



About the Exam

Program Requirements

You must successfully pass a minimum of any two Fortinet NSE 5 certification exams:

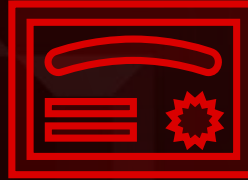
FortiAnalyzer

FortiClient EMS

FortiEDR

FortiManager

FortiSIEM



About the Exam

FortiAnalyzer 7.2

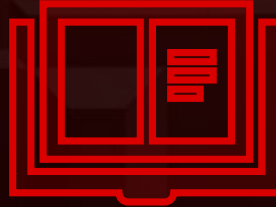
Exam series: NSE5_FAZ-7.2

Number of questions: 35

Exam time: 60 minutes

Language: English and Japanese

Product version: FortiAnalyzer 7.0



Demo Environment

FortiAnalyzer

<https://fortianalyzer.fortidemo.com/p/login/>

USERNAME: demo PASSWORD: demo

- 01 Introduction and Initial Access
- 02 Logging
- 03 FortiSoC—Incidents and Events
- 04 Reports
- 05 FortiSoC—Playbooks

Conclusions

Requirements

Exam

Demo Environment



Introduction and Initial Access

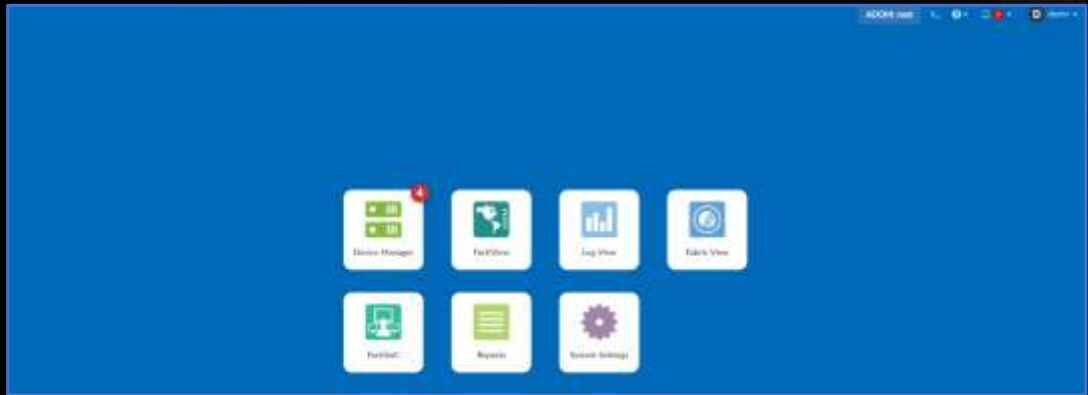
Overview

- Purpose of the FortiAnalyzer
- Understand Basic Concepts and Features
- Identify the tools you can use to access FortiAnalyzer

Overview

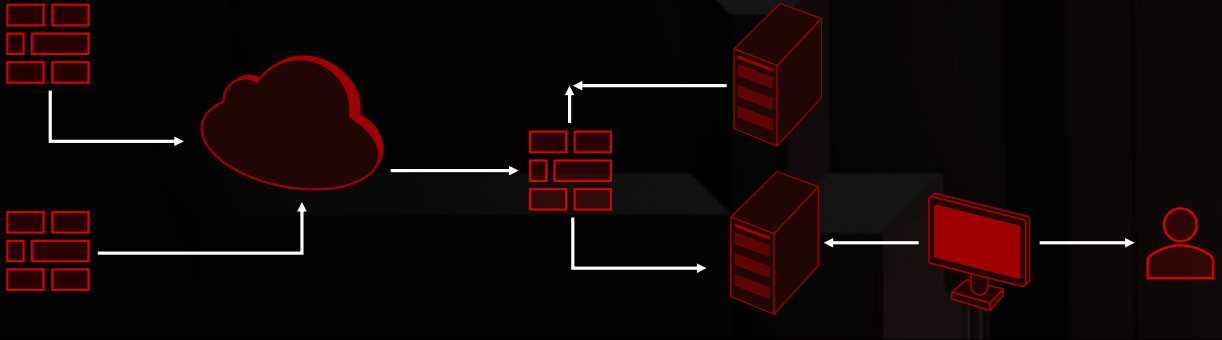


Overview



Centralized Log Repository

- Aggregates log data from one or more Fortinet devices
- Create a single view of security events taking place on a range of devices



Centralized Log Repository

Registered devices send logs to FortiAnalyzer

Buffers Reorganizes and store logs

Admins

View and search logs

Configure, request, and view reports

FortiGate

FortiCarrier

FortiAnalyzer

FortiCache

FortiClient

FortiDDos

FortiMail

FortiManager

FortiSandBox

FortiWeb

Syslog

Chassis

Reports, Events and Content Archiving



Reports

Network-wide reporting of events and trends on supported devices

Archived Filtered and mined for compliance or historical analysis



Events

Identify and react to threat quickly when conditions are met

View events through event monitor GUI email SNMP or syslogs



Content Archiving

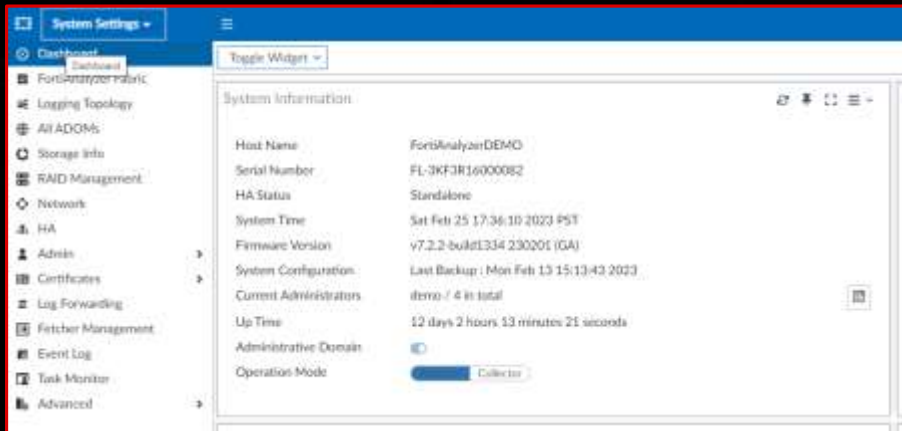
Logs and archives full or summary copies of content transmitted over the network

Prevent sensitive information from getting out of your network

Database Language Support

- Supports SQL for logging and reporting
- Inserts log data into SQL database for log view and report generation
- Uses a PostgreSQL database
- Advanced reporting does require SQL knowledge

