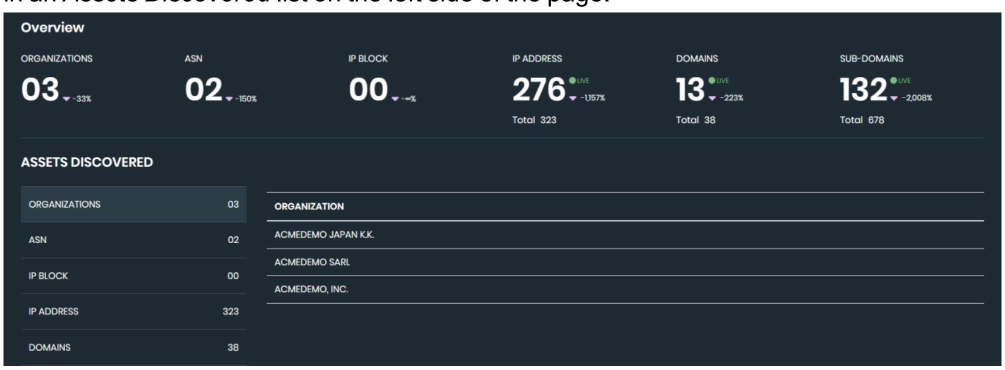
Viewing asset details

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.

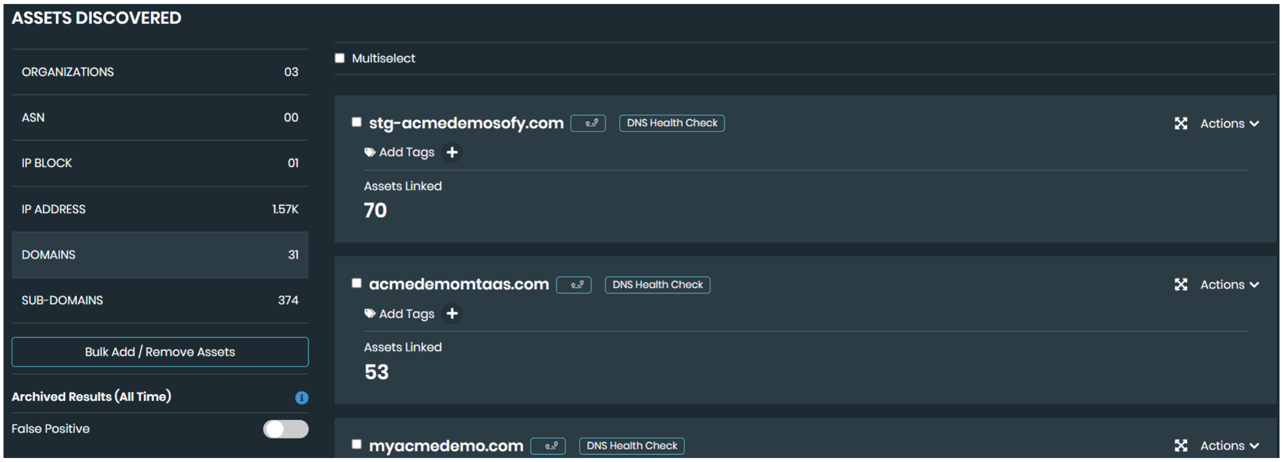


The following information is available:

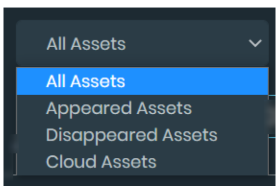
Organizations	The number of organizations that have been detected as belonging to you.
ASN	The number of autonomous system numbers (ASNs) that are linked to the detected organizations.
IP blocks	The number of IP blocks associated with the ASNs.
IP address	The number of IP addresses that are linked to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



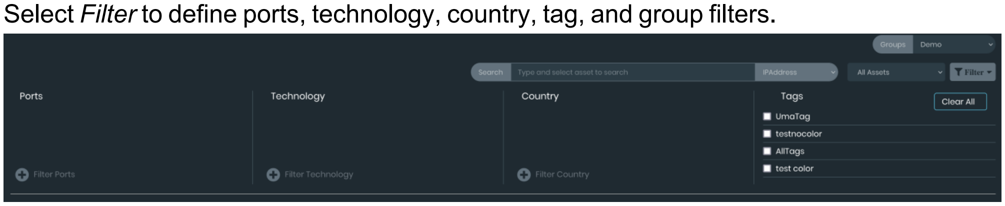
3. Filter the assets from the dropdown menu:



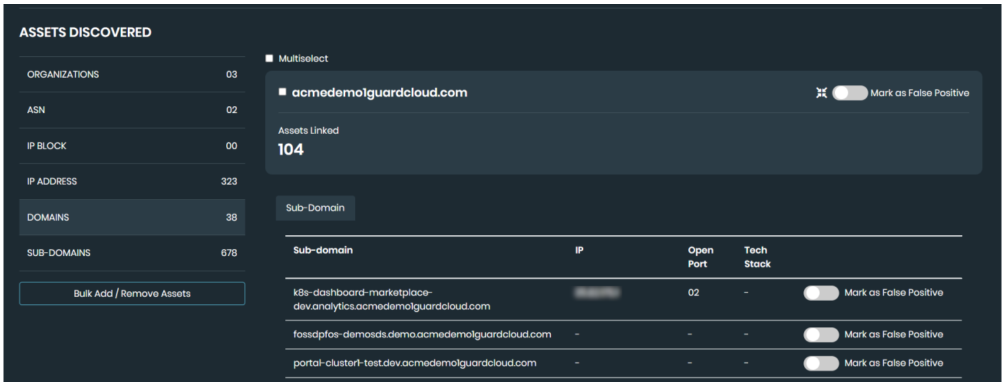
   a. Select *Appeared Assets* to show assets that appeared in the latest scan.
   b. Select *Disappeared Assets* to show assets that disappeared in the latest scan.
   c. Select *Cloud Assets* to show cloud-based assets.

> Cloud assets can only be filtered if the AWS cloud environment has been integrated. See Integrations on page 41.

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



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



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 22.

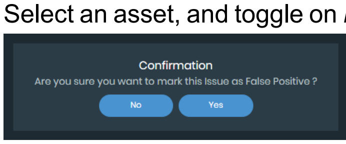
Marking assets as false positives

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*.



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*.

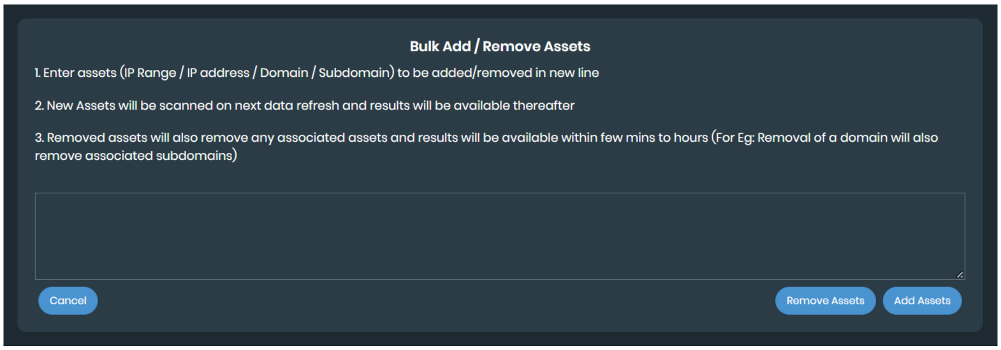
Adding assets manually

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.



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.

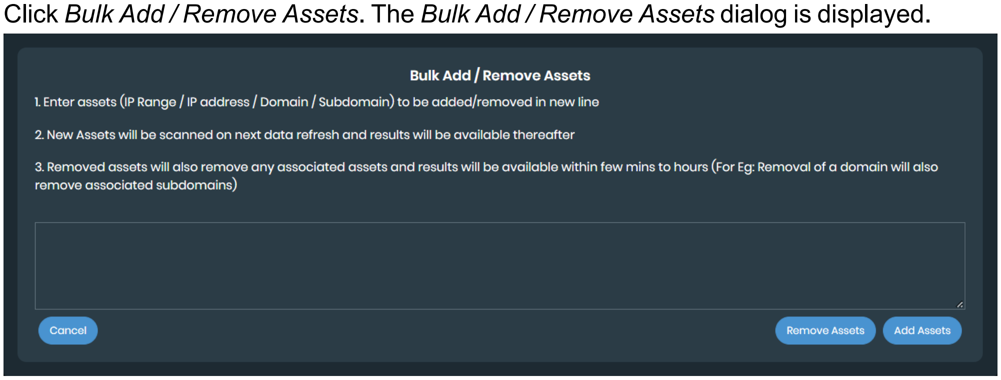
Removing assets manually

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.



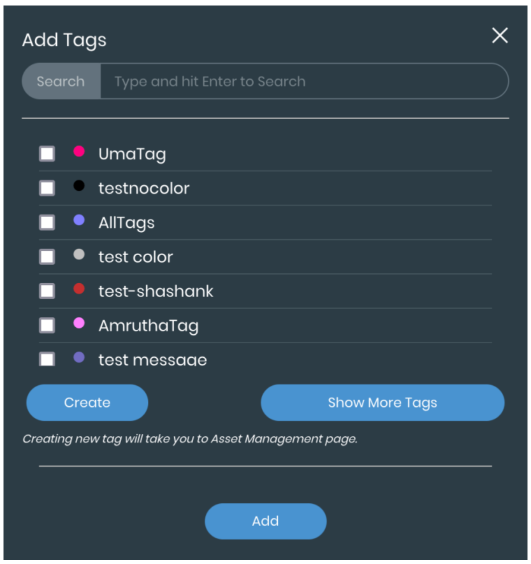
3. Enter the assets, and click *Remove Assets*.

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 32.

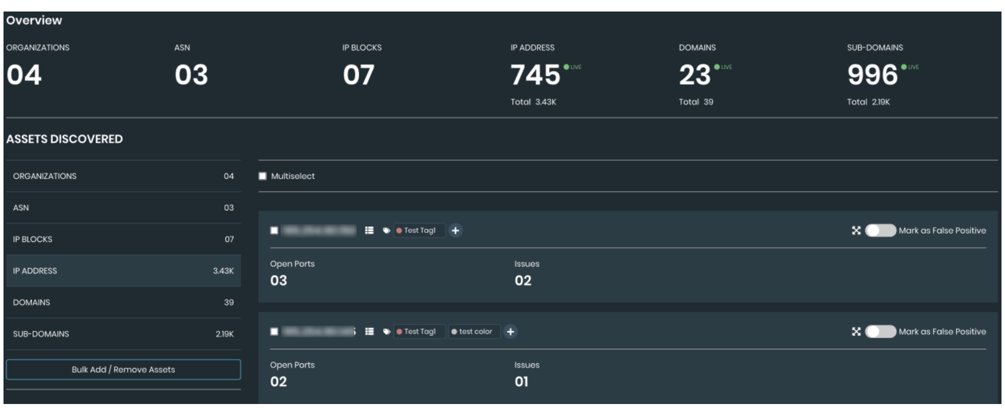
To assign a tag to an asset:

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



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 32.

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



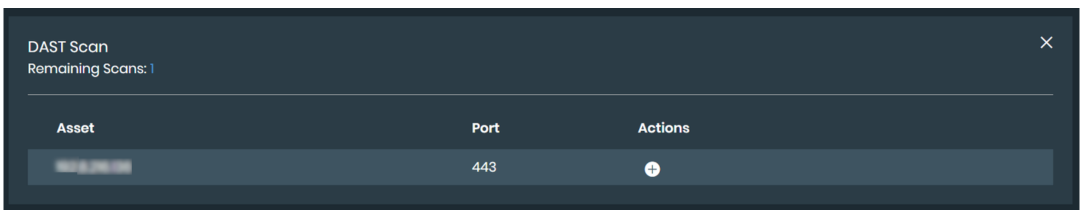
Performing a FortiDAST scan

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.

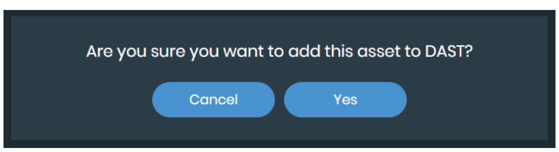
To scan an asset with FortiDAST:

1. Add a FortiDAST integration to FortiRecon. See Adding integrations on page 42.
2. Go to *EASM* > *Asset Discovery*.
3. Navigate to the asset you want to scan.
4. Select *Actions* > *DAST Scan*.

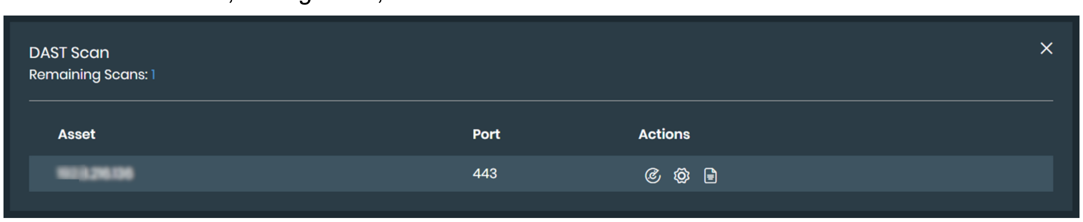
The *DAST Scan* dialog opens with number of *Remaining Scans* displayed.



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



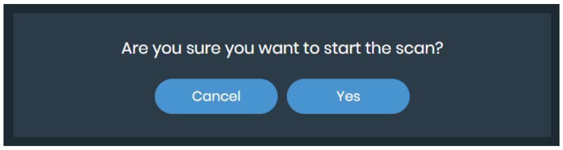
6. Click *Yes*. The *Scan*, *Config Scan*, and *View Result* buttons become available for the asset.



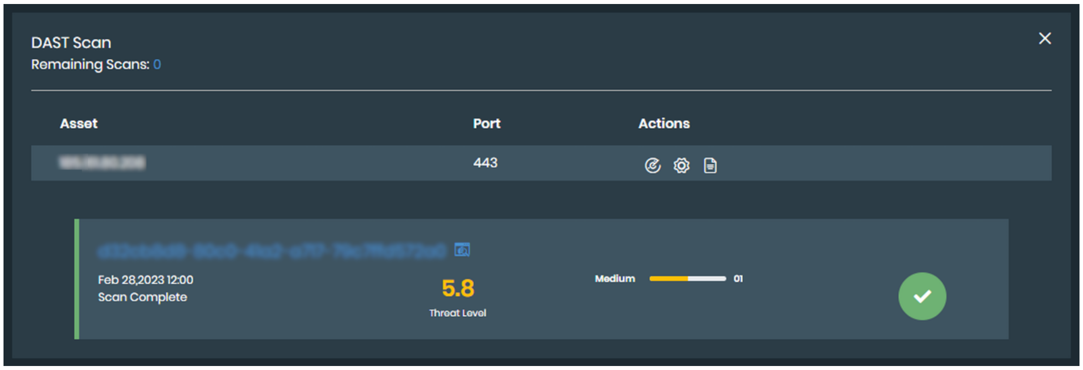
7. Click *Config Scan*. You will be redirected to FortiDAST.

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.



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



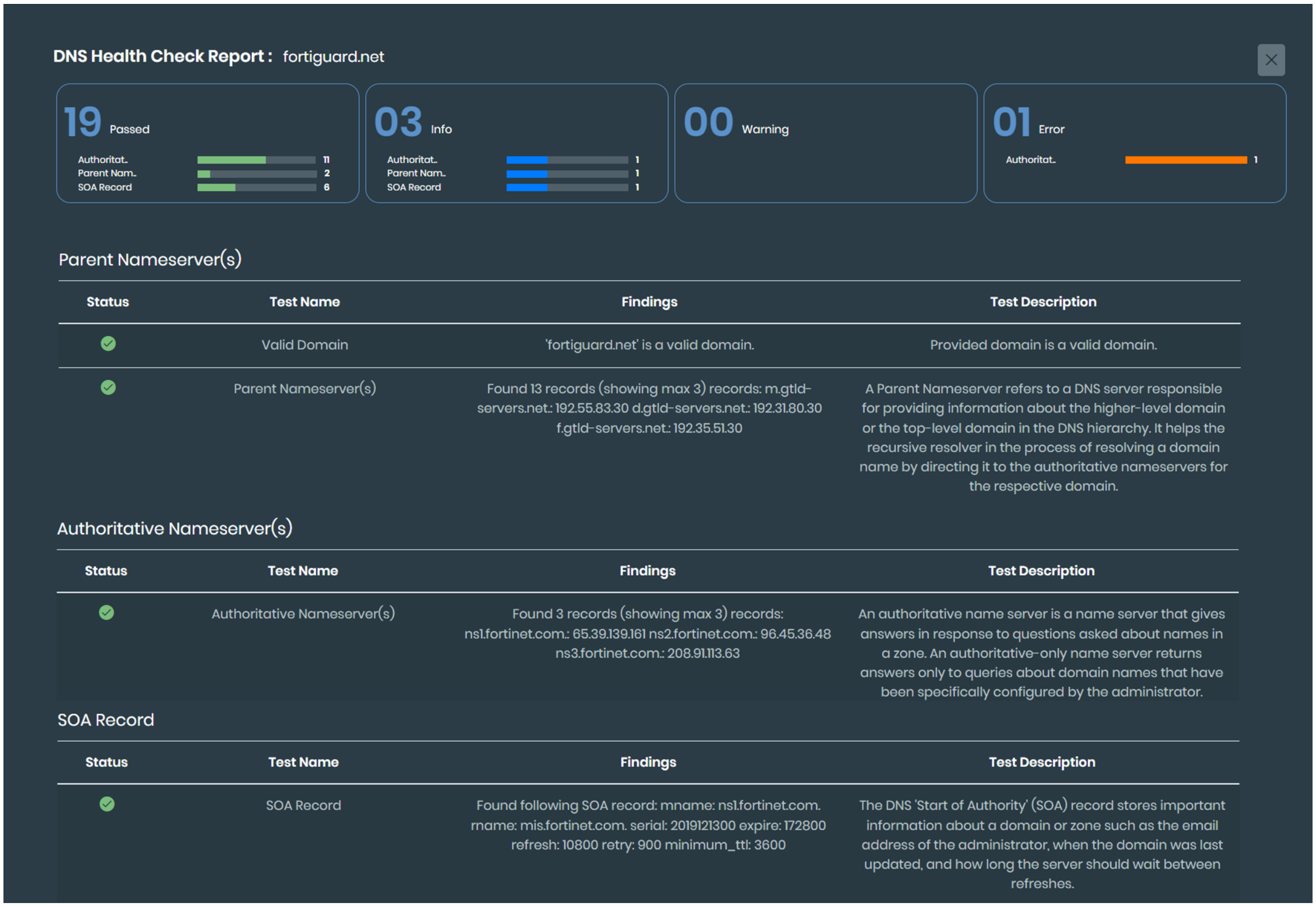
You can scan the same asset again by selecting *ReScan*.

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*.



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 27.
- Apply filters to the list of security issues to hone in on specific issues. See Filtering security issues on page 29.
- 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 31.
- Add a comment to explain status changes made to security issues. See Adding a comment to a security issue on page 32.

