Admin Guide

FortiTIP Cloud 25.2

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

FORTINET VIDEO LIBRARY
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

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

(Undefined variable: FortinetVariables.Publication Datex)
FortiTIP Cloud 25.2 Admin Guide
00-400-000000-20221031

TABLE OF CONTENTS

Change Log

Date	Change Description
8/15/2025	Initial release.

Overview

This guide contains information on how to customize and manage Fortinet Threat Intelligence Platform (FortiTIP Cloud), including system settings, security management, user management, and configuring multi-segmented networks.

It also provides a comprehensive overview of FortiTIP Cloud, designed to enhance an organization's ability to identify, manage, and respond to cyber threats in an effective and coordinated manner.

FortiTIP Cloud is a cloud-hosted threat intel platform designed to enhance an organization's ability to identify, manage, and respond to cyber threats in an effective and coordinated manner. The platform integrates several key functions including *Outbreak Management*, *Threat Intel Search*, *Threat Intel Management*, and *CVE Correlation* with *Threat Feeds*. These features work in tandem to provide a unified view of potential threats, vulnerabilities, and incidents across an organization's network and digital assets on customizable pre-built dashboards.

Key Features

The following are the key features of this solution:

- **Outbreak Management**: Provided by FortiGuard, this feature equips the platform with tools to monitor and manage the containment and resolution of widespread attacks or breaches. It enables organizations to rapidly assess the scope and impact, ensuring efficient coordination of response efforts.
- **Threat Intel Search**: The platform enables users to query FortiGuard's extensive threat intelligence database to uncover details about Indicators of Compromise (IOCs), including associated malware, threat actors, CVEs, and related threat correlations. This empowers analysts with contextual insights to accelerate threat validation and informed response.
- **Threat Intelligence Management**: This component allows users to collect, analyze, and store threat intelligence from multiple sources. It facilitates the enrichment of data with contextual insights to better understand the nature, intent, and tactics behind threats.
- **CVE Correlation with Threat Feeds**: By correlating CVE (Common Vulnerabilities and Exposures) data with active threat feeds, the platform helps organizations quickly identify which vulnerabilities are actively being targeted by adversaries. This feature enables proactive defense by focusing resources on high-risk vulnerabilities.

This Threat Intelligence Platform is a vital tool in enhancing cybersecurity resilience, providing organizations with the tools to stay ahead of evolving threats and mitigating risks before they become significant issues.

FortiTIP Cloud is built on the FortiSOAR platform and shares the same administrative interface and core configuration workflows. To avoid duplication and to ensure consistency, this documentation links to relevant sections of the FortiSOAR documentation where applicable. Unless otherwise noted, the procedures and settings described in the linked content apply equally to FortiTIP Cloud.

Getting Started

The Setup Guide helps administrators configure FortiTIP Cloud according to best practices. It covers essential configurations and the installation of solution packs for optimal performance, such as setting up network proxies, enabling audit logs, and configuring playbook features. For details, including permissions required to view the Setup Guide, see the section Prerequisites in Setup Guide documentation.

The minimum permissions required to view and use the *Setup Guide* are `Read` and `Update` permissions for both **Security** and **Application** and `Read` permission for **Widget** and **Solution Pack**. Additionally, ensure that the **Enable Setup Guide** option is selected on the **Settings** > System Settings on page 37 page, which is also the default setting.

When administrators log into FortiTIP Cloud for the first time, the Setup Guide is displayed. You can minimize it by clicking > . To reopen, click the **Setup Guide** in the top-right corner of FortiTIP Cloud. To hide the icon, clear the **Enable Setup Guide** option on the **Settings** > **System Settings** page.

For more details, refer to the section Setup Guide, under the chapter **General Features & Navigation**.

Tasks and Permissions

To manage different modules in FortiTIP Cloud, appropriate user roles and permissions must be assigned. In FortiTIP Cloud, modules are applied to roles, for example, the *Security* module is applied to the `Security Administrator` role. Permissions are based on the Create, Read, Update, and Delete model (CRUD). Each module within FortiTIP Cloud has explicit CRUD permissions that can be customized within a role.

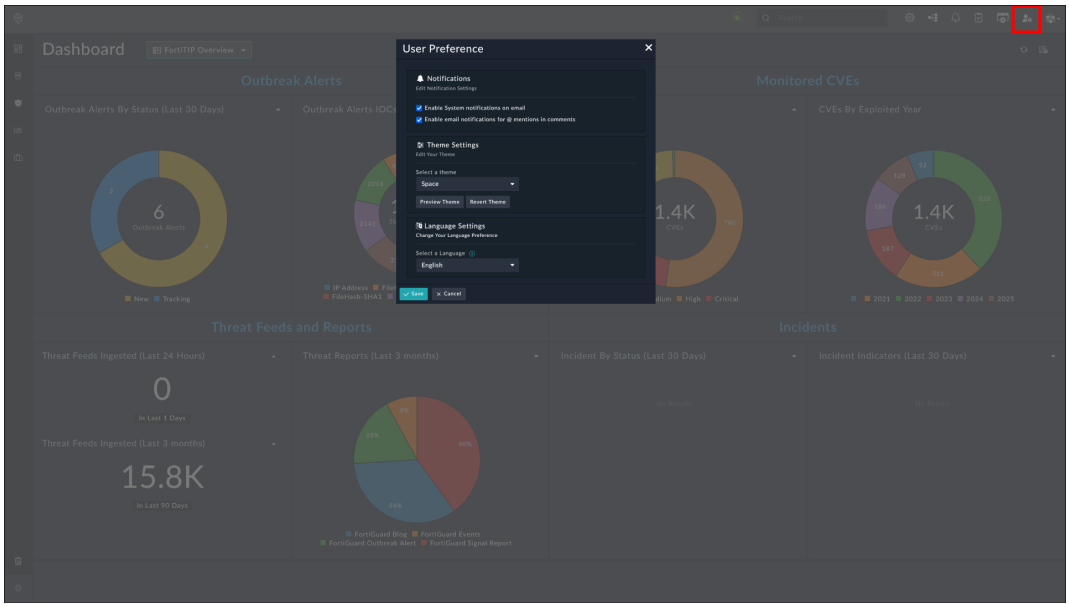
For example, to perform all tasks for System Settings, you must be assigned a role that has `CRUD` permissions on the *Application* module, or to be able to add and manage users, you must be assigned a role that at the minimum has `Create` and `Update` permissions on the *People* module.

Task	Permissions required on the module
System Settings: Customizing FortiTIP Cloud and configure several default options used throughout the system, including setting up authentication mechanisms and configuring dashboards and templates.	Create, Read, Update, and Delete (CRUD) permissions on `Application` module. Default Role - *Application Administrator*.

Security management: Managing teams and roles.	CRUD permissions on `Security` module. Default Role - *Security Administrator*. The security administrator role also has CRUD permissions on the `Secure Message Exchange` and `Tenants` modules, so that this role can configure multi-tenant systems.
User management: Adding and removing users and editing their permissions.	CRUD permissions on `People` module.
Appliances management: Managing appliances and access keys.	CRUD permissions on `Appliances` module.
Password Vault management: Integrating with third-party external vaults to manage sensitive data	CRUD permissions on `Connectors` module and Read permission on `Application` module.
Playbook management: Configuring playbook collections and playbooks	CRUD permissions on `Playbook` module. Default Role - *Playbook Administrator*.

User Preferences

Users can change their UI preferences like notifications, themes, and language by clicking  .



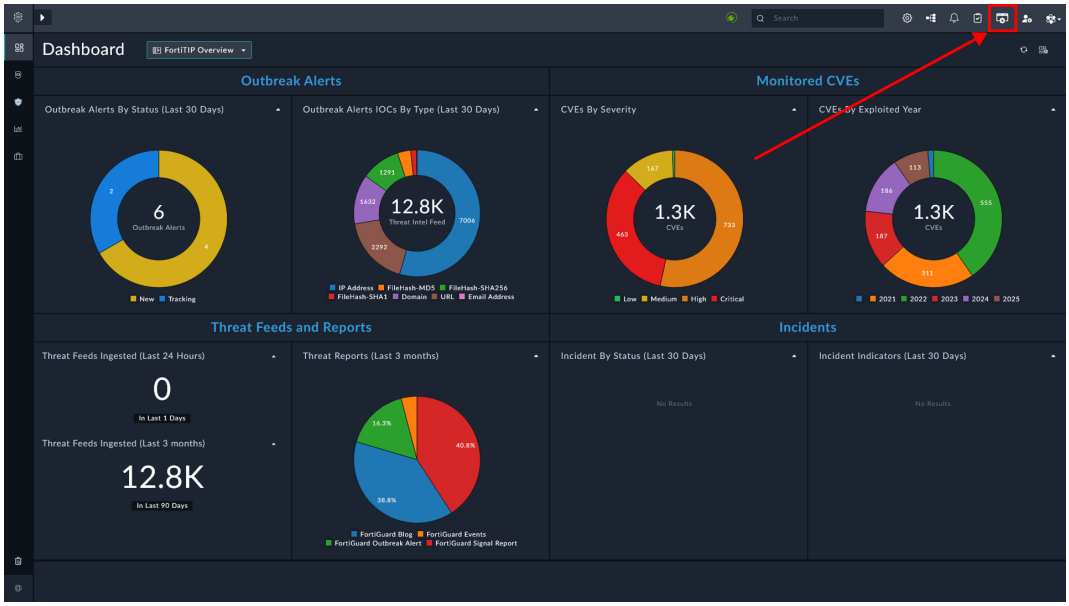
The *User Preferences* section in FortiSOAR Cloud Deployment Guide describes this section in greater detail.

General Features & Navigation

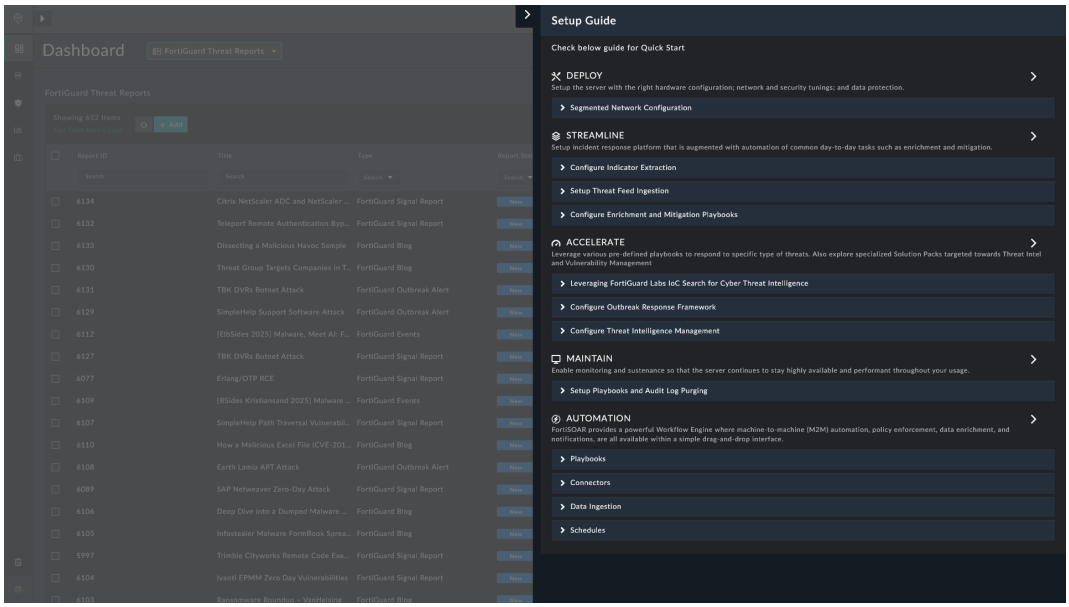
The FortiTIP Cloud interface is based around a common navigation bar on the left side of the application, a global search bar, and various conditional filtering options within modules. The Navigation menu and its options become available depending on the permissions given as part of the Role-based Access Control (RBAC). For example, you can view alert records only if you have been given read permissions to the *Alerts* module.