FortiAnalyzer Operating Modes



FortiAnalyzer Operating Modes



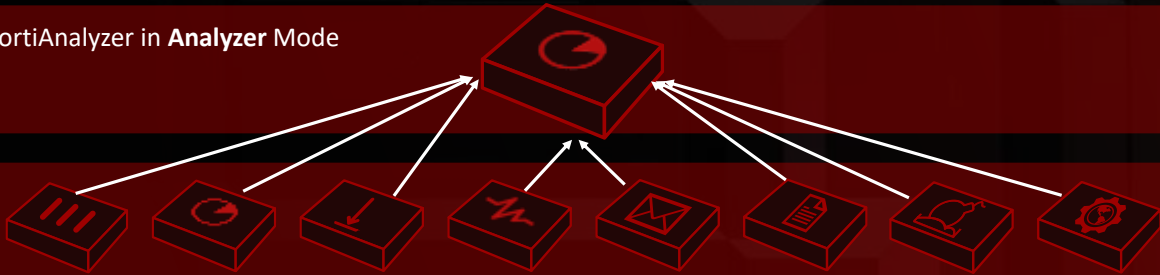
Analyzer

Default Mode

Central log for one or more devices in collector mode

Can still forward logs to another FortiAnalyzer or syslog/CEF server

FortiAnalyzer in **Analyzer** Mode



Fortinet Devices directly send logs to a central log management platform

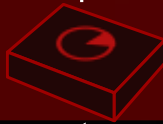
FortiAnalyzer Operating Modes

Collects logs from multiple devices and forwards to FortiAnalyzer in analyzer mode
Can forward to syslog/CEF server in real-time forward mode only

FortiAnalyzer in **Analyzer Mode**



FortiAnalyzer in **Collector Mode**



Devices send logs to log collector

Security Fabric Logging

- FortiAnalyzer supports the SecurityFabric by storing and analyzing the logs from the units in a SecurityFabric as if the logs were from a single device

- SecurityFabric as a whole logs each session once

 - The 1st FortiGate that handles a session in the SecurityFabric logs the session

 - Any UpStream FortiGate that is a member of the SecurityFabric does not create duplicate logs

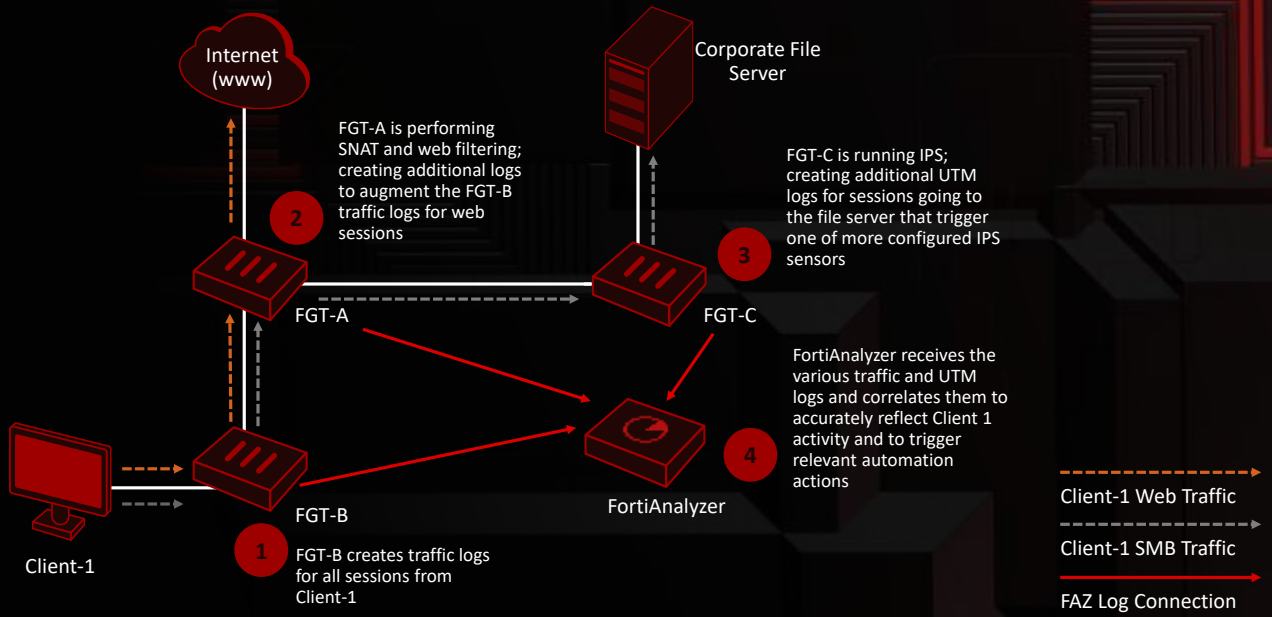
 - Exceptions

 - UpStream FortiGate performs NAT

 - UpStream FortiGate devices still log UTM events if configured

- FortiAnalyzer does UTM and traffic log correlation so that the session details UTM events reporting and automation work correctly

Security Fabric Logging



FortiAnalyzer Fabric



Enables centralized viewing of devices, incidents, and events across multiple FortiAnalyzers



Ideal for environments with many FortiAnalyzers and high log volume



2 Operations modes

Supervisor – one per fabric acts as root

Member – Sends information to supervisor



Must be configured in same time zone



Supervisors include on the following modules

Device Manager

Log View

FortiSoc

Systems Settings

Management Extensions

Administrative Domains (ADOMs)



ADOMs group devices for admins to monitor and manage

One or more devices assigned to ADOMs and admins are assigned to administrator on or more ADOMs



Purpose

Restrict access

Virtual Domain (VDOM) further restricts access

Efficiently manage data policies and disk space allocation

Set for each ADOM not each device

Administrative Domains (ADOMs)

- Purpose of the FortiAnalyzer
- Understand Basic Concepts and Features
- Identify the tools you can use to access FortiAnalyzer



Logging

Overview

Purpose of Collecting and
storing logs

Log file workflow

Purpose of Logging

Log messages record information containing specific details about what is occurring

Determine load on devices

Track services used

Support Incident response and forensic analysis

Examine multiple logs to discover the chain of activity that led to a breach



Log Storage Regulations

Regulatory requirements may mandate how logs are managed

Levels and analysis requirements are often defined by legislation

Ensure logging is enabled and recording data levels to satisfy regulations

Logs can provide evidence to deal with offending parties when unauthorized activity is detected

Logging data must be able to stand up in court

Monitoring of logs is hampered by extensive amounts of data being captured and the lack of means to manage, correlate and analyze that data

Logging should be set high enough to satisfy any regulation and you to do your job

