



Security Operations Architecture Guide

FortiAnalyzer



DEFINE / DESIGN / DEPLOY / DEMO



Table of Contents

Change Log	3
What is Security Operations architecture?	4
Intended Audience	5
About this guide	5
Technology used	7
Data lake	7
SIEM	8
SOAR	11
Services	12
Additional features	13
Design concepts and considerations	14
What is your SOC going to look like?	14
When to add FortiAnalyzer units?	15
Design examples	16
Small SOC	16
Small SOC features	18
Medium SOC	26
Medium SOC features	28
More information	34
Feature documentation:	34



Change Log

Date	Change Description
2025-03-20	Initial release.



What is Security Operations architecture?

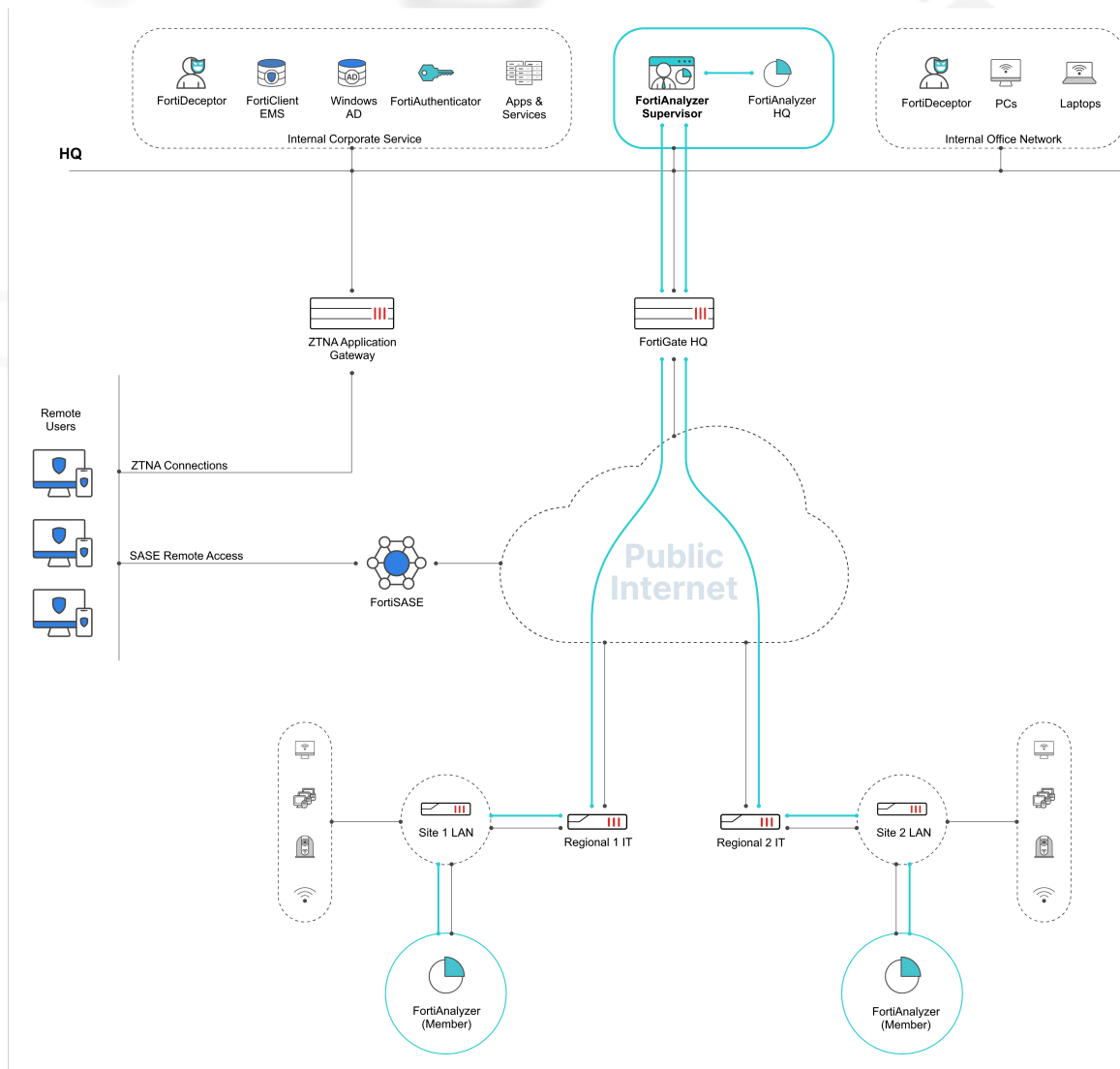
Based on the concepts described in the Concept guide, we will dive deeper into the Security Operations architecture and explore the features and components that can be utilized to build a Security Operations Center (SOC). In this exploration, we consider topologies where various forms of security are applied on the network.

For instance:

- NGFW on the edge providing security, SD-WAN connectivity, VPN connectivity between sites and various types of inspection on incoming and outgoing traffic (N-S traffic)
- ISFW that further implements micro-segmentation on the internal network to prevent malware from moving laterally in the E-W direction
- VPN gateway providing remote access into the internal network
- Zero trust application gateway to provide access control with added security posturing
- SASE to deliver security and connectivity for remote endpoints
- Endpoint security, from client based web, AV, application scanning to EDR software used to detect, contain, investigate and remediate cyber threats

Given the different types of scanning and monitoring that are deployed, a vast amount of logs and information about potential threats can be collected. By centrally storing these logs in a data lake, further analysis can be performed on the raw data to understand threats to users and devices on the network. Based on this analysis or based on predefined rules, responses to the threats can be launched using playbooks and connectors to remediate and neutralize the threats.

Below shows a topology of a medium sized enterprise that has deployed Fortinet's security fabric:



We will examine the tools, features, and components needed to effectively operate a SOC in a fabric-enabled enterprise.

Intended Audience

This document is for customers deploying an architecture that uses FortiAnalyzer device(s) as a data lake to benefit their internal or dedicated Security Operations Center (SOC). It assumes the reader has a working knowledge of FortiAnalyzer and their network architecture.

About this guide

The examples in this guide are based on FortiAnalyzer 7.6.

This document explains the technology in FortiAnalyzer which allows it to be used effectively in a security operations deployment. See [Technology used on page 7](#).

ABOUT THIS GUIDE

This document then suggests design considerations for implementing FortiAnalyzer and the relevant technologies in an architecture for an efficient SOC. See [Design concepts and considerations on page 14](#).

Finally, this document presents design examples for SecOps deployments with varying sizes of network architectures. See [Design examples on page 16](#).



Technology used

Data lake

FortiAnalyzer acts as the data lake, storing data from the devices in the Security Fabric for analytics and reporting. This data can include:

- Logs from Fortinet devices, such as FortiGate, FortiAuthenticator, FortiDeceptor, and more.
- Logs from third-party devices, such as Juniper, Zscaler, or SonicWall firewalls, and more. These logs are parsed using predefined log parsers built-in to FortiAnalyzer and from FortiGuard with a subscription to the [FortiAnalyzer SOC Automation Service](#).
- Unstructured data from Fortinet devices, such as mail attachments, PCAP files, and quarantined files.

Depending on how large your data retention needs are, you may use a combination of multiple FortiAnalyzer instances, FortiAnalyzer Collectors, or a FortiAnalyzer Fabric. Each of these components contribute to the FortiAnalyzer data lake; the principal difference is in how logs are stored.

The table below briefly explains how the data lake differs in these general architectures.

FortiAnalyzer architecture	Data lake description
<p>FortiAnalyzer</p>	<p>FortiAnalyzer stores logs in a columnar “Analytics” database as well as a compressed raw log “Archive”. Additional databases store normalized Fabric logs for SIEM functions.</p> <p>The log storage policy governs the allocation of storage between the Analytics database and Archive, including how long logs are stored before they are pruned. Note that SIEM and SOAR functions operate on the Analytics database. However, logs can be re-imported from the Archive to the Analytics database at any time.</p> <p>FortiAnalyzer units in Collector mode provide two main benefits; a log-stream buffer for high log volumes and an additional tier of “warm” log storage. The group of Collectors and Analyzer instances act as the data lake; SIEM and SOAR functions performed by the FortiAnalyzer(s) in Analyzer mode.</p> <p>If there are multiple FortiAnalyzer units in Collector mode, they can forward their logs to the FortiAnalyzer in Analyzer mode. The group of FortiAnalyzer units act as the data lake, and all SIEM and SOAR functions can be performed on the FortiAnalyzer in Analyzer mode.</p>
<p>FortiAnalyzer Fabric</p>	<p>Logs (Analytics and Archive) are stored on the FortiAnalyzer Fabric members, and the FortiAnalyzer Fabric supervisor can also act as a single pane of glass for data on all members of the FortiAnalyzer Fabric. The key differentiator compared to an architecture with multiple FortiAnalyzer Collectors is that the regional SOC teams can also benefit from a fully functional Analyzer when using their FortiAnalyzer Fabric member. The Collectors, by contrast, provide a historical log view which can be easily recovered central Analyzer using the log pull function.</p> <p>For more information, see the FortiAnalyzer Fabric Deployment Guide.</p>

In each of these scenarios, FortiAnalyzer is an integrated data lake which allows you to perform SIEM and SOAR functions directly on the device.

SIEM

Security information and event management (SIEM) functions can be performed directly on the FortiAnalyzer; you can use logs in the data lake to detect incidents, investigate threat information and affected assets, and respond with integrated playbooks and connectors.