Viewing security issues

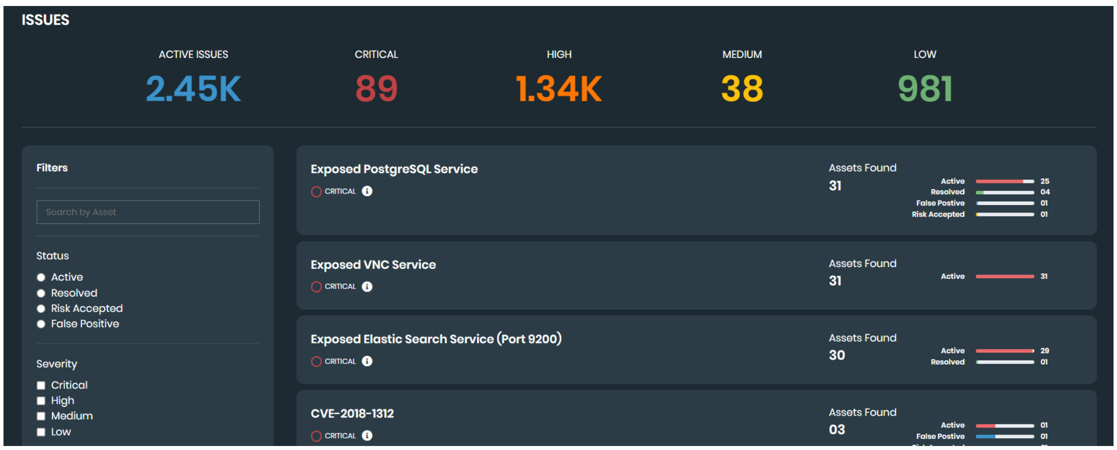
The *EASM* > *Security Issues* page displays the number of active security issues and how many of the active security issues are rated critical, high, medium, and low. Color indicates the severity of a security issue:

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.

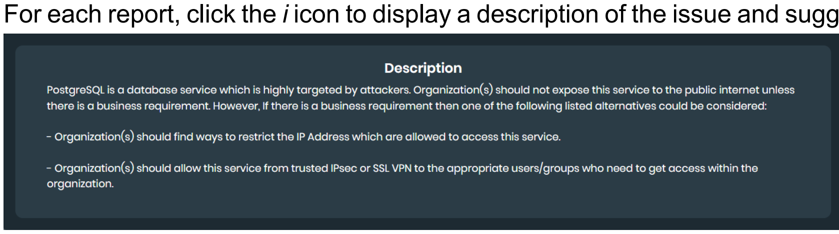
You can use search and filters to change the list of reports that are displayed, and then click each report to display its details.

To view security issues:

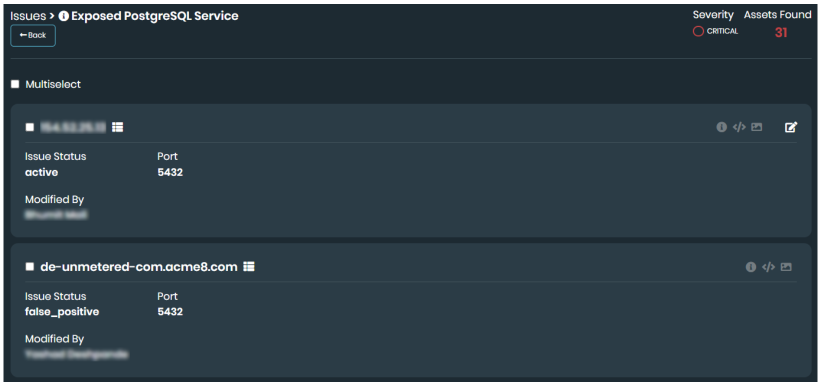
1. Go to *EASM* > *Security Issues*. The security issues are displayed.
   The *Issues* bar across the top displays the number of active security issues and the number of active security issues that are rated critical, high, medium, and low security risk.
   For each report, the number of affected assets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



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.



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



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

   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 31.

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.

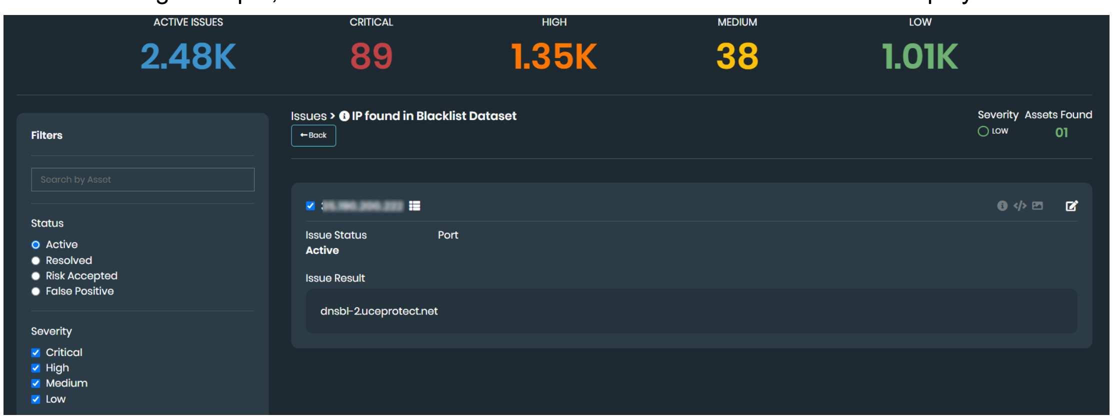
You can search for specific security issues using the *Search by Asset* field. Enter IP address information, such as 192.168.10.10 or 192.168.12.0/24.

To filter security issues:

1. Go to *EASM* > *Security Issues*. The list of security issues is displayed.
2. Add advanced search features:
   a. Click the filter icon. The advanced search fields are displayed.
   b. Select the *Search Type*.
   c. Click *Search*.
3. 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: • 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.
4. (Optional) In the *Filters* list, toggle on *False Positive*. The list displays only issues marked with a status of *False Positive*.
5. Click an issue title to display its details.
   In the following example, the details for the *IP found in blacklist dataset* issue are displayed:



6. 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

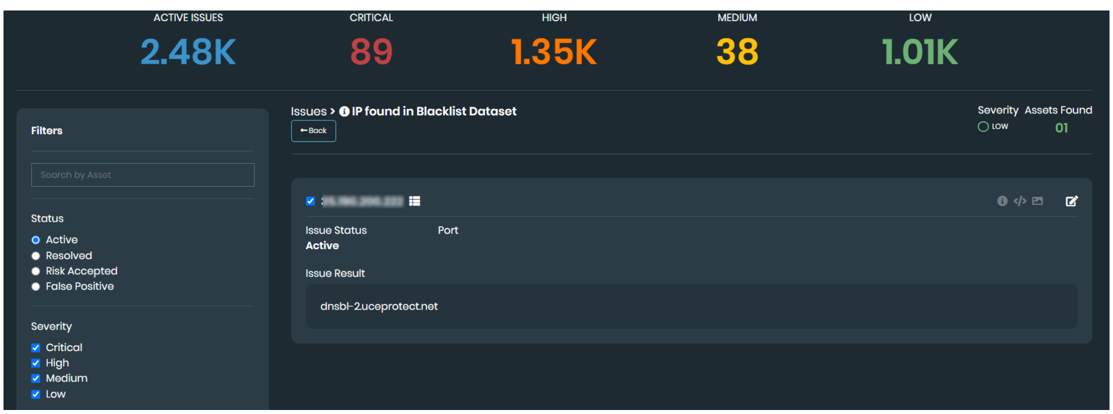
7. Click *Back* to display the list of issues again.
8. In the *Filters* list, click *Clear* to remove all filters.

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 *IP found in blacklist dataset* 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*.

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 32.
- Assign individual and bulk assets to an asset tag. See Adding assets to a tag on page 33.
- Manage, edit, and delete asset tags. See Managing tags on page 34.
- Create a new asset group. See Creating a group on page 35.
- Assign individual and bulk assets to an asset group. See Adding assets to a group on page 35.
- Manage, edit, and delete asset groups. See Managing groups on page 36.
- Filter *EASM* pages by group. See Filtering by group on page 37.
- Limit access to specific assets and security issues using groups and tags. See Limiting access to assets and issues on page 38.

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 20. 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

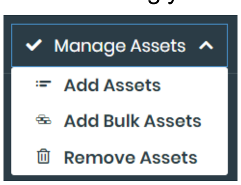
You can add individual or bulk assets to a tag from the *Tag Management* tab.

Assets must be included in *EASM* > *Asset Discovery* before they can be tagged. See Adding assets manually on page 23.

Tags can also be assigned to assets in *EASM* > *Asset Discovery*. See Assigning tags on page 24.

To add assets to a tag:

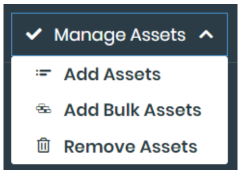
1. Go to *EASM* > *Asset Management*.
2. Select the *Tag Management* tab.
3. Locate the tag you want to add assets to and click *Manage Assets*. A dropdown menu is displayed.



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.



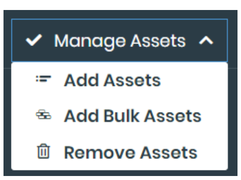
4. Select *Add Bulk Assets*.
5. Enter the asset information in the left field.
6. Select *Propagate the tag to asset* to apply tags to the asset associations. Select the *i* icon for more information.
7. Click *Validate*. Once validated, assets are displayed in the right field. Any assets that failed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



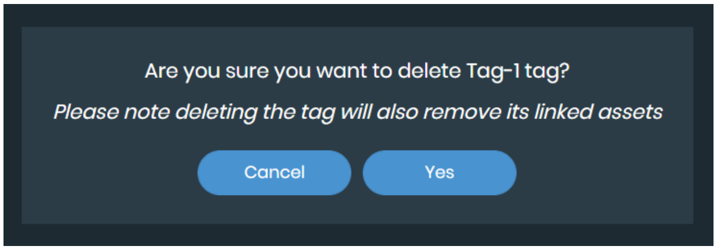
4. Select *Remove Assets*.
5. Select the assets you want to remove or click *Select All*.
6. Click *Remove Selected*.

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.



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 35.

Adding assets to a group

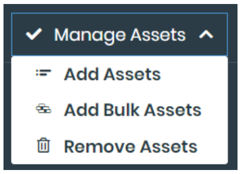
You can add individual or bulk assets to a group from the *Group Management* tab.

Assets must be included in *Asset Discovery* before they can be tagged. See Adding assets manually on page 23.

To add assets to a group:

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

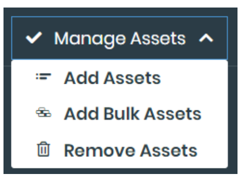
3. Locate the group you want to add assets to and click *Manage Assets*. A dropdown menu is displayed.



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.



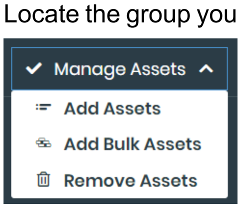
4. Select *Add Bulk Assets*.
5. Enter the asset information in the left field.
6. Select *Propagate the tag to asset* to apply tags to the asset associations. Select the *i* icon for more information.
7. Click *Validate*. Once validated, assets are displayed in the right field. Any assets that failed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

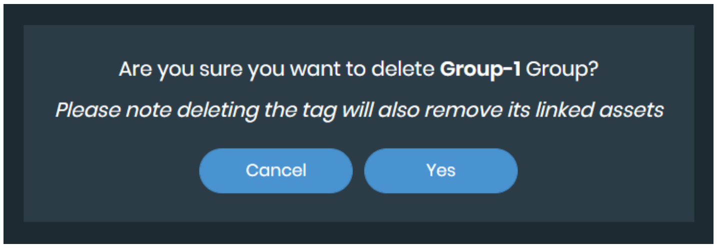
5. Select the assets you want to remove or click *Select All*.
6. Click *Remove Selected*.

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 38.
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.



4. Click *Yes*.

Filtering by group

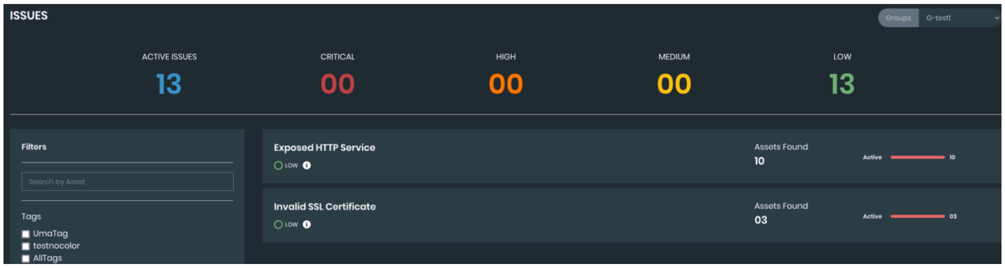
Once a group has been created, you can filter by group in the *EASM* > *Security Issues* and *EASM* > *Asset Discovery* pages using the *Groups* dropdown menu. The Groups filter will be set to all assets of the organization by default.

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.



Limiting access to assets and issues

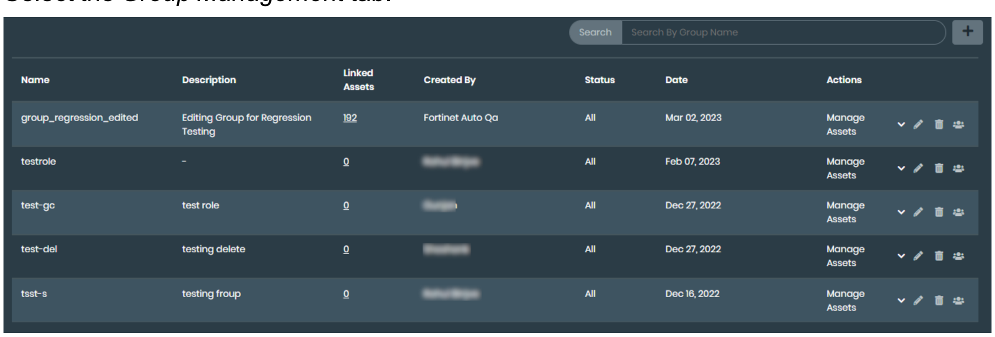
User access to specific assets and security issues can be limited through the use of groups and tags. User asset and security issue visibility is limited to the groups they are assigned to and any tags associated with these group assets.

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

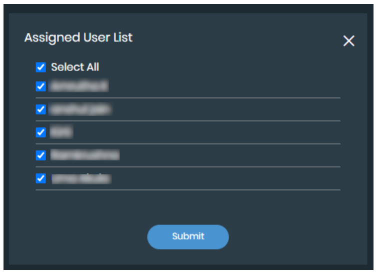
User assigned to	Visible assets	Hidden assets
A single group with no tags assigned	• All assets that have been added to the group	• Assets that have not been added to the group
A single group with tags assigned to the assets	• Assets that have been added to the group that also have the tags assigned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



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



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:

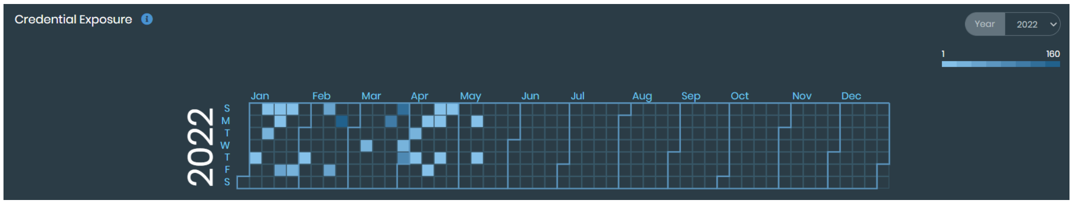
- View leaked credentials by year. See Viewing leaked credentials by year on page 39.
- View breached datasets. See Viewing breached datasets on page 40.
- View leaked credential details. See Viewing leaked credential details on page 41.
- Export a list of leaked accounts. See Exporting leaked accounts on page 41.

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 41.

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

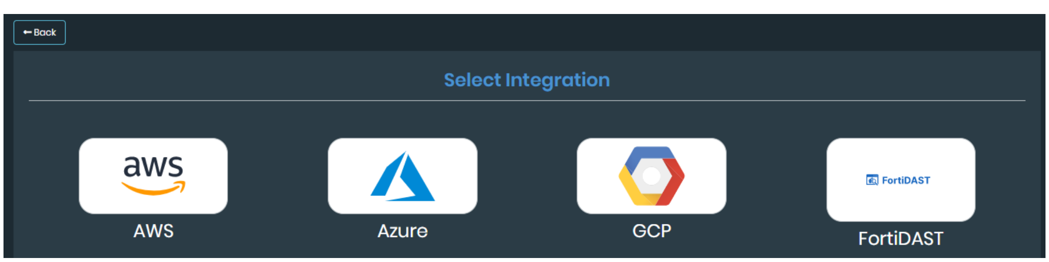
You can export a list of leaked accounts to Microsoft Excel format.

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, and FortiDAST. See Adding integrations on page 42.
- Edit and delete existing integrations. See Editing integrations on page 44.

Adding integrations

The *EASM* > *Integrations* page displays all existing AWS, Azure, Google Cloud Platform, and FortiDAST integrations. You can manually add new integrations as needed.

To add a new AWS integration:

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

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.

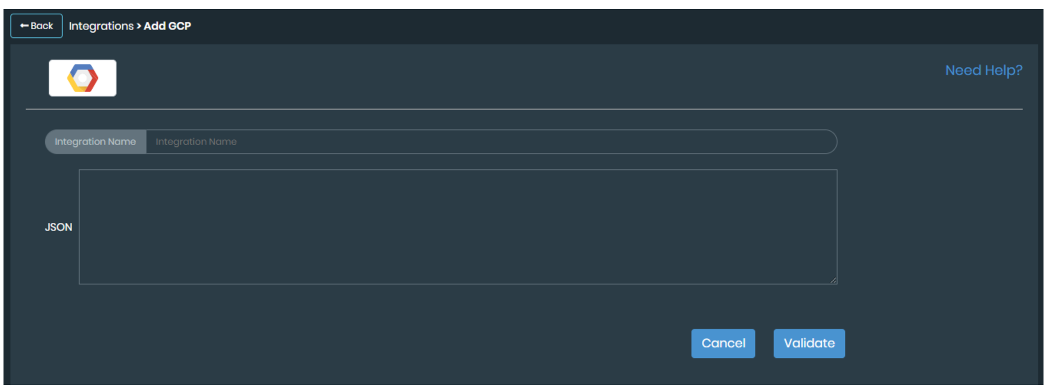
These four values are necessary to create read-only access for your Azure cloud account. For information on generating these values, click *Need Help?*.

---

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.

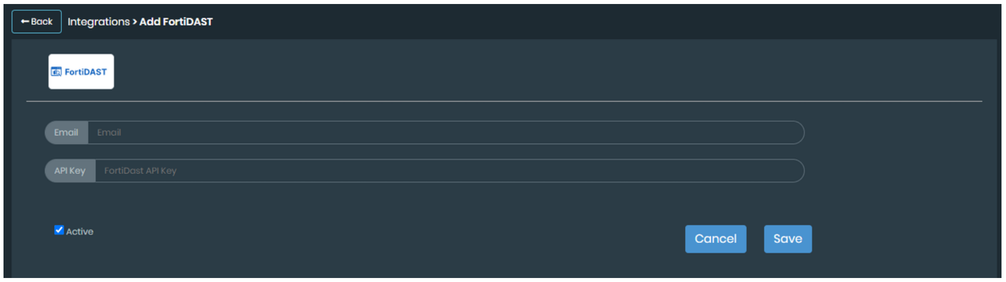
For information on generating the GCP key file and downloading JSON, click *Need Help?*.

---

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 .