To much data is as bad as to little



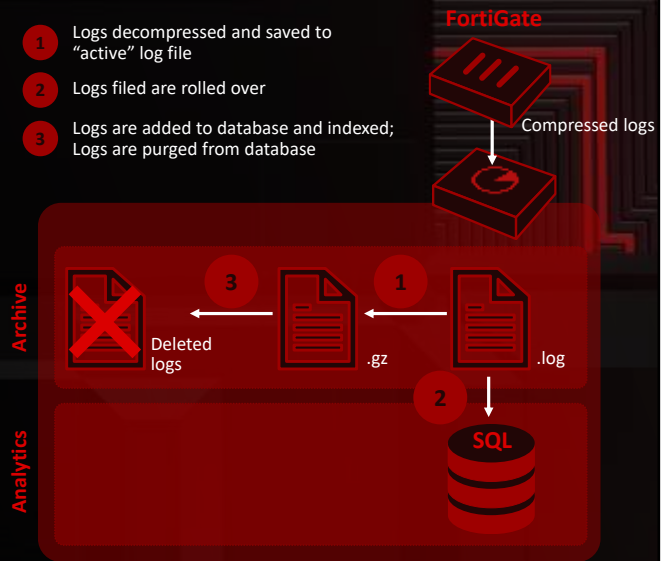
Log Type by Device

Device	Log Type
Fabric	All
FortiGate	Traffic (forward, local, sniffer, multicast) Event (Endpoint, HA, Compliance, Security Rating, SDN Connector, SD-WAN, Switch-controller, FortiExtender, System (Application Control, Antivirus, Data Leak Prevention, Web Application Firewall, Web Filter, Email Filter, File Filter, DNS, Intrusion Prevention, SSH, SSL, VoIP, Vulnerability Scan, FortiClient)
FortiCache	Traffic, Event, Antivirus, Web Filter
FortiClient	Traffic, Event, Vulnerability Scan
FortiMail	History, Event, Antivirus, Email Filter
FortiManager	Event
FortiSandbox	Malware, Network Alerts
FortiWeb	Event, Intrusion Prevention System (IPS), Traffic
Syslog	Generic (used for compatibility with older FortiGate, or for non-Fortinet devices)

LogFile WorkFlow

Log Phase	FortiAnalyzer Location	Immediate Analytic Support
Logs Received from registered device	Active log file, saved with .log extension	No. (can view in Log Browse)
Indexed (Analytic logs)	Added to SQL database and indexed	Yes. Considered "online" (can view in Log View, FortiView, FortiSoC and Reports)
Logs rolled over and compressed (Archive logs)	Compressed in log file and saved with .gz extension	No. Considered "offline" (can view in Log Browse)

- 1 Logs decompressed and saved to "active" log file
- 2 Logs filed are rolled over
- 3 Logs are added to database and indexed; Logs are purged from database



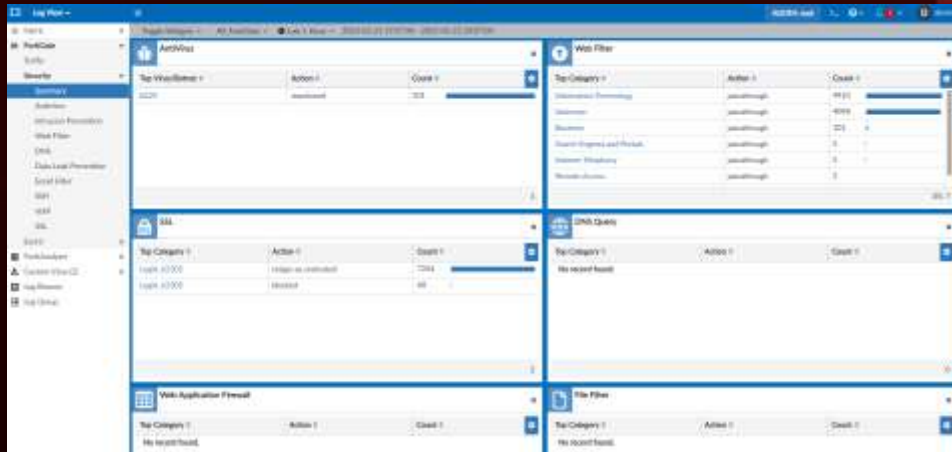
Log View

View all logs in each ADOM

You can choose to view only specific devices,
fabric, or log groups



Summary Dashboard

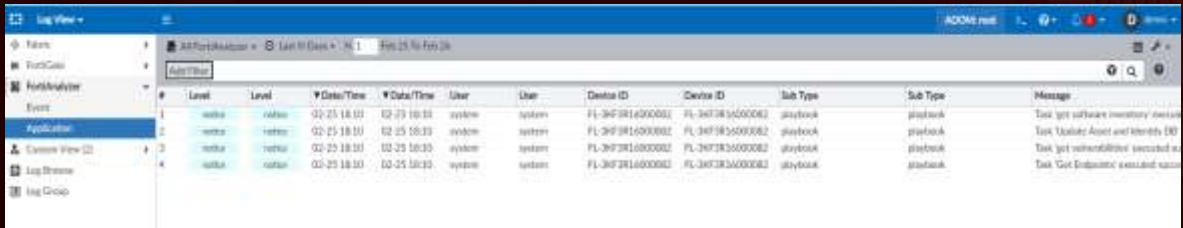


Searching

The screenshot shows the Windows Security Log Viewer interface. The left-hand pane is expanded to show 'New Filter' selected. The main pane displays a table of log events with the following columns: #, Policy ID, Date/Time, Source, Host Name, Classification ID, Service, Action, Category Description, and URL. The events listed are primarily related to Windows Defender and Windows Security, with actions such as 'scan through' and 'update through'.