Feature	Description
SIEM log parsers	<p>The predefined SIEM log parsers will parse, normalize, and correlate logs from Fortinet products as well as other third-party products. These logs are inserted into the SIEM database, and they are visible in FortiAnalyzer <i>Log View</i>. These logs can also be used in reports, event handlers, and FortiView monitors. For more information, see SIEM log parsers in the FortiAnalyzer Administration Guide.</p> <p>The FortiAnalyzer Security Automation Service is required to leverage premium predefined log parsers for many third-party products. This license provides monthly content packs released from FortiGuard. These tools are designed to help you detect, investigate, and respond to security incidents. For a complete list of predefined log parsers, see the FortiAnalyzer Fabric Normalization Reference. Additional predefined log parsers are available from FortiGuard with a valid license for the Security Automation Service.</p>
FortiView monitors	<p>FortiView is a comprehensive monitoring system for your network that integrates real-time and historical data into a single view. It can be used to log and monitor threats to networks, filter data on multiple levels, keep track of administrative activity, and more.</p> <p>Monitors are designed for network and security operation centers where dashboards are displayed across multiple large monitors. For more information, see FortiView > Monitors in the FortiAnalyzer Administration Guide.</p>
Indicators of Compromise	<p>The Indicators of Compromise (IOC) Service is a licensed feature. It helps to detect compromised hosts (endpoints) by comparing the IP, domain, and URL visited against the FortiGuard Threat Intelligence Database (TIDB). The TIDB package is updated daily from the FortiGuard distribution network (FDN) using Fortinet's global threat intelligence network. Compromised hosts are shown in FortiAnalyzer's FortiView. This enables operators to easily drill into compromised endpoints to display detected threats, which can be followed up with reports, event handlers, and incident reports.</p> <p>For more information, see Indicators of Compromise in the FortiAnalyzer Administration Guide.</p>

Feature	Description
Reports	<p>Summarize and analyze log data using predefined reports generated in FortiAnalyzer. Alternatively, you can use the predefined report templates, charts, and datasets to create custom reports according to your needs. Reports can be scheduled, automatically generated, and viewed in any of the following formats: HTML, PDF, XML, CSV, and JSON. For example, you can schedule reports according to threat trends, compliance requirements, or operational efficiency.</p> <p>For a list of predefined reports, see the List of report templates in the FortiAnalyzer Administration Guide.</p> <p>The following services from FortiGuard provide additional predefined reports that can support you in detecting and investigating security incidents.</p> <ul style="list-style-type: none"> • Security Automation Service • OT Security Service • Attack Surface Rating and Compliance • Outbreak Detection Service
Event handlers	<p>Event handlers generate events in FortiAnalyzer according to the logs. There are predefined event handlers available to detect threats, and you can also create custom event handlers according to your own needs. In FortiAnalyzer, you can review MITRE ATTACK® matrices to assess the event handler coverage in your network.</p> <p>You can respond to these events using SOAR functions to create incidents, quarantine endpoints, and perform further incident investigation.</p>
Incident reports	<p>Incidents can be created automatically or manually in FortiAnalyzer to track and analyze events. You can quarantine endpoints, execute playbooks, and block indicators using directly from incidents, allowing you to respond to the threats efficiently from the FortiAnalyzer.</p>
Indicator enrichment	<p>Indicators are suspicious IP addresses, domains, and URLs. A list of indicators can be found within the FortiAnalyzer GUI, and they can be enriched to provide security analysts with up-to-date, comprehensive threat intelligence from FortiGuard and VirusTotal.</p> <p>This feature allows the analysts to evaluate the risk posed by the indicator, so they can quarantine endpoints and proceed accordingly with related incidents. For ease of use, indicators can be enriched from the list in FortiAnalyzer or directly from the incidents that contain these indicators, streamlining the process for analysts to follow up.</p> <p>For more information, see Indicator enrichment in the FortiAnalyzer Administration Guide.</p>

Feature	Description
Outbreak Alerts	<p>An outbreak alert is a comprehensive report that provides in-depth insights into cybersecurity threats serving as a vital tool for organizations to stay informed about critical and or emerging cybersecurity risks that may compromise sensitive data, disrupt business operations, and pose significant risks to the organization's overall security.</p> <p>Each report provides the background of the attack, the timeline of events, affected technologies, and related threat intelligence such as Indicators of Compromise (IoCs), Tactics, Techniques, and Procedures (TTPs), and Attack sequences used by the adversaries. The related predefined reports and event handlers for these outbreak alerts require a valid license for the Outbreak Detection Service.</p> <p>For more information, see Outbreak Alerts in the FortiAnalyzer Administration Guide.</p>

SOAR

Security orchestration, automation, and response (SOAR) functions can be performed directly in the FortiAnalyzer, allowing you to respond to threats in your network quickly and efficiently.

Feature	Description
Connectors	<p>FortiAnalyzer connectors can be used for automation in playbooks, incident settings, and notification profiles. The basic suite of connectors includes FortiGuard, VirusTotal, and a connector for native FortiAnalyzer functions such as incident creation and report generation. Connectors and actions can also be created for third-party platforms such as ServiceNow, Slack, and Microsoft Teams. For example, connectors can automatically post incidents in ServiceNow or send notifications to a Slack or Teams channel.</p> <p>Connectors can also be used to integrate with the other Fortinet Fabric products such as FortiMail, FortiAuthenticator, and FortiSandbox. These connectors allow you to leverage your security fabric efficiently as part of playbooks within FortiAnalyzer.</p>
Playbooks	<p>Playbooks can be run in FortiAnalyzer to create/update incidents, enrich/block indicators, and quarantine endpoints. You can also perform many custom actions when the appropriate connectors are configured to the related Fortinet or third-party product.</p> <p>There are predefined playbooks to enrich indicators and create incidents for indicators of compromise, including other actions performed with the predefined connectors (FortiGuard, FortiAnalyzer).</p> <p>Some predefined playbooks are created automatically when you configure a connector, such as an EMS connector for FortiCASB connector. For example, once a FortiCASB connector is created, the <i>Get Cloud Service Data (FortiCasb Connector)</i> playbook is created to help detect shadow IT events in the network. For more information, see Connector actions in the FortiAnalyzer Administration Guide.</p>

Feature	Description
Notification profiles	Notification profiles are used to send alert notifications when an event is generated by an event handler. You can configure the notification profile to send the alert to an email address, SNMP community, and/or syslog server. You can also configure the notification profile to send the alert through a connector, such as Slack or MS Teams.

Services

FortiAnalyzer security services may be required to provide and enhance the SIEM and SOAR services described above. Below is a brief description of the core services and how they can be a benefit to SecOps deployments.

Service	Description
Security Automation Service	This service provides monthly content packs released from FortiGuard. You can leverage these premium predefined reports, event handlers, and log parsers in FortiAnalyzer to help detect, investigate, and respond to security incidents. A key benefit of this service is to integrate FortiAnalyzer with third-party devices using predefined log parsers for cross-platform reporting and automation. See FortiAnalyzer SOC Automation on the FortiGuard website.
Outbreak Detection Service	This service allows you to view outbreak alerts from the FortiAnalyzer GUI, providing real-time insights. It also provides predefined reports and event handlers to detect and respond to these outbreak alerts. These reports and event handlers are automatically downloaded from FortiGuard when they are available. See Outbreak Detection Service on the FortiGuard website.
OT Security Service	This service benefits those monitoring Operational Technology (OT) environments. It provides information regarding OT/IoT vulnerabilities displayed in the FortiAnalyzer GUI, including: A breakdown of OT/IoT vulnerabilities with corresponding severity Top 10 OT/IoT vulnerabilities by number of occurrences Top 10 assets with OT/IoT vulnerabilities Details of the vulnerabilities per endpoints In addition to the advanced analytics displayed within the FortiAnalyzer GUI, this service also provides predefined risk/compliance reports and event handlers to monitor the OT environment. See the FortiAnalyzer Data Sheet .
Attack Surface Rating and Compliance	Also known as the FortiGuard Security Rating Update, this service supports compliance reporting and continuous risk assessment.

Service	Description
Indicators of Compromise Service (IOCS)	<p>This service empowers security teams with forensic data from the IOCs daily, used in combination with FortiAnalyzer analytics to identify suspicious usage and artifacts observed on the network or in an operations system. These indicators of compromise have been determined with high confidence to be malicious infections or intrusions. In FortiAnalyzer, you can also perform a historical rescan of logs for threat hunting using the IOC information. See Indicators of Compromise on the FortiGuard website.</p> <p>For more information, see the related Indicators of Compromise feature described above in SIEM on page 8.</p>

Additional features

The following are additional features in FortiAnalyzer which may also support your SecOps deployment, including your use of the SIEM and SOAR features in FortiAnalyzer.

Configuring a FortiAnalyzer Fabric for hierarchical visibility:

When you are using multiple FortiAnalyzer devices, configuring a FortiAnalyzer Fabric expands the size of your data lake and provides a single pane of glass for data on all those devices. In short, one of the FortiAnalyzer devices acts as a supervisor and it can perform SOC actions using data across all the FortiAnalyzer devices that are acting as members. The members can still be used independently as well, allowing you to leverage multiple SOC teams across different regions or sectors according to your architecture.

For more information about FortiAnalyzer Fabric, see the [FortiAnalyzer Fabric Deployment Guide](#).

Configuring High Availability (HA) for redundancy:

A FortiAnalyzer HA cluster can have a maximum of four units: one primary unit with up to three secondary units. All units in the cluster must be of the same FortiAnalyzer series. All units are visible on the network. All units must run in the same operation mode: Analyzer or Collector.

A FortiAnalyzer HA cluster provides real-time redundancy in case a FortiAnalyzer primary unit fails. Logs are synchronized securely among the units in the cluster, which protects the data lake. In addition, the HA alleviates the load on the primary unit by using secondary units for SIEM processes such as running reports.

You can also deploy an active-active HA cluster for a geo-redundant solution.

For more information, see [High Availability](#) in the FortiAnalyzer Administration Guide.

Leveraging FortiAI for efficiency in SOC processes:

A FortiAI subscription can be used in FortiAnalyzer for incident investigation, response, and threat hunting. The FortiAI assistant can interpret security events, generate detailed summaries, identify potential impacts, and make remediation recommendations. FortiAI can also simplify the FortiAnalyzer platform usage with natural language prompts. For example, the FortiAI assistant can create complex database queries, generate reports, write event handler and correlation rules, and execute many other FortiAnalyzer functions during typical workflow.

For more information, see [FortiAI](#) in the FortiAnalyzer Administration Guide.



Design concepts and considerations

What is your SOC going to look like?

FortiAnalyzer allows you to effectively establish an internal or dedicated Security Operations Center (SOC). The SOC analysts can use FortiAnalyzer as a data lake and to efficiently identify and respond to incidents within the network.

When using FortiAnalyzer as part of a SOC deployment, is important to consider the following:

- What are the existing components in your network?
 - Depending on the data you are collecting in your network, you may leverage specific features in FortiAnalyzer, or you may consider licenses for different services that benefit your network.
- What is the size of your company?
 - Based on the size of your company, you may require more FortiAnalyzer units to collect data to account for a large number of logs, or you may consider creating a FortiAnalyzer Fabric to establish a hierarchical SOC structure monitoring different regions.
- Are there compliance requirements for your industry?
 - You may have uptime requirements that influence your need to use an HA cluster for FortiAnalyzer. Additionally, you may benefit from existing predefined premium reports that are available through a licensed service. For example, the HIPAA Compliance Security Rating Report requires a license for the FortiGuard Security Rating Update.
- What are your data retention requirements?
 - Most organizations will have pre-existing views or regulations for how long to keep “live” data, and separate views or regulations for long-term storage and redundancy. Analytics data is the live data used for FortiAnalyzer SIEM, SOAR, FortiView, and IOC functions. Most organizations would choose to have a minimum of 30 days of live data on hand, with a comfort factor of 60 days or more. For archive data, most organizations would require 365 days of archive on hand, but financial services and governmental organizations often require seven years or more. Both the Analytics and Archive data must be considered separately, and they must be factored into the data lake design.