Editing integrations

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

To edit an integration:

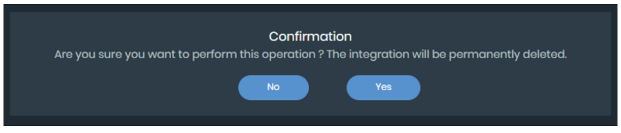
1. Go to *EASM* > *Integrations*.
2. Click *Edit*. The integration details are displayed.
3. Edit the fields you want to change.

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.



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 45.
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 48.
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 52.
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 60.
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 68.
Open Bucket Exposure	Displays a list of files exposed in open buckets. See Open Bucket Exposure on page 70.
Take Down	Displays a list of takedown request tickets and their current status. See Take Down on page 71.

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 46.
- View a summary of brand abuse, such as rogue apps or social media threats. See Viewing the brand abuse summary on page 46.
- View a summary of information exposure, including code and file exposure. See Viewing the information exposure summary on page 47.

- View trends and important alerts of threats to your brand. See Viewing the alert summary on page 47.
- View total credits used and available for domain takedown. See Viewing the takedown credit summary on page 48.

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.

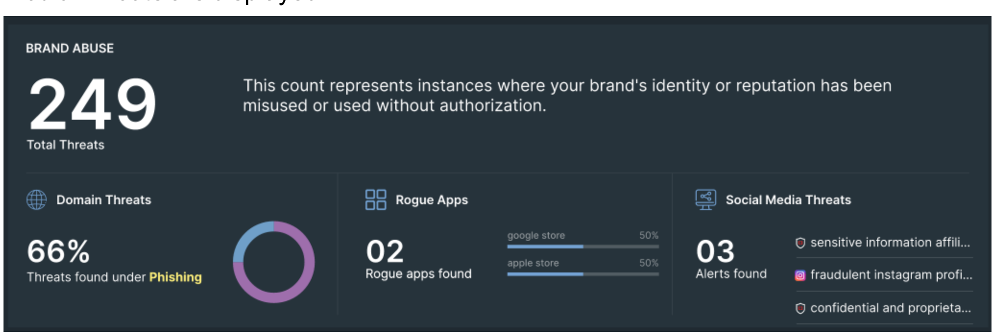
3. Hover over the threat type distribution bar to see the number of threats for each type.

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.



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:

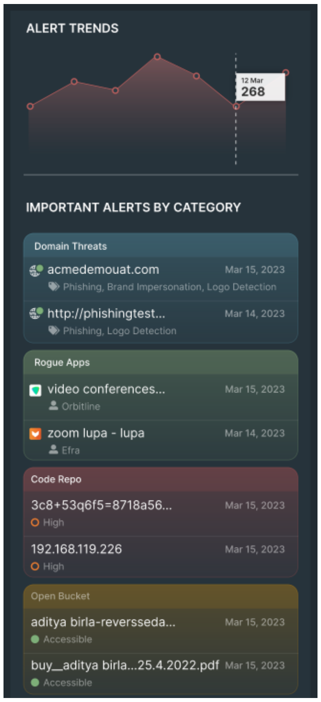
1. Go to *Brand Protection* > *Dashboard*.
2. Scroll to the *Information Exposure* widget. High level information about code and file exposure is displayed.

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.



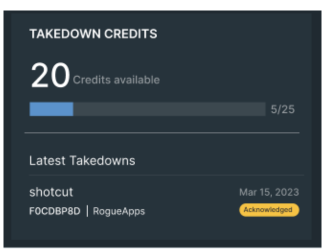
3. Hover over the graph for more information on daily alerts.

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.



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 49.
- Take action against impersonating domains, such as requesting domain takedown. See Managing domain threats on page 49.
- Filter the list of domains. See Filtering domains on page 49.
- Create a digital watermark. See Digital watermark on page 50.

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:
   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 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.

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.

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

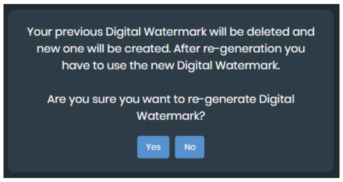
You can edit digital watermarks through the *Brand Protection > Phishing* page.

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.

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.



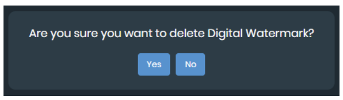
4. Click *Yes*.

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.



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 52.
- Take action against impersonating profiles, such as requesting profile takedown. See Managing social media threats on page 53.
- Filter the list of profiles. See Filtering social media threats on page 53.
- Add official social media profiles. See Adding official profiles on page 54.
- Export information on discovered profiles. See Exporting impersonating profiles.
- View archived alerts. See Alerts on page 55.

Reviewing social media threats

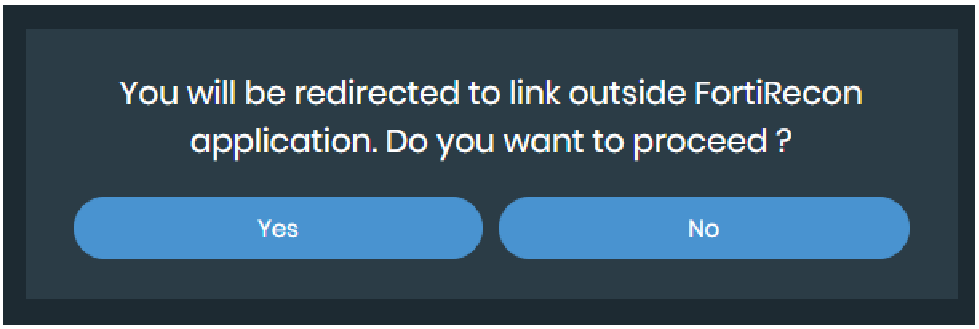
You can review information about social media threats in the *Brand Protection > Social Media Threats* page. Information displayed about social media threats includes:

- 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.



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:

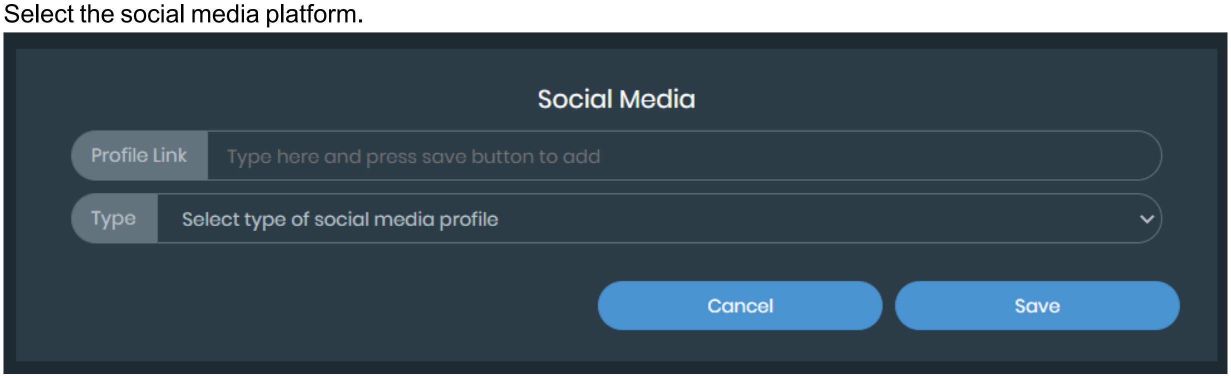
1. Go to *Brand Protection* > *Social Media Threats*
2. Filter threats by a date range:
   a. Click *Filter By Date Range*. Two calendars are displayed.
   b. In the left calendar, select a month, year, and day to specify the start date of the range.
   c. Select a month, year, and day to specify the 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.

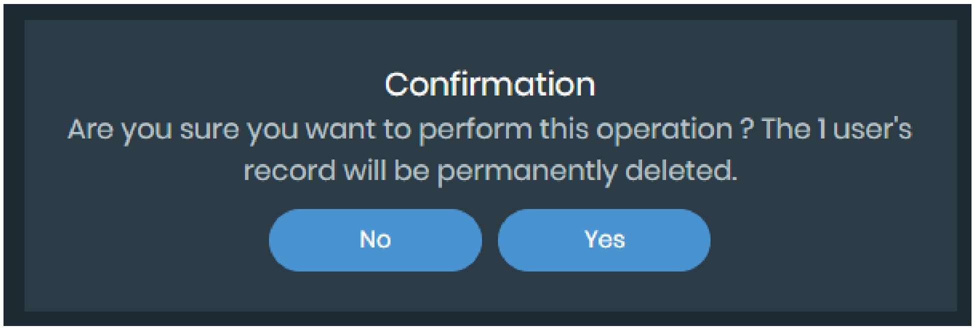


5. You can also add official social media profiles in bulk by uploading excel (XLS) file containing profile information including profile URL and type.
   a. Click Upload XLS icon.
   b. Browse and select the file. Click *Open*.

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*.



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 55.
- Filter through all flash reports available. See Filtering reports on page 56.
- Download flash reports as threat intelligence reports in PDF or as an observable Microsoft Excel file. See Downloading reports on page 56.
- Email and share links to flash reports with others. SeeSharing reports on page 58
- Rate flash reports for relevance. See Rating reports on page 59.
- Review reports and send queries to FortiRecon. See Reviewing reports on page 59.

Viewing flash reports

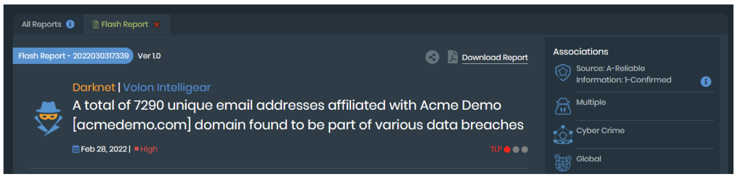
The *Brand Protection > Social Media Threats > Show Archived* page displays all the flash reports archived to you. By default all reports are displayed, starting with the latest report. Reports include in depth information, such as:

- 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.



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

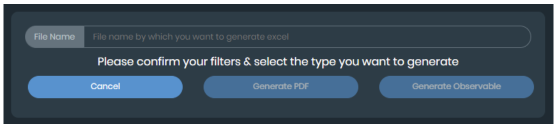
You can download reports from the *Alerts* tab as brand protection alerts in PDF or as an observable Microsoft Excel file. Brand protection alerts provide information from a flash report whereas observables outline any Indicators of Compromise (IOCs) highlighted in the flash report.

Downloaded reports can be set to include:

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

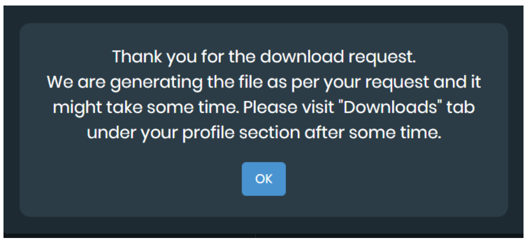
To download all reports available:

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



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.

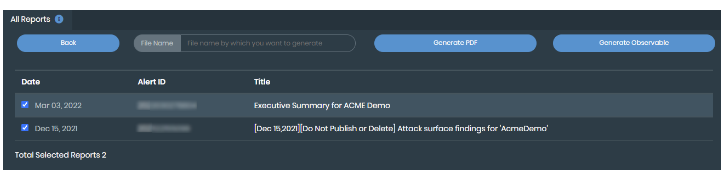
   The following message is displayed:



4. Click *OK*.
5. Retrieve the report. See Retrieving downloads on page 117.

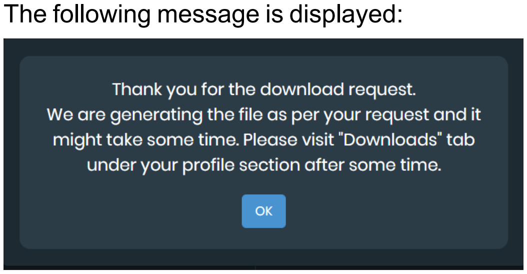
To download specific reports:

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 56
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.



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.

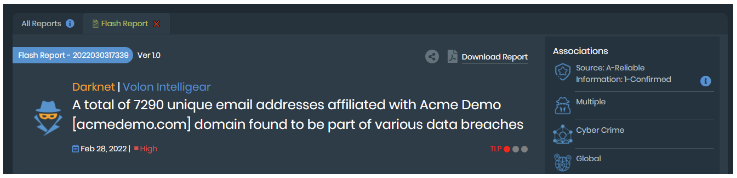
   The following message is displayed:



7. Click *OK*.
8. Retrieve the report. See Retrieving downloads on page 117.

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.



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.

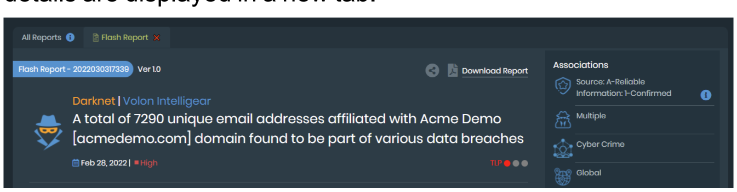
Only recipients who have a FortiRecon account can access reports through a shared link.

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

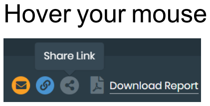
- *TLP Red*: The report cannot be shared outside of your organization and should be restricted only to personnel who need to know.
- *TLP Amber*: The report can only be shared with members of your organization and clients who need to know the information to protect themselves.
- *TLP Green*: The report 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.



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.

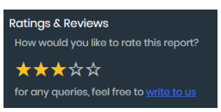
You cannot share Executive Summaries.

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.
   

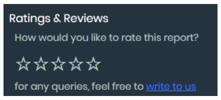
3. Click the star that corresponds to your rating out of five.
   Your rating is saved, and you can change it at any time by selecting a different star.

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*.



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:

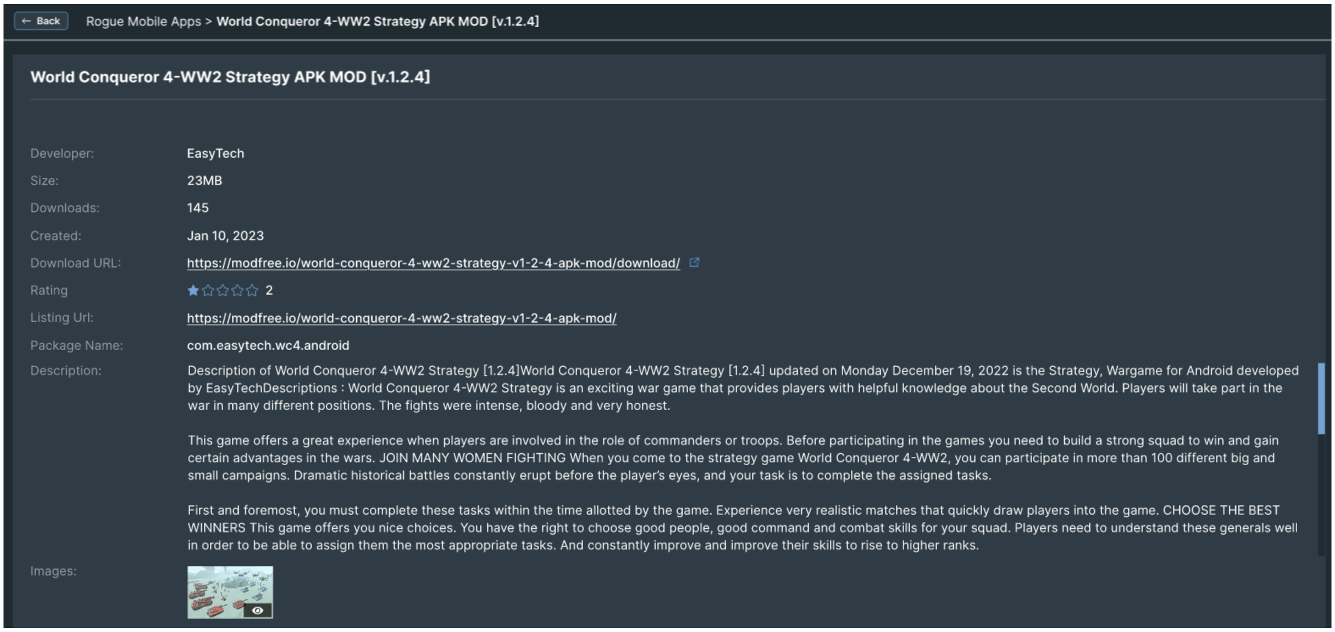
- View information on monitored applications. See Reviewing rogue applications on page 60.
- Filter for specific mobile applications. See Filtering rogue applications on page 61.
- Add official applications. See Adding official applications on page 61.
- Assign an app status. See Assigning application status on page 63.
- Initiate takedown of a rogue application. See Taking down rogue apps on page 63.
- Export information on applications. See Exporting rogue applications on page 64.

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 61.
4. Select the application you want to review. The app information is displayed in a new tab.



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:

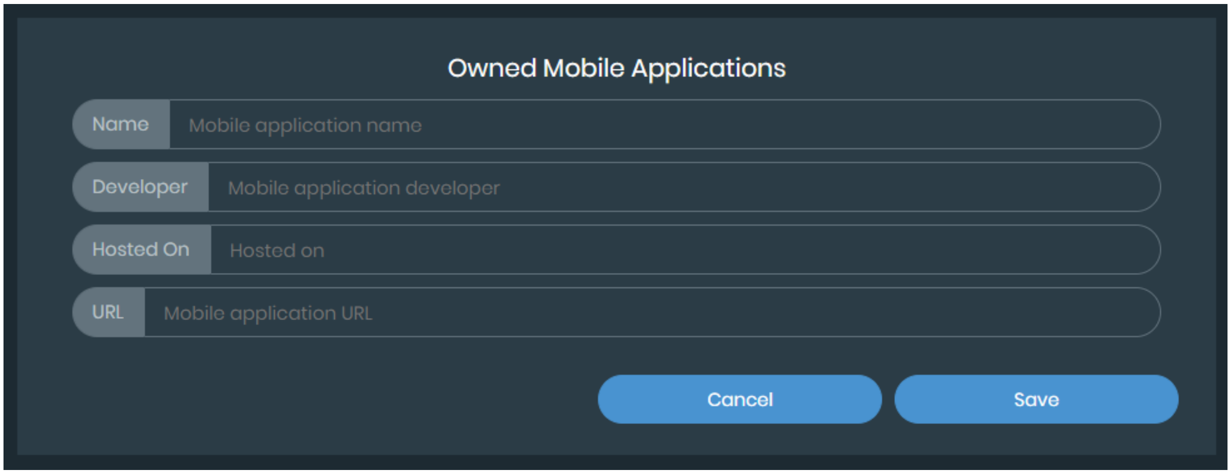
1. Go to *Brand Protection* > *Rogue Mobile Apps*.
2. Filter reports by a date range:
   a. Click *Filter By Date Range*. Two calendars are displayed.
   b. In the left calendar, select a month, year, and day to specify the start date of the range.
   c. In the right calendar, select a month, year, and 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

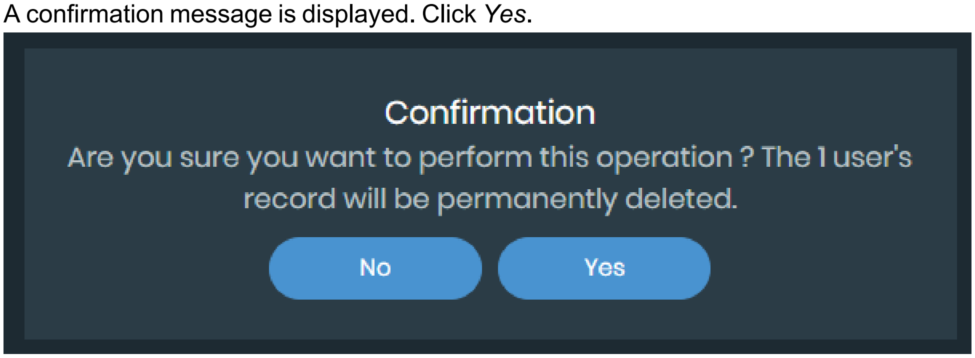


5. You can also add official applications in bulk by uploading excel (XLS) file containing application information including application name, mobile app developer, hosted on and app URL.
   a. Click Upload XLS icon.
   b. Browse and select the file. Click *Open*.