#	Policy ID	Date/Time	Source	Host Name	Classification ID	Service	Action	Category Description	URL
1	22	2008-50	10.88.130.131	www.windows.com	4205.02	Windows Defender	scan through	Information Technology	https://www.windows.com/
2	22	2008-50	10.88.130.131	www.windows.com	4205.02	Windows Defender	scan through	Information Technology	https://www.windows.com/
3	22	2008-49	10.88.130.131	www.windows.com	4205.02	Windows Defender	scan through	Information Technology	https://www.windows.com/
4	22	2008-49	10.88.130.131	www.windows.com	4205.02	Windows Defender	scan through	Information Technology	https://www.windows.com/
5	22	2008-49	10.88.130.131	www.windows.com	4205.02	Windows Defender	scan through	Information Technology	https://www.windows.com/
6	22	2008-45	10.88.130.131	www.windows.com	4205.02	Windows Defender	scan through	Information Technology	https://www.windows.com/
7	22	2008-45	10.88.130.131	www.windows.com	4205.02	Windows Defender	scan through	Information Technology	https://www.windows.com/
8	22	2008-45	10.88.130.131	www.windows.com	4205.02	Windows Defender	scan through	Information Technology	https://www.windows.com/
9	22	2008-45	10.88.130.131	www.windows.com	4205.02	Windows Defender	scan through	Information Technology	https://www.windows.com/
10	22	2008-45	10.88.130.131	www.windows.com	4205.02	Windows Defender	scan through	Information Technology	https://www.windows.com/
11	22	2008-45	10.88.130.131	www.windows.com	4205.02	Windows Defender	scan through	Information Technology	https://www.windows.com/
12	22	2008-44	10.88.130.131	www.windows.com	4205.02	Windows Defender	scan through	Information Technology	https://www.windows.com/
13	22	2008-44	10.88.130.131	www.windows.com	4205.02	Windows Defender	scan through	Information Technology	https://www.windows.com/
14	22	2008-44	10.88.130.131	www.windows.com	4205.02	Windows Defender	scan through	Information Technology	https://www.windows.com/
15	22	2008-44	10.88.130.131	www.windows.com	4205.02	Windows Defender	scan through	Information Technology	https://www.windows.com/
16	22	2008-44	10.88.130.131	www.windows.com	4205.02	Windows Defender	scan through	Information Technology	https://www.windows.com/
17	22	2008-41	10.88.130.131	www.windows.com	4205.02	Windows Defender	scan through	Information Technology	https://www.windows.com/
18	22	2008-40	10.88.130.131	www.windows.com	4205.02	Windows Defender	scan through	Information Technology	https://www.windows.com/
19	22	2008-40	10.88.130.131	www.windows.com	4205.02	Windows Defender	scan through	Information Technology	https://www.windows.com/

Application Logs



The screenshot shows a log viewer window with a table of application logs. The table has columns for ID, Level, Level, Date/Time, Date/Time, User, User, Device ID, Device ID, Sub Type, Sub Type, and Message. The logs are filtered for the date Feb 25, 2018.

ID	Level	Level	Date/Time	Date/Time	User	User	Device ID	Device ID	Sub Type	Sub Type	Message
1	info	info	02-25 18:33	02-25 18:33	system	system	FL-34F3816000002	FL-34F3836000002	playbook	playbook	Task 'get software inventory' started successfully
2	info	info	02-25 18:33	02-25 18:33	system	system	FL-34F3816000002	FL-34F3836000002	playbook	playbook	Task 'Unlink Asset and identify IP' started successfully
3	info	info	02-25 18:33	02-25 18:33	system	system	FL-34F3816000002	FL-34F3836000002	playbook	playbook	Task 'get vulnerability' started successfully
4	info	info	02-25 18:33	02-25 18:33	system	system	FL-34F3816000002	FL-34F3836000002	playbook	playbook	Task 'Get Endpoint' started successfully

FortiView

FortiView has two panes

1. FortiView: Comprehensive monitoring system that displays real-time and historical data
2. Monitors: designed for NOC/SOC with big monitors displaying in dashboards

Each ADOM has its own data in FortiView



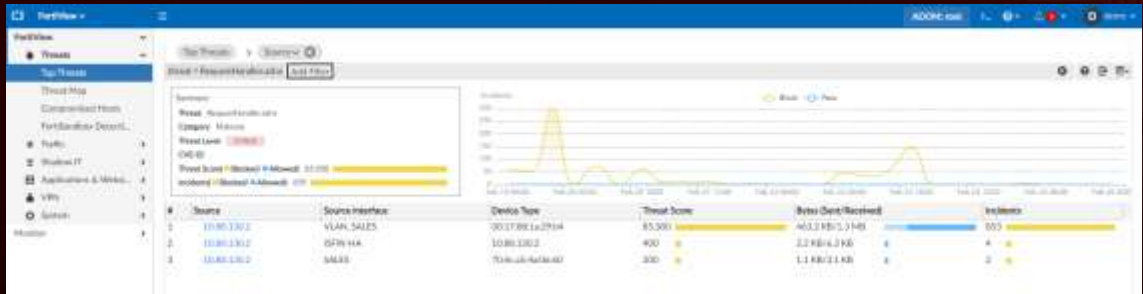
FortiView Pane

Integrates real-time and historical data in a summary view

Analytics logs only



Using Information on a Widget



Indicators of Compromise

Indicators of Compromise (IOC) engine detects end users with suspicious web usage (Based on FortiGuard Subscriptions)

Uses FortiGuard threat Intelligence to provide visibility of today's threats

Flow:

FAZ downloads threat intelligence FortiGuard packages every day

FortiGate sends logs to FAZ

FAZ runs real-time threat detection when it receives logs

Customers can see consolidated view of compromised devices

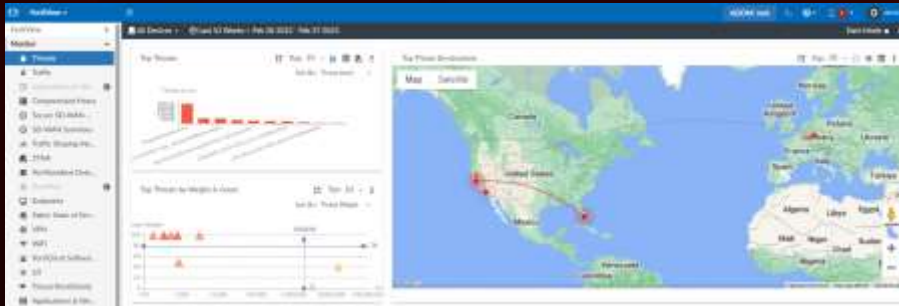
Branch Detection engine parses logs into categories

1. Infected
2. Highly Suspicious

Monitors Pane

Displays both real-time monitoring and historical trends in several dashboards

Dashboards contained customizable widgets



Log Fetching

Retrieve archived logs from another FAZ and then run queries or reports on those logs
FAZ fetch queries the remote FAZ fetch server to retrieve data



Log Fetching

Client and server should run same firmware version

Source and Destination ADOMs should be of same type

Destination ADOM has enough space for imported logs

Data Policy on client must retain logs for time requested

Logs outside the data policy constraints are deleted

You must add devices to device manager before you can see logs in the client

You can add log fetching device before adding devices, but you won't be able to see the logs

Filters:

Specific devices

Specific types and values

Specific time frame

Fabric View

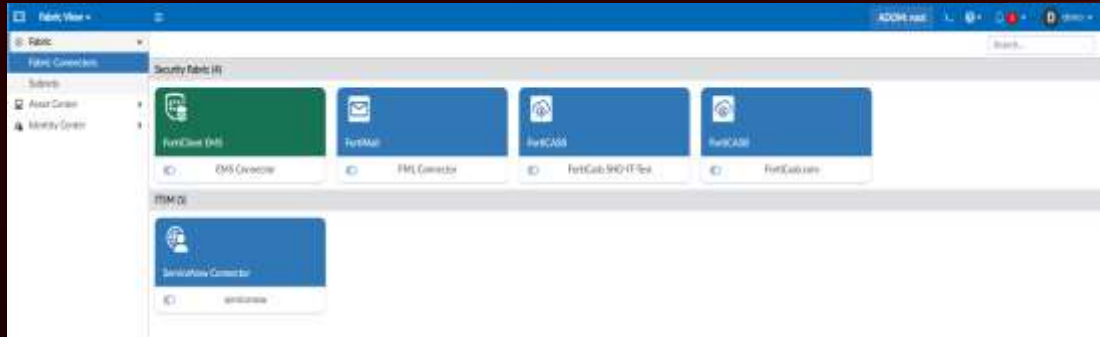
Module enables

- Creation of fabric connectors
- Creation of subnets and subnet groups
- Viewing list of endpoints

Create connectors

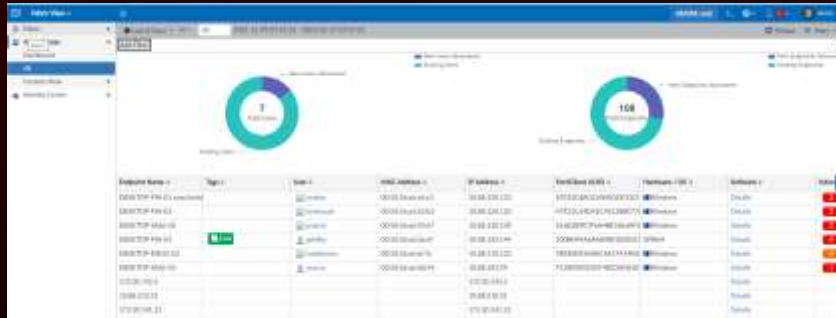
- ITSM
- Storage
- Security Fabric

Fabric View Screen Cap



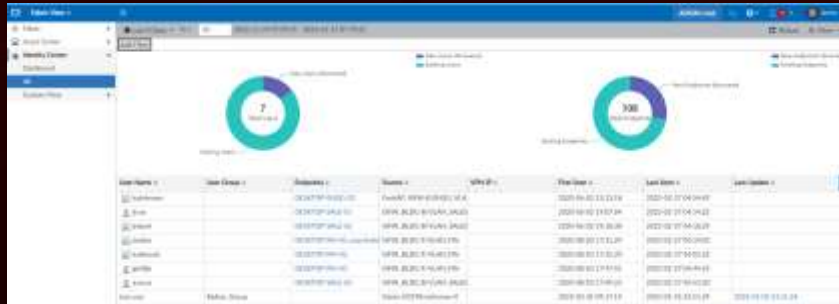
Asset Center

Pane provides endpoint and user information grouped by endpoint
Useful in compliance and incident response investigation



Identity Center

Pane provides endpoint and user information grouped by user
Useful in compliance and incident response investigation



Gathering LogRate and Device Usage Stats

What to Investigate	Log Type
What is the log receive rate for each second?	# diagnose fortilogd lograte
What are the log receive rate totals?	# diagnose fortilogd lograte-total
What is the device log rate?	# diagnose fortilogd lograte-device
What is the log rate for each log type?	# diagnose fortilogd lograte-type
What is the message receive rate for each second?	# diagnose fortilogd msgrate
What is the SQL insertion status?	# diagnose sql status sqlplugind
What is the device log usage for all logging devices?	# diagnose log device

Gathering LogRate and Log Volume per ADOM

What to Investigate	CLI Command to Use
Log receive rate for all, or a specific ADOMs?	<pre># diagnose fortilogd lograte-adom {all adom-name}</pre>
Log volume for all, or a specific ADOM?	<pre># diagnose fortilogd logvol-adom {all adom-name}</pre>