Launching Setup Guide

The **Setup Guide** helps first-time, and recurrent, FortiTIP Cloud™ administrators to optimally set up FortiTIP Cloud™ based on best practices. It helps administrators perform various important configurations and install solution packs vital for the smooth working of their FortiTIP Cloud™ environment.



Click  to open a list of tasks.



The task list is divided into sections. Some tasks open features in FortiTIP Cloud™, where you can complete the task. Others link to product documentation with instructions for performing the task.

- **Deploy**: FortiTIP Cloud supports segmented networks to help investigate a multi-segmented network by allowing secure remote execution of connector actions. Use *FSR Agents* to remotely run connector actions. For more information, refer to Segmented Network Support section, in FortiSOAR Administration Guide.
- **Streamline**: The streamline section lists tasks related to configuring indicator extraction, setting up threat feed ingestion, and configuring enrichment and mitigation playbooks.
- **Accelerate**: Use predefined playbooks to respond to specific types of threats. Explore *FortiGuard Labs IoC Search* for cyber threat intelligence, configure the *Outbreak Response Framework*, and set up *Threat Intel Management*. These tasks help streamline your threat response workflows and improve detection and mitigation efficiency.
- **Maintain**: Set up regular log purging to manage disk space by automatically rotating logs at set intervals. This prevents excessive log accumulation, which can impact system performance and storage capacity.
- **Automation**: FortiTIP Cloud offers a powerful Workflow Engine with a simple drag-and-drop interface for automation, policy enforcement, data enrichment, and notifications. You can build workflows using playbooks, connectors, data ingestion sources, and schedules–all in one unified platform.

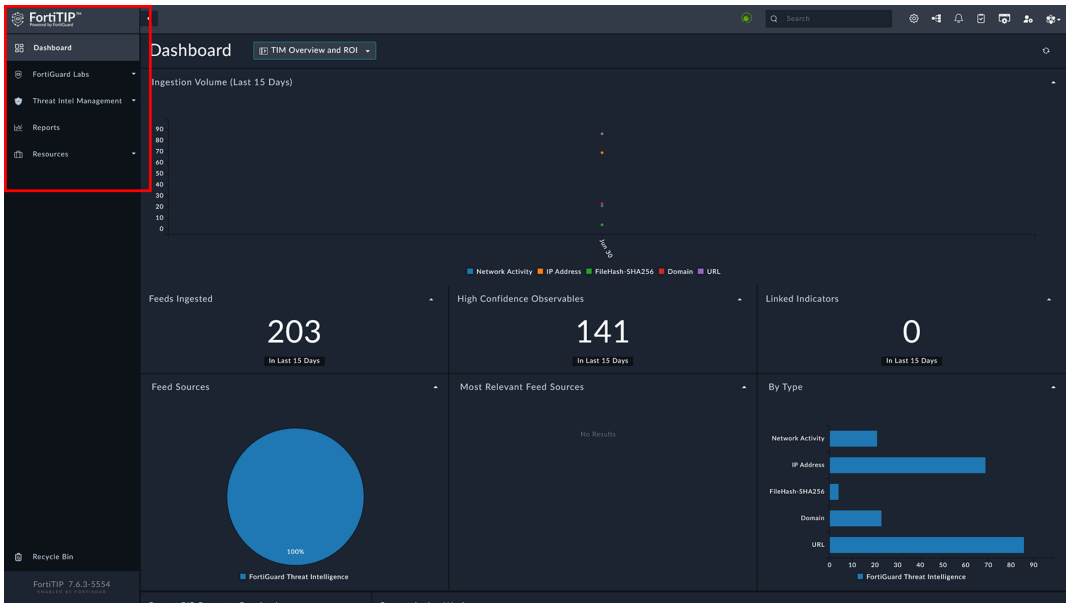
Managing Setup Guide Tasks

For each task you have three options:

- **Mark as Done**: Click this button to mark the task as done, once you complete it.
  - Click **Reset Task Options** button to bring back the task, in case you clicked *Marked as Done* in error.
- **I will complete later**: Select this button to skip that task and complete it at a later time. Clicking the button collapses the task, but the task options remain active.
- **Not Applicable**: Select this button if a task does not apply to your FortiTIP Cloud environment.
  - Click **Reset Task Options** button to bring back the task, in case you clicked *Not Applicable* in error.

Navigation Menu

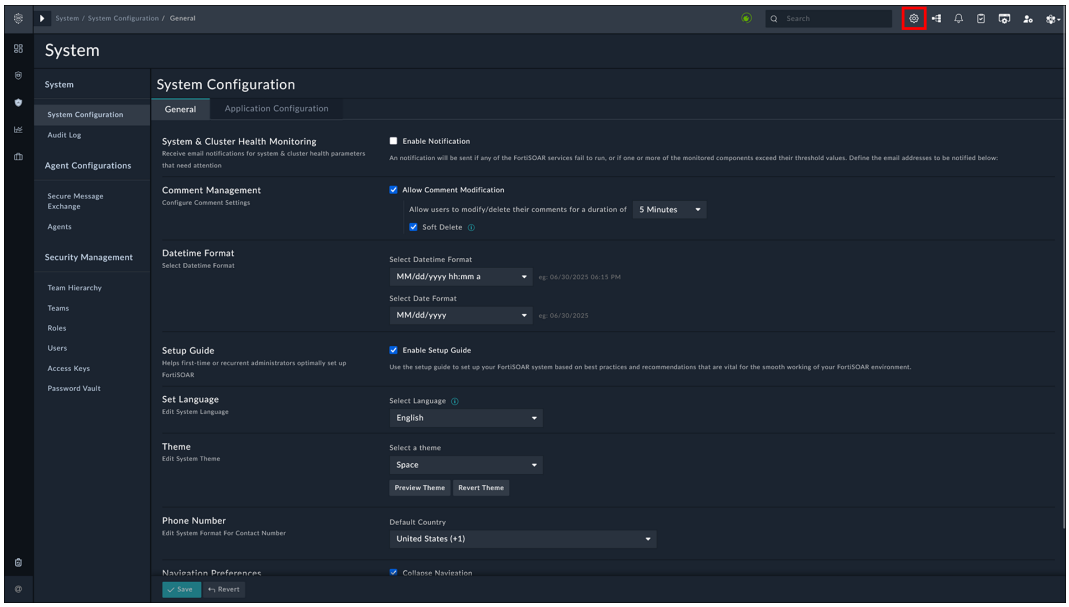
The navigation menu gives quick access to multiple tools that help review and process information as part of FortiTIP Cloud.



Click ▶ to expand the navigation menu. Alternatively, you can hover over individual navigation menu items to view included features.

Settings

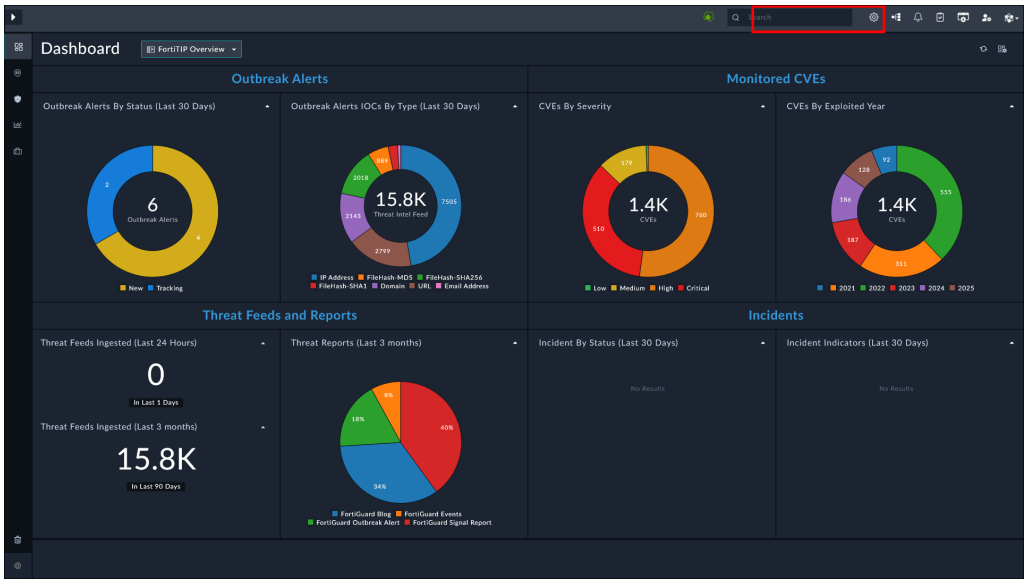
Click ⚙ on the top-right corner of your screen to configure and customize FortiTIP Cloud. Your administrator would already have configured these options, and hence you must not edit these options. For various settings available in FortiTIP Cloud, refer to the chapter System Settings within this document.



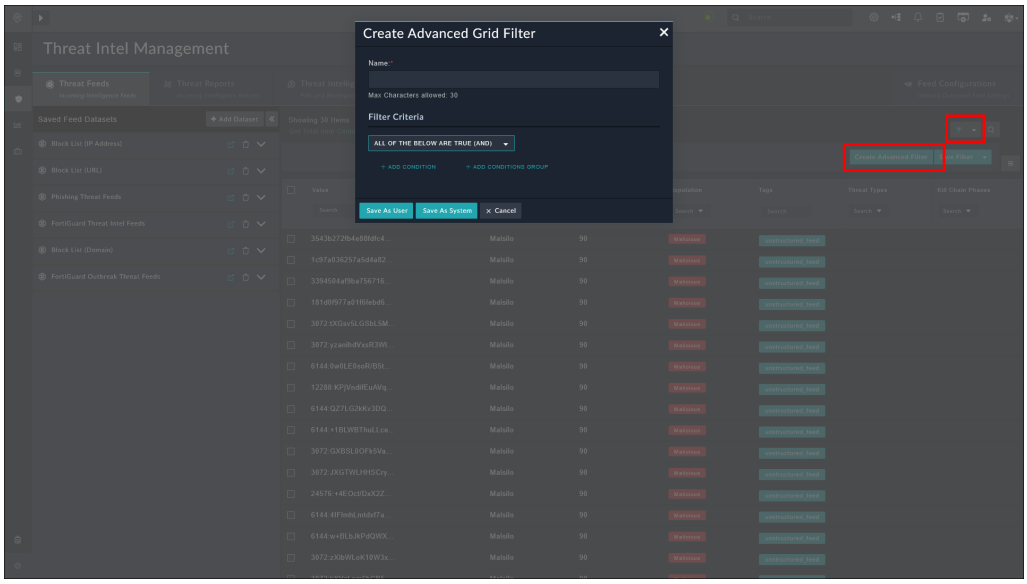
Search

There are three methods of searching within FortiTIP Cloud:

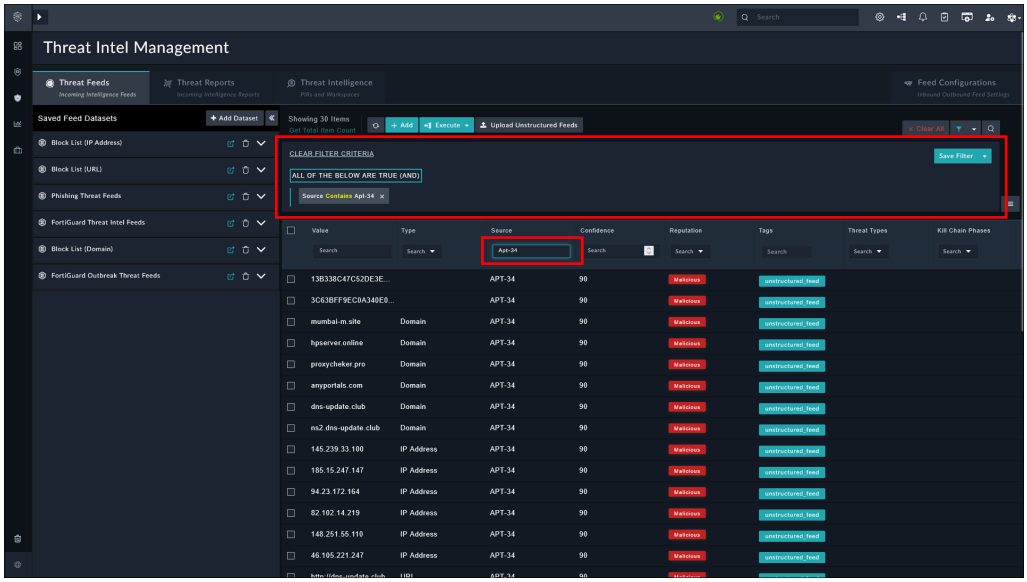
- **Global Search**: The Global search bar at the top of the screen helps you to search for one or more keywords across all records within the system.