   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*.



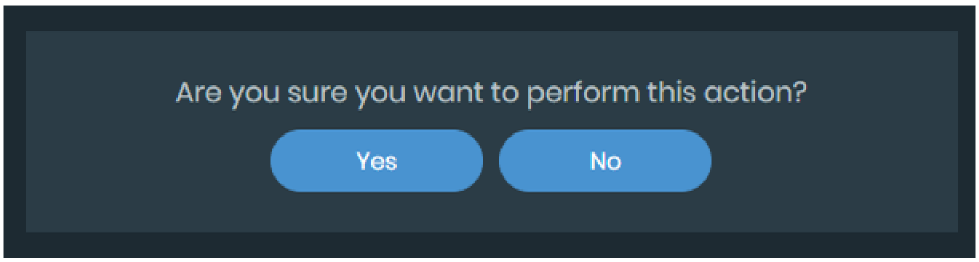
Assigning application status

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.



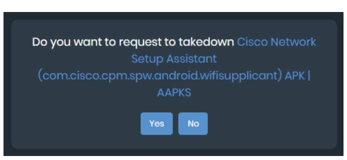
3. Click *Yes*.

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 63.
3. Click *Takedown*. A confirmation message is displayed.



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

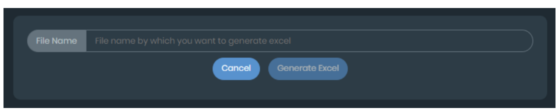
Exporting rogue applications

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

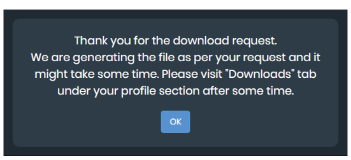
- App name and size
- Description
- Developer name and URL
- Download count and URL
- Date the app was discovered
- Listing URL
- Package name
- Source name
- Status

To export rogue application details:

1. Go to *Brand Protection > Rogue Mobile Apps*.
2. Set the desired filters. See Filtering rogue applications on page 61
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.



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.

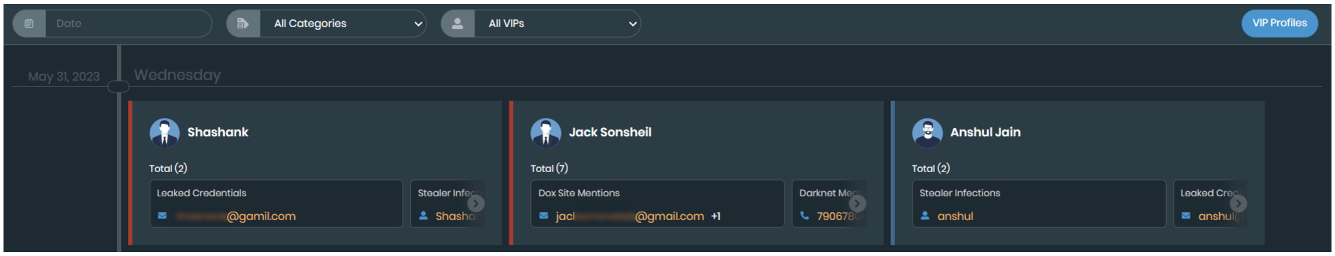
VIP Monitoring

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 65.
- Filter the list of VIP profile threats. See Filtering VIP profile threats on page 66.
- Add official VIP profiles. See Adding VIP profiles on page 66.

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



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.

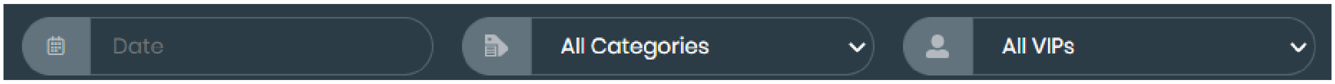
Threat Category	Description
Leaked credentials	Instances where the VIP's credentials have been exposed or compromised.
Telegram Mentions	References or discussions related to the VIP on the Telegram messaging platform.
Dox Site Mentions	Mentions or references of the VIP on websites known for sharing personal 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.

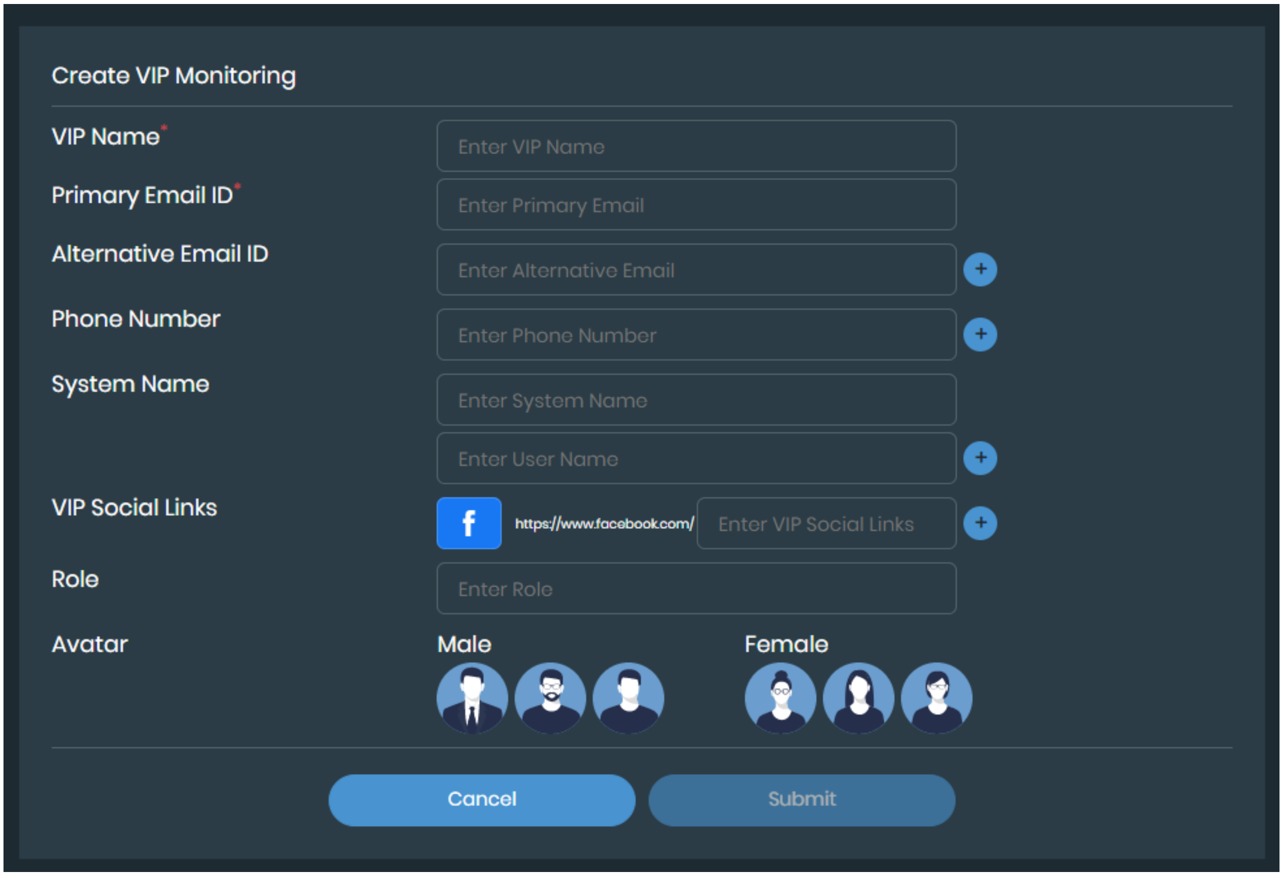
Adding VIP profiles

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*.

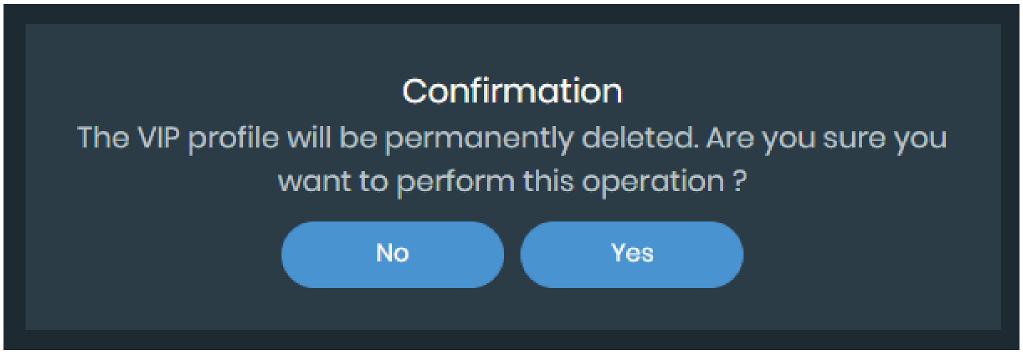


To edit a VIP profile:

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*.



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 68.
- Take action against the discovered attributes. See Managing attributes on page 68.
- Filter attributes. See Filtering attributes on page 69.

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 70.
- Take action against discovered files. See Managing files on page 70.
- Filter files. See Filtering files on page 71.

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 72.

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:
   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 requests 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 *Ticket* number, and press *Enter*.
   The requests are filtered to display only requests with the keyword.
   b. 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:
   a. *Requested*: You have requested that the fraudulent product be taken down.
   b. *Acknowledged*: The FortiRecon team has acknowledged that they have received the request for takedown.
   c. *Work In Progress*: The FortiRecon team is currently working on taking down the fraudulent product.
   d. *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 73.
Reports	Displays all the intelligence reports available to you. See Reports on page 77.
Card Fraud	Displays information about credit or debit cards that are for sale on darknet marketplaces. See Card Fraud on page 83.
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 85.
OSINT - Cyber Threats	Displays OSINT-based intelligence reports about threat events. See OSINT Cyber Threats on page 89.
Vulnerability Intelligence	Displays information on monitored CVEs. See Vulnerability Intelligence on page 93.
Ransomware Intelligence	Displays information on total and potential ransomware incidents. See Ransomware Intelligence on page 97.
Vendor Risk Assessment	Displays information on a vendor watchlist and the vendor's security hygiene. See Vendor Risk Assessment on page 102.
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 106.

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 74.
- View your organization's risk exposure. See Viewing risk exposure summary on page 74.
- View global threat reports. See Viewing global threat report summary on page 75.

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*.

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

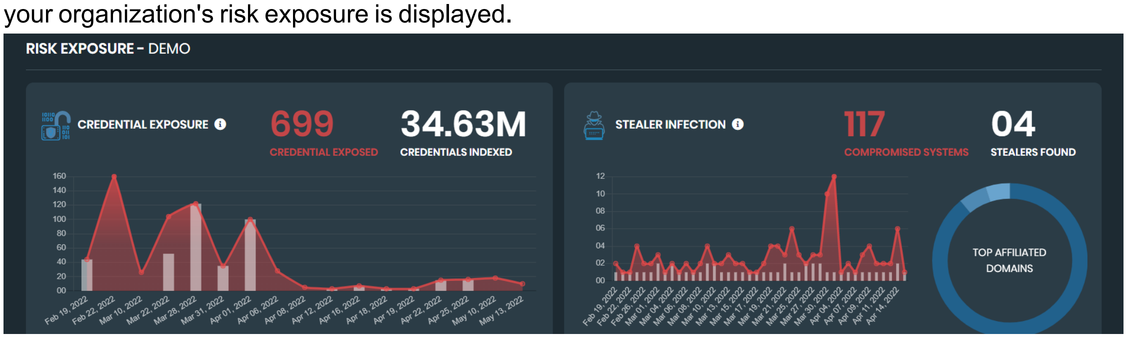
Viewing risk exposure summary

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. Hover your mouse over a dot on the chart to view the number of exposed email addresses on a specific date.
Stealer Infection	Displays data from potentially infected systems that are affiliated with your employees or end-users and are for sale on credential stealer marketplaces on the darknet. The number of compromised systems and the number of stealers found are displayed. Hover your mouse over a dot on the chart to view the number of compromised systems on a specific date. Hover your mouse over a section of the *Top Affiliated Domains* circle to view the name of the affiliated domain.
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.

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 77.
- Apply filters to the list of reports to hone in on specific reports. See Filtering reports on page 79.
- Download a PDF of reports. See Downloading reports and observables on page 80.
- Share reports. See Sharing reports on page 81.
- Export observables to Microsoft Excel format. See Exporting observables on page 82.

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 79.

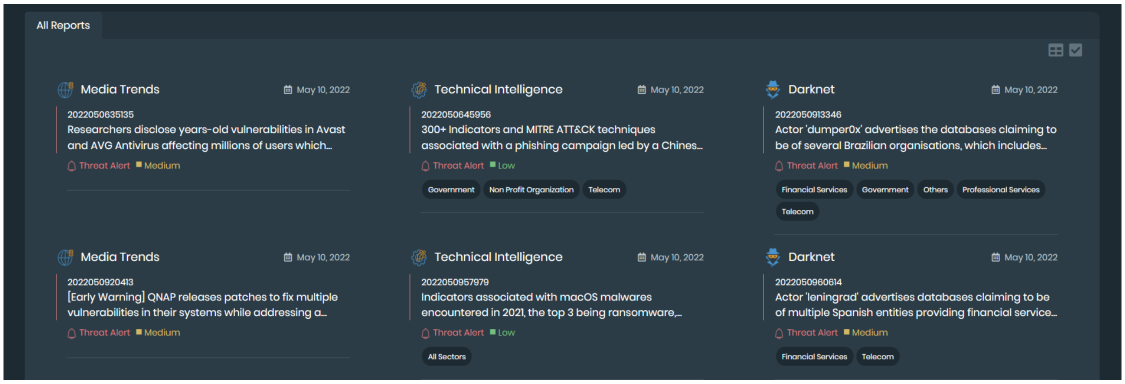
When you open a report, its details are displayed on a separate tab, and you can download a PDF of the report, share the report with another person, and access related reports. When the report contains associated observables, you can download them in Microsoft Excel format.

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.

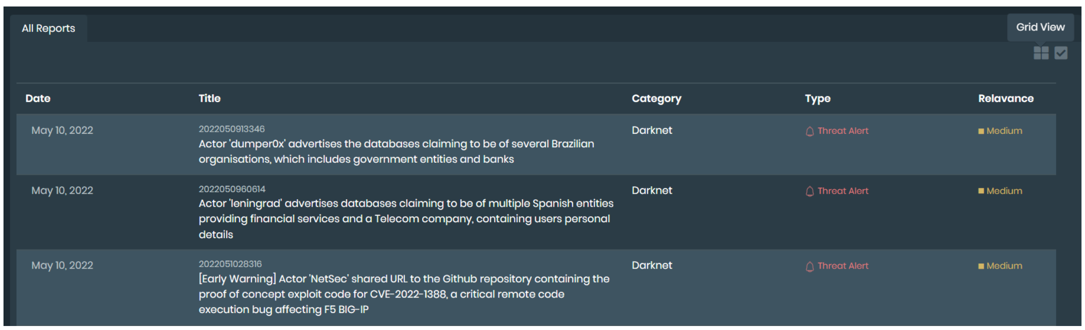
See also Rating reports on page 59.

To view reports:

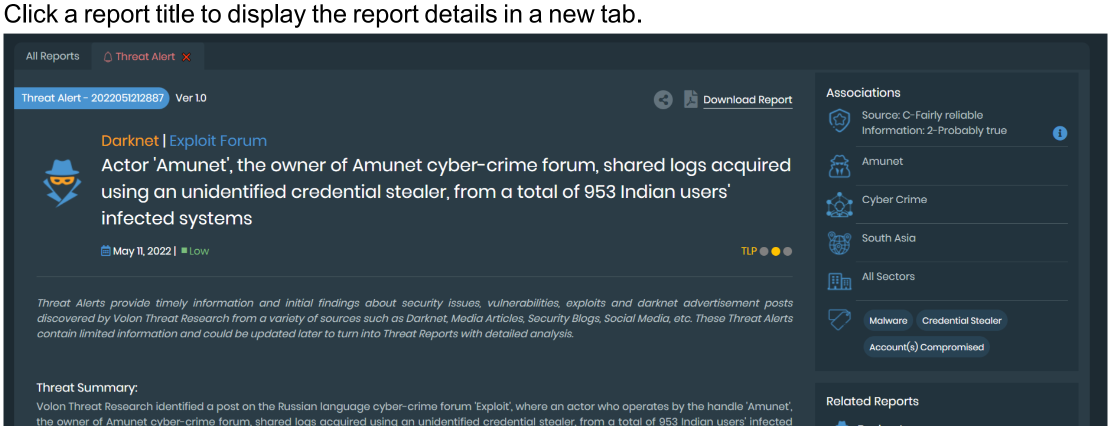
1. Go to *Adversary Centric Intelligence* > *Reports*. All reports are displayed in the *All Reports* tab.



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*.



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



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:

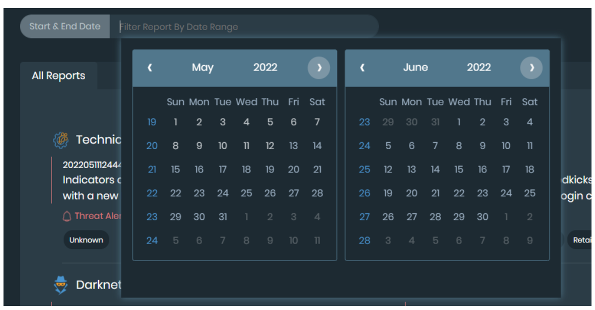
- View a list of reports related to the open report.
- Click a related report to open it in a new tab.
- Click a tag to return to the *All Reports* tab to view the list of reports filtered on the selected tag.

Filtering reports

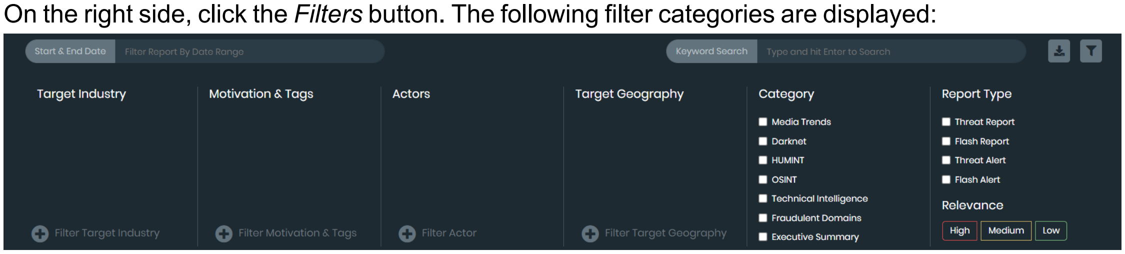
Reports can by filtered by date range, keywords, categories of filters, and relevance to your organization.

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.