Conclusions

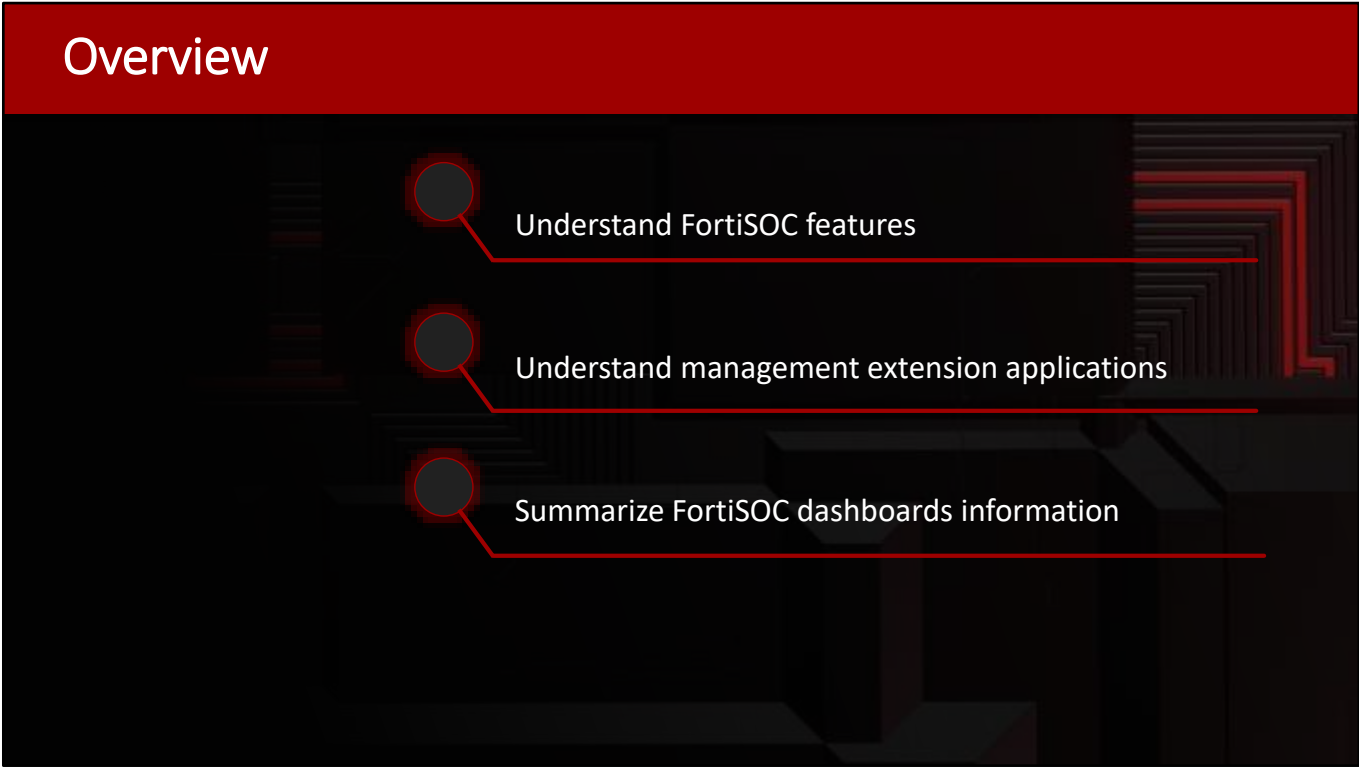
Purpose of Collecting and storing logs

Log file workflow



FortiSoc

Overview



Understand FortiSOC features

Understand management extension applications

Summarize FortiSOC dashboards information

FortiSoc Features

Incident Management

Incident/Case Management

Indicators attachment for incidents

API to FortiSOAR for Escalation

SOC Automation

FortiSOC Module

Playbook Templates and Automation

Connectors for Playbooks

Visual Playbook Editor

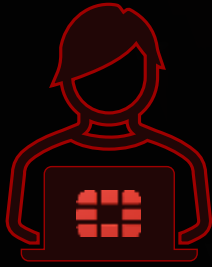
Playbook Execution

Playbook Monitor

Fabric Analytics

SOC Analytics

FortiSoc Features



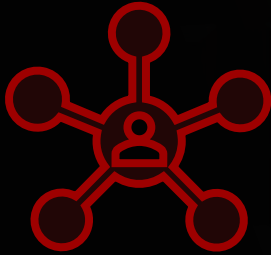
FortiSOC capabilities

SOAR – Security Orchestration,
Automation and Response

SIEM – Security Information and
Event Management

Requires a subscription to run at
full capacity

Management Extensions



Management extensions allow you to enable licensed application and run them on the FAZ

Management extensions are full-fledged running instances of a product in the form of a docker container

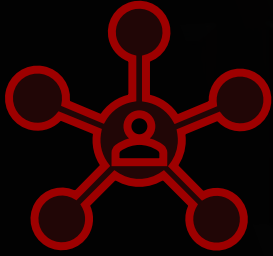
Allows you to use and monitor different solutions from Fortinet using a single pane of glass

Two Management extension Applications available on the FAZ

FortiSOAR – Allows you to manage your security operations using FAZ without need for separate instance

FortiSIEM – Alleviates the need for a separate FortiSIEM connector node

Management Extensions



FortiSOAR



FortiSIEM Collector

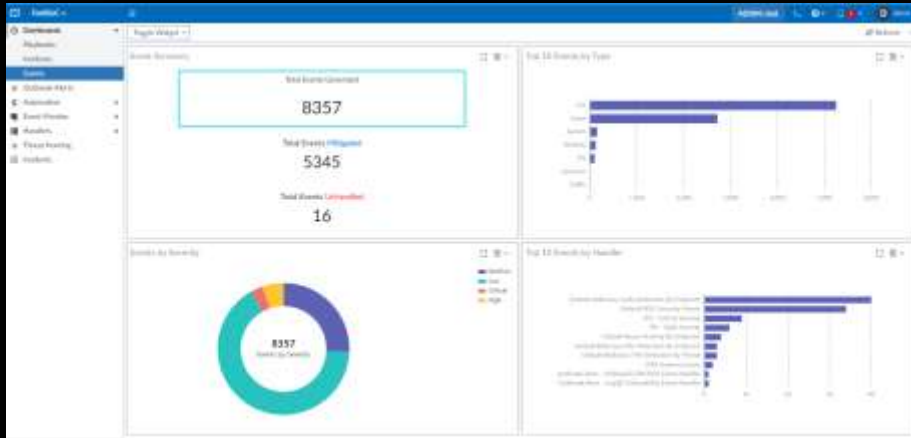
Dashboards

FortiSOC includes 3 dashboards

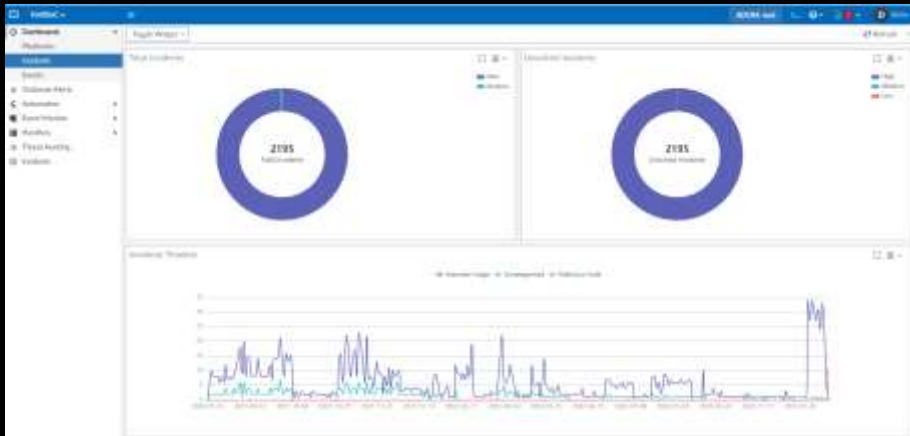
1. PlayBooks
2. Incidents
3. Events



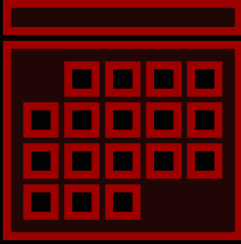
Events Dashboards



Incident Dashboards



Events Generated



FAZ generates events based on the details included in the logs it received

Only logs matching specified criteria will generate alerts

Event handlers are responsible of determining if an event needs to be created

- Matches a set of criteria of filters

- Generates events only from analytics logs

May predefined event handlers defined

- Can be cloned and customized

- Can be created from scratch

Generated events can be viewed under Event Monitored

Managing Event Handlers

Event handlers look for specific conditions in the logs
FAZ comes with many pre-determined
Enable/Disable as needed
Clone and customized as required