- **Records Search**: The Records search helps you to search for specific records within a module, such as *Threat Intel Feed*, by applying or defining filter conditions. Click > **Create Advanced Filter** and define the filter conditions in the **Create Advanced Grid Filter** dialog box.

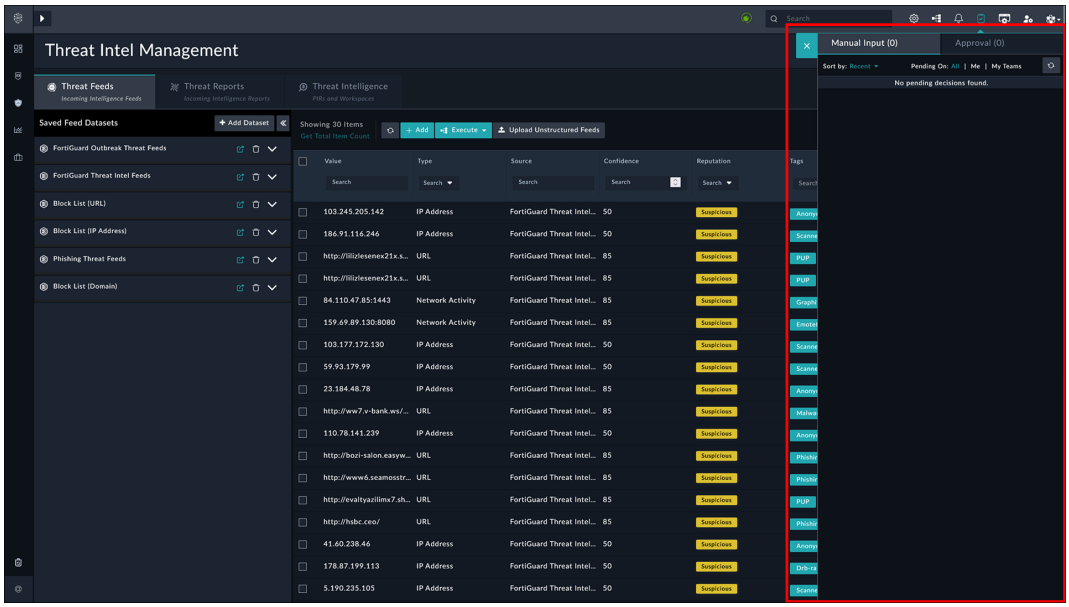


- **Column Search**: The Column search helps you to search specific records from a module, such as *Threat Intel Feed*, within the individual data column on the records table.



Notifications

The **Notifications** icon appears with badges to denote an unread notification. Notifications include informative information, such as failure of workflows, assignment of user on created and updated alerts, incidents, tasks, etc., and actions that require user review. Click to display the **Notifications Panel**:



In the **Notification Panel**, use the **Search** box to search for a particular notification, or filter notifications as follows:

- Click **All** to display all notifications, both *read* and *unread*.
- Click **Action Required** to display notifications that are pending for some user action, such as an approval.
- Click **@Mentions** to display a list of comments where you have been tagged.
- Select **Show only Unread** to display unread notifications. Notifications are marked *read* once you click them to open their contents.

You can also delete notifications from the **Notifications Panel** by clicking the **Delete** icon. However, you can delete only those notifications that are assigned to you and not those that are assigned to a team, or any other user, or system (global) notifications such as workflow failures.

Users with a minimum of **Update** permissions on the **Security Module** can also click the **Purge All** icon to display the *Purge Notifications* dialog. Click **Purge All** to delete all notifications.

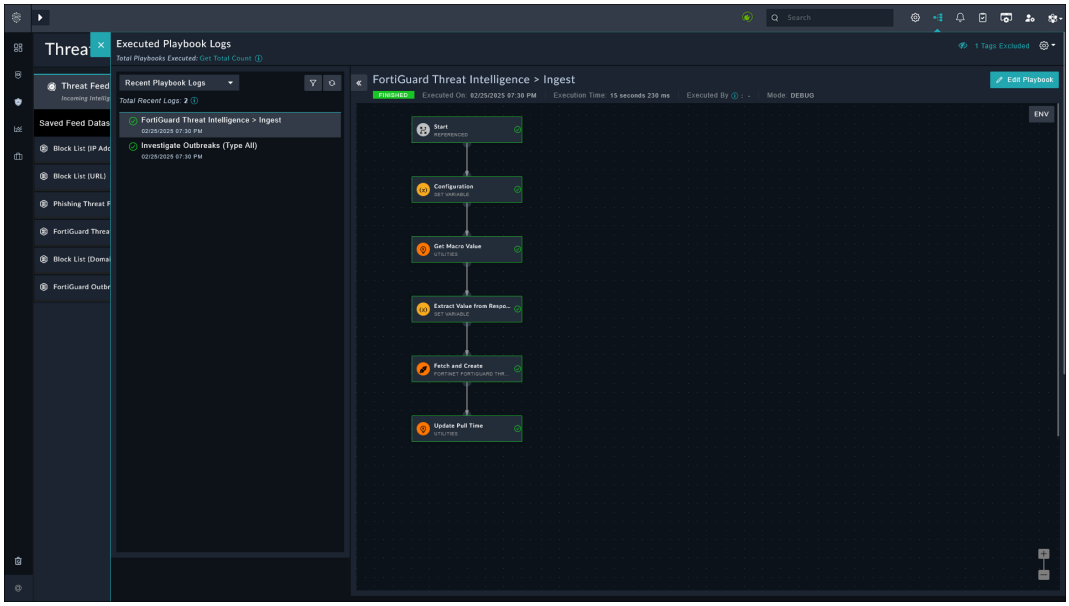
Pending Tasks

The **Pending Tasks** icon appears with badges to denote the number of pending tasks for approvals and manual inputs, both. Click to display the **Pending Tasks** panel. For more information on the pending tasks panel, manual inputs, and approvals, see the *Triggers and Steps* chapter in the FortiSOAR Playbooks Guide.

To view and interact with approval notifications, you must have *Create*, *Read*, and *Execute* permissions to the **Playbook** module along with *Read* and *Update* permissions to the **Approvals** module.

Executed Playbook Logs

Click to view the executed playbook logs.



Dashboards

A Dashboard is generally the default landing and home page for users logging into FortiTIP Cloud. The subsequent sections describe the various out-of-the-box dashboards that are available for users of FortiTIP Cloud.

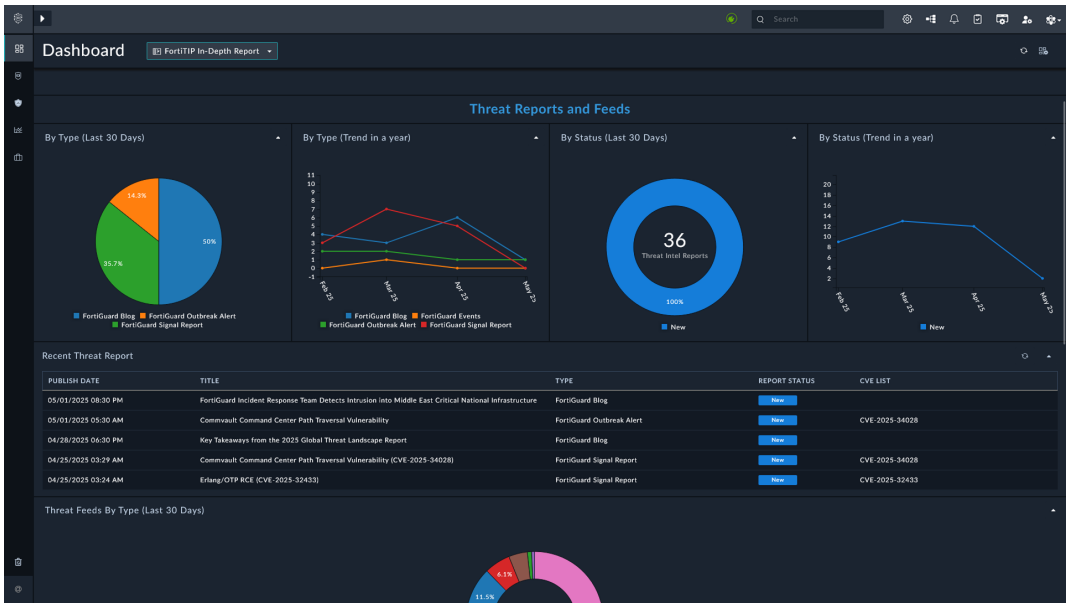
FortiTIP Overview

This dashboard presents a focused view of critical threat intelligence and security posture data. The **Outbreak Alerts** section displays alerts categorized by status over the past 30 days, along with associated Indicators of Compromise (IOCs) classified by type for the same period. In the **Monitored CVEs** section, vulnerabilities are organized by severity and by the year they were exploited, offering insight into risk prioritization. The **Threat Feeds and Reports** area highlights the volume of threat feeds ingested within the last 24 hours and over the past 3 months, as well as published threat reports from the last 3 months. Finally, the **Incidents** section summarizes active and historical incidents by status and showcases related threat indicators identified in the last 30 days.

FortiTIP Cloud In-Depth Report

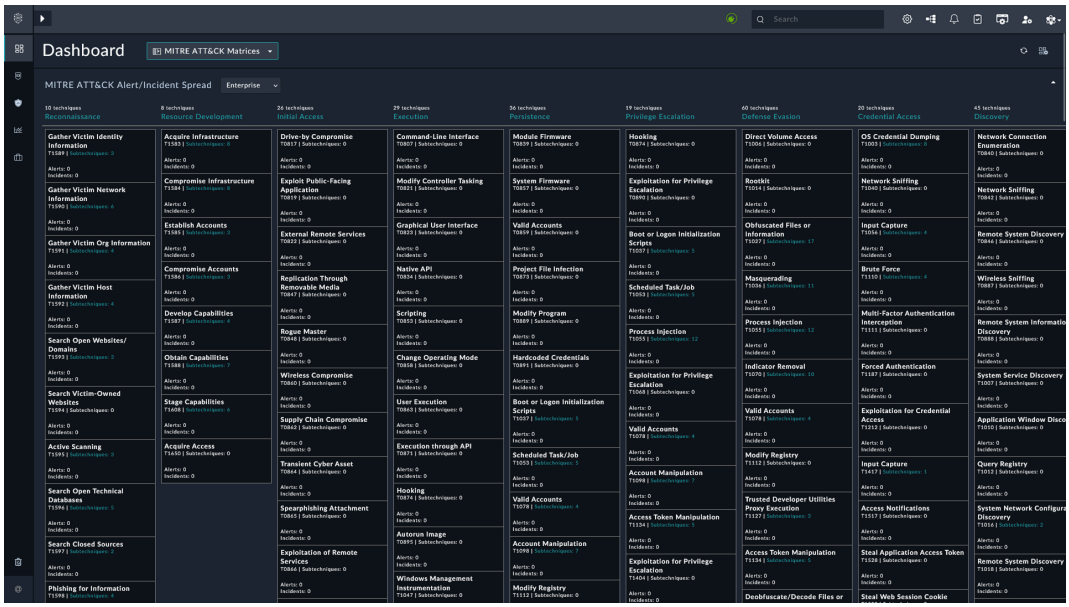
The dashboard provides a comprehensive overview of threat intelligence and security activity, segmented into key focus areas. The **FortiGuard Outbreak** section includes visualizations of outbreak data categorized by severity and status over the last 30 days, as well as year-long trends. It also features a **Recent Outbreaks** table highlighting the most current and significant threat events. The **Threat Reports and Feeds** section presents threat intelligence by type and status across the last 30 days and historical trends, supported by a **Recent Threat Reports** grid for quick access to

notable publications. Additionally, a dedicated chart displays **Threat Feeds by Type (Last 30 Days)** for more granular feed analysis. The **Monitored CVEs** section breaks down known vulnerabilities by severity and year of exploitation, helping prioritize response efforts. Lastly, the **Security Incidents** section provides insight into incident trends, sources, and statuses over the past 30 days, along with key indicators and affected assets, enabling teams to track and respond to active security issues efficiently.