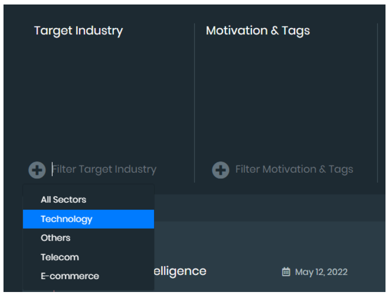


   b. In the left calendar, select a month, year, and day to specify the start date of the range.
   c. In the right calendar, select a month, year, and day to specify the end date of the range.
   Only reports from the date range are displayed.
   d. Click the *Filter Report by Date Range* box, and click *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

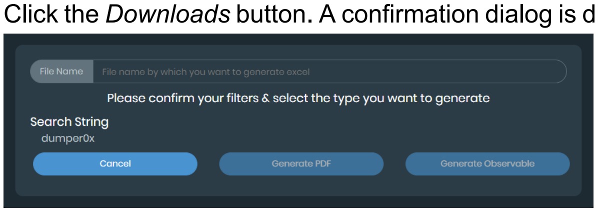
You can download a PDF of the reports displayed on the *Adversary Centric Intelligence* > *Reports* page to your hard drive. A maximum of 300 reports can be downloaded at one time.

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

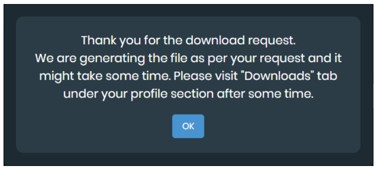
When you open a report, you can download a PDF of the open report.

To download reports:

1. Go to *Adversary Centric Intelligence* > *Reports*.
2. Filter the reports. See Filtering reports on page 79.
   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.

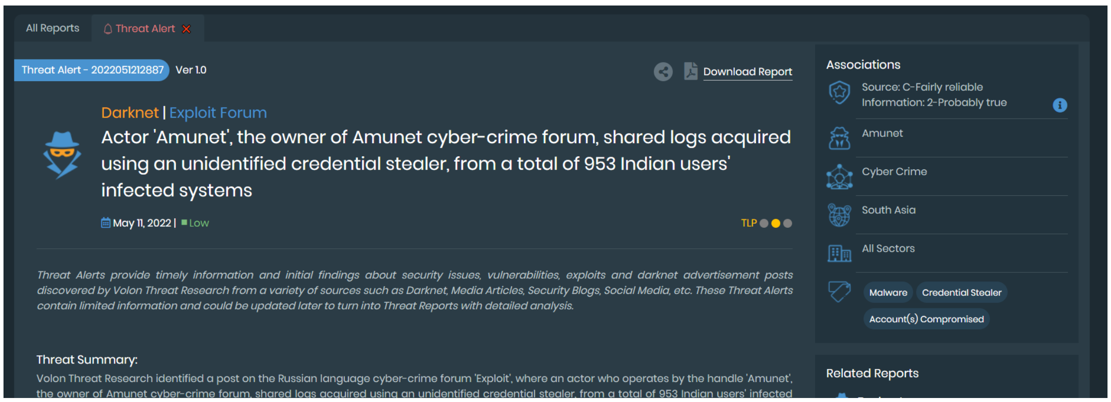


5. In the *File Name* box, type a name.

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.
   

8. Click *OK*.
9. Retrieve the download. See Retrieving downloads on page 117.

To download a PDF from an open report:

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

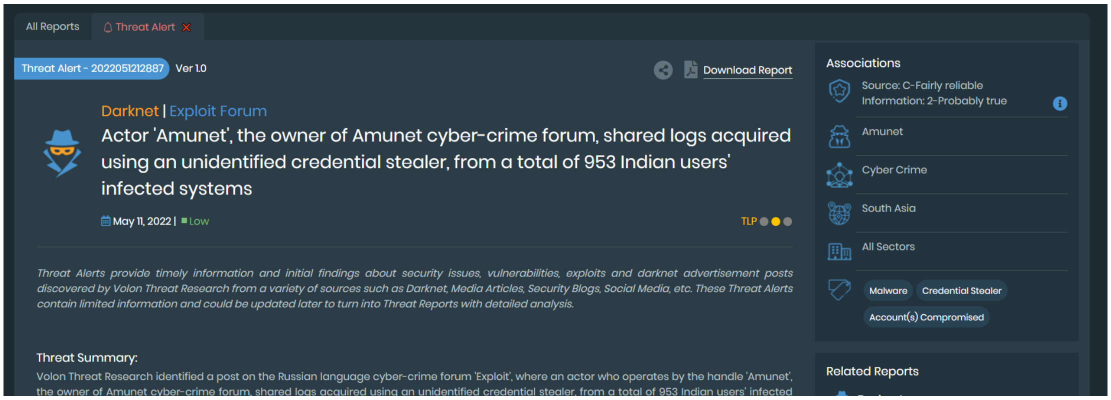
3. Click the *Download Report* button.
   A PDF of the report is downloaded to your computer.

Sharing reports

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

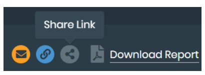
To share a report:

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



3. Click the *Share Link* button.

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



Exporting observables

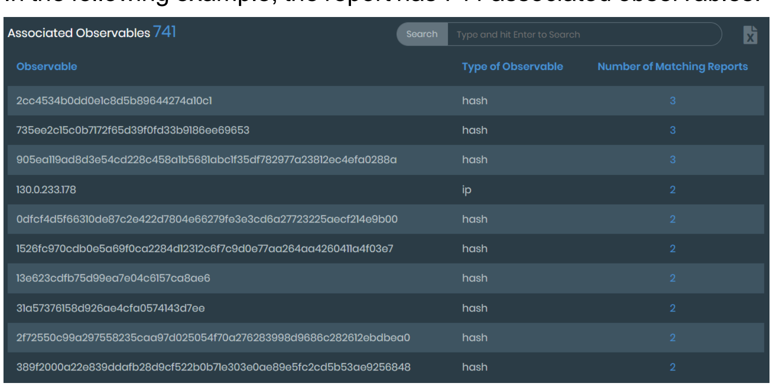
When a report has associated observables, they are displayed at the bottom of the report in the *Associated Observables* section.

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 77.
2. Scroll down to the *Associated Observables* section.

   In the following example, the report has 741 associated observables:

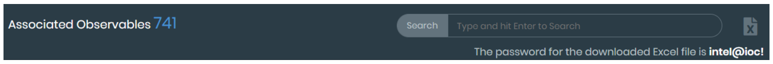


Associated Observables 741

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 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 83.
- Filter the information. See Filtering leaked card information on page 84.
- Download the list of leaked cards to Microsoft Excel format. See Exporting a list of leaked cards on page 84.

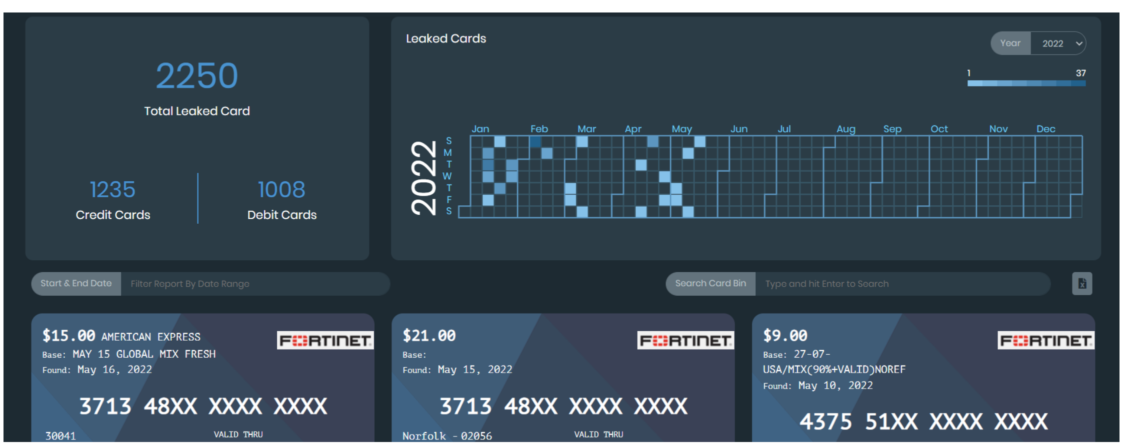
Viewing leaked card information

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.



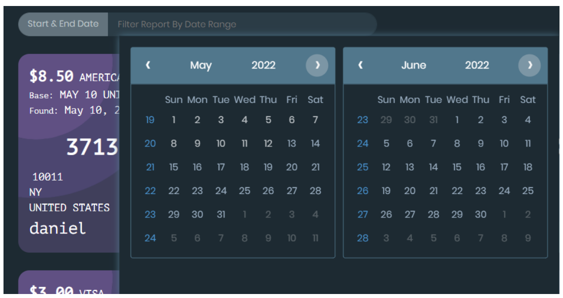
2. You can filter the displayed information. See Filtering leaked card information on page 84.

Filtering leaked card information

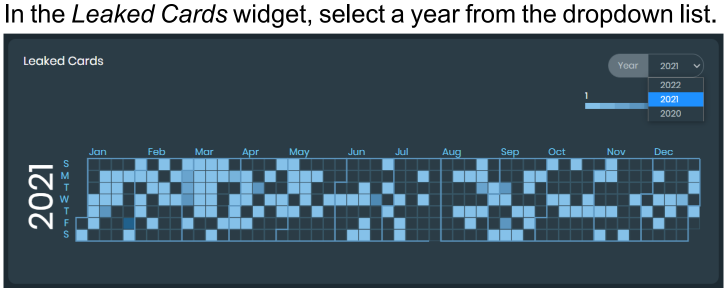
You can filter information about leaked cards by year, date range, and bank identification number (BIN).

To filter leaked card information:

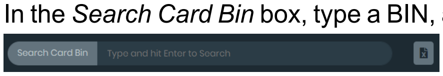
1. Go to *Adversary Centric Intelligence* > *Card Fraud*.
2. Filter reports by a date range:
   a. Click *Filter Report by Date Range*. Two calendars are displayed.



   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*.

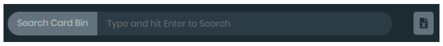


Exporting a list of leaked cards

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.

On the *Stealer Infection* page, you can:

- View information about stealer infections. See Viewing stealer infection information on page 85.
- Filter stealer infection information. See Filtering stealer infection information on page 86.
- Export market place data. See Exporting market place data on page 87.
- Move affiliated domains to the hidden tab. See Hiding affiliated domains on page 88.
- Unsubscribe from affiliated domain notifications. See Unsubscribing from affiliated domain notifications on page 88.

Viewing stealer infection information

The *Adversary Centric Intelligence* > *Stealer Infections* 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 stealer infection information:

1. Go to *Adversary Centric Intelligence* > *Stealer Infections*. The *Stealer Infections* page is displayed.

2. Use the following widgets to review information about stealer infections:

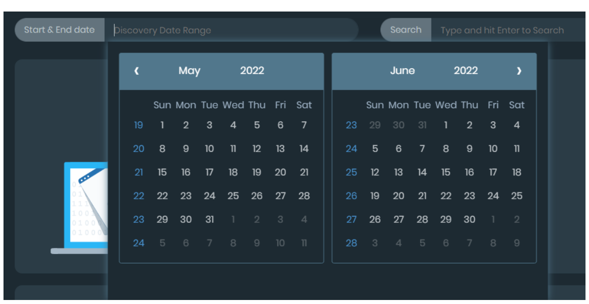
Total compromised systems affiliated with <organization name>	Displays the total number of compromised systems affiliated with your organization.
Stealers Found	Display the number of stealers found and the names of the stealers.
Latest	Displays the latest number of stealer events and the date that the event was discovered.
Market Place Calendar	Displays a summary of the 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.
Affiliated Domains	Lists the domain names affiliated with the stealer events and the number of affected systems. Click the *Click to Hide* icon to move the affiliated domain to the hidden tab.
Systems Infected	Displays a list of infected systems. Expand the affiliated domain to view a list of identified sites.

Filtering stealer infection information

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

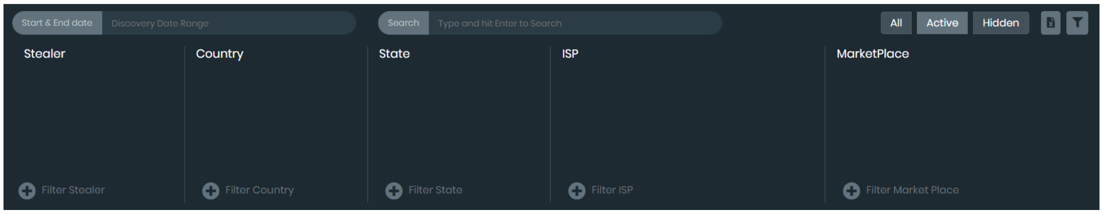
To filter stealer infection information:

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



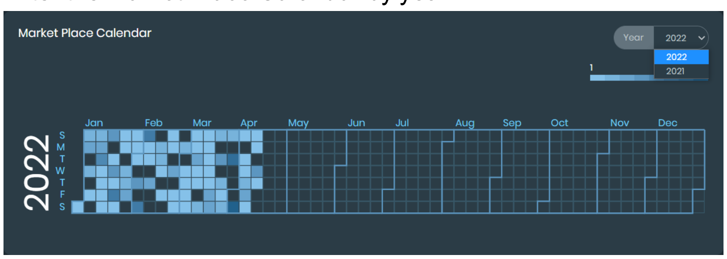
    b. In the left calendar, select a month, year, and day to specify the start date of the range.
    c. In the right calendar, select a month, year, and day to specify the end date of the range.
    Only information from the date range is displayed.
    d. Click the *X* in the *Start & End Date* box to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

4. Click *All*, *Active*, or *Hidden* to use those filters.
   For example, click *Hidden* to display only information from the hidden tab.
5. Filter reports by categories:
   a. On the right-side, click the *Filters* button. The following filter categories are displayed:



   - *Stealer*
   - *Country*
   - *State*
   - *ISP*
   - *MarketPlace*

   b. Click *Filter <category>* , and select one or more filters.
6. Filter the *Market Place Calendar* by year:



Exporting market place data

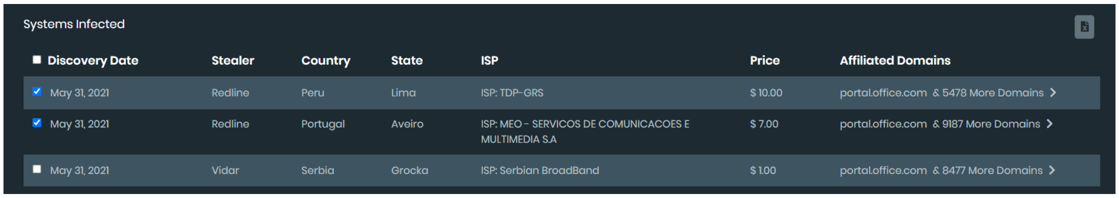
You can download all the market place information to download an *All Market Place.xlsx* file in Microsoft Excel format. Alternately you can limit the export to infected systems and download a *Market Place.xlsx* file.

To export market place:

1. Go to *Adversary Centric Intelligence* > *Stealer Infections*.
2. (Optional) Filter the data. See Filtering stealer infection information on page 86.
3. Click the *Export to Market Place* button.
   An *All Market Place.xlsx* file is downloaded.

To export infected systems:

1. Go to *Adversary Centric Intelligence* > *Stealer Infections*, and scroll down to the *Systems Infected* widget.
2. Select the checkmark for the systems to include in the export. The *Export Market Place* button becomes available.



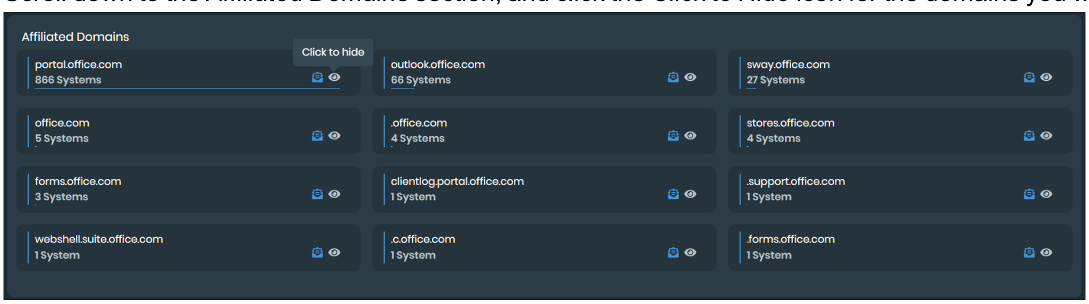
3. Click the *Export to Market Place* button.
   A *Market Place.xlsx* file is downloaded.

Hiding affiliated domains

You can move affiliated domains to the *Hidden* tab. You can view the *Hidden* tab by clicking *Hidden* at the top-right of the page.

To hide affiliated domains:

1. Go to *Adversary Centric Intelligence* > *Stealer Infections*.
2. Scroll down to the *Affiliated Domains* section, and click the *Click to Hide* icon for the domains you want to hide.



   The domain is moved to the hidden tab.

Unsubscribing from affiliated domain notifications

You can unsubscribe from affiliated domain notifications.

To unsubscribe from affiliated domain notifications:

1. Go to *Adversary Centric Intelligence* > *Stealer Infections*.
2. Scroll down to the *Affiliated Domains* section, and click the *Click to Unsubscribe and Stop Email Notifications* icon.

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:

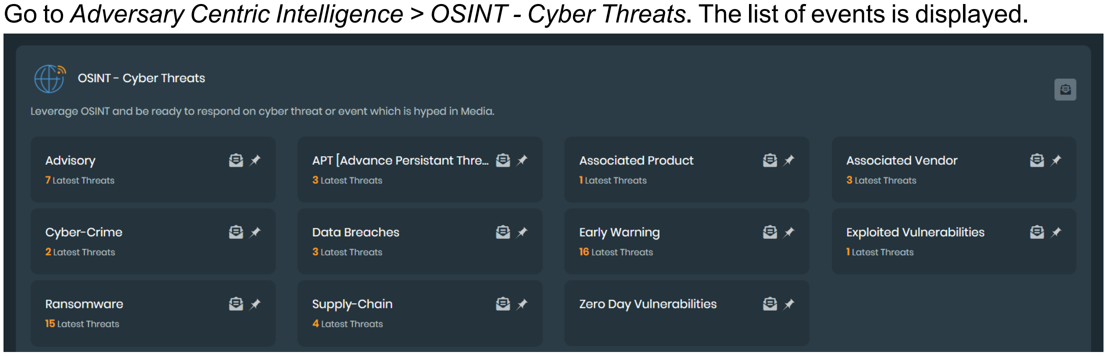
- Review threat events. See Reviewing threats on page 89.
- Pin threat events to the top of the list. See Pinning events on page 90.
- Subscribe to threat event notifications. See Subscribing to event notifications on page 91.
- Subscribe other FortiRecon users to event notifications. See Adding subscriptions on page 92.