Rule ID	Name	Data Selector	Notification Profile	Automatic Status	Events
Rule 1	Outbreak Alarm - MEDT Follow Event Handler 1 - Outbreak MEDT Full			No	
Rule 2	Outbreak Alarm - MEDT Follow Event Handler 1 - Outbreak MEDT Full			No	
Rule 3	Outbreak Alarm - MEDT Follow Event Handler 1 - Outbreak MEDT Full			No	
Rule 4	Outbreak Alarm - MEDT Follow Event Handler 1 - Outbreak MEDT Full			No	
Rule 1	Outbreak Alarm - Zulu Expired Event Handler 1 - Outbreak Zulu Expired			No	
Rule 2	Outbreak Alarm - Zulu Expired Event Handler 1 - Outbreak Zulu Expired			No	
Rule 3	Outbreak Alarm - Zulu Expired Event Handler 2 - Outbreak Zulu Expired			No	
Rule 4	Outbreak Alarm - Zulu Expired Event Handler 2 - Outbreak Zulu Expired			No	
Rule 1	IMS - Critical Severity 1 - Severity Equal To Critical			No	IMS
Rule 2	Outbreak Alarm 1 - Level 1 - Outbreak Alarm 1 - Level 1 - Outbreak - MEDT Full			No	

Matching Filters

Match Criteria

Device (By name)

Subnets

Pre-Filters

Device Type

Log Type

Log Match

Log Field

Generic

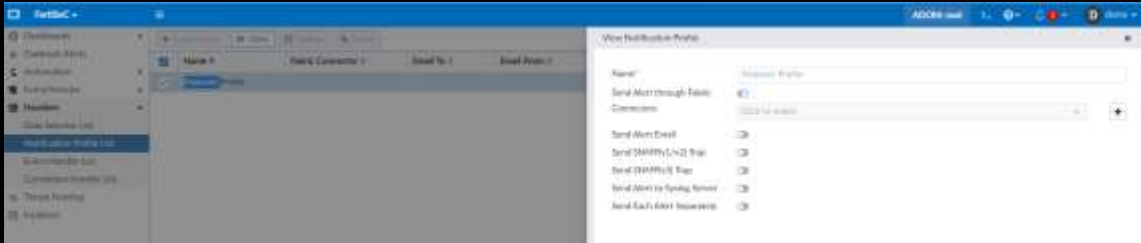
Can use multiple filters for more in-depth criteria

Operator	Meaning
==	Equal (exact match)
!=	Not equal (not matching)
<	Smaller than
<=	Smaller than or equal
>	Greater than
>=	Great than or equal
~	Contained (included somewhere in the string)
!~	Not contained (not included)

Event Details

Network Properties		Identity	
Destination IP	172.30.72.53	Device ID	FC181FTH22901825
Source IP	172.30.72.29	Device Name	NGFW_PBE
Type		User	admin
Method	https	User Interface	https(172.30.72.38)
Sub-Type	system	Alerts	
Type	event	Action	login
General		Level	Warning
Log Description	Admin login failed	Reason	password_failed
Log ID	D100033002	Others	
Message	Administrator admin login failed from https(172.30.72.29) because of invalid password	Date/Time	00:57:48
SN	0	Destination End User ID	3
Status	failed	Destination Endpoint ID	3
Virtual Domain	root	Device Time	2023-03-04 00:57:48
		Event Time	1677933248584130041
		Time Stamp	2023-03-04 00:57:48
		Time Zone	-0800
		UEBA Endpoint ID	3
		UEBA User ID	3
		logver	302041396

Event Notifications



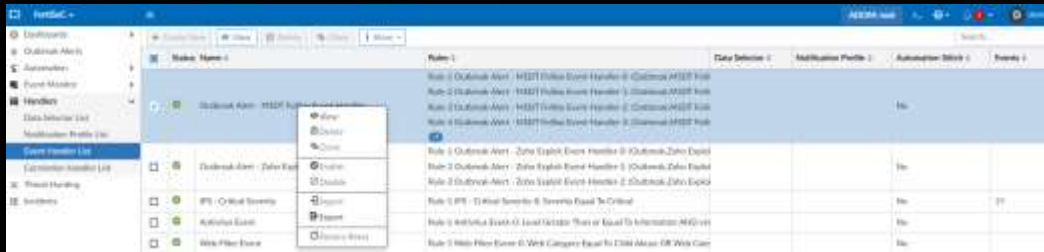
Event Status

#	Event	Event Status	Event Type	Count	Severity	First Occurrence	Last Update	Additional Info	Handler
1	Files dropped due to poor network connection (86)		Event	1822	Med.	7 days ago	A minute ago		EC5 Event Log Higher Th...
2	48.119.249.226 (75)								
	Instance SS, Connection blocked from DESKTOP-SALE-03	Mitigated	SS	8	Low	2023-03-04 02:07...	2023-03-04 02:07...	Server certificate is re-sign...	Default-Risk-Controllat...
	Instance SS, Connection blocked from DESKTOP-ENG5-02	Mitigated	SS	1	Low	2023-03-03 23:47...	2023-03-03 23:50...	Server certificate is re-sign...	Default-Risk-Controllat...
	Instance SS, Connection blocked from DESKTOP-FR9-02	Mitigated	SS	1	Low	2023-03-03 20:58...	2023-03-03 21:01...	Server certificate is re-sign...	Default-Risk-Controllat...
	Instance SS, Connection blocked from DESKTOP-FR9-03	Mitigated	SS	6	Low	2023-03-03 20:13...	2023-03-03 20:16...	Server certificate is re-sign...	Default-Risk-Controllat...
	Instance SS, Connection blocked from DESKTOP-ENG2-03	Mitigated	SS	6	Low	2023-03-03 16:33...	2023-03-03 16:51...	Server certificate is re-sign...	Default-Risk-Controllat...
	Instance SS, Connection blocked from DESKTOP-SALE-02 corp...	Mitigated	SS	8	Low	2023-03-03 16:33...	2023-03-03 16:54...	Server certificate is re-sign...	Default-Risk-Controllat...
	Instance SS, Connection blocked from FORTICENT-DM6	Mitigated	SS	1	Low	2023-03-03 16:33...	2023-03-03 16:20...	Server certificate is re-sign...	Default-Risk-Controllat...

Event Status	Description
Unhandled	The Security event risk is not mitigated or contained, so it is considered open
Contained	The risk source is isolated
Mitigated	The security risk is mitigated by being blocked or dropped
Blank	Other scenarios

Exporting and Importing Event Handlers

- Event handlers are configured per ADOM
- Can export from one ADOM to another
 - If name conflict a time stamp will be added to the name
- Use JSON format