MITRE ATT&CK Matrices

The **MITRE ATT&CK Matrices** dashboard provides a structured view of cyber adversary tactics and techniques, aligned with the MITRE ATT&CK framework. It categorizes threat activity across various stages of the attack lifecycle, including **Reconnaissance**, **Resource Development**, **Initial Access**, **Execution**, **Persistence**, **Privilege Escalation**, **Defense Evasion**, **Credential Access**, and **Discovery**. Each technique is grouped under its corresponding tactic, displaying the number of associated sub-techniques and summarizing current **Alerts** and **Incidents** for each. This matrix-based layout allows security teams to quickly identify which adversarial behaviors have been observed in the environment and to assess gaps in detection coverage. The dashboard supports proactive threat hunting and incident response by offering visibility into how real-world threats map to MITRE-defined techniques.

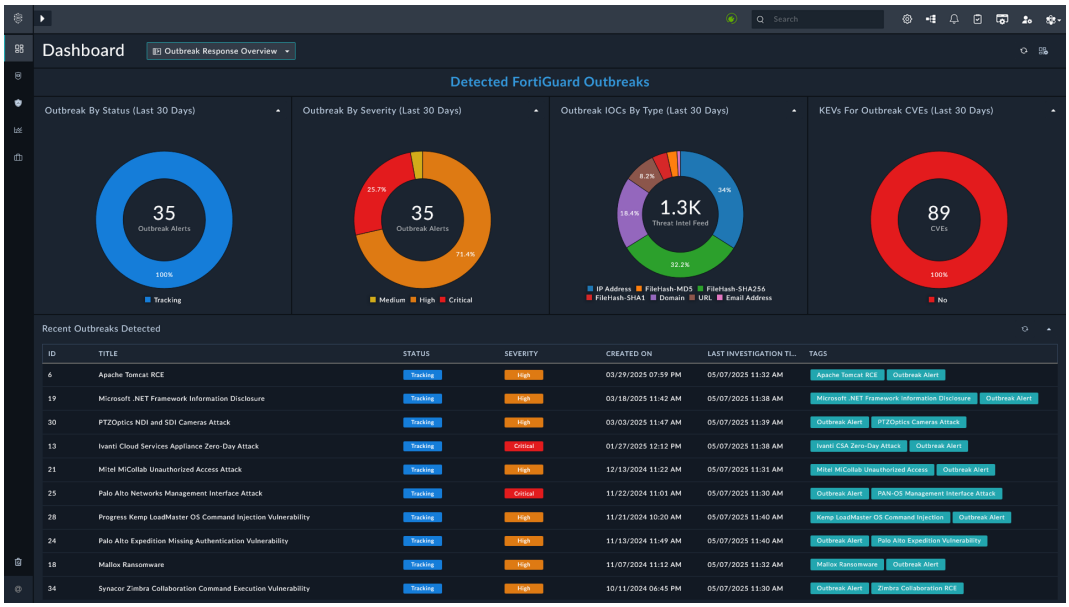


Outbreak response Overview

The **Outbreak Response Overview** dashboard provides centralized visibility into recent FortiGuard-detected threat outbreaks and their associated indicators and impacts. At the top, summary panels display outbreak alerts categorized by **status**, **severity**, and **indicator type** over the last 30 days, alongside a count of **known exploited vulnerabilities (KEVs)** linked to these outbreaks. A detailed table of **Recent Outbreaks Detected** offers drill-down insights into specific threats, including severity levels, detection timestamps, investigation history, and tagging for contextual correlation.

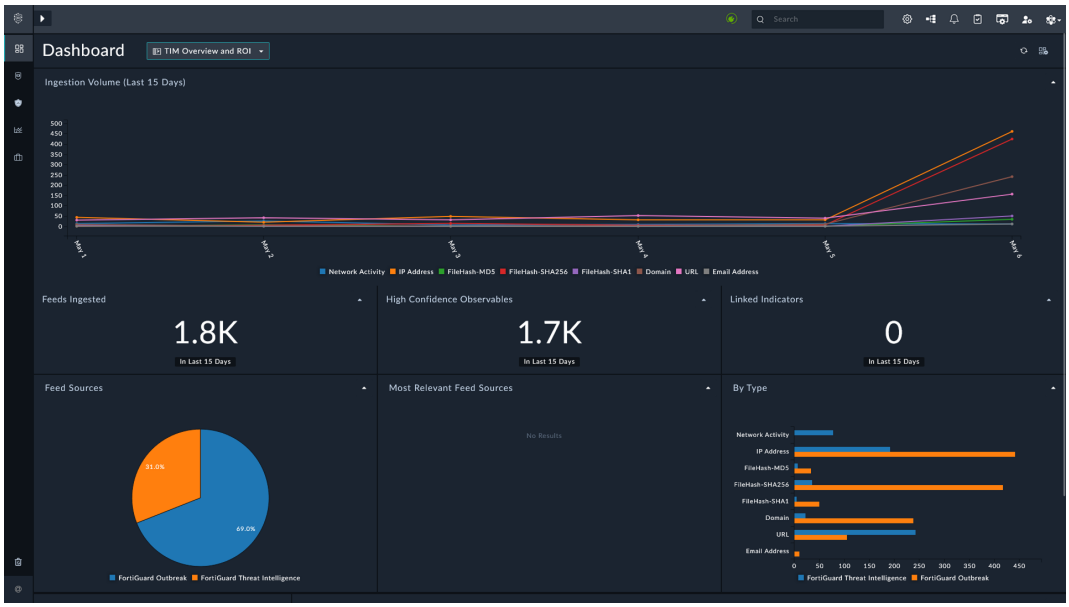
Supporting charts highlight the **Top 10 Outbreak Threat Feeds**, showing the most prevalent IOC categories–such as IP addresses, file hashes, and email indicators–used in recent detections. While the **Top 10 Outbreak KEVs** panel is currently unpopulated, it is designed to surface vulnerabilities frequently exploited in outbreak scenarios. The lower section of the dashboard covers **Confirmed Security Incidents**, organizing them by **source**, **status**, **indicators**, and **impacted assets** within the last 30 days. This enables teams to correlate outbreak data with active incidents for more efficient threat response and containment.

The Outbreak Configuration Wizard must be run before this feature can be used. Refer to the section Setup Outbreak Response Framework in Outbreak Response Framework documentation.



TIM Overview and ROI

The **TIM Overview and ROI** dashboard provides threat intelligence teams with actionable insights into the value and performance of their threat data ingestion efforts. It highlights the volume and quality of ingested feeds, surfaces high-confidence observables, and enables tracking of indicator relevance over time. By offering visibility into source contribution and indicator types, this dashboard helps quantify the return on investment for threat intelligence platforms, supports validation of feed effectiveness, and ensures teams are focusing on observables that truly matter. It serves as a strategic tool for optimizing threat data workflows and prioritizing operational response.

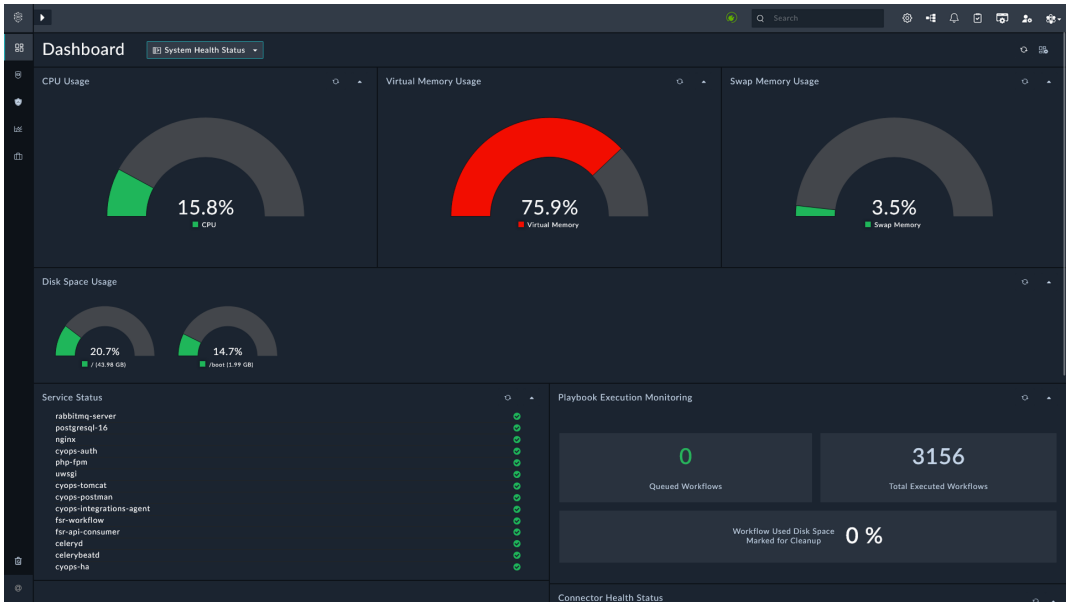


System Health Status

The **System Health Status** dashboard provides a consolidated view of infrastructure and integration performance across the platform. Key performance metrics are displayed at the top, including **CPU usage**, **virtual memory usage**, **swap memory usage**, and **disk space utilization**, offering real-time insight into system resource consumption. Indicators such as **high virtual memory usage** are visually flagged to help administrators promptly identify resource constraints.

Below, the **Service Status** panel confirms the operational state of essential backend services like `rabbitmq-server`, while the **Playbook Execution Monitoring** section allows teams to verify workflow automation functionality. The **System Health Status** panel lists core internal components—such as integration agents, workflow engines, and job handlers—with their status, ensuring end-to-end visibility of platform reliability.