When to add FortiAnalyzer units?

There are a few reasons you may consider adding more FortiAnalyzer units to your architecture.



In all cases, consider the type of units you are using in your architecture. Some FortiAnalyzer units will provide more storage capacity than others. FortiAnalyzer units forming an HA cluster must be the same type.

The [FortiAnalyzer datasheet](#) and [FortiAnalyzer BigData datasheet](#) provide the maximum constant log message rate that each FortiAnalyzer platform can maintain for minimum 48 hours without system performance degradation. To estimate your log rate, see [Log Rate](#) in the FortiAnalyzer Architecture Guide.

To estimate your storage requirements, see [Storage Requirements](#) in the FortiAnalyzer Architecture Guide.

Increase storage for data to hold more archive logs:

In this case, consider adding FortiAnalyzer units in Collector mode. These units forward logs for analytics to a unit in Analyzer mode; however, the storage space on the collectors can be used for archive logs.

Increase storage for data to use in analytics and/or create a hierarchical view across regions:

FortiAnalyzer units in Collector mode will not provide more space for data to use in analytics because the analytics are done with logs forwarded to the unit in Analyzer mode. In this case, consider adding FortiAnalyzer units to form a FortiAnalyzer Fabric. This allows you to use more units in Analyzer mode and also allows you to have one unit with central visibility. If there is a significant number of logs, you may also want to consider a larger FortiAnalyzer unit or FortiAnalyzer-BigData.

In addition to increasing storage for analytics, a FortiAnalyzer Fabric also establishes overarching visibility across the multiple FortiAnalyzer units. In particular, this is a benefit when the units are deployed across multiple regions or multiple SOC teams. One FortiAnalyzer unit at the SOC headquarters operates in supervisor mode while all other FortiAnalyzer units for the regional SOC teams act as members. Incident and event information is synced from members to the supervisor using the API. The members can be used as regular FortiAnalyzer units to review the data that they have collected individually; meanwhile, the supervisor can be used to review and correlate data collected by all members.

Add redundancy to reduce downtime:

In this case, you must add FortiAnalyzer units in an HA cluster. You can add up to four units in an active-passive cluster, and you must use the same type of FortiAnalyzer units to build the cluster. Creating an HA cluster does not increase the storage capacity. In an active-passive cluster, only the HA primary can receive logs and archive files from its directly connected device and forward them to HA secondary.

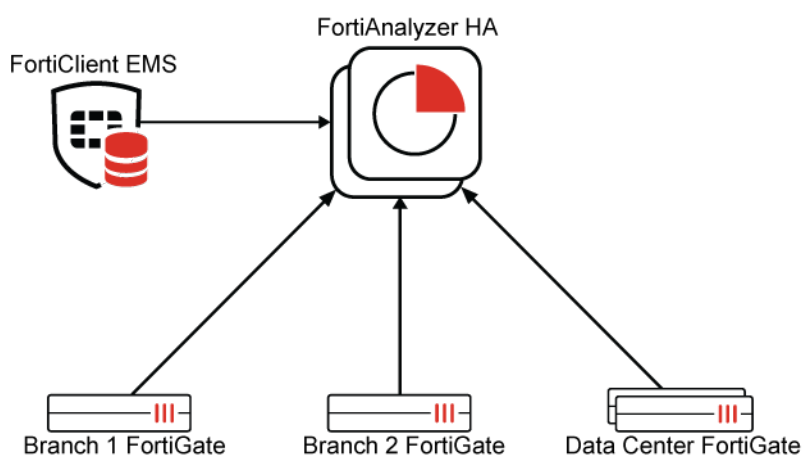
In an active-active cluster, all HA members can receive logs and archive files from its directly connected device and forward logs and archive files to its HA peer. However, this does not increase the total storage capacity.



Design examples

Small SOC

Topology



The above architecture is an example of a small SOC, where one FortiAnalyzer unit or cluster provides the data lake capabilities for the entire organization. This architecture may be appropriate for a small organization with a single site or a few sites in the same region that deploy FortiGates to uniformly log to a central FortiAnalyzer. In addition, a FortiClient EMS is used for managing remote endpoints running FortiClient.

A small SOC team will utilize the FortiAnalyzer Data Lake to monitor and respond to security activities that occur at each site. The FortiAnalyzer is used to generate reports and analyze logs from the FortiGate devices. The FortiAnalyzer is HA enabled for redundancy to maintain real-time logging without interruption for the SOC.

This example demonstrates the core concept of the SOC model as it relates to FortiAnalyzer. In short, there are components collecting logs in the network and sending the information to the data lake: FortiAnalyzer. While the network may get larger, this model of components sending data to the FortiAnalyzer remains the same. The SOC analysts can use FortiAnalyzer to respond to this data with:

- Event handlers to detect and identify threats
- *Log View* and *Reports* to review threats in more detail
- Incident reports to document follow up on threats in detail
- Playbooks to respond to threats immediately

Benefits

In this small SOC example, the following benefits are realized:

Component	Feature	Description
Multiple FortiAnalyzer units	HA redundancy	The FortiAnalyzer units are configured in HA active-passive mode to prevent interruption. This allows the SOC analysts to maintain visibility to the data from the FortiGate devices and FortiClient endpoints.
FortiGate devices	Network protection	As traffic traverses the FortiGate devices and inspection occurs, they send traffic, security, and event logs to the FortiAnalyzer. These logs can be reviewed in FortiAnalyzer <i>Log View</i> and they can also be used to create reports for further analysis. Logs that indicate threats to the network can also trigger predefined event handlers, creating incidents that can be followed up on by the SOC analysts. For some cases, the SOC analysts can configure playbooks in FortiAnalyzer which automate immediate response to these incidents. For example, the playbooks could automatically create and attach information to incident reports or forward the information to the affected parties through fabric connectors.
	Asset (IoT/OT) monitoring	When the FortiGate and FortiAnalyzer devices have licenses for IoT and OT monitoring, the SOC analysts can monitor the IoT/OT inventory and related vulnerabilities. The IoT dashboard provides an overview of the asset inventory and vulnerabilities; however, analysts can also use the <i>Asset Identity Center</i> in FortiAnalyzer to review assets and users in more detail for incident response and compliance.
FortiClient EMS	Endpoint vulnerability detection and response	The FortiClient EMS sends traffic, event, and vulnerability scan information to the FortiAnalyzer. The SOC analysts can review this information in dashboards and reports to respond accordingly. For example, the <i>Endpoint Security Vulnerability Report</i> provides a comprehensive security rating overview and historical trends specifically for all managed endpoints based on the vulnerabilities. This report utilizes retrieved data from FortiClient EMS and FortiGuard, including the outbreak alert and endpoint vulnerability information.
	Event correlation with user and device information	Configuring an EMS Connector allows the FortiAnalyzer to call the EMS API to get all endpoints and vulnerabilities data, and this information will be inserted as fabric (SIEM) logs. This allows FortiAnalyzer to correlate these logs with logs from other devices as part of event handlers and reports. The information is also used to populate dashboards, such as the <i>Endpoint Vulnerability</i> dashboard.

Small SOC features

The following features can be used in FortiAnalyzer as part of this small SOC example:

- [Event handlers](#)
- [Log View](#)
- [Incidents](#)
- [Connectors and playbooks](#)
- [SOC dashboard](#)
- [IoT dashboard](#)
- [Asset Identity Center](#)
- [Endpoint vulnerability dashboard](#)

Event handlers

Event handlers allow the SOC analysts to proactively monitor threats. Many event handlers that use FortiGate logs are enabled by default. SOC analysts can review these event handlers to integrate them into their workflow, including how to respond to the resulting events.

Enterprise_FortiAnalyzer					
<div> <div> Dashboards Device Manager FortiView Log View Fabric View Incidents & Events Incidents Event Monitor Event Handlers Indicators Outbreak Alerts Automation Log Parsers Safeguarding FortiAI Reports System Settings </div> <div> Event Handlers Data Selectors Notification Profiles </div> </div>					
<div> <div> + Create New Edit Delete Clone More </div> <div>Search...</div> </div>					
Statu	Name	Rules	Origin	Data Selector	
<input type="checkbox"/>	Default-Access-to-a-Suspicious-Domain-After-Risky-App-Detected High/Critical risk App detected followed by connection to a new registered d...	Risky App Detected FOLLOWED_BY[10m] Access to...	Built-in		
<input type="checkbox"/>	Default-Access-to-a-Suspicious-Domain-and-Malware-Downloaded Access to a suspicious domain and attempted to download malware but bloc...	Malware Download Detected AND Access to Suspici...	Built-in		
<input type="checkbox"/>	Default-Attack-Event-Detected-After-Malware-Downloaded Malware download detected followed by an attack event may indicate the en...	Malware Download Detected FOLLOWED_BY[10m] ...	Built-in		
<input type="checkbox"/>	Default-Botnet-Communication-Detection Default event handler to detect botnet communication and report to FortiGate	Rule-1 Traffic to Botnet CnC blocked in virus log: (Defau Rule-2 Traffic to Botnet CnC detected in virus log: (Defai Rule-3 DNS traffic to Botnet CnC blocked: (Default,Botn Rule-4 Traffic to Botnet CnC detected in ips log 1: (Defai	Built-in		
<input type="checkbox"/>	Default-Botnet-Communication-Detection-By-Endpoint Default event handler to detect botnet communication in network grouped b...	Rule-1 Traffic to Botnet CnC blocked in virus log: (Defau Rule-2 Traffic to Botnet CnC detected in virus log: (Defai Rule-3 DNS traffic to Botnet CnC blocked: (Default,By_E Rule-4 Traffic to Botnet CnC detected in ips log 1: (Defai	Built-in		
<input type="checkbox"/>	Default-Botnet-Communication-Detection-By-Geo-Location Default event handler to detect botnet communication in network grouped b...	Rule-1 Traffic to Botnet CnC blocked in virus log: (Defau Rule-2 Traffic to Botnet CnC detected in virus log: (Defai Rule-3 DNS traffic to Botnet CnC blocked: (Default,By_C Rule-4 Traffic to Botnet CnC detected in ips log 1: (Defai	Built-in		
0% 266					

In the example below, the event handler "Default-Malicious-Code-Detection-By-Threat" generates an event according to the rule "Intrusion blocked group by dstendpoint". The SOC analysts can respond to this event by following up with an incident report or by initiating a custom

playbook, if needed.