Reviewing threats

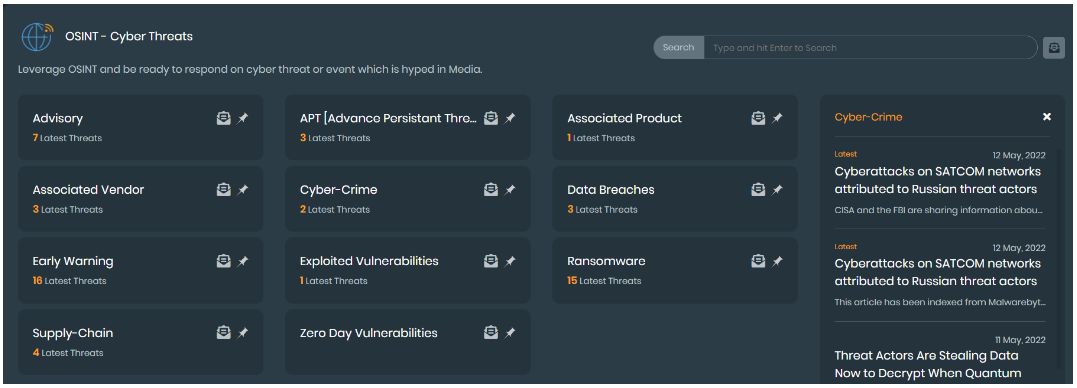
You can view more information about each threat.

To review threats:

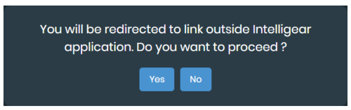
1. Go to *Adversary Centric Intelligence* > *OSINT - Cyber Threats*. The list of events is displayed.



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:



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



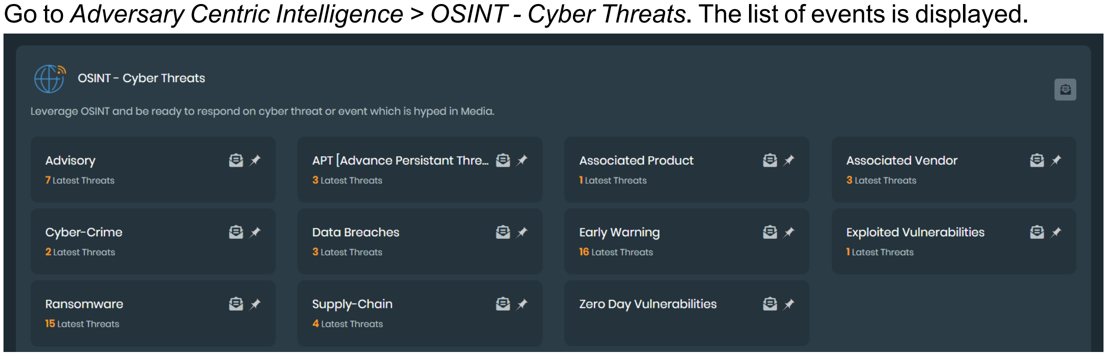
4. Click *Yes* to open the link in a new tab in your browser.

Pinning events

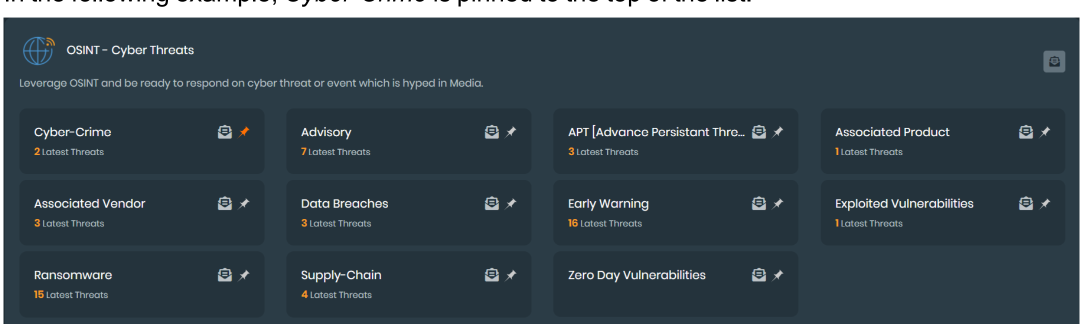
You can pin events to the top of the list. Pinned events have an orange *Pin* icon. Unpinned events have a white *Pin* icon.

To pin events:

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



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.



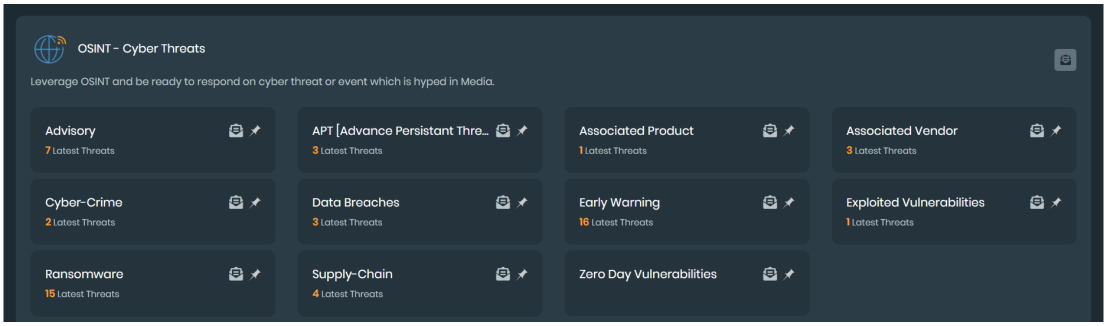
   Click the *Pin* icon again to turn the pin white and unpin the event from the top of the list.

Subscribing to event notifications

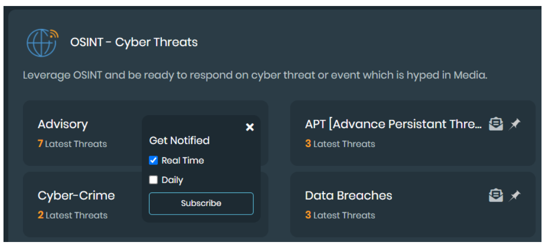
You can enable subscriptions to receive notifications for one or more threat events. You can also change subscriptions and unsubscribe.

To subscribe to event notifications:

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



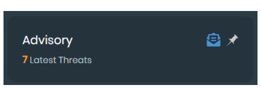
2. For an event, click the *Subscribe* icon. The subscription options are displayed for the event.
   In the following example, subscription options are displayed for the *Advisory* event:



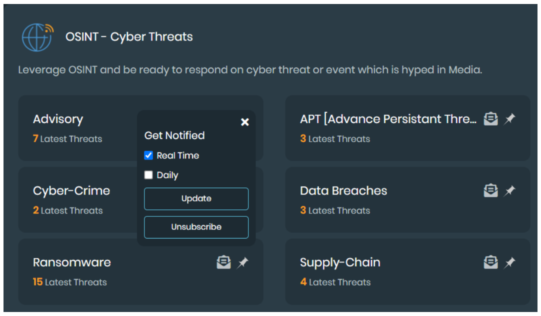
3. Select one of the following options to specify when to receive the notification:

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.



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.


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

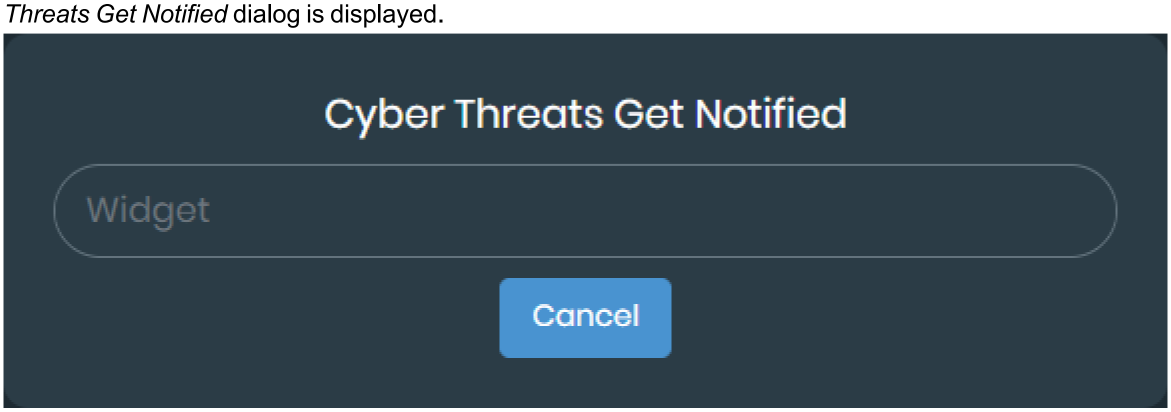
To unsubscribe from event notifications:

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.

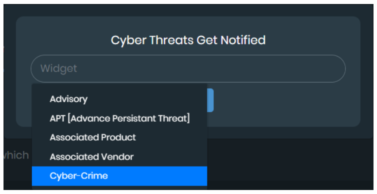
Adding subscriptions

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

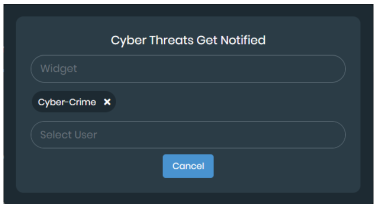
To add subscriptions:

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


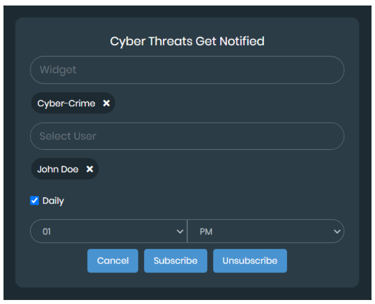
2. Click the *Widget* box, and select the threat events.
   In the following example, *Cyber-Crime* is selected.



The *Select User* box is displayed.



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



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:

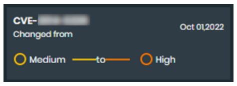
- Review known CVEs. See Vulnerability exposure on page 93.
- Review the notable global CVEs. See Global notable vulnerabilities on page 95.
- View specific CVE reports. See Viewing and filtering CVE reports on page 95.
- Export a list of CVEs. See Exporting CVEs on page 97.
- Bulk add CVEs to monitor. See Manually adding CVEs on page 97.

Vulnerability exposure

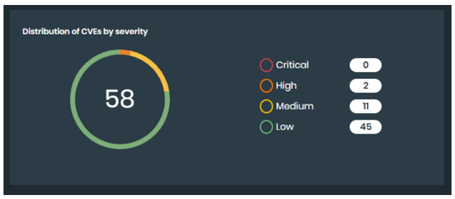
Monitored CVEs can be reviewed at a high level from the *Adversary Centric Intelligence* > *Vulnerability Intelligence* page in the *Vulnerability exposure* section:

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

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



- *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*.

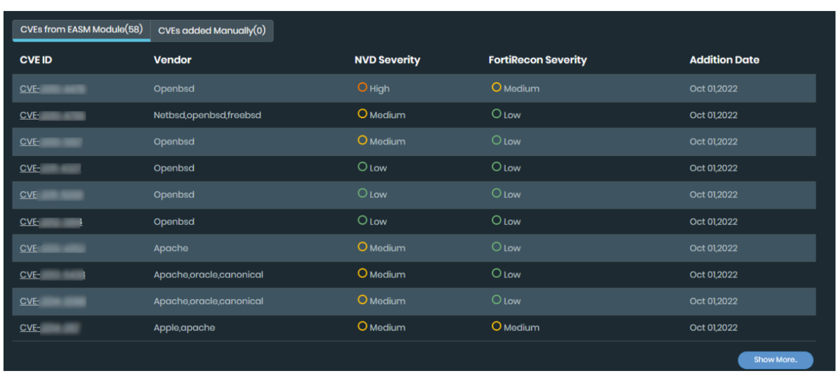


- *Top 10 vendors by CVEs*: Displays a list of the vendors with the most CVEs monitored and the severity range from *Low* to *Critical*. Select a *Vendor Name* or *Severity* to view more information.

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.



CVEs from EASM Module(58) CVEs added Manually(0)

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

Show More..

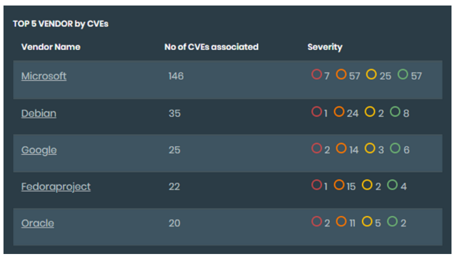
- *CVEs added Manually*: Displays a list of CVEs added by the user.

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.

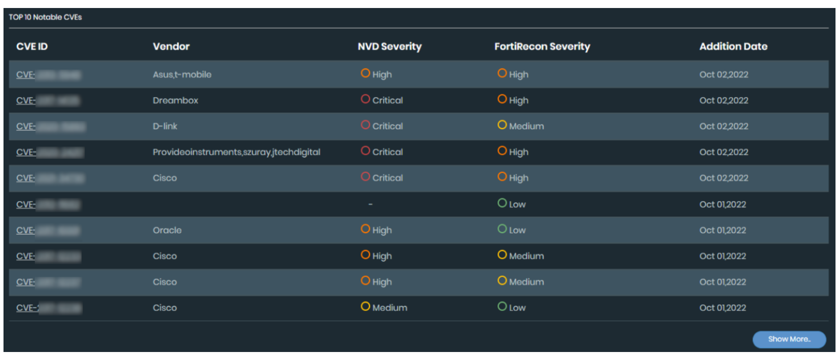
- *Top 5 vendors by CVEs*: Displays a list of the vendors with the most notable CVEs monitored and the severity range from *Low* to *Critical*. Select a *Vendor Name* to view more information.



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

Show More..

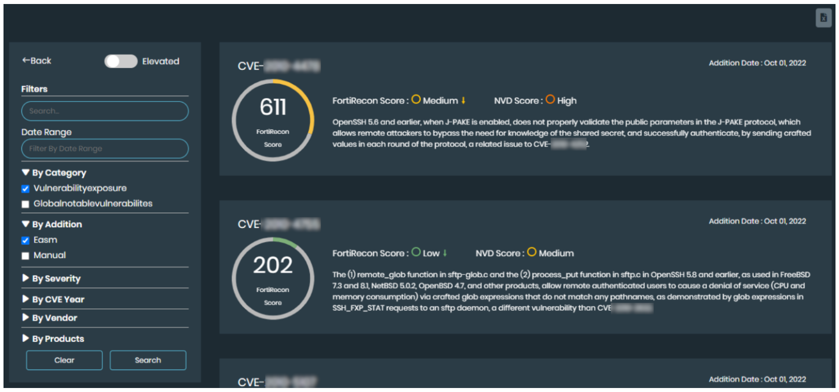
Viewing and filtering CVE reports

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

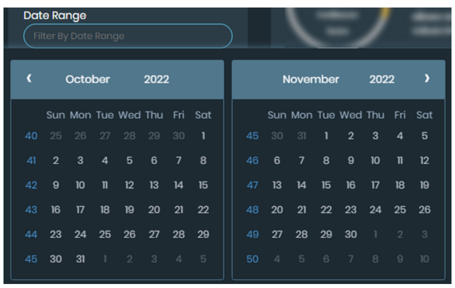
- Selecting the CVE ID from the *Vulnerability exposure* > *CVEs from EASM Module* and *CVEs added Manually* tabs.
- Selecting the CVE ID from the *Global notable vulnerabilities* > *Top 10 Notable CVEs*.
- Filtering the vendor reports from *Vulnerability exposure* > *Top 10 vendor by CVEs* or *Global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



3. Filter information by a date range:
   a. Click *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.
   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:

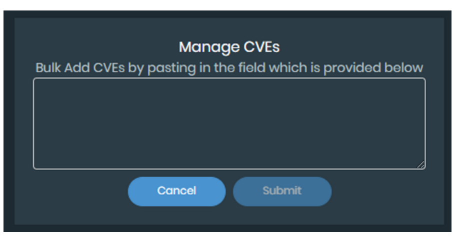
1. Go to *Adversary Centric Intelligence* > *Vulnerability Intelligence*.
2. Select a *Vendor Name* or the *Show More* button. The CVE cards page is displayed.
3. Filter for the reports you want included in the Excel file. See Viewing and filtering CVE reports on page 95.
4. Click *Export CVE List*. 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.



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. From the *Ransomware Intelligence* page, you can:

- View past and potential ransomware incidents. See Viewing ransomware intelligence on page 98.
- Filter ransomware incident information. See Filtering ransomware intelligence on page 99.

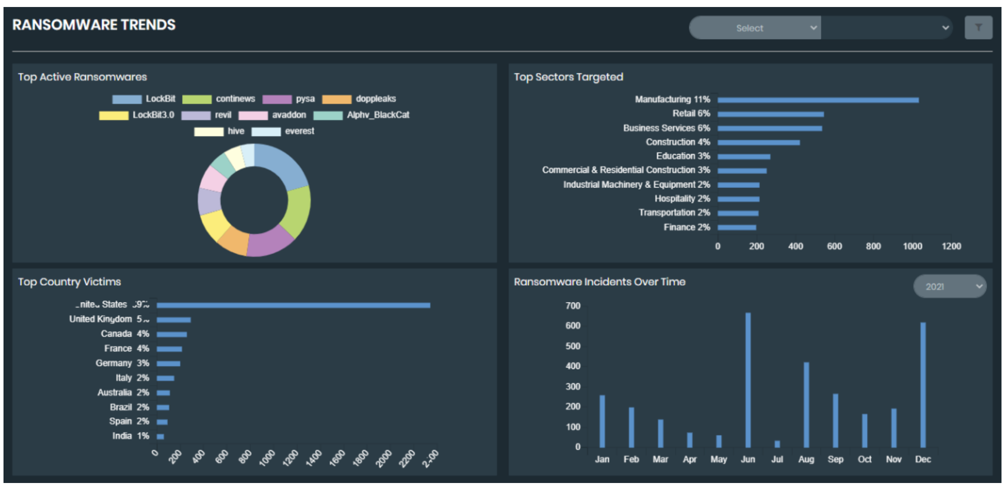
- Export information on ransomware incidents to an Excel file. See Exporting ransomware information on page 100.
- Create, edit, and monitor a ransomware watchlist. See Managing My Watchlist on page 101.

Viewing ransomware intelligence

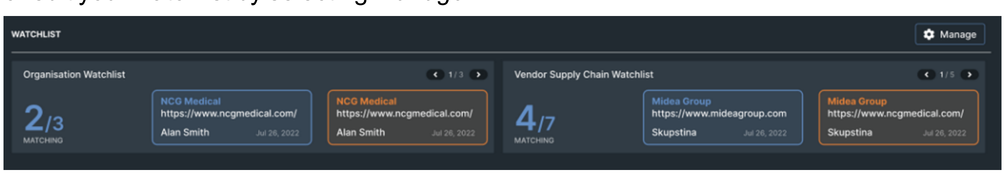
The *Ransomware Intelligence* page contains multiple sections that display high level information on the ransomware threat landscape. Sections include:

- *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*.

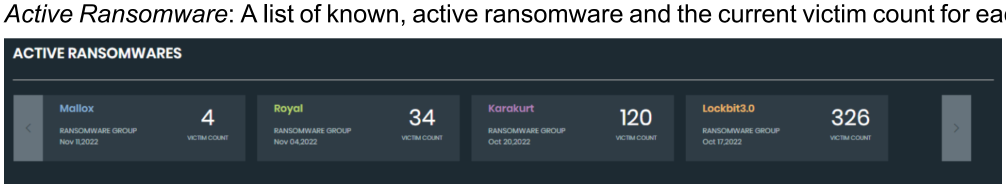
- *Ransomware Trends*: Graphical representations of ransomware trends, including top targeted sectors and victimized countries. The trends will adjust to reflect a particular trend if a card is selected in the *Summary*.



- *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*.



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



- *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

Show More..

- *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

Show More..