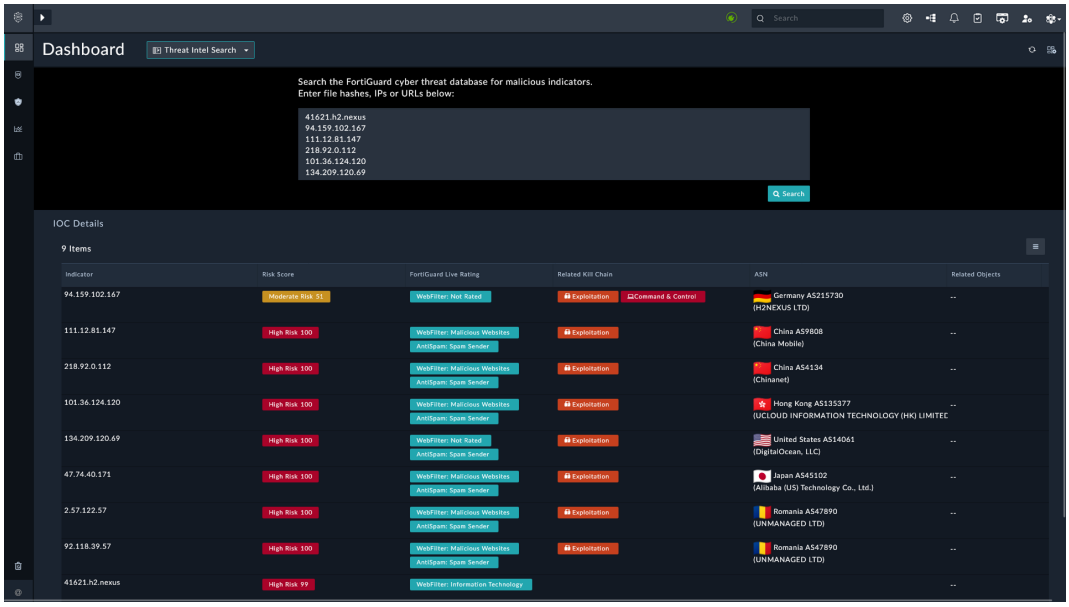
On the right, the **Connector Health Status** panel shows the availability and monitoring state of key integrations, including Fortinet Fabric (e.g., FortiAnalyzer, FortiGuard), third-party advisories (e.g., CISA, NIST), and communication protocols (e.g., SMTP). Together, these components enable continuous monitoring of operational readiness and integration integrity, supporting proactive system maintenance and threat response continuity.



Threat Intel Search

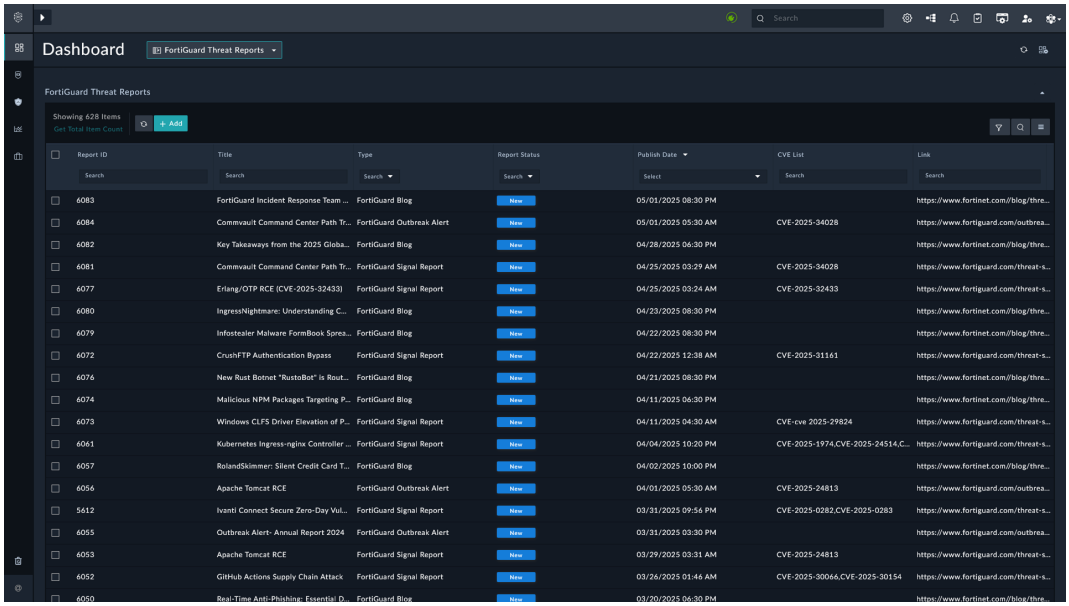
The **Threat Intel Search** dashboard allows analysts to query up to 10 indicators at a time using line-separated values to retrieve intelligence from the FortiGuard cyber threat database. It enriches the input IOCs with contextual details such as **risk scores**, **threat classification**, and **attribution**. For instance, in the following image, indicators like `101[dot]36[dot]124[dot]120`, `111[dot]12[dot]81[dot]147`, and `218[dot]92[dot]0[dot]112` are flagged as high risk with associated tags like *Malicious Websites* and *Spam Sender* and are linked to the exploitation phase of the cyber kill chain. The dashboard also attributes IP addresses to ASN and geographic origins, such as DigitalOcean in the U.S.,

Alibaba in Japan, or UCLOUD in Hong Kong. The dashboard provides a concise, interactive view that supports faster decision-making during threat investigations or proactive threat hunting.



FortiGuard Threat Reports

FortiGuard Threat Reports are in-depth cybersecurity intelligence publications developed by Fortinet's FortiGuard Labs. They provide curated, concise, and actionable insights into emerging cyber threats, combining clear technical details, expert analysis, and practical mitigation strategies. This dashboard displays the reports in a tabular format. Click any report to see the summary and source of the information in a detailed view.



FortiGuard Labs

FortiGuard Labs offers a range of features to enhance threat detection and response by leveraging FortiGuard Labs' global threat intelligence data:

- **FortiGuard Hub**: Launches the Outbreak Response Overview Dashboard that provides a comprehensive view of recent outbreaks and security incidents. It tracks FortiGuard outbreaks by status, severity, and IOC type over the last 30 days, highlighting Known Exploited Vulnerabilities (KEVs) for CVEs. The dashboard includes outbreak trends, recent detections, and top threat feeds, along with detailed analysis of confirmed security incidents by source, status, indicators, and affected assets, enabling swift and informed responses. For details, refer to the chapter FortiGuard Hub.
- **Outbreak Alerts**: Leverages outbreak-specific response solution packs to import outbreak alerts and their associated Sigma and YARA rules to search through log data. This in turn helps in hunt campaigns for threats and other events across large volumes of data. For details, refer to the chapter Outbreak Alerts.
- **Threat Intel Search**: Accepts IOCs (Indicator of Compromise) as input and searches through FortiGuard's cyber threat database to help track and analyze malicious activity. The search retrieves a comprehensive IOC summary, displaying top tags, associated kill chain phases, and top visiting countries. It offers detailed IOC information, including indicators, risk scores, and FortiGuard live rating in the form of a table. Additionally, it links related kill chain phases and provides ASN details, allowing for in-depth analysis and proactive threat mitigation based on a specified or searched IOCs. For details, refer to the chapter Threat Intel Search.
- **Threat Reports**: Displays FortiGuard Threat Reports ingested from FortiGuard and contains report title, type, source, and link to FortiGuard reports among other information. For details, refer to the chapter Threat Reports.

These features collectively provide powerful tools for proactive threat management and intelligence-driven defense.

FortiGuard Hub

The FortiGuard Hub features the **Outbreak Response Overview** dashboard which provides a comprehensive, data-driven view of recent outbreaks and security incidents; designed for security analysts, incident response teams, and managers. With daily updated data, users can quickly assess outbreak status, severity, and related IOCs over the past 30 days. The dashboard highlights critical insights such as Known Exploited Vulnerabilities (KEVs) for CVEs, outbreak trends, and recent detections.

The Outbreak Configuration Wizard must be run before this feature can be used. Refer to the section Setup Outbreak Response Framework in Outbreak Response Framework documentation.

The Outbreak by **Status**, **Severity**, and **IOC Type** charts offer clear visualizations for tracking the progress of ongoing threats, while **Top 10 Outbreak Threat Feeds** and **Top 10 Outbreak KEVs** (displayed as bar graphs) provide an overview of the most impactful feeds and vulnerabilities. The **Recent Outbreaks Detected** table offers granular details about each incident, enabling users to dive into specifics when necessary. By using trend line graphs and pie charts, the dashboard ensures efficient monitoring of outbreak trends and security incidents, facilitating informed, timely decision-

making. With its user-friendly design and actionable insights, the dashboard empowers teams to respond proactively to emerging threats and vulnerabilities.

For more information related to Outbreak Response Framework, refer to the Outbreak Response Framework documentation.

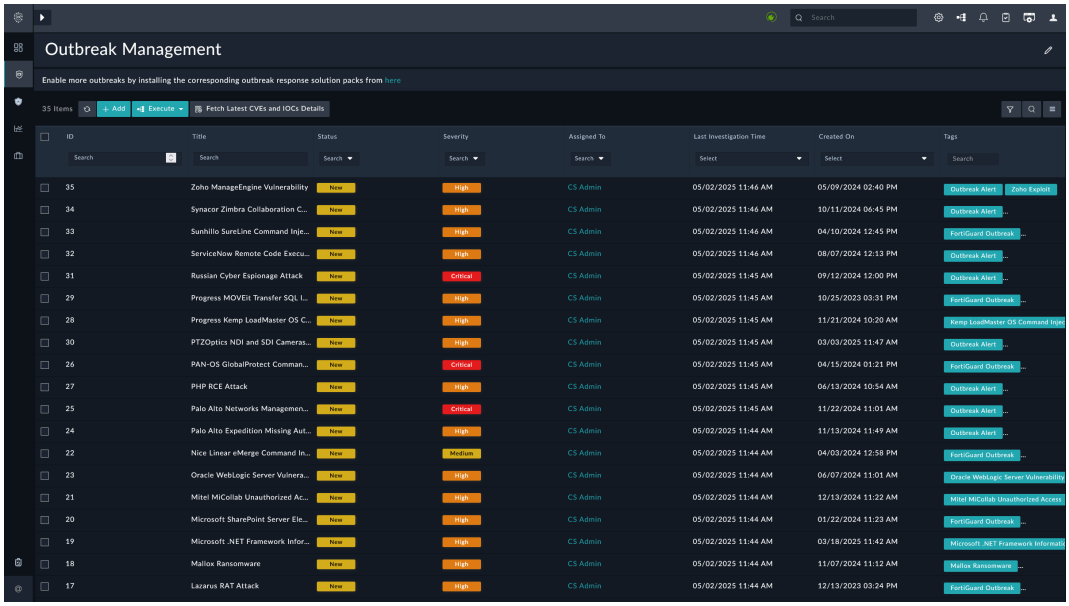
Outbreak Alerts

Outbreak Alerts from *FortiGuard Labs* are real-time notifications that inform users about emerging security outbreaks or active threats detected by FortiGuard's threat intelligence systems. These alerts typically contain details such as the nature of the threat (e.g., malware, ransomware, phishing), the affected systems or applications, and recommended mitigation strategies. Additionally, the alerts may include specifics on the threat's propagation methods, exploited vulnerabilities, and Indicators of Compromise (IOCs), which help in identifying the presence of a threat within a network.