The screenshot shows the Fortinet Enterprise FortiAnalyzer Event Monitor interface. The left sidebar contains navigation options: Dashboards, Device Manager, FortiView, Log View, Fabric View, Incidents & Events (with sub-items: Incidents, Event Monitor, Event Handlers, Indicators, Outbreak Alerts, Automation, Log Parsers, Safeguarding), FortiAI, Reports, and System Settings. The main panel displays a table of events filtered by 'By Threat'. The table has columns: Event, Event Status, Event Type, Count, Severity, First Occurrence, and Handler. The selected event is 'MS.SMB.Server.SMB1.MID.FID.' with a status of 'Mitigated' and a count of 10. Below the table, it indicates '1 Selected'.

Event	Event Status	Event Type	Count	Severity	First Occurrence	Handler
VBA/Agent.LAG/tr.dldr (2)	Mitigated	Antivirus	2	Medium	6 minutes ago	Default-Malicious-File-Detection-By-Threat
MS.SMB.Server.SMB1.MID.FID.	Mitigated	IPS	10	Medium	25 minutes ago	Default-Malicious-Code-Detection-By-Threat
Intrusion from LAN-SALE-SIMUL/	Mitigated	IPS	2	Medium	2025-01-16 13:52:11	Default-Malicious-Code-Detection-By-Threat
Intrusion to DMZ-PUBLIC-SERVE	Mitigated	IPS	5	Medium	2025-01-16 13:37:44	Default-Malicious-Code-Detection-By-Threat
Intrusion from 10.100.94.15 block	Mitigated	IPS	3	Medium	2025-01-16 13:37:44	Default-Malicious-Code-Detection-By-Threat
BlackMoon (2)	Unhandled	IPS	7	High	33 minutes ago	Default-Botnet-Communication-Detection-By
Malware.Sinkhole (4)	Unhandled	IPS	22	High	31 minutes ago	Default-Malicious-Code-Detection-By-Threat
176.31.62.76 (21)	Unhandled	Traffic	258	Critical	43 minutes ago	Default-Compromised-Host-Detection-IOC-By
Hikvision.Devices (1)	Unhandled	Application Control	8	High	40 minutes ago	Default-Risky-App-Detection-By-Threat

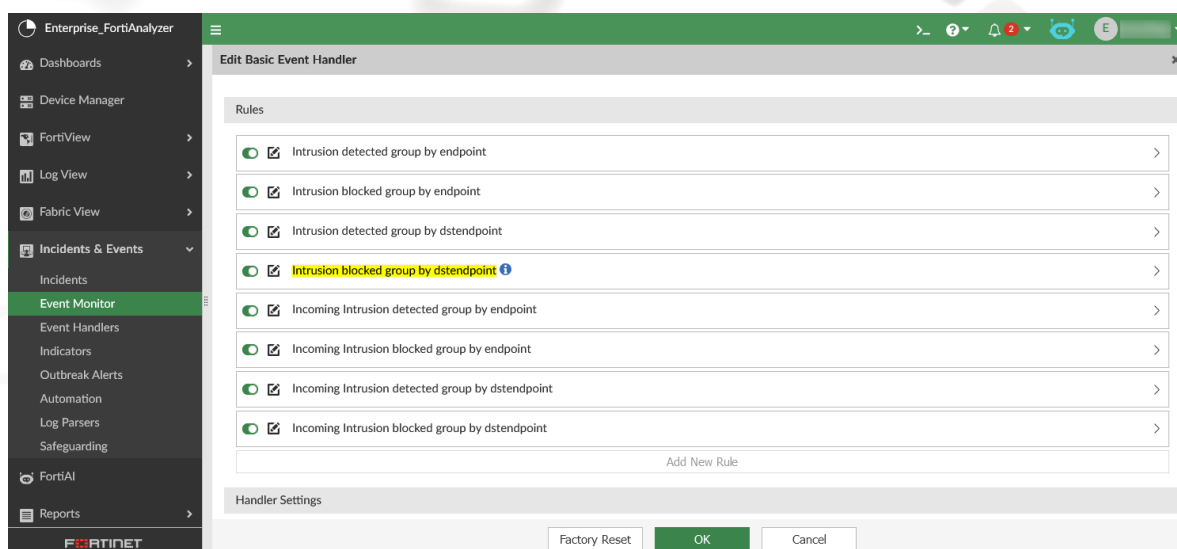
The screenshot shows the 'Edit Basic Event Handler' configuration page in Fortinet Enterprise FortiAnalyzer. The left sidebar is the same as the previous screenshot. The main panel contains the following fields:

- Status:** On (toggle)
- Name:** Default-Malicious-Code-Detection-By-Threat
- Description:** Default event handler to detect attacks and malicious codes in network traffic grouped by threat
- MITRE Tech ID:** Click to select
- Data Selector:** Default Intrusion Selector For Malicious Code Detection
- Automation Stitch:** Off (toggle)
- Automatically Create Incident:** Off (toggle)

Below these fields is a 'Rules' section with a list of rules, each with a checkbox and a right arrow:

- ☒ Intrusion detected group by endpoint
- ☒ Intrusion blocked group by endpoint
- ☒ Intrusion detected group by dstendpoint
- ☒ Intrusion blocked group by dstendpoint
- ☒ Incoming Intrusion detected group by endpoint

At the bottom, there are buttons for 'Factory Reset', 'OK', and 'Cancel'.



Additionally, SOC analysts can review the event handlers that are disabled by default and enable them according to their needs. If needed, SOC analysts can configure custom event handlers and rules to identify threats in the network.

Log View

The SOC analysts can filter *Log View* to review data from the FortiGate devices in detail.

#	Date/Time	Data Source	Event Message	Event Type	Event Severity	Source IP	Destination IP	Host Name	User ID	Application Name
1	2025-02-07 1	FGVM02TM2		traffic	notice	10.1.100.118	172.18.62.16	DESKTOP-B2	ec_frank118	HTTPS
2	2025-02-07 1	FGVM02TM2	Network.Servi	utm	information	10.100.92.13	10.100.88.5			SSL_TLSv1.3
3	2025-02-07 1	FGVM02TM2	Network.Servi	utm	information	10.100.92.13	10.100.88.5			SSL
4	2025-02-07 1	FGVM02TM2		traffic	notice	10.100.92.12	142.251.33.7			YouTube
5	2025-02-07 1	FGVM02TM2		traffic	notice	10.100.92.12	157.240.3.35			Facebook
6	2025-02-07 1	FGVM02TM2		traffic	notice	10.100.93.2	2.17.85.56	LAN-IT-ADMI		HTTPS.BROWSER
7	2025-02-07 1	FGVM02TM2		traffic	notice	10.100.92.12	142.251.33.1			Google.Services
8	2025-02-07 1	FGVM02TM2		traffic	notice	10.100.92.12	10.100.88.5			SSL_TLSv1.3
9	2025-02-07 1	FGVM02TM2		traffic	notice	10.100.92.19	8.8.8.8	LAN-FINANC		DNS
10	2025-02-07 1	FGVM02TM2		traffic	notice	10.100.92.19	8.8.8.8	LAN-FINANC		DNS
11	2025-02-07 1	FGVM02TM2		traffic	notice	10.100.92.19	8.8.8.8	LAN-FINANC		DNS
12	2025-02-07 1	FGVM02TM2		traffic	notice	10.100.92.19	8.8.8.8	LAN-FINANC		DNS
13	2025-02-07 1	FGVM02TM2		traffic	notice	10.100.92.19	8.8.8.8	LAN-FINANC		DNS
14	2025-02-07 1	FGVM02TM2		traffic	notice	10.100.92.19	8.8.8.8	LAN-FINANC		DNS
15	2025-02-07 1	FGVM02TM2		traffic	notice	10.100.93.2	142.251.33.7	LAN-IT-ADMI		YouTube



It is most efficient to review logs from *Log View > Logs > All*. This pane includes all analytic logs on the FortiAnalyzer, including normalized logs. This makes it easier for the SOC analysts to filter and correlate information from multiple Fortinet and third-party logging devices.

Incidents

When following up on data from the FortiGate devices, the SOC analysts can create incident reports within FortiAnalyzer. These incident reports support thorough follow-up by identifying the severity of the incident and attaching relevant details, such as reports and events. The SOC analysts can perform actions directly from the incident; for example, they can quarantine endpoints or execute playbooks.

The screenshot shows the FortiAnalyzer Incident Analysis interface. The left sidebar contains navigation options: Dashboards, Device Manager, FortiView, Log View, Fabric View, Incidents & Events (selected), Incidents (selected), Event Monitor, Event Handlers, Indicators, Outbreak Alerts, Automation, Log Parsers, Safeguarding, FortiAI, Reports, and System Settings. The main panel displays incident details for IN00000001, which is marked as High severity. The incident summary includes fields for Incident Number, Incident Name, Incident Date / Time, Incident Update Date / Time, Incident Category (Malicious Code), MITRE Tech ID (Click to select), Severity (High), Status (Analysis), Affected Endpoint (10.100.91.100), Description (IPS incident created for endpoint), and Assigned To (Not Assigned). The Affected Endpoint/User section shows 'No related user available.' and 'Last Seen' as 2025-01-16 10:58:03. The Affected Assets table lists the endpoint and a note: 'ep is not mature enough to tag epid into logs'. The interface includes buttons for Edit Layout, Export Incident, Enrich, Block, Execute Playbook, Run Report, Quarantine, and Refresh.