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. Click the filter icon and select how you would like to filter the results:
   - *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 99.
5. Click the *Export List* icon. The file is downloaded to your computer.

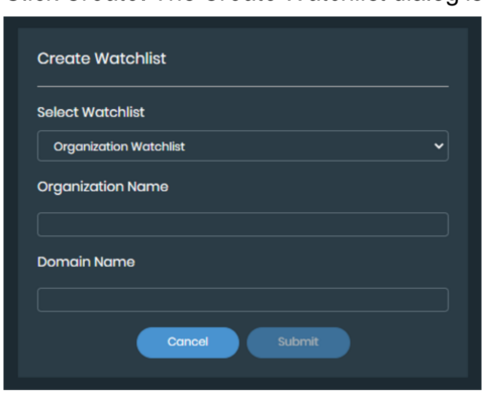
Managing My Watchlist

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 99.

To create a new asset to manage:

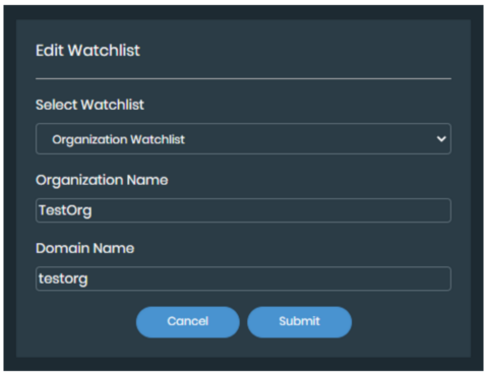
1. Go to *Adversary Centric Intelligence* > *Ransomware Intelligence*.
2. In the *Watchlist* section, click *Manage*. The *My Watchlist* page is displayed.
3. Click *Create*. The *Create Watchlist* dialog is displayed.



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 edit a monitored asset:

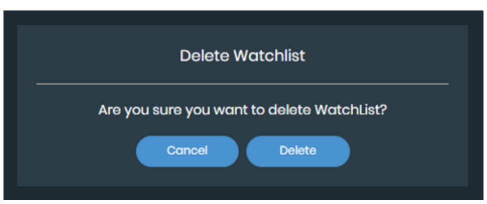
1. Go to *Adversary Centric Intelligence* > *Ransomware Intelligence*.
2. In the *Watchlist* section, click *Manage*. The *My Watchlist* page is displayed.
3. Find the asset you want to edit and click *Edit*. The Edit Watchlist dialog is displayed.



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*. A confirmation dialog is displayed.



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 103.
- View the security hygiene assessment of a vendor. See Viewing the vendor risk assessment on page 103.

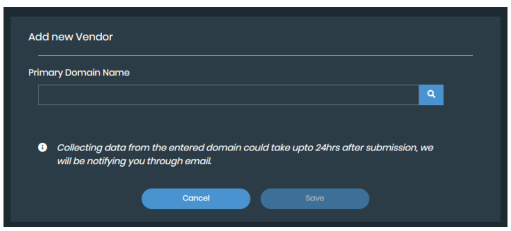
Adding a new vendor to the watchlist

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:

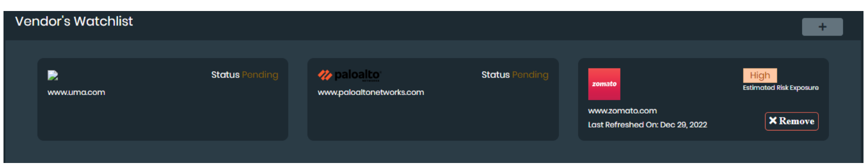
1. Go to *Adversary Centric Intelligence* > *Vendor Risk Assessment*.
2. Click *Add Vendor*. The *Add new Vendor* dialog is displayed.



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

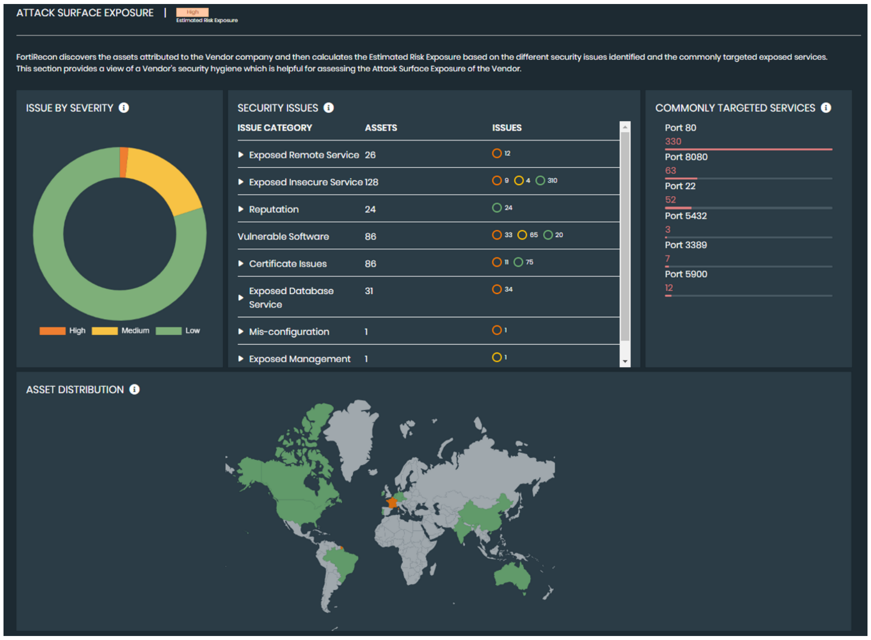
You can have a maximum of 25 individual vendors in the watchlist. To remove a vendor from the watchlist, click *Remove* on its watchlist card.



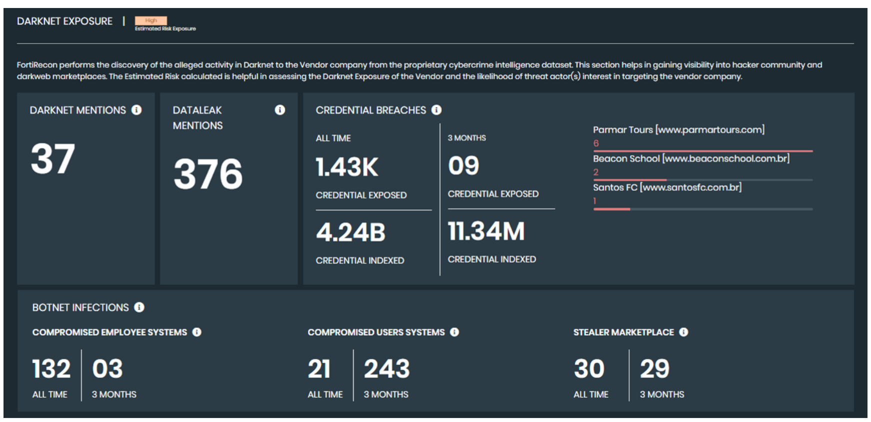
Viewing the vendor risk assessment

The vendor risk assessment organizes the generated vendors data into:

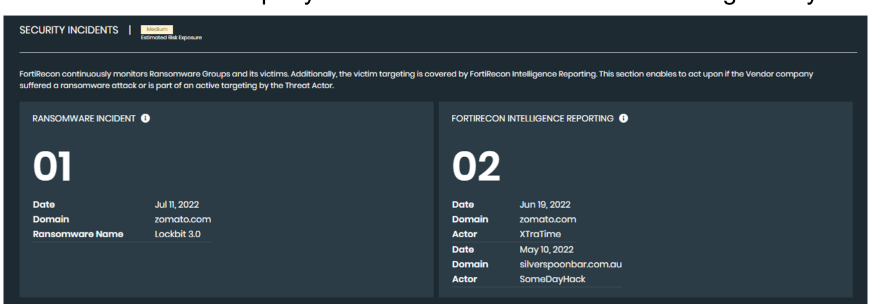
- *Attack Surface Exposure*: Provides an overview of the vendor company's assets and current security hygiene to assess the estimated risk exposure.



- *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.



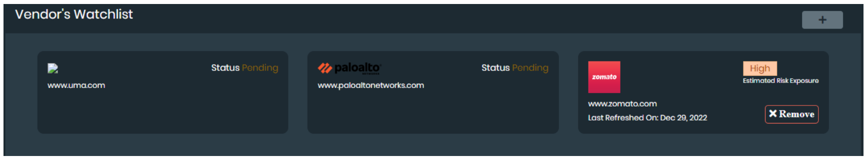
- *Security Incidents*: Provides an overview of ransomware incidences and intelligence reporting so that action can be taken if the vendor company suffers a ransomware attack or is targeted by a threat actor.



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*.

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.

Investigation

The *Adversary Centric Intelligence* > *Investigation* page displays information about investigations into security events. From the *Investigation* page, you can:

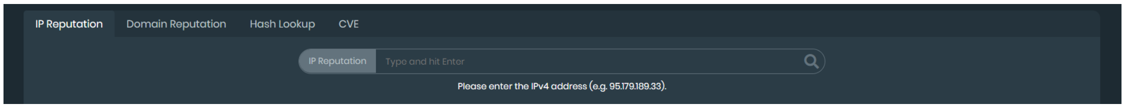
- Review the reputation of IPv4 addresses. See Reviewing IP address reputation on page 106.
- Review the reputation of a domain. See Reviewing domain reputation on page 107.
- Review a file hash. See Reviewing a file hash on page 107.
- Review a CVE. See Reviewing a CVE on page 107.

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.



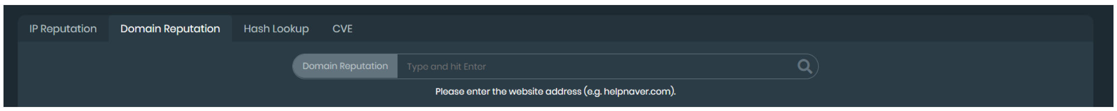
2. Type the IPv4 address, and press *Enter*.

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.



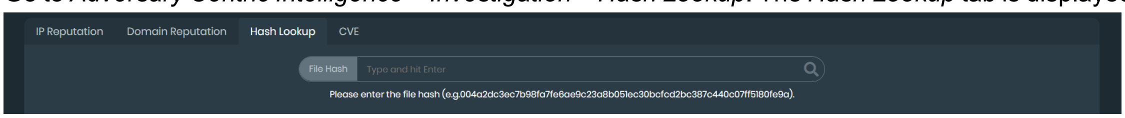
2. Type the domain name, and press *Enter*.

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.



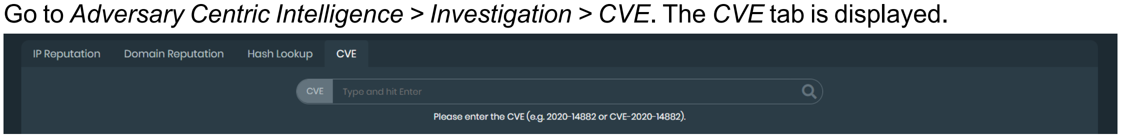
2. Type the file hash, and press *Enter*. The results are displayed.

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.



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 108. 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:

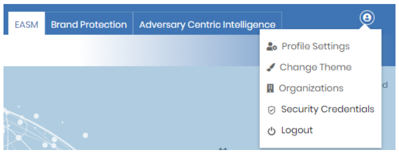
Profile	Displays information about your personal FortiRecon account. You can edit details of your account, configure daily digest reports, and enable custom email alerts. See Profile on page 109.
Users	Displays account information for members of your organization. Administrators can add, edit, and delete user accounts. See Users on page 112
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 115.
Change Password	Allows you to change your personal account password. See Change password on page 116.
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 117.
Integrations	Displays the webhook integrations with Microsoft Teams and Slack. You can create, edit, disable, and delete integrations. See Integrations on page 118.
Seeds	Displays the domains, card BINs, and mobile applications of your organization that are being monitored by FortiRecon. See Seeds on page 121.

Accessing profile settings

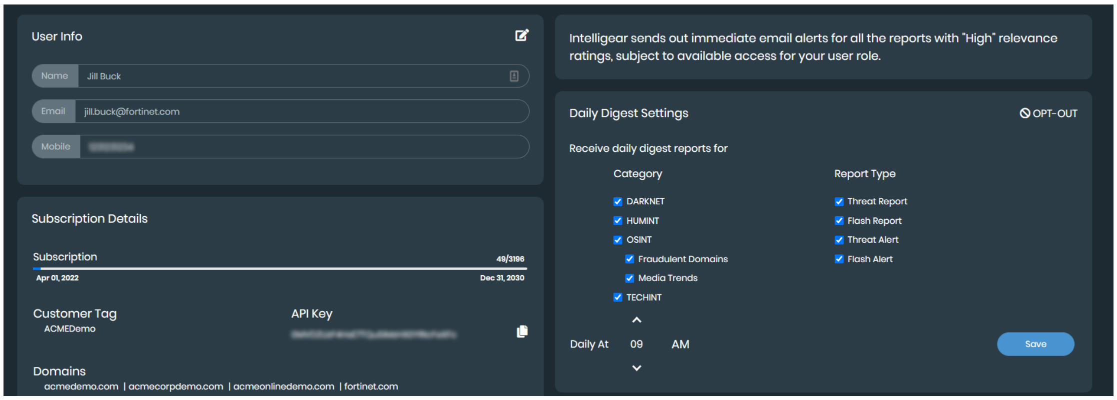
You can access the *Profile Settings* from any page by selecting the menu in the top-right corner.

To access profile settings:

1. Hover over the profile menu in the top-right corner, and select *Profile Settings*.



The *Profile* page is displayed.



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 109.
- Configure daily reports on recent FortiRecon activity. See Opting in to daily digest reports on page 110.
- Opt-out of daily reports on recent FortiRecon activity. See Opting out of daily digest reports on page 110.
- View information about your subscription, such as registered domains, target industries and geography, keywords, and your API key. See Viewing subscription details on page 111.
- Copy your API key for sharing. See Sharing the API key on page 111.
- Configure personalized email notifications when specific keywords occur in FortiRecon reports. See Receiving custom email alerts on page 112.

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 113.

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.

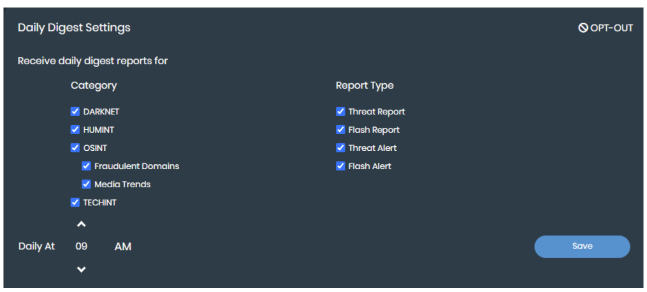
3. Enter new information into *Name*, *Email*, and *Mobile* as needed.
4. Click *Update*. Your personal user information is updated.

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.



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.

Viewing subscription details

Subscription Details provides information on your subscription, including domains, license serial number, contract information, and your API key.

To view subscription details:

1. Go to *Profile Settings* > *Profile*.
2. Scroll to *Subscription Details* to view information on your:
   - Subscription
   - Customer Tag
   - API Key
   - Domains
   - License Serial
   - Keywords
   - Contract
   - Target Industry
   - Target Geography

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 112.
- Add new users. See Adding users on page 113.
- Edit existing users. See Editing users on page 113.
- Delete users. See Deleting users on page 114.

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:

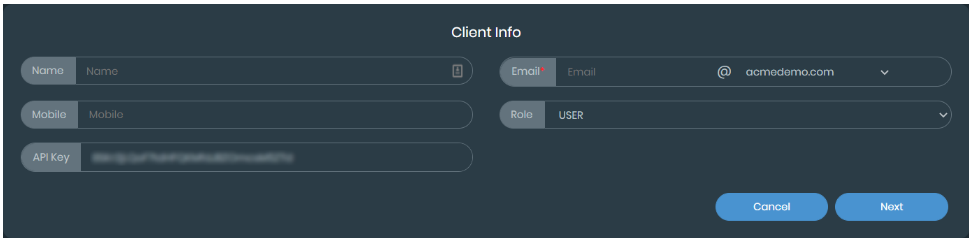
1. Go to *Profile Settings* > *Users*.
2. Search for keywords:
   a. In the *Type and hit Enter to Search* box, type a name or email, and press *Enter*.
      The user accounts are filtered to display only accounts with the keyword.
   b. Click the *X* beside the keyword to remove the filter.

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 115.

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.



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.

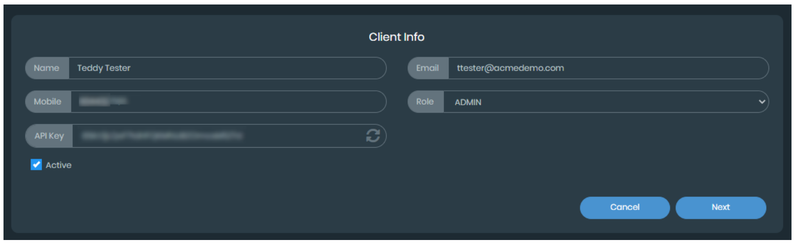
Editing users

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.



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.

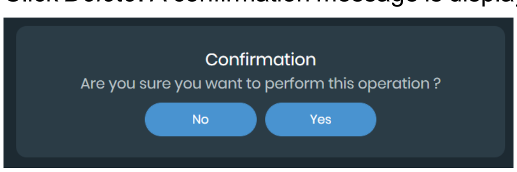
4. Select a new *User Template* from the dropdown, if needed. The *Main Modules*, *Sub Modules*, and *Access* are adjusted to the template's settings.
5. Click *Save*. The user information and access permissions are updated.

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.



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 113

From the *Profile Settings* > *Access Template* page, you can:

- View available access templates. See Viewing access templates on page 115.
- Add a new access template. See Adding a template on page 115.
- Edit an existing access template. See Editing a template on page 116.

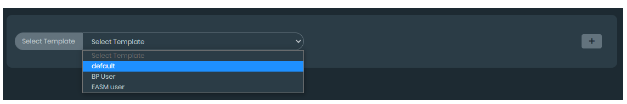
Viewing access templates

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

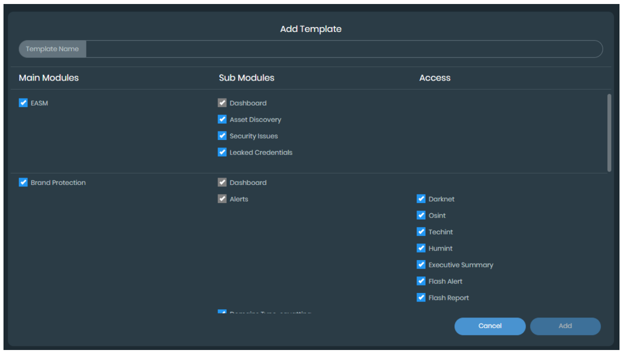
You can create new templates in the *Access Templates* page, and they can include any of the *Main Modules*, specific *Sub Modules*, and *Access* settings.

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.



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.

Change password

You can change your personal account password. The new password must:

- Contain at least one lower case letter
- Contain at least one upper case letter
- Contain at least one special character
- Be at least 10 characters long

To change your password:

1. Go to *Profile Settings* > *Change Password*.
2. Enter your existing password in the *Current password* box.
3. Enter the new password in the *New password* box.
4. Enter the new password again in the *Confirm password* box. The *Set Password* button becomes available.
5. Click *Set Password*. Your password is updated.

Passwords entered into *New password* and *Confirm password* boxes must match. The fields are case sensitive. If the passwords do not match, the *Set Password* button remains unavailable.