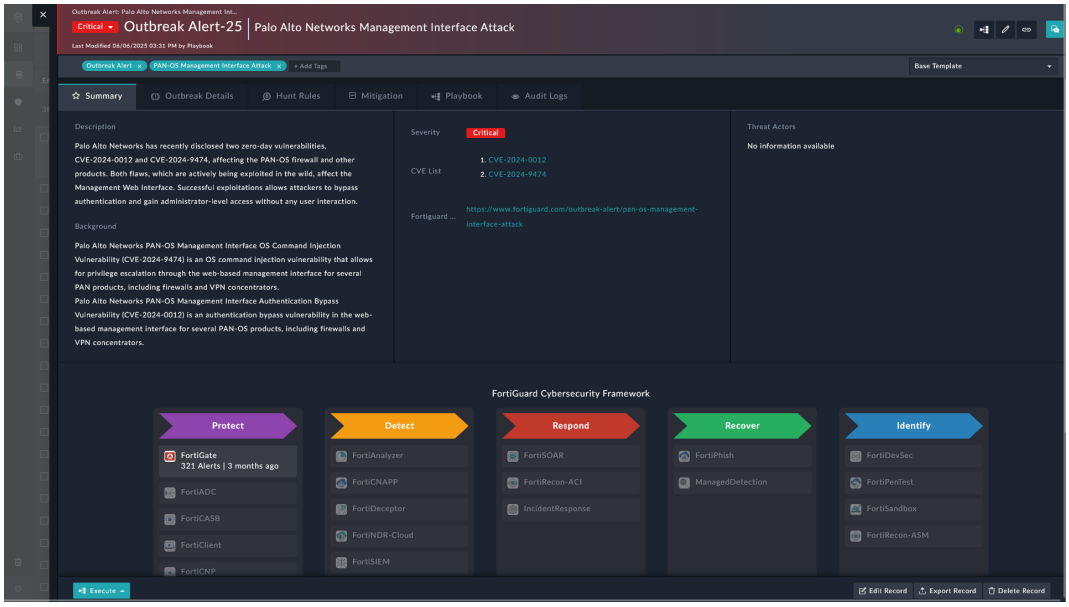
The **Outbreak Response Framework** processes these alerts and compiles critical data, including:

- **Attack Narrative**: A detailed description of the attack, including its timeline and the technologies affected. The narrative includes:
  - **Description**: An in-depth analysis of the vulnerability being exploited.
  - **Background**: Contextual information explaining the factors contributing to the vulnerability.
  - **Announcement**: Early warnings about zero-day vulnerabilities.
  - **Latest Developments**: Updates on mitigation measures.
  - **CVE List**: A compilation of CVEs (Common Vulnerabilities and Exposures) relevant to the threat, serving as a reference for publicly known security issues .
- **Indicators of Compromise (IOCs)**: A list of known IOCs associated with the outbreak, aiding in the detection and identification of the threat within affected systems.

The Outbreak Configuration Wizard must be run before this feature can be used. Refer to the section Setup Outbreak Response Framework in Outbreak Response Framework documentation.



Click an alert to open its details page. The following screenshot displays a *Critical* Outbreak Alert in FortiTIP Cloud, detailing a newly discovered exploitation targeting Palo Alto Networks' PAN-OS management interfaces:



The **Summary** tab also displays available solutions as part of ***FortiGuard Cybersecurity Framework***. The solutions that have been configured in FortiAnalyzer appear *active* under each of– *Protect*, *Detect*, *Respond*, *Recover*, and *Identify*; Solutions that have not been configured in FortiAnalyzer appear *inactive*.

For more information on how to respond to an alert, refer to the example - Outbreak Response on Progress MOVEit Transfer SQL Injection Vulnerability under Outbreak Response Framework documentation.

Threat Intel Search

Threat Intel Search is a tool provided by **FortiGuard Labs** that allows users to search for and analyze **Indicators of Compromise (IOCs)**. IOCs are pieces of evidence, such as IP addresses, domain names, file hashes, or URLs, that can help detect and track malicious activity within a network.

The tool enables security teams to input specific IOCs and retrieve detailed information related to them. The details it typically returns include:

- **Indicator Type**: The type of IOC, such as IP address, domain, URL, file hash, etc.
- **Risk Score**: A rating that indicates the potential threat level associated with the IOC.
- **FortiGuard Live Tracking**: Real-time updates on the status of the IOC, including any active threat intelligence or malicious activity associated with it.
- **Related Kill Chain**: The stages of the cyber attack associated with the IOC, helping to identify which part of the attack lifecycle the IOC is linked to.
- **ASN (Autonomous System Number)**: The network or entity associated with the IOC, providing context for the attack's origin.

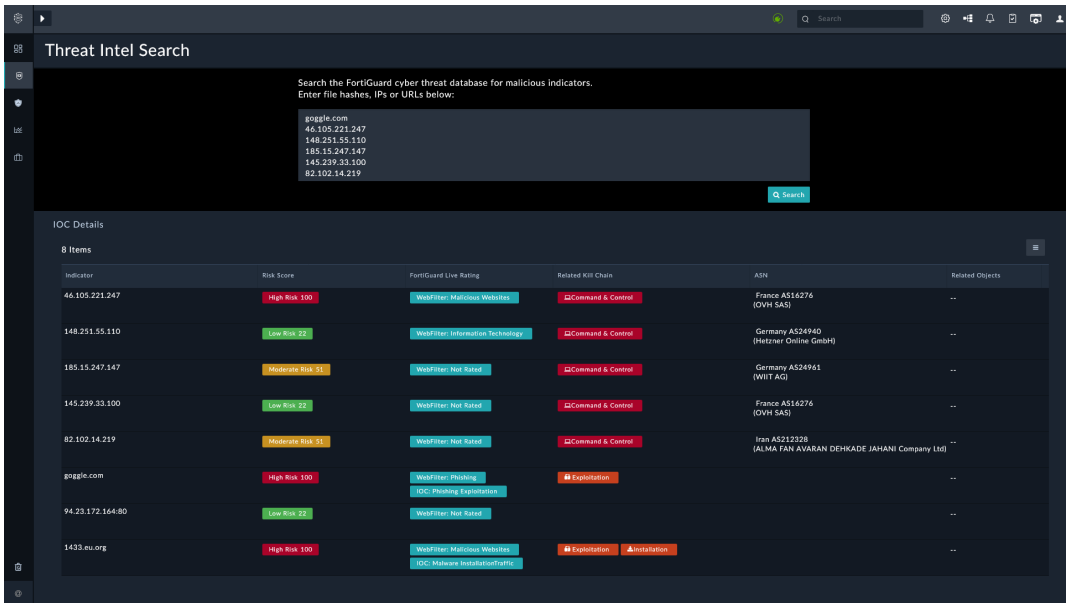
Threat Intel Search provides security teams with valuable intelligence, enabling efficient investigation, threat hunting, and incident response.

On the IOC search page, enter indicators separated by a line break. Maximum of 10 indicators are allowed. Click the button **Search** when done.

As an example, let's enter the following indicators in the **IOC Search** box and click **Search**:

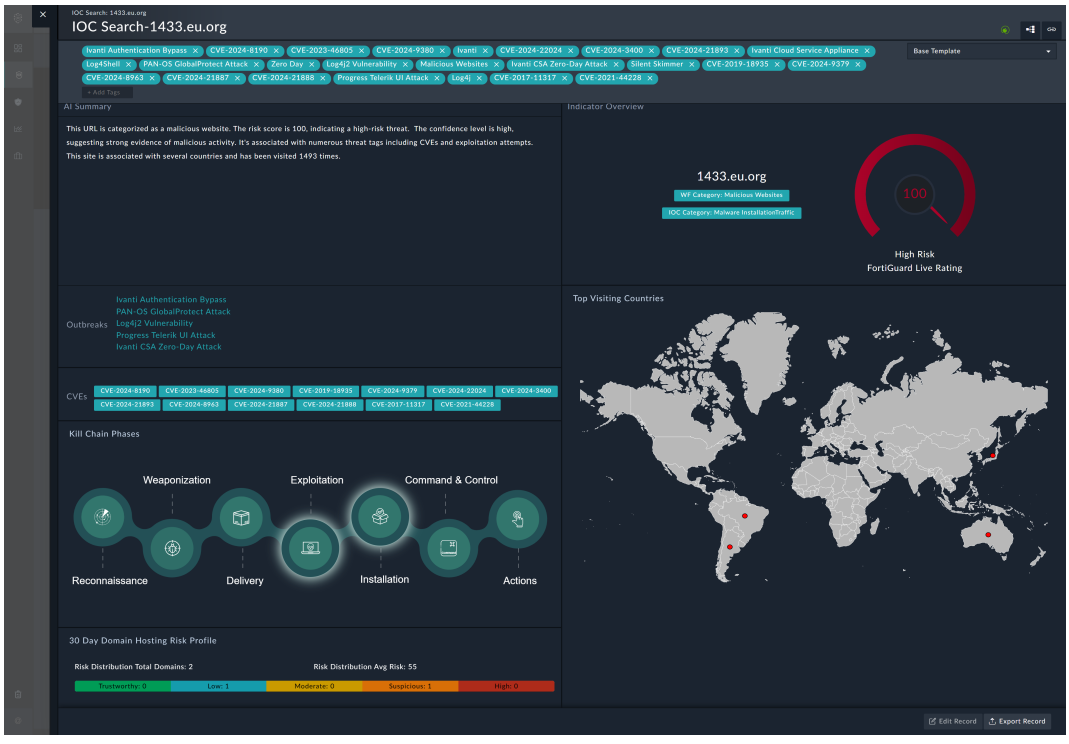
```
goggle.com
46.105.221.247
148.251.55.110
185.15.247.147
145.239.33.100
82.102.14.219
94.23.172.164:80
1433.eu.org
```

The following is the results page after searching for these IOCs:



Dashboard

The dashboard presents a threat intelligence snapshot of a high-risk IOC (`1433.eu.org`) based on *CVEs*, *outbreak mapping*, and *adversary tactics*. The following is a description of each section:



The phases do not appear highlighted in Mozilla's Firefox browser.

AI Summary

Located at the top-center, this section provides an automated risk analysis summary. For example, for `1433.eu.org` you can see the following:

- **Risk Score**: 100 (High Risk)
- **Confidence Level**: High
- **Threat Indicators**: Strong evidence of malicious activity, exploitation attempts, and threat tags.
- **Reputation Insight**: Site visited over 1,493 times and tied to multiple geographies.

Indicator Overview

Displays the risk score as a percentage value of the IOC. For example, for `1433.eu.org` you can see the following:

- **Indicator**: 1433.eu.org
- **Web Filter Category**: Malicious Websites
- **IOC Category**: Malware Installation/Traffic
- **Live Threat Score**: Visualized using a red dial gauge marked at 100 (maximum risk).

Tags

A series of tags summarize the following:

- Associated CVE identifiers
- Named threats and exploits (For example: Log4J, Zero Day, Silent Skimmer)
- Mapped outbreaks and exploitation techniques

Top Visiting Countries

The world map displays geo-located interaction:

- Red dots indicate top visitor origins (For example: East Asia, Australia, and South America).
- Useful for understanding global exposure and potential threat spread.

Outbreaks

This section highlights active threat campaigns or vulnerabilities with which the IOC is associated. For example, for `1433.eu.org` you can see the following:

- Ivanti Authentication Bypass
- PAN-OS GlobalProtect Attack
- Log4J Vulnerability

- Progress Telerik UI Attack
- Ivanti CSA Zero-Day Attack

CVEs

The CVE panel includes a horizontal scroll list of relevant vulnerabilities. For example, for `1433.eu.org` you can see the following:

- CVEs span from 2017 to 2024
- Includes critical flaws like `CVE-2024-8190`, `CVE-2023-46805`, `CVE-2017-11317`
- Helps contextualize how the threat is exploiting known weaknesses

Kill Chain Phases

This section maps IOCs to Lockheed Martin's **Kill Chain Phases**: `Reconnaissance` > `Weaponization` > `Delivery` > `Exploitation` > `Installation` > `Command & Control` > `Actions`

- The phase in which the IOC currently is highlighted.
- Indicates that the IOC is tied to **full-lifecycle attack activity**

30-Day Domain Hosting Risk Profile

Displays hosting reputation and activity over the past month. For example, for `1433.eu.org` you can see the following:

- **Total Domains:** 2
- **Average Risk Score:** 55
- **Trust Level Distribution**:
  - High Risk: 1
  - Suspicious: 1
  - Moderate, Low, Trustworthy: 0

Threat Reports

FortiGuard Threat Reports provide in-depth analysis of active cyber threats, designed to help defenders respond quickly and effectively. These reports follow standard industry conventions and typically include the following critical components:

- **Threat Summary**: A high-level overview of the threat, including:
  - Threat Name / Campaign Identifier (For example: *Horabot*)
  - Initial Discovery Date
  - Primary Objective (e.g., phishing, credential theft, malware delivery)
  - Target Geography / Sectors
- **Threat Actors (Attribution)**: Details on the group(s) behind the attack, if known:
  - Associated APT groups
  - Known aliases

  - Motivation (e.g., financial gain, espionage)
- **Attack Vector & Delivery Method**: Describes how the attack begins, such as:
  - Phishing emails or malicious attachments
  - Compromised websites or drive-by downloads
- **Technical Analysis**: In-depth details about the malware or exploit, covering:
  - Malware behavior and capabilities (e.g., keylogging, lateral movement)
  - Indicators of Compromise (IOCs)
  - Command & Control (C2) infrastructure
  - Evasion techniques
- **Detection & Mitigation**: Practical guidance including:
  - Detection signatures and platform support from Fortinet Fabric (FortiGate, FortiEDR, etc.)
  - Recommended mitigation steps
  - Patches or configuration changes
  - Threat hunting tips using SIEM tools
- **CVE References**: If vulnerabilities are exploited, relevant **CVE identifiers** are listed to help patching.