The screenshot shows the FortiAnalyzer Incident Analysis interface with the Events tab selected. The Events table lists four events related to the incident IN00000001:

Event	Count	Severity	Last Occurrence	Handler	Indicators
Threat ssl-anomaly detected	96	high	2025-01-16 10:57:18	SIEM_Alerts_Normalized_Logs	
Threat ip_dst_session detected	2	high	2025-01-16 10:56:25	SIEM_Alerts_Normalized_Logs	
Threat ip_src_session detected	2	high	2025-01-16 10:56:25	SIEM_Alerts_Normalized_Logs	
endpoint:10.100.91.100 attack:ip_dst_sessio	2	critical	2025-01-16 10:56:25	Intrusion Detection	

The Audit History section shows a timeline with a blue dot at 2025-01-16 11:48:25, indicating a report was attached to the incident. The Executed Playbooks table shows three playbooks:

Playbook	Status	Trigger
Demo Playbook- Run Vuln Scan	Success	IN00000001
Demo Playbook- Get Process List	Success	IN00000001
Demo Playbook- Get Software Inventory	Failed	IN00000001

Connectors and playbooks

To efficiently respond to these incidents, you can create playbooks using connectors to other devices in your security fabric. You can also leverage existing playbook templates for common tasks in the SOC. For example, with a valid EMS connector, you can use a playbook designed to quarantine endpoints directly from FortiAnalyzer. This playbook will also attach the data to an incident for further follow up from the SOC analysts.

Further playbook templates are also available for other tasks that can be completed in this small SOC example. For example, there are playbook templates for attaching reports to an incident (uses the localhost connector), quarantining endpoints from FortiGate (requires the FortiGate connector), and creating incidents for compromised hosts (uses the local host connector and requires an IOC license). Automating these tasks with playbooks help the SOC respond more efficiently to threats in the network.

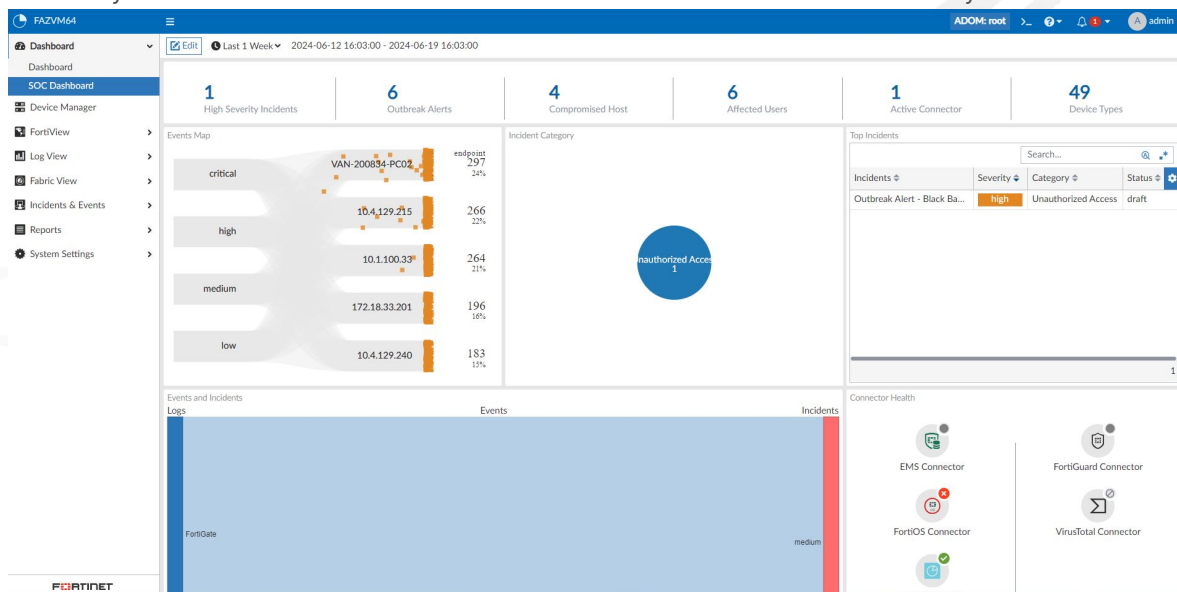
Name	Description	Status	Created Time	Modified Time	Protected
Get IP Reputation	Playbook to get IP reputation report through VirusTotal c...	Enabled	01/23/2024	01/23/2024	Yes
Get Domain Reputation	Playbook to get domain reputation report through VirusT...	Enabled	01/23/2024	01/23/2024	Yes
Get URL Reputation	Playbook to get URL reputation report through VirusTot...	Enabled	01/23/2024	01/23/2024	Yes
Incident - Run Report	Playbook to generate incident report	Enabled	05/02/2024	05/02/2024	Yes
EMS - Get Endpoint Process	Playbook to get endpoint process	Enabled	05/02/2024	05/02/2024	Yes
Quarantine Endpoint by EMS	Playbook to quarantine endpoint by EMS connector	Enabled	03/07/2024	03/07/2024	Yes
Indicator Enrichment	Enrich indicator with different connectors	Enabled	03/07/2024	03/07/2024	Yes
Quarantine Endpoint by EMS - AI	Playbook to quarantine endpoint by EMS connector - AI	Enabled	05/03/2024	05/03/2024	Yes

SOC dashboard

In this example, the SOC analysts can also benefit from using the SOC Dashboard in each of the FortiAnalyzer members. This dashboard includes the following information to support an efficient SOC team:

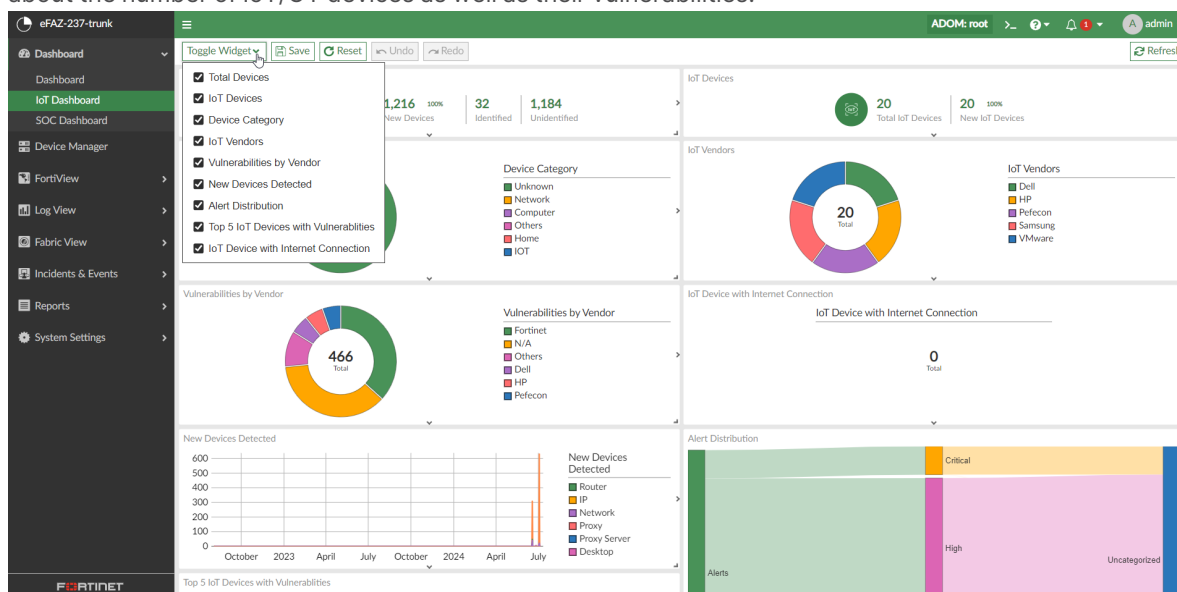
- Number of high severity incidents
- Number of outbreak alerts (with a valid license for the FortiAnalyzer Outbreak Detection)
- Number of compromised hosts (with a valid license for the Indicators of Compromise service)
- Connector health

SOC analysts can use the dashboard to drill down into these statistics for further analysis.



IoT dashboard

When the FortiGate and FortiAnalyzer devices have licenses for IoT and OT monitoring, the SOC analysts can use the IoT Dashboard to monitor IoT devices on the network. This dashboard includes information about the number of IoT/OT devices as well as their vulnerabilities.



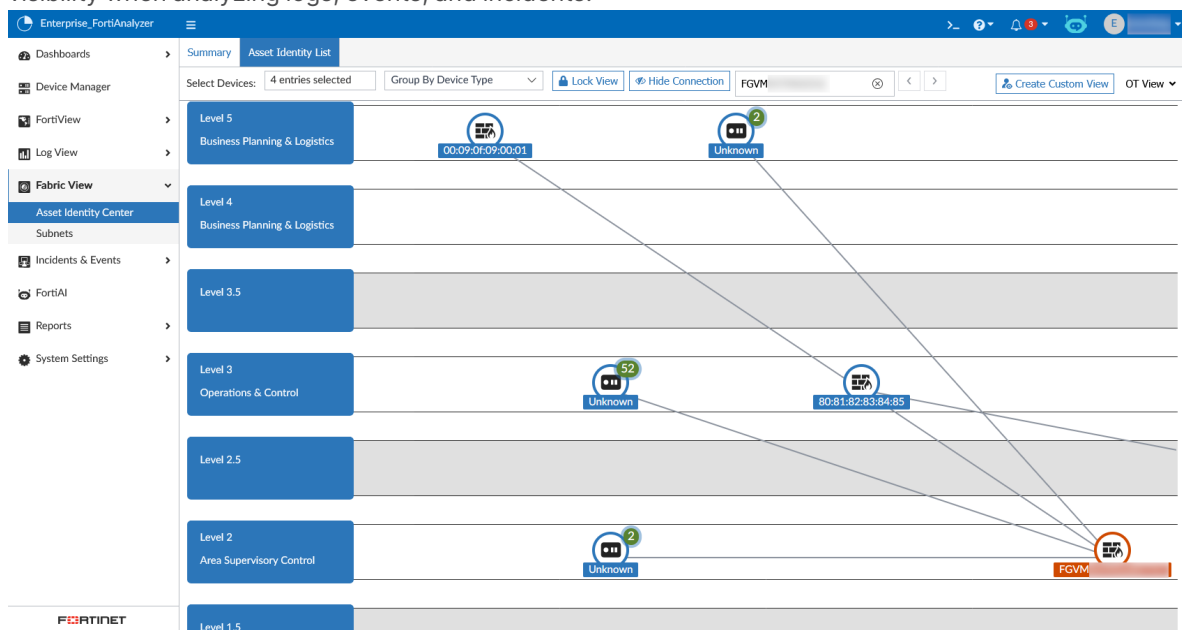
Asset Identity Center

In addition to the IoT dashboard, SOC analysts can also leverage the *Asset Identity Center* in the FortiAnalyzer GUI to view endpoint and user information. This pane allows for more detailed follow-up, including information for incident response and compliance. To view user information, there must be FortiClient devices in the architecture as well.

Analysts can use this pane to check assets that are infected or vulnerable and identify unknown or non-compliant users and endpoints.