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:

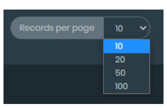
- View all downloads from the past 30 days. See Viewing downloads on page 117.
- Retrieve downloads from the past 30 days. See Retrieving downloads on page 117.
- Delete downloads. See Deleting downloads on page 118.

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:

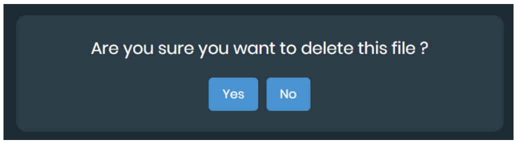
1. Go to *Profile Settings* > *Downloads* and find the file you want.
2. Click the file in the *Download* column. The file is downloaded to your computer.

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.


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 118.
- Create new integrations. See Adding integrations on page 119.
- Edit existing integrations. See Editing integrations on page 120.
- Disable integrations. See Disabling integrations on page 120.
- Delete integrations. See Deleting and disabling integrations on page 120.

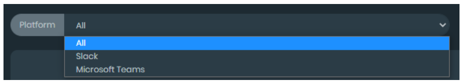
Viewing integration details

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:

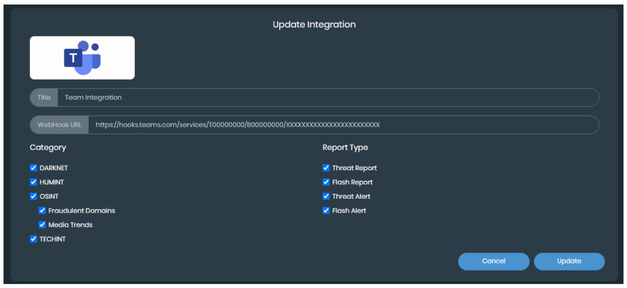
i. Select the *Platform* dropdown. A list of available integration platforms is displayed.



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.



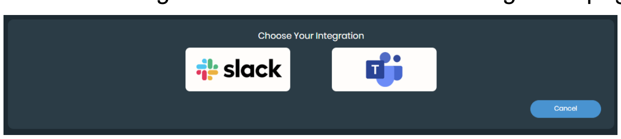
Adding integrations

You can add multiple webhook integrations to your account in FortiRecon.

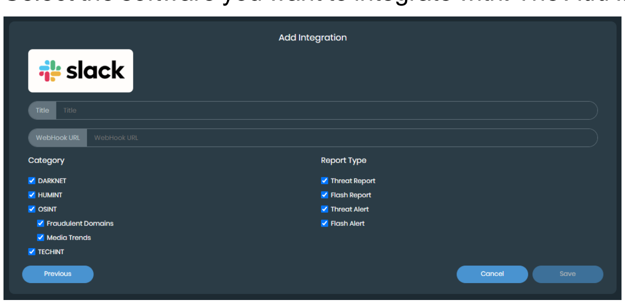
You must retrieve the webhook URL from Microsoft Teams and Slack before adding an integration to FortiRecon. See Microsoft Teams Webhooks and Connectors and Slack API Sending messages using Incoming Webhooks for more information.

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.



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.

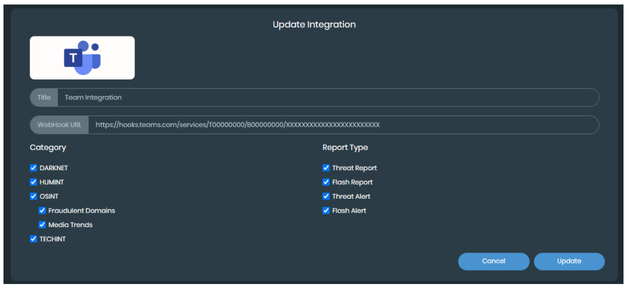
7. Clear any fields that you want to exclude from the integration.
8. Click *Save*. The integration is added.

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.



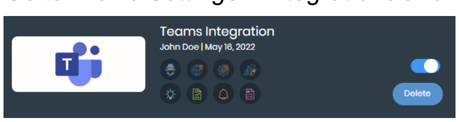
3. Edit the *Title* and *WebHook URL* text boxes, as needed.
4. Select the *Category* and *Report Type* fields that you want to include in the integration.
5. Clear any fields that you want to exclude from the integration.
6. Click *Update*. The webhook integration is updated.

Disabling integrations

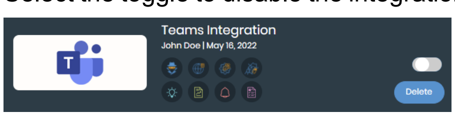
You can temporarily disable unused integrations, and then enable them again in the future. The integration toggle allows you to enable and disable an integration as needed.

To disable an integration:

1. Go to *Profile Settings* > *Integrations* and find the integration.



2. Select the toggle to disable the integration. The notifications are no longer sent to the software.

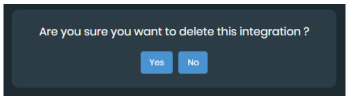


3. Select the toggle again to enable the integration.

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.


3. Click *Yes*. The integration is deleted.

Seeds

You can input your organization's information in the *Seeds* page to enable FortiRecon to track any malicious activity against your assets or impersonating your assets.

From the *Profile Settings* > *Seeds* page, you can:

- View your organization's registered assets. See Viewing your assets on page 121.
- Download a sample Microsoft Excel file to determine the format needed to upload data. See Downloading a sample data file on page 122.
- Upload a Microsoft Excel file to simultaneously upload your organization's data in bulk. See Uploading a data file on page 122.
- Export a global master file containing all of your organization's registered assets. See Exporting global masters on page 123.
- Add, edit, and delete domain names. See Domains on page 123.
- Add, edit, and delete all BIN numbers used by your organization to issue credit, debit, and gift cards. See Card BIN on page 125.
- Add, edit, and delete all mobile applications belonging to your company. See Owned mobile applications on page 127.

Viewing your assets

On the *Seeds* page, you can view the domain names, card BINs, and mobile apps of your organization that are being monitored by FortiRecon. You can toggle between the following pages to view your organization's assets:

- Domains
- Card BIN
- Owned Mobile Applications

To view your organization's assets:

1. Go to *Profile Settings* > *Seeds*.
2. Navigate between asset types by selecting the:
   - *Domains* tab
   - *Card BIN* tab
   - *Owned Mobile Applications* tab

3. Search for assets:
   - Enter a keyword in the *Global Search* box to search simultaneously for *Domains*, *Card BINs*, and *Owned Mobile Applications*.
   - Navigate to one of the tabs, and search for a keyword in the *Search* box to look for entries specific to that asset type.

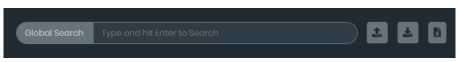
Downloading a sample data file

You can use a Microsoft Excel file to upload bulk information to the *Seeds* page. The Microsoft Excel file requires a specific format, and you can download a sample file to review the needed format.

If you intend to upload data for *Domains*, *Card BIN*, and *Owned Mobile Applications* simultaneously, select the global sample file.

To download a global sample file:

1. Go to *Profile Settings* > *Seeds*.
2. Select *Download Sample XLS* in the top right.



The global sample file is downloaded to your computer.

To download a sample file for a specific entry type:

1. Go to *Profile Settings* > *Seeds*.
2. Select the entry type you want:
   - *Domains*
   - *Card BIN*
   - *Owned Mobile Applications*
3. Select *Download Sample XLS* in the tab.

The sample file is downloaded to your computer.

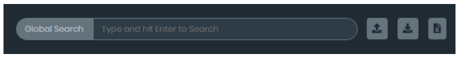
Uploading a data file

You can upload a Microsoft Excel file of your organization's information to FortiRecon. You can upload information in one global file for all entry types, or you can upload multiple, individual files.

The Microsoft Excel file requires a specific format. See Downloading a sample data file on page 122.

To upload a global sample file:

1. Go to *Profile Settings* > *Seeds*.
2. Select *Upload XLS* in the top right.

   Your computer file explorer is displayed.
3. Select the file and click *Open*. The data entries are displayed in the *Seeds* pages.

To upload a sample file for a specific entry type:

1. Go to *Profile Settings* > *Seeds*.
2. Select the entry type you want:
   - *Domains*
   - *Card BIN*
   - *Owned Mobile Applications*
3. Select *Upload XLS* in the tab.

   Your computer file explorer is displayed.
4. Select the file and click *Open*. The data entries are displayed in the selected *Seeds* tab.

Exporting global masters

You can download a master list in Microsoft Excel format from FortiRecon that contains all domains, card BINs, and owned mobile applications. The file contains three tabs, with each tab dedicated to one of the three *Seeds* tabs.

To download a global master list:

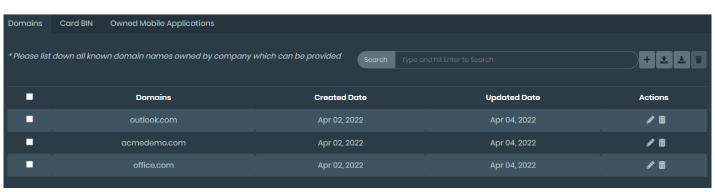
1. Go to *Profile Settings* > *Seeds*.
2. Click *Export Global Masters*. The master list is downloaded to your computer as a Microsoft Excel file.

Domains

Providing domains allows FortiRecon to monitor for typo-squatting and phishing by actors that may be trying to impersonate your organization. See Domains Typo-squatting and Phishing.

From the *Profile Settings* > *Seeds* > *Domains* tab, you can:

- Add new domain names. See Adding domains on page 124.
- Edit existing domain names. See Editing domains on page 124.
- Delete domain names. See Deleting domains on page 124.



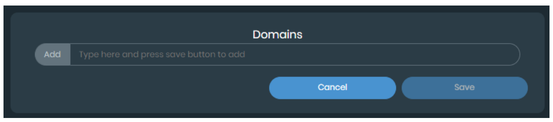
The *Domains* list is synced with the *EASM* scan, maintaining the asset list throughout FortiRecon. See EASM on page 16 for more information on scans.

Adding domains

You can add new domains in the *Domains* tab, as needed.

To add a new domain:

1. Go to *Profile Settings* > *Seeds* > *Domains*.
2. Click *Add*. The *Domains* dialog is displayed.



3. Enter the domain name in the *Add* text box.
4. Click *Save*. The domain is added.

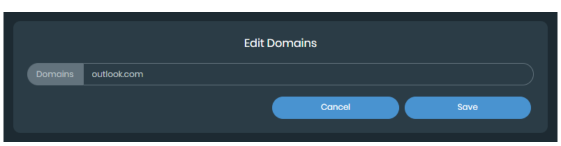
You must include a top-level domain when entering the domain name, such as *.com* or *.org*.

Editing domains

You can edit a pre-existing domain name in the *Domains* tab.

To edit a domain name:

1. Go to *Profile Settings* > *Seeds* > *Domains* and find the domain name.
2. Click the edit icon in the *Actions* column. The *Edit Domains* dialog is displayed.



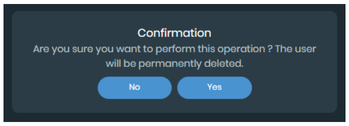
3. Edit the text in the *Domains* text box.
4. Click *Save*. The domain name is changed.

Deleting domains

You can delete domain names from the *Domains* tab. You can delete single domain names or groups of domain names.

To delete a single domain name:

1. Go to *Profile Settings* > *Seeds* > *Domains* and find the domain name.
2. Click the delete icon in the *Actions* column. A confirmation message is displayed.

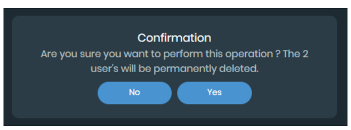


3. Click *Yes*. The domain name is deleted from the list.

To delete multiple domain names:

1. Go to *Profile Settings* > *Seeds* > *Domains*.
2. Select the domain names by using one of the following methods:
   - Select the checkbox in the first row to select all domain names, and then clear the checkbox beside any domain names that you want to keep.
   - Select the checkbox beside specific domain names to mark them for deletion.

   The *Delete Rows* icon becomes available.
3. Click *Delete Rows*. A confirmation message is displayed and lists the number of selected domains.



4. Click *Yes*. The domain names are deleted from the list.

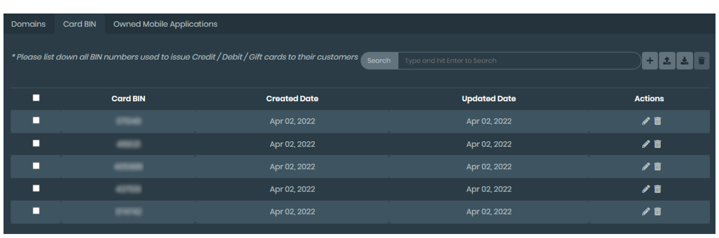
Card BIN

Providing your organization's card bank identification numbers (BINs) allows FortiRecon to monitor for card fraud by actors that may be trying to steal credit, debit, or gift card information. See Card Fraud on page 83.

Card BIN information is needed only when your organization issues credit, debit, or gift cards.

From the *Profile Settings* > *Seeds* > *Card BIN* tab, you can:

- Add new card BINs. See Adding a card BIN on page 126.
- Edit existing card BINs. See Editing a card BIN on page 126.
- Delete existing card BINs. See Deleting a card BIN on page 126.

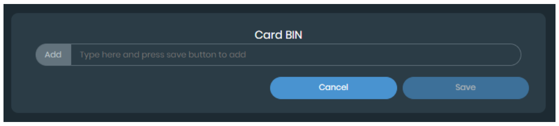


Adding a card BIN

You can add new BINs in the *Card BIN* tab, as needed. BINs must be at least six characters long.

To add a new card BIN:

1. Go to *Profile Settings* > *Seeds* > *Card BIN*.
2. Click *Add*. The *Card BIN* window is displayed.



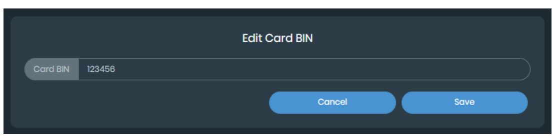
3. Enter the BIN in the *Add* text box.
4. Click *Save*. The card BIN is added.

Editing a card BIN

You can edit a pre-existing card BIN in the *Card BIN* tab.

To edit a card BIN:

1. Go to *Profile Settings* > *Seeds* > *Card BIN* and find the card BIN.
2. Click the edit icon in the *Actions* column. The *Edit Card BIN* window is displayed.



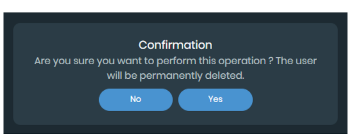
3. Edit the text in the *Card BIN* text box.
4. Click *Save*. The card BIN is edited.

Deleting a card BIN

You can delete BINs from the *Card BIN* tab. You can delete a single BIN or groups of BINs.

To delete a single card BIN:

1. Go to *Profile Settings* > *Seeds* > *Card BIN* and find the BIN.
2. Click the delete icon in the *Actions* column. A confirmation message is displayed.

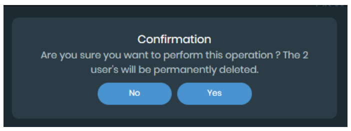


3. Click *Yes*. The BIN is deleted from the list.

To delete multiple card BINs:

1. Go to *Profile Settings* > *Seeds* > *Card BIN*.
2. Select the BINs by using one of the following methods:
   - Select the checkbox in the first row to select all BINs, and clear the checkbox beside any BINs that you want to keep.
   - Select the checkbox next to specific BINs to mark them for deletion.

   The *Delete Rows* icon becomes available.
3. Click *Delete Rows*. A confirmation message is displayed and lists the number of selected BINs.



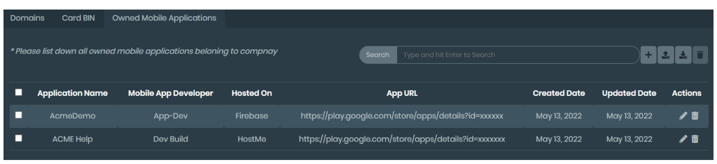
4. Click *Yes*. The BINs are deleted from the list.

Owned mobile applications

Providing app information allows FortiRecon to monitor for rogue mobile apps that are trying to impersonate your organization. See Rogue Mobile Apps on page 60.

From the *Profile Settings* > *Seeds* > *Owned Mobile Applications* tab, you can:

- Add new mobile apps. See Adding an owned mobile application on page 127.
- Edit existing mobile apps. See Editing an owned mobile application on page 128.
- Delete mobile apps. See Deleting an owned mobile application on page 128.

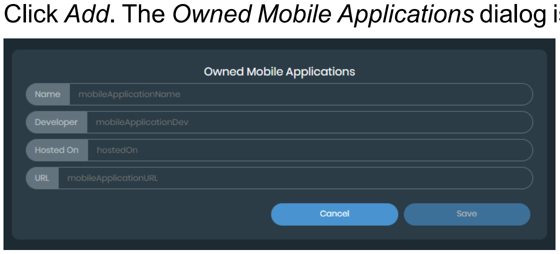


Adding an owned mobile application

You can add new apps in the *Owned Mobile Applications* tab, as needed.

To add a new app:

1. Go to *Profile Settings* > *Seeds* > *Owned Mobile Applications*.
2. Click *Add*. The *Owned Mobile Applications* dialog is displayed.



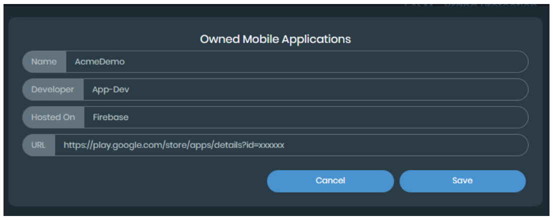
3. Click the text boxes to enter text for *Name*, *Developer*, *Hosted On*, and *URL*.
4. Click *Save*. The app is added.

Editing an owned mobile application

You can edit app information in the *Owned Mobile Applications* tab.

To edit an app:

1. Go to *Profile Settings* > *Seeds* > *Owned Mobile Applications* and find the app.
2. Click the edit icon in the *Actions* column. The *Owned Mobile Applications* dialog is displayed.



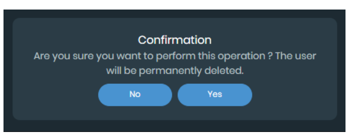
3. Edit the *Name*, *Developer*, *Hosted On*, or *URL* boxes.
4. Click *Save*. The app information is edited.

Deleting an owned mobile application

You can delete apps from the *Owned Mobile Applications* tab. You can delete a single app or groups of apps.

To delete a single app:

1. Go to *Profile Settings* > *Seeds* > *Owned Mobile Applications* and find the app.
2. Click the delete icon in the *Actions* column. A confirmation message is displayed.

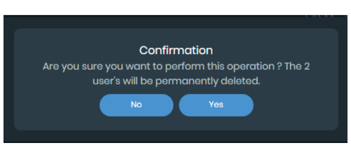


3. Click *Yes*. The app is deleted from the list.

To delete multiple apps:

1. Go to *Profile Settings* > *Seeds* > *Owned Mobile Apps*.
2. Select the apps by using one of the following methods:
   - Select the checkbox in the first row to select all apps, and clear the checkbox beside any apps that you want to keep.
   - Select the checkbox beside specific apps to mark them for deletion.

   The *Delete Rows* icon becomes available.
3. Click *Delete Rows*. A confirmation message is displayed and lists the number of selected apps.



4. Click *Yes*. The apps are deleted from the list.

www.fortinet.com