With FortiTIP Cloud's Threat Reports you can perform the following using a single source of truth:

- Focus on the **Summary, IOCs, and Mitigation** first for operational action.
- Use **Threat Actor** and **TTPs (Tactics, Techniques, Procedures)** for contextual threat hunting.
- Integrate **IOCs into detection systems** and cross-check against internal telemetry.
- Regularly check **CVE status** and apply relevant patches.

Threat Intel Management

Modern cybersecurity challenges are largely about persistent, smart, and well-armed threat actors, an overload of security alerts, false alarms (aka Alert Fatigue), disparate security systems, and a dearth of skilled professionals. A well-designed Threat Intelligence Framework (powering a practice) helps to mitigate these challenges.

Contextual, actionable threat intelligence is the key, and the FortiTIP Cloud threat intelligence solution, fueled by the threat intelligence lifecycle, is built on that premise. It is purpose-built for threat intelligence teams, as it is contextual, collaboration-friendly, and easily understood, it allows for preparing actionable and timely intelligence, and most importantly, it is evolving in nature, such that it eventually meets its requirements.

The Threat Intelligence Management gathers raw data about emerging or existing threat actors and threats from several sources. It then analyzes and filters this data to produce threat intelligence feeds and reports that contain information to help automate security control solutions. The following are some of the notable features:

- **Aggregation of intelligence from multiple sources** - A mature threat intelligence platform consumes and correlates data from external and internal sources, providing threat intelligence analysts with more comprehensive insights into known or suspected threats. The feeds can be structured (STIX, CSV) or unstructured (PDF threat reports).
- **Curation, normalization, enrichment, and risk scoring of data**: Many of the inputs to a threat intelligence platform can be duplicate, no longer malicious, or not enough of a threat to merit action. FortiTIP Cloud sorts the information and weighs the individual indicators of compromise (IOCs) based on a multitude of factors that are relevant to cyber threats. Curated indicators appear in an easy-to-read format with a risk score and associated intelligence.
- **Integration**: FortiTIP Cloud acts as an intermediary between information and your existing security solutions, eliminating the need to configure a connection manually. Various systems process these indicators as follows:
  - Firewalls and intrusion detection systems receive indicators for active blocking;
  - SIEMs and endpoint solutions correlate these indicators against available information to prioritize alerts
  - Orchestration platforms to use these indicators to improve workflows.
    The flexibility of these integrations rapidly improves the ability of a security team to identify and counter threats. This holds true whether an organization's security stack is entirely cloud-based, on-premises, or any combination of the two.
- **Analysis and sharing of threat intelligence**: Securely sharing threat intelligence creates more comprehensive, reliable outputs that help analysts quickly respond to threats. Threat actors reuse many of their techniques, tactics, procedures, and strategies to target similar organizations and infrastructures. Comprehensive information and context around malicious actors make it quicker and easier for your security team to prevent them from doing significant harm.

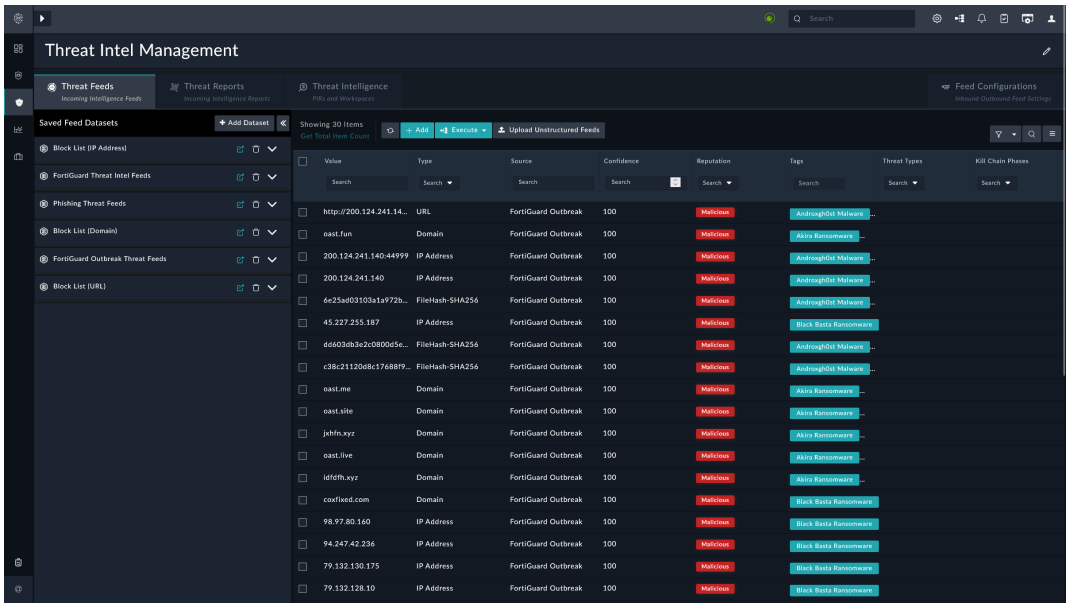
Threat Intel Feeds

FortiTIP Cloud's **Threat Intel Management** brings Security Orchestration and Automated Response (SOAR) and Threat Intel Management (TIM) worlds closer by introducing advanced Threat Intel Management capabilities.

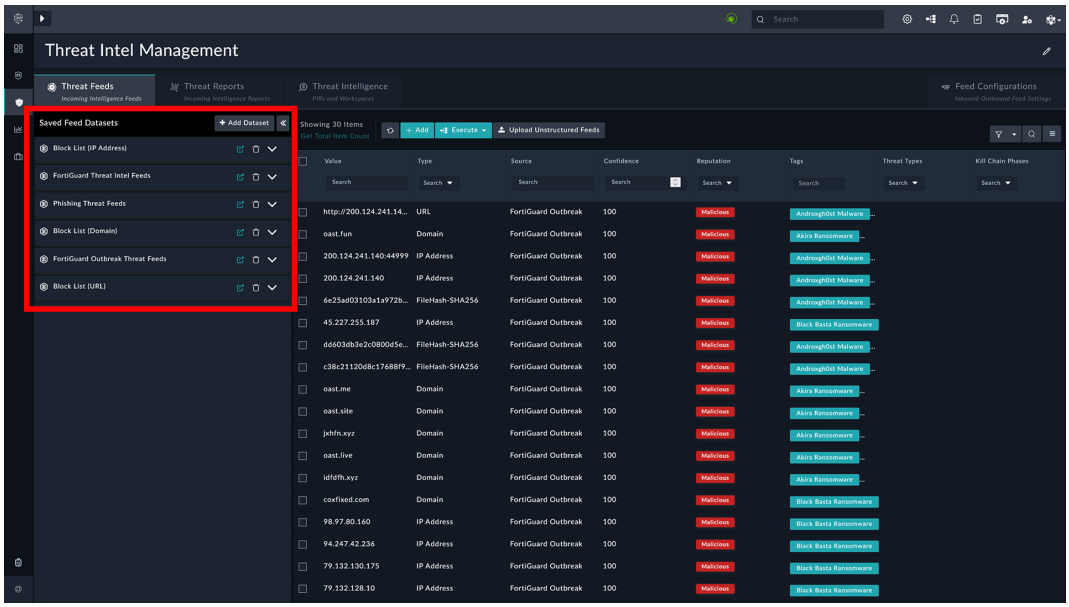
The solution provides multiple ways to manage the volume of threat feeds data by parameters such as feed and source confidence, TLP, severity, Expiry/Age, etc. Additionally, the solution helps create feed datasets to filter and group relevant feeds for use in sharing, exporting, or eventually as useful data reference while creating contextual threat intelligence.

The Threat Intel Management Configuration Wizard must be run before this feature can be used. Refer to the section Setup Threat Intel Management in Threat Intel Management documentation.

Using a wide variety of feed integrations that are available on the **Content Hub**, you can seamlessly ingest feeds and get a normalized and aggregated view of the feeds on the **Threat Feeds** tab of **Threat Intel Management** > **Threat Intel Feeds**:



The noise associated with the feeds is the main hurdle to managing feeds and deriving utility from these feeds. Therefore, as a first-level of filtration, FortiTIP Cloud's **Threat Intel Management** allows you to create **Datasets**. The **Manage Datasets** arrow » can be used to hide, and bring into view, the datasets created out-of-the-box or to add new datasets:



The time of the creation of feeds at intel source appears under the field *Created at Source*. Similarly, *Modified at Source* shows the time of modification at the intel source.

Feed Configurations

The Feed Configuration tab contains settings for easy feed management and dissemination. It has following tabs:

- **Feed Sources**: Directs you to a Content Hub page that lists and helps install connectors that can fetch threat intel feeds.
- **Threat Feed Rules**: Helps manage incoming threat feeds through rules. For more information, refer to the Configuring Feed Rules.

Importing Feeds from Files

1. Enable the option **Ingest Threat Feeds From Files** under **Feed Configurations** > **Ingest Unstructured Threat Feeds** and click **Save**.
2. Navigate to **Threat Intel Management** > **Threat Feeds Tab**.
3. Click the button **Upload Unstructured Feeds**.
4. Under **File to Import**, click to browse and upload the file. Supported file formats are `csv`, `txt`, `pdf`, `eml`, `json`, and `xlsx`.
5. **Confidence**: Specify the confidence score to assign to the ingested unstructured threat feeds.
6. **Reputation**: Select the reputation to assign to the ingested unstructured threat feeds.
7. **TLP**: Select the TLP to assign to the ingested unstructured threat feeds.
8. **Feed Expiry**: Specify the number of days after which the ingested unstructured threat feeds are marked as expired for deletion.
9. **Feed Source**: Specify a value to be updated as *Source* for all ingested unstructured threat feeds.
10. **Tags**: Specify comma-separated values to be assigned as tags to the ingested unstructured threat feeds.
11. Select the option **Automatic Block IOC** to block threat feeds immediately on ingestion. Leave unchecked to manually block threat feeds later.

Adding a Dataset

You can create a different dataset from the feeds to filter unwanted noise:

1. Navigate to **Threat Intel Management** > **Threat Intel Feeds**.
2. Click the button **+ Add Dataset**, under the tab **Threat Feeds**.
3. Enter the **Dataset Label** and **Filter Criteria** to filter the targeted dataset.
4. Click **Save Dataset**.

For more information related to Threat Intel Management, refer to the Threat Intel Management documentation.

MITRE ATT&CK

The MITRE ATT&CK module in FortiTIP enhances threat intelligence by aligning adversary behaviors with the globally recognized MITRE ATT&CK framework. This feature allows security teams to map observed indicators and threats to known Tactics, Techniques, and Procedures (TTPs), enabling improved detection, investigation, and threat hunting.

FortiTIP organizes ATT&CK data into six dedicated tabs:

- **Groups**: Known adversary groups and their associated techniques.
- **Tactics**: High-level objectives attackers pursue (e.g., Initial Access, Execution)
- **Techniques**: Specific methods used to achieve a tactic (e.g., Spearphishing Attachment).
- **Sub-Techniques**: Granular forms of techniques offering deeper behavioral context.
- **Software**: Tools, malware, and utilities used by adversaries.
- **Mitigations**: Defensive actions to prevent or reduce the impact of techniques.