Endpoint Name	MAC Address	IP Address	Hardware / OS	Software	OT/IoT Vulnerabilities	Vul
10.200.1.4		10.200.1.4	Linux	Details		
10.2.0.21		10.2.0.21	Linux	Details		
10.100.91.3		10.100.91.3	Linux	Details		
10.100.94.14		10.100.94.14	Linux	Details		
10.100.92.10		10.100.92.10	Tizen	Details		
10.100.92.18		10.100.92.18	Tizen	Details		
Y-BRANCH-01-CUS		10.1.0.9	Tizen	Details		
10.1.0.4		10.1.0.4	Tizen	Details		
Y-BRANCH-01-CUS		10.1.0.2	Tizen	Details		
Y-BRANCH-01-CUS		10.1.0.3	Tizen	Details		
Y-BRANCH-02-SHI		10.2.0.14	Tizen	Details		
10.100.92.16		10.100.92.16	Windows	Details		
10.100.92.13		10.100.92.13	Windows	Details		

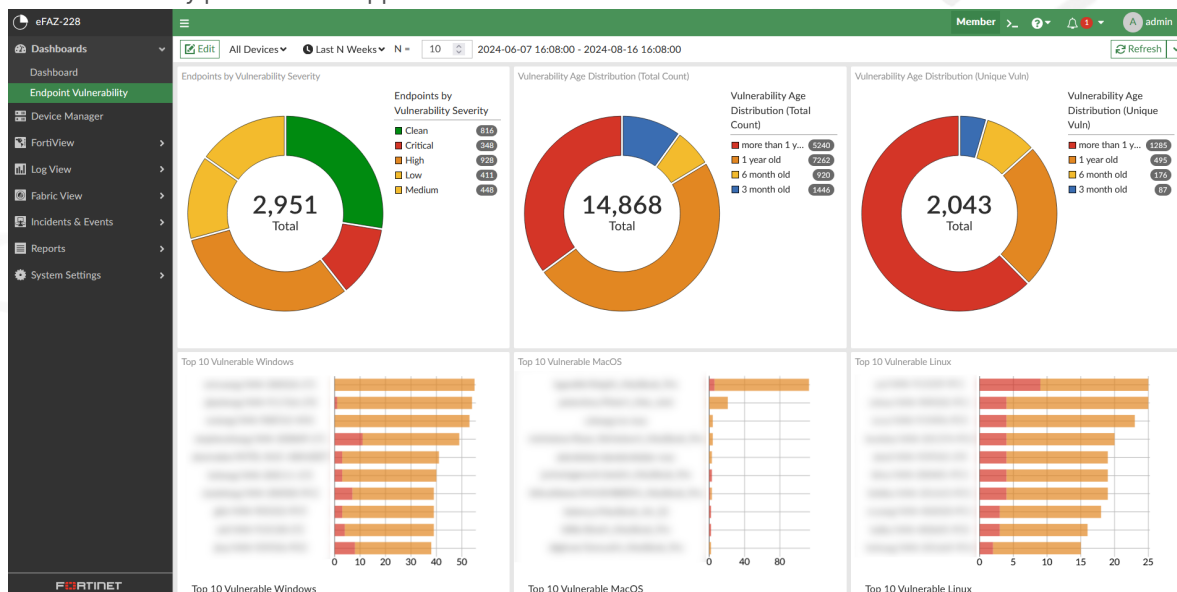
Analysts can also use the *Asset Identity Center* for user and endpoint mapping, which provides better visibility when analyzing logs, events, and incidents.



Endpoint vulnerability dashboard

After adding a FortiClient EMS device in the FortiAnalyzer, you can create an EMS connector and use it as a data source for the SIEM database. This allows you to use the *Endpoint Security Vulnerability Report* and the *Endpoint Vulnerability* dashboard. Both of these tools enable you to monitor vulnerability logs for endpoints in the network.

The *Endpoint Vulnerability* dashboard includes widgets for the number vulnerabilities and top vulnerabilities by platform and application.



Similarly, the *Endpoint Security Vulnerability Report* displays the total endpoints, users, applications, and vulnerabilities. This report displays the top vulnerable endpoints as well.

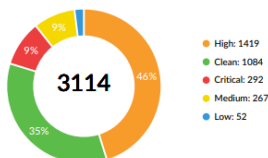


SUMMARY

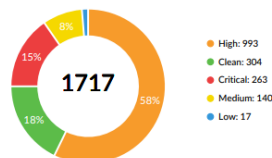
This report provides a comprehensive security rating overview and historical trend specifically for all managed endpoints based on the vulnerabilities. It utilizes retrieved data from FCT EMS and FortiGuard, including the outbreak alert and endpoint vulnerability information.

3,114 Endpoints **1,717** Users **1,819** Vulnerabilities **163** Applications **69 / 51** +/- Endpoints

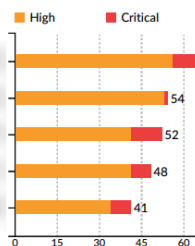
Endpoints by Vulnerability Severity



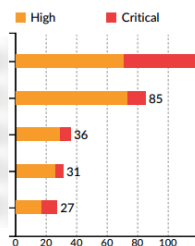
Users by Vulnerability Severity



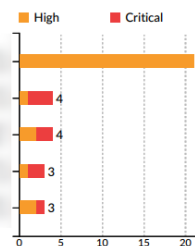
Top 5 Vulnerable Windows Endpoints



Top 5 Vulnerable Linux Endpoints

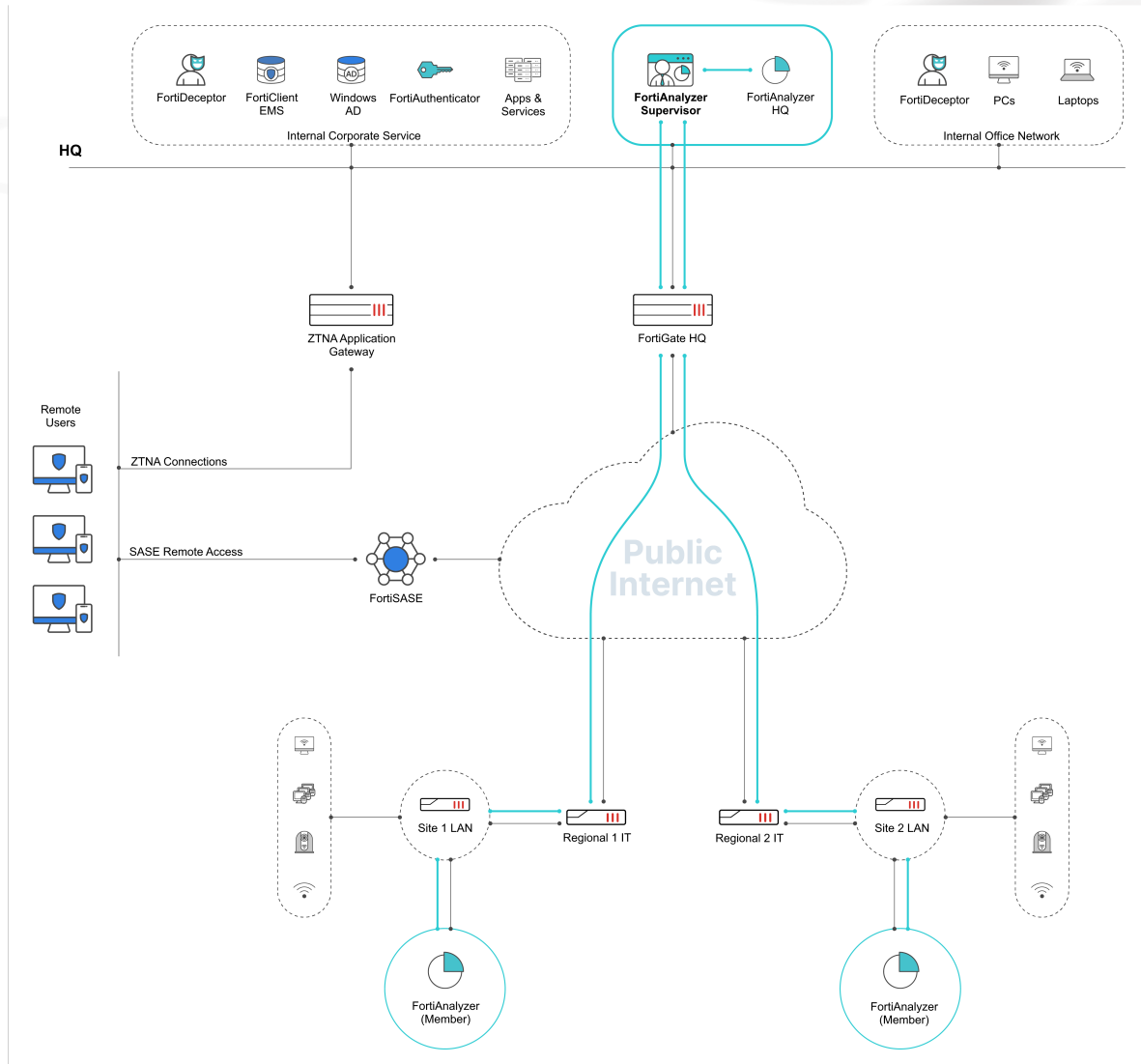


Top 5 Vulnerable MacOS Endpoints



Medium SOC

Topology



In the above architecture, an organization utilizes more security tools to protect their vast network. Besides FortiGate NGFWs, they also utilize FortiSASE for remote access, FortiAuthenticator for Identity and Access management, FortiClient EMS for managing remote endpoints running FortiClient, and FortiDeceptor to detect malicious infiltration. Furthermore, the FortiGate NGFWs may be provisioned with more complexity, utilizing a wider array of features such as SD-WAN, ADVPN, ZTNA and more advanced security controls. This generates more logs from a wide variety of devices and features.

Additionally, with branches that may be more geographically dispersed, FortiAnalyzer can be deployed regionally to collect logs relevant to that region, but at the same time can be viewed by the supervisor unit in the headquarters.

FortiAnalyzer units are deployed as a FortiAnalyzer Fabric with three members. These members collect data for three distinct regions:

- Site 1
- Site 2
- HQ

Each of these regions have their own SOC teams focused solely on the data collected by their FortiAnalyzer member. This includes logs from within their region's network, as sent by the connected devices. The FortiAnalyzer supervisor, on the other hand, allows the SOC analysts at HQ to report on data from the FortiAnalyzer units in all regions (Site 1, Site 2, and HQ).

Benefits

In this medium SOC example, the following benefits are realized:

Component	Feature	Description
Multiple FortiAnalyzer units	FortiAnalyzer Fabric	The FortiAnalyzer Fabric allows for unified log visibility across the entire environment and streamlined security operations workflows with actionable insights. The FortiAnalyzer supervisor can view logs, events, and SOC information (<i>FortiView</i>) from all members in the Fabric. It can also generate reports using data from all members. Using these capabilities, SOC analysts can respond to threats across all regions efficiently. While it is not represented in this example, HA is supported by all members and the supervisor to provide redundancy and limit downtime.
FortiGate	Network protection	As traffic traverses the FortiGate devices and inspection occurs, they send traffic, security, and event logs to the FortiAnalyzer. These logs can be reviewed in FortiAnalyzer <i>Log View</i> and they can also be used to create reports for further analysis. Logs that indicate threats to the network can also trigger predefined event handlers, creating incidents that can be followed up on by the SOC analysts. For some cases, the SOC analysts can configure playbooks in FortiAnalyzer which automate immediate response to these incidents. For example, the playbooks could automatically create and attach information to incident reports or forward the information to the affected parties through fabric connectors.
	Asset (IoT/OT) monitoring	When the FortiGate and FortiAnalyzer devices have licenses for IoT and OT monitoring, the SOC analysts can monitor the IoT/OT inventory and related vulnerabilities. The IoT dashboard provides an overview of the asset inventory and vulnerabilities; however, analysts can also use the <i>Asset Identity Center</i> in FortiAnalyzer to review assets and users in more detail for incident response and compliance.
FortiAuthenticator	Identity protection	The FortiAuthenticator device sends authentication event logs to FortiAnalyzer. The FortiAnalyzer uses predefined event handlers to generate alerts and reports, detecting threats such as brute force attacks, impossible travel, and suspicious logins. In addition, the SOC analysts can create a FortiAuthenticator connector to automate actions, such as retrieving reports for endpoint actions, users, and user lockout policy details.

Component	Feature	Description
FortiClient EMS	Endpoint vulnerability detection and response	The FortiClient EMS sends traffic, event, and vulnerability scan information to the FortiAnalyzer. The SOC analysts can review this information in dashboards and reports to respond accordingly. For example, the <i>Endpoint Security Vulnerability Report</i> provides a comprehensive security rating overview and historical trends specifically for all managed endpoints based on the vulnerabilities. This report utilizes retrieved data from FortiClient EMS and FortiGuard, including the outbreak alert and endpoint vulnerability information.
	Event correlation with user and device information	Configuring an EMS Connector allows the FortiAnalyzer to call the EMS API to get all endpoints and vulnerabilities data, and this information will be inserted as fabric (SIEM) logs. This allows FortiAnalyzer to correlate these logs with logs from other devices as part of event handlers and reports. The information is also used to populate dashboards, such as the <i>Endpoint Vulnerability</i> dashboard.
FortiDeceptor	Detect threat hunting activities	Event logs are collected from the FortiDeceptor devices, and they can be used in FortiAnalyzer to report on threat hunting activities and to detect lateral movements. These event logs can also trigger a predefined event handler for honey pot detection.
App & Services	Third-party log parsers	Predefined log parsers in FortiAnalyzer can parse, normalize, and correlate logs from third-party apps and services.

Medium SOC features



The examples described below are unique to the Medium SOC. For examples that also apply to the small SOC, such as the FortiGate and EMS components, see [Small SOC features on page 18](#).

The following features can be used in FortiAnalyzer as part of this medium SOC example:

- [Data analysis from the FortiAnalyzer Fabric supervisor](#)
- [Event management from the FortiAnalyzer Fabric supervisor](#)
- [Third-party log parsers](#)
- [FortiAuthenticator event handlers on page 30](#)
- [FortiAuthenticator connectors and playbooks](#)
- [FortiDeceptor event handlers and report](#)

Data analysis from the FortiAnalyzer Fabric supervisor

In the FortiAnalyzer Fabric supervisor, *Log View* displays logs collected on all FortiAnalyzer Fabric members. The logs contain the same information as displayed in the host FortiAnalyzer device they were collected on. For example, see below where the *FortiAnalyzer Host Name* column indicates which

FortiAnalyzer the logs were collected on.

All Devices ▾ Last 1 Hour ▾ 12:55:27 To 13:55:26											
Device ID = "FGVMULTM" 48" Device ID != "FGVULVTM" 99" Action = "all-accept" Add Filter											
#	FortiAnalyzer Host Name	ADOM	▼ Date/Time	Device ID	Action	Source	User	Destination IP	Service	Application	Security Event List
1	eFAZ-52	root	13:55:02	FGVMULTM 48	✓	10.3.120.207		10.3.120.240	HTTPS	HTTPS	
2	eFAZ-52	root	13:55:01	FGVMULTM 48	✓	10.3.120.207		10.3.120.240	HTTPS	HTTPS	
3	eFAZ-55	fabric	13:54:36	FGVMULTM 48	✓	10.3.120.207		10.3.120.240	HTTPS	HTTPS	
4	eFAZ-52	root	13:54:36	FGVMULTM 48	✓	10.3.120.207		10.3.120.240	HTTPS	HTTPS	
5	eFAZ-52	root	13:54:32	FGVMULTM 48	✓	10.3.120.207		10.3.120.240	HTTPS	HTTPS	
6	eFAZ-55	fabric	13:54:32	FGVMULTM 48	✓	10.3.120.207		10.3.120.240	HTTPS	HTTPS	
7	eFAZ-55	fabric	13:54:32	FGVMULTM 48	✓	10.3.120.207		10.3.120.240	HTTPS	HTTPS	
8	eFAZ-52	root	13:54:32	FGVMULTM 48	✓	10.3.120.207		10.3.120.240	HTTPS	HTTPS	
9	eFAZ-55	fabric	13:54:31	FGVMULTM 48	✓	10.3.120.207		10.3.120.240	HTTPS	HTTPS	
10	eFAZ-52	root	13:54:31	FGVMULTM 48	✓	10.3.120.207		10.3.120.240	HTTPS	HTTPS	
11	eFAZ-55	fabric	13:54:17	FGVMULTM 48	✓	10.3.120.207		10.2.120.30	tcp/514	tcp/514	
12	eFAZ-52	root	13:54:17	FGVMULTM 48	✓	10.3.120.207		10.2.120.30	tcp/514	tcp/514	
13	eFAZ-52	root	13:54:16	FGVMULTM 48	✓	10.3.120.207		10.2.120.30	tcp/514	tcp/514	
14	eFAZ-55	fabric	13:54:16	FGVMULTM 48	✓	10.4.120.219		10.2.120.30	tcp/514	tcp/514	
15	eFAZ-55	fabric	13:54:16	FGVMULTM 48	✓	10.3.120.207		10.2.120.30	tcp/514	tcp/514	
16	eFAZ-52	root	13:54:16	FGVMULTM 48	✓	10.4.120.219		10.2.120.30	tcp/514	tcp/514	

For Reports, the FortiAnalyzer Fabric supervisor is able to fetch and aggregate data from multiple members in the FortiAnalyzer Fabric. This enables the SOC analysts at HQ to find correlations between sites and respond accordingly. In the example below, the report can be configured to display information from multiple FortiAnalyzer units and ADOMs.

The screenshot shows the FortiAnalyzer Fabric supervisor interface. The left sidebar contains navigation options: Dashboard, Device Manager, FortiView, Log View, Incidents & Events, Reports, Report Definitions, Advanced Settings, and System Settings. The main panel is titled 'Edit: Daily Summary Report' and has three tabs: Generated Reports, Settings, and Editor. The 'Settings' tab is selected, showing configuration options for the report. A dropdown menu is open for the 'Subnets' field, displaying a list of devices and ADOMs. The list includes eFAZ-204 (with sub-items for root, Fortinet, Internal, QA, and Correlation), eFAZ-205 (with sub-items for root, Lab, Office, Data, and Correlation), All_root_adoms, and Test. The 'OK' button is highlighted at the bottom of the dropdown.

Event management from the FortiAnalyzer Fabric supervisor

Events generated by event handlers on the FortiAnalyzer Fabric members are visible on the supervisor. The SOC analysts can review these events for correlations between the members, so they can be managed together more efficiently rather than individually across the sites.

The event handlers must be configured on each of the FortiAnalyzer members; however, the related logs that trigger the event handler rules are visible from the supervisor.

FAZ Name	Group	Event Status	Event Type	Severity	count	First Occurrence	Last Update	Device Name	Acknowledge
FAZVM-S-903	10.2.175.43		Traffic	Medium	120	2021-04-07 10:45:18	2021-04-08 10:46:58	FAZVMST...	No
FAZVM-S-903	10.2.126.95		Traffic	Medium	104	2021-04-07 10:45:00	2021-04-08 10:46:48	FAZVMST...	No
FAZVM-S-903	10.2.115.2		Traffic	Medium	103	2021-04-07 10:45:38	2021-04-08 10:46:48	FAZVMST...	No
FAZVM-S-903	10.2.60.111	open	IPS	High	451	2021-04-07 10:45:27	2021-04-08 10:46:47	FAZVMST...	No
FAZVM-S-903	10.2.60.46		Traffic	Medium	104	2021-04-07 10:45:01	2021-04-08 10:46:46	FAZVMST...	No
FAZVM-S-903	VAN-200289-US1	open	Traffic	High	124	2021-04-07 10:45:02	2021-04-08 10:46:39	FAZVMST...	No
FAZVM-S-903	10.2.60.93		Traffic	Medium	104	2021-04-07 10:45:00	2021-04-08 10:46:39	FAZVMST...	No
FAZVM-S-903	10.2.60.45		Traffic	Medium	86	2021-04-07 14:49:27	2021-04-08 10:46:35	FAZVMST...	No
FAZVM-S-903	10.2.60.121		Traffic	Medium	104	2021-04-07 10:45:04	2021-04-08 10:46:33	FAZVMST...	No
FAZVM-S-903	10.2.60.94		Traffic	Medium	103	2021-04-07 10:45:02	2021-04-08 10:46:31	FAZVMST...	No
FAZVM-S-903	10.2.175.45		Traffic	Medium	86	2021-04-07 14:49:24	2021-04-08 10:46:28	FAZVMST...	No
FAZVM-S-903	10.2.0.250		Traffic	Medium	176	2021-04-07 14:11:41	2021-04-08 10:46:28	FAZVMST...	No
FAZVM-S-903	10.2.123.9		Traffic	Medium	104	2021-04-07 10:45:02	2021-04-08 10:46:28	FAZVMST...	No
FAZVM-S-903	10.2.175.118		Traffic	Medium	104	2021-04-07 10:45:04	2021-04-08 10:46:26	FAZVMST...	No
FAZVM-S-903	10.2.175.116		Traffic	Medium	105	2021-04-07 10:45:00	2021-04-08 10:46:25	FAZVMST...	No
FAZVM-S-903	10.2.60.141	open	Traffic	High	283	2021-04-07 10:45:35	2021-04-08 10:46:24	FAZVMST...	No
FAZVM-S-903	10.2.175.46		Traffic	Medium	104	2021-04-07 10:45:09	2021-04-08 10:46:23	FAZVMST...	No
FAZVM-S-903	10.2.60.101		Traffic	Medium	104	2021-04-07 10:45:02	2021-04-08 10:46:16	FAZVMST...	No

Third-party log parsers

FortiAnalyzer log parsers can parse, normalize, and correlate logs from Fortinet products and third-party products. These logs are stored in the SIEM database and are used for reports and event handlers, providing greater visibility in the network.