An **Add** button on each tab enables users to manually create entries for the currently active category, ensuring custom or emerging data can be tracked alongside standard MITRE information.

For more information related to The MITRE® ATT&CK Framework, refer to the MITRE® ATT&CK Framework documentation.

Reports

Reports in FortiTIP Cloud provide users with detailed, customized views of security events, incidents, and threat intelligence. These reports are essential for summarizing critical data, analyzing trends, and sharing insights with stakeholders. Users can generate, filter, and export reports based on specific criteria such as incident types, attack vectors, and response times, facilitating comprehensive analysis and informed decision-making.

For more detailed information, please visit the FortiSOAR Reports documentation.

Resources

The **Resources** menu in FortiTIP Cloud offers a set of powerful tools and modules to enhance threat intelligence management and automation within the platform:

1. **Attachments**: Allows users to upload and store files in FortiTIP Cloud. These files can be submitted to third-party tools for scanning and analysis to assess suspicious files. For more details, refer to the Attachments section in FortiSOAR's user guide.
2. **Email Templates**: Pre-defined, customizable templates for automating email responses. These templates help streamline communication in response to security events and incidents. For more details, refer to the Email Templates section in FortiSOAR's user guide.
3. **Key Store**: A database of key-value pairs, which can also include JSON records. This feature supports automation and serves as an alternative to global variables. For more details, refer to the Key Store section in FortiSOAR's user guide.
4. **Assets**: A database for storing organizational assets, integrated with vulnerability management to help safeguard your environment from threats. For more details, refer to the Assets section in FortiSOAR's user guide.
5. **Content Hub**: A marketplace offering solution packs, widgets, and connectors to enable automated protection and seamless integration. For more details, refer to the Content Hub section in FortiSOAR's user guide.

This menu empowers users to manage critical resources effectively, ensuring streamlined threat intelligence operations and automation.

System Settings

Settings Configuration Page

You can customize FortiTIP Cloud and configure default system options, such as user display settings and notification preferences. To modify these settings, you must have CRUD permissions for the `Application` module, which is assigned by default to the `Application Administrator` role. For more information about roles, refer to the *Default Roles* section in the Security Management chapter.

Click the **Settings** icon to access the `System Settings`) page. Use this page and its tabs to customize FortiTIP Cloud as according to your needs:

- General Settings on page 37: Edit default options, particularly in the user profile.
- Application Configuration on page 39: Configure various administrative options for FortiTIP Cloud.

Additionally, use the `Viewing and Managing Audit Logs in FortiTIP Cloud on page 41` page (**Settings** > **Audit Log**) to view a chronological record of all actions across FortiTIP Cloud.

General Settings

On the `General` page, you can configure system settings, particularly those related to user profiles across FortiTIP Cloud. To apply changes, edit the settings and click **Save**. To undo changes, click **Revert**.

For detailed information on these settings, see the FortiSOAR Administration Guide.

Configuring System Health Monitoring

You can set up system monitoring for your FortiTIP Cloud instance. To receive email notifications of any FortiTIP Cloud service failure, or of any monitored threshold exceeding the set threshold, etc., click the **Enable Notification** checkbox in the `System & Cluster Health Monitoring` section, and then configure the various settings as per your requirements.

Managing Comments

A user with `Security Update` permissions can edit comments of any FortiTIP Cloud user, while a user with `Security Delete` permissions can delete comments of any FortiTIP Cloud user. There is no time limit for the Security user for these actions.

Users can edit and delete their own comments in the "Collaboration" window or in the Comments widget, provided the administrator has enabled comment modification settings and the user has appropriate CRUD permissions on the `Comments` module.

Setting the formats for Date and DateTime fields on the FortiTIP Cloud UI

You can customize the formats for Date and DateTime fields in the FortiTIP Cloud UI using standard syntax outlined in the Angular DatePipe documentation.

Customizing the behavior of the FortiTIP Cloud Setup Guide

The FortiTIP Cloud Setup Guide helps administrators configure FortiTIP Cloud to optimally based on best practices. By default, the **Setup Guide** icon is visible in the top-right corner of the FortiTIP Cloud UI.

To hide the **Setup Guide** icon, navigate to the `System Settings` page, clear the **Enable Setup Guide** option (selected by default), and click **Save**. Once the updated setting is saved, you will observe that the Setup Guide icon will not be visible in the top-right corner of the FortiTIP Cloud UI.

For more information on the FortiTIP Cloud Setup Guide, see the Setup Guide documentation.

Setting a language other than English for your FortiTIP Cloud system

FortiTIP Cloud supports 'Internationalization', allowing FortiTIP Cloud o adapt to the linguistic and cultural needs of specific locales. By default, the FortiTIP Cloud UI is in English, with additional support now available for the following languages:

- Japanese (Preview)
- Korean (Preview)
- Simplified Chinese (Preview)

'Preview' indicates that these translations were created using tools, which may result in inaccuracies or incomplete translations. Your feedback is essential to improving their accuracy. Changing the language may also impact the FortiTIP Cloud UI's layout, such as label text overflowing or buttons misalignment.

To change the system language for all users, select the desired language from the **Select Language** drop-down list in the `Set Language` section, then click **Save** to apply the change.

Configuring Themes

You can configure the FortiTIP Cloud theme that will apply to all the users in the system.

Non-admin users can change the theme by editing their user profile. Changes made by a non-admin user to the theme are applicable only to those users who have not changed their default user profile settings.

There are currently three theme options, **Dark**, **Light**, and **Space** (default). To change the theme, select your preferred option from the **Select a Theme** drop-down list. Click **Preview Theme** to view the changes and click **Save** to apply the theme. To revert to the default theme, click **Revert Theme**.

Configuring Default Country Code

You can configure the default country code format for contact numbers across the system. In the `Phone Number` section, select the **Default Country** and thereby the default country code that you want to apply across FortiTIP Cloud, and click **Save** to apply the code.

Configuring Navigation Preferences

You can configure the behavior of the left navigation bar across FortiTIP Cloud. You can choose whether you want the left navigation bar to collapse to just display icons of the modules or expand to display both icons and titles of modules. In the `Navigation Preferences` section, click **Collapse Navigation** to collapse the left navigation bar and click **Save** to apply the behavior of the left navigation bar across the system.

Enabling Light Mode Setting

You can enable the 'Light Mode' for the 'Grid' widget across modules by toggling the **Enable light mode** setting to **Enabled** (default is **Disabled**). This lighter version of the grid widget enhances performance and usability.

Application Configuration

Click the **Application Configuration** tab on the `System Settings` page to open the `Application Configuration` page. Here, you can configure various administrative settings that apply across FortiTIP Cloud. YAfter editing the settings, click **Save** to apply the changes or **Revert** to undo them.

For detailed information on these settings, see the FortiSOAR Administration Guide.

Purging audit logs, executed playbook logs, and recycle bin records, and reclaiming unused disk space

You can schedule the purging of audit logs and executed playbook logs globally. In the `Purge Logs` section, you can define the schedule for purging both Audit Logs and Executed Playbook Logs.

Configuring the logging level for Playbook Execution Logs

You can define the logging levels for playbook execution logs, both globally and at the individual playbook level. In the `Playbook Execution Logging Level` section, select either `INFO` or `DEBUG` as the global logging level.

Configuring Playbook Recovery

Use the autosave feature in playbooks to recover drafts in case of accidental closure your browser or if you face any issues while working on a playbook.

In the `Playbook Recovery` section, you can define the following:

- To disable playbook draft saving, clear the **Enable Playbook Recovery** option. By default, this option is checked.
- In the **Save Drafts Every** field, set the time (in seconds) after which FortiTIP Cloud will save drafts. By default, FortiTIP Cloud saves playbook drafts **15** seconds after the last change, with the minimum of **5** seconds.

Configuring playbook log movement to historical storage

FortiTIP Cloud optimizes storage by moving playbook logs to historical storage after playbooks complete their execution. By default, completed playbook logs are moved to historical storage every 15 minutes, while logs for failed or terminated playbooks is transferred every 60 minutes. In the `Playbook Log Movement` section, you can customize these settings.

Configuring the Simplified Expression View

By default, the **Simplified Expression View** option is selected, which renders a simplified expression based on tags rather than the full Jinja expression in the playbook designer. If you deselect this option, then the full Jinja expressions are displayed in the playbook designer.

Configuring the default timezone for exporting reports

You can set a timezone that will be applied by default to all reports that you export from the `Reports` page. To apply the default timezone, in the `Report Export` section, click the **Enable Timezone Selection** option, then search for and choose the desired timezone from the **Timezone** drop-down list and click **Save**.

Managing user listings in `People` Lookup fields

To display only active users in 'people lookup' fields, such as `assignedTo`, across FortiTIP Cloud, ensure that the **Restrict people lookups to active users** checkbox in the `People Lookup Filter` section is selected. If cleared, then both active and inactive users will be displayed in people lookup fields.

Enabling `MIME` type validations for file uploads

You can restrict specific MIME types from being uploaded in Attachments, Comments, or any other modules that have fields of type 'File'. Using this option, administrators can restrict potentially malicious files of types such as .exe, .bat, etc.

from being uploaded into FortiTIP Cloud. FortiTIP Cloud has not added this restriction as defaults since there could be business use cases such as where users as part of automation read the file being sent to them in emails, and then upload the same to FortiTIP Cloud to be used in the future for different operations like sandboxing, etc. Administrators can enable MIME type validations for file uploads as per their organization's policies by adding MIME types in the **Restricted File MIME Types** section.

Additionally, you can block specific HTML tags and attributes from being added to HTML content in Rich Text fields. For more information, see the `Blocking specific HTML tags and attributes` section in the FortiSOAR Administration Guide.

Viewing and Managing Audit Logs in FortiTIP Cloud

To view the Audit Log, click **Settings** > **Audit Log**. The `Audit Log` page provides a chronological record of all actions performed across FortiTIP Cloud.

You can view the historical record of activities across FortiTIP Cloud using the Audit Log, the User-Specific Audit Logs, and the graphical representation of the Audit Log in the detail view of a record.

Audit Log Permissions

To access audit logs, ensure your role has the appropriate permissions:

- To view your own audit logs, you must have a role with a minimum of `Read` permission on the `Audit Log Activities` module. To view audit logs of all users, you must have a role with a minimum of `Read` permission on the `Security` and `Audit Log Activities` modules.
- To filter audit logs based on users you must have a role with a minimum of `Read` permission on the `People`, `Appliances`, and `Audit Log Activities` modules.
- To delete your own audit logs, you must have a role with a minimum of `Delete` permission on the `Audit Log Activities` module. To delete audit logs of all users, you must have a role with a minimum of `Delete` permission on the `Security` and `Audit Log Activities` modules.
  Note: The `Delete` permission on the `Audit Log Activities` module is removed for both `csadmin` and playbook appliances roles, and also this will not be enabled (checked) by default for the **Full App Permissions** role. Therefore, if you want any user or role to have the right to delete audit logs, you must explicitly assign the `Delete` permission on the `Audit Log Activities` module to that particular user or role.

If you cannot access the Audit Log, you must ask your administrator for access. FortiTIP Cloud displays an error if you attempt to access the logs without the necessary permissions.

You can explore activity history through:

- **Audit Log**: A chronological list of all the actions across all FortiTIP Cloud modules.
- **User-Specific Audit Logs**: A chronological list of actions for a specific user.
- **Detailed view of a record**: A graphical or grid view of actions performed on a specific record, displayed using the `Timeline` widget.

For detailed information about audit logs, see the FortiSOAR Administration Guide.

www.fortinet.com

Copyright© 2025 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's Chief Legal Officer, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.