Predefined log parsers are available for many Fortinet products and some third-party products, such as Apache and Nginx web servers. Premium log parsers are available for third-party products with a valid license for the Security Automation Service. For more information, see the [FortiGuard website](#). For example, see below log parsers with the *Origin* from FortiGuard.

Name	Application/Vendor	Category	Origin	Status
Barracuda Firewall Log Parser	Barracuda	Network Devices	FortiGuard	Disabled
Palo Alto PAN-OS Log Parser	Palo Alto	Network Devices	FortiGuard	Disabled
Arms Platform Log Parser	Arms	Network Devices	FortiGuard	Disabled
Zscaler Firewall Log Parser	Zscaler	Network Devices	FortiGuard	Disabled
Juniper Firewalls Log Parser	Juniper	Network Devices	FortiGuard	Disabled
Aruba CX Log Parser	Aruba	Network Devices	FortiGuard	Disabled
Nozomi Networks Log Parser	Nozomi	Operational Technology	FortiGuard	Disabled
Generic CEF Log Parser	CEF	Generic System	FortiGuard	Disabled
Clavister Firewall Log Parser	Clavister	Network Devices	FortiGuard	Disabled
McAfee Anti-Virus Log Parser	McAfee	Security Solutions	FortiGuard	Disabled
Linux DHCP Log Parser	DHCP	Network Devices	FortiGuard	Disabled
SonicWall Firewalls Log Parser	SonicWall	Network Devices	FortiGuard	Disabled
CheckPoint Log Parser	CheckPoint	Network Devices	FortiGuard	Disabled
Brocade Log Parser	Brocade	Network Devices	FortiGuard	Disabled
Dragos Platform Log Parser	Dragos	Operational Technology	FortiGuard	Disabled
GitLab Log Parser	GitLab	Applications	FortiGuard	Disabled

FortiAuthenticator event handlers

The authentication event logs collected from FortiAuthenticator can be used to trigger predefined event handlers on FortiAnalyzer. The rules in these event handlers trigger events where there may be brute force attacks, impossible travel, or other suspicious logins.

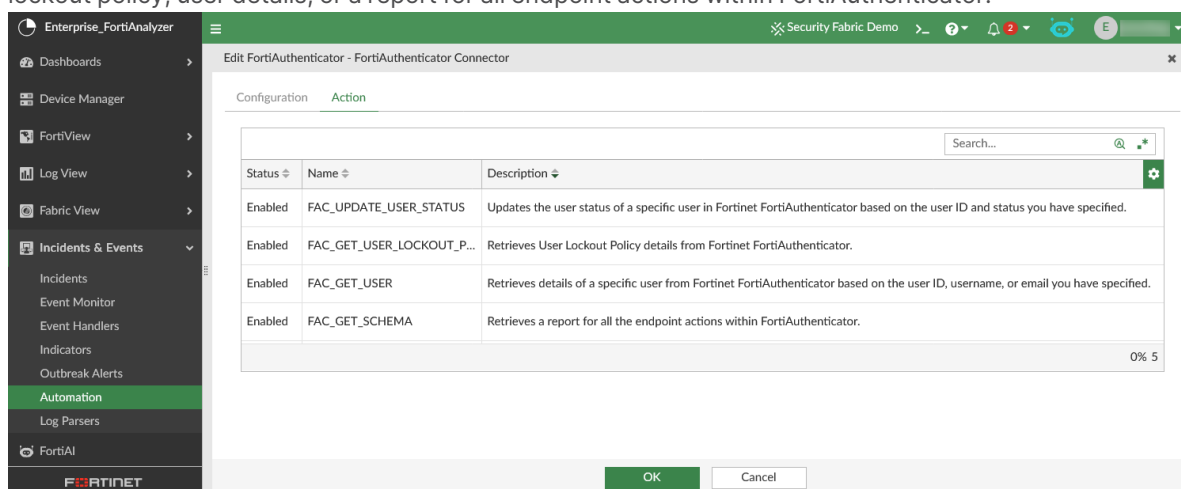
See below for the event handlers and their rules:

Event handler	Rules
ZTNA Brute Force Login	High Volume of Failed Authentications from Multiple Non-Existing Users
	Authentication Failed from Multiple Geo Locations
	Brute Force Login Attack
	High Volume of Failed Authentications to Same Non-Existing User
ZTNA Login Anomaly Detection	Authentication to Multiple Services Failed
	Successful Authentication from Multiple Geo Locations
	Successful Authentication from Multiple Endpoints
	Successful Authentication from Sanctioned Countries

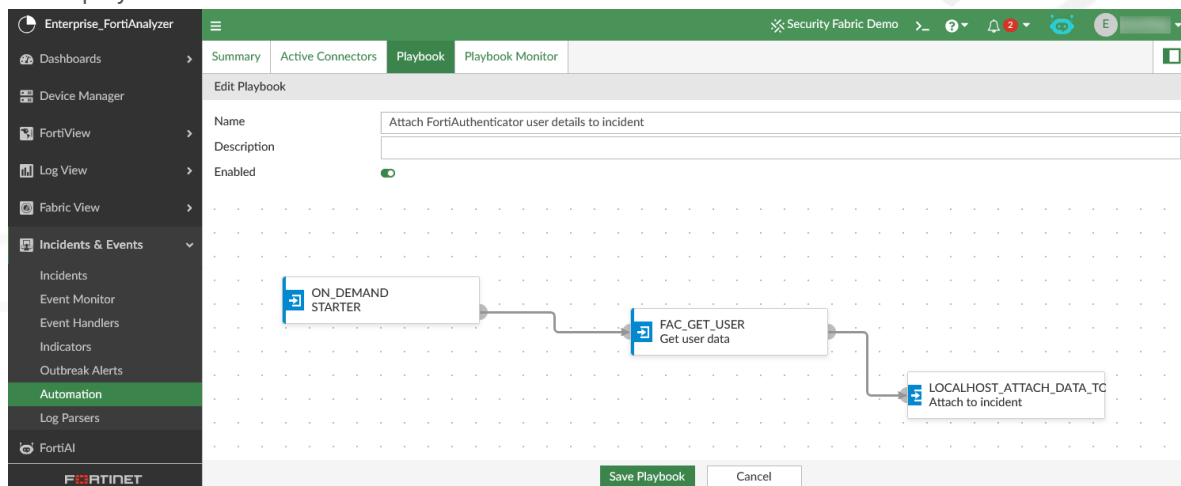
An event will be generated when the conditions for any of the rules within an event handler are met. You can identify which rule triggered the event generation by reviewing the event in the *Event Monitor* of FortiAnalyzer. This information can assist in following up with an incident report, if needed.

FortiAuthenticator connectors and playbooks

In addition to the predefined FortiAuthenticator event handlers, you can also create a FortiAuthenticator connector to use in playbooks. This connector allows you to automate tasks, such as retrieving the user lockout policy, user details, or a report for all endpoint actions within FortiAuthenticator.



To automate these actions with the connector, you can create a custom playbook. For example, the below playbook can be used to retrieve the user details and attach it to an incident.



FortiDeceptor event handlers and report

Using event logs collected from the FortiDeceptor, SOC Analysts can generate a report in FortiAnalyzer with deception alerts to identify and monitor lateral movements and advanced attack tactics. This report displays charts that list the top attackers, victims, and the related tools and services related to those incidents.

FORTINET

Summary

FortiDeceptor is based on deception technology that complements an organization's existing breach protection strategy, designed to deceive, expose and eliminate attacks originating from either external or internal sources before any real damage occurs.

This report provides a quick summary of incidents and alerts generated by FortiDeceptor.

Top 10 Attackers by Incidents

FortiDeceptor provides early breach detection and block attackers before they can gain access to sensitive company assets, and assists security operations teams to identify those threats. Attacks can come in from many different sources and IP's, both external and internal.

The following chart provides the Top 10 Attackers IPs by count of number of Incidents

10.95.4.88	1,110
10.95.4.156	808
10.95.4.244	751
10.95.4.162	125
10.95.4.83	68
10.95.4.84	50
10.95.4.10	50
10.95.4.81	32
10.95.4.153	9
10.95.4.164	7
Others	3



Additionally, there is a predefined event handler that can be enabled when FortiDeceptor is an authorized logging device to FortiAnalyzer. Using event logs from FortiDeceptor, the `Default-FDC-Honey-Pot-Detection` event handler generates events for honey pot attacks.

Enterprise_FortiAnalyzer

Dashboards

Device Manager

FortiView

Log View

Fabric View

Incidents & Events

Incidents

Event Monitor

Event Handlers

Indicators

Outbreak Alerts

Automation

Log Parsers

FortiAI

Reports

System Settings

FORTINET

Security Fabric Demo

65/1024

Edit Basic Event Handler

Status

Name *
Default-FDC-Honey-Pot-Detection

Description
Default event handler for FortiDeceptor Honey Pot event detection

MITRE Tech ID
Click to select

Data Selector
Click to select

Automation Stitch

Automatically Create Incident

Rules

Attack detected by FDC

(Default,FortiDeceptor)
subtype="attack"

Add New Rule

Factory Reset

OK

Cancel



More information

Feature documentation:

- [FortiAnalyzer Architecture Guide](#)
- [FortiAnalyzer Fabric Deployment Guide](#)
- [FortiAnalyzer Administration Guide](#)
- [FortiAnalyzer Data Sheet](#)



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.