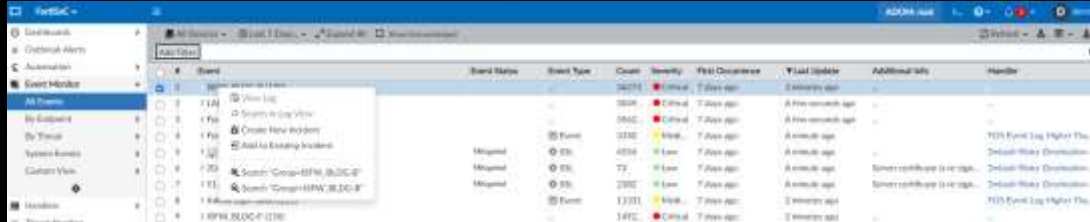
Managing Events



Event ID	Event Status	Event Type	Count	Severity	First Occurrence	# Last Update	Additional Info	Handler
1	OK	IPV6	16278	Info	7 days ago	8 days ago		
2	OK	IPV6	3091	Critical	7 days ago	8 days ago		
3	OK	IPV6	2342	Critical	7 days ago	8 days ago		
4	OK	IPV6	3201	Warn	7 days ago	8 days ago		
5	OK	IPV6	4254	Warn	7 days ago	8 days ago		
6	OK	IPV6	73	Warn	7 days ago	8 days ago		
7	OK	IPV6	2383	Warn	7 days ago	8 days ago		
8	OK	IPV6	11311	Warn	7 days ago	8 days ago		
9	OK	IPV6	1476	Critical	7 days ago	8 days ago		
10	OK	IPV6	4530	Warn	7 days ago	8 days ago		

Creating an Incident

Created when an event needs further investigation
Can be created manually or automatically via a playbook



Creating an Incident

Created when an event needs further investigation

Can be created manually or automatically via a playbook



The screenshot shows a Splunk dashboard window titled 'Incidents'. The main content is a table with the following columns: Incident Number, Incurred Date & Time, Incident Reporter, Incident Category, Severity, Status, Affected Endpoint, and Description. The table contains six rows of incident data.

Incident Number	Incurred Date & Time	Incident Reporter	Incident Category	Severity	Status	Affected Endpoint	Description
040000210	2023-03-03 03:03:17	Critical Incident Reporter - 2023...	Malicious Scan	High	Analyze		Incursion detected
040000210	2023-03-03 03:03:20	Critical Incident Reporter - 2023...	Malicious Scan	High	Analyze		Incursion detected
040000210	2023-03-03 03:03:15	Critical Incident Reporter - 2023...	Malicious Scan	High	Analyze		Incursion detected
040000210	2023-03-03 03:03:16	Critical Incident Reporter - 2023...	Malicious Scan	High	Analyze		Incursion detected
040000210	2023-03-03 03:03:14	Critical Incident Reporter - 2023...	Malicious Scan	High	Analyze		Incursion detected
040000210	2023-03-03 03:03:18	Critical Incident Reporter - 2023...	Malicious Scan	High	Analyze		Incursion detected

Analyzing an Incident

The screenshot displays a security incident response dashboard for incident ID IN00002235. The incident is categorized as 'Malicious Code' and is currently 'Not Assigned' for 'Analysis'. The dashboard is divided into several sections:

- Affected Endpoint/User:** Shows 'No assessment available' and a 'Last Seen' timestamp of 2023-03-04 09:32:18.
- Executed Playbooks:** A table with columns for 'PLAYBOOK', 'STATUS', and 'TRIGGER'. A 'View all Playbooks' button is located below the table.
- Incident Timeline:** A horizontal timeline from 2023-03-03 00:00:00 to 2023-03-03 09:00:00. A red dot on the timeline indicates the incident's start time at 09:32:18. A 'Reset Zoom' button is on the right.
- Comments:** A text input field with a 'POST' button.
- Audit History:** A vertical timeline showing a 'New Incident Created' event at 2023-03-04 09:32:18, triggered by a 'Playbook Critical Incident'.

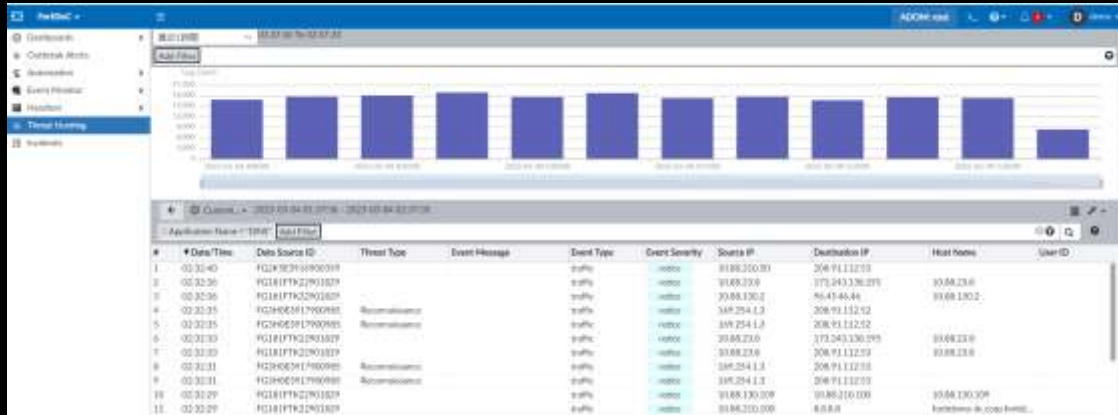
Editing an Incident

The screenshot shows a dialog box titled "Edit Incident" with the following fields:

- Incident Number: 100000000
- Incident Date / Time: 2023-02-07 09:20:15
- Incident Category: Malicious Code
- Severity: High
- Status: Analysis
- Affected Endpoints: (empty)
- Description: Intrusion detected.
- Assigned To: (empty)

Buttons for "OK" and "Cancel" are located at the bottom right of the dialog.

Threat Hunting



Log Count Chart



SIEM Log Analytics

Table contains many elements to gain insights in SOC

Statistical data for each field of interest and details can be filtered and viewed


ID	Application Service	Client	Sent Bytes	Session Duration
1	web5253	11.4021191	0.0 KB	
2	HTTP	20.6030191	282.3 MB	1min
3	web5253	00.0050191	0.0 KB	
4		10.0040191		23m-20s
5	web5253	04.2040191	5.4 MB	50m-20s
6	HTTP	12.0040191	4.2 MB	15s
7	web5253	01.1040191	13.9 MB	50s
8	web5253	00.0040191	1.1 MB	70m-00s
9	web5253	0.0030191	286.4 KB	50s
10	web5253	8.7030191	2.8 MB	10m-20s
11	HTTP	7.0030191	1.2 MB	5m-27s
12	web5253	7.0030191	0.0 KB	
13	web5253	0.0030191	8.7 MB	27s
14	web5253	6.0030191	0.2 MB	22m-27s
15	web5253	0.0030191	24.1 MB	71s
16	web5253	3.1030191	19.3 MB	44s
17	web5253	0.0030191	406.2 KB	30s

Outbreak Detection Service


Licensed
Receive information about malware outbreaks
Auto download new event handlers and reports outbreak




Conclusions



Understand FortiSOC features



Understand management extension applications



Summarize FortiSOC dashboards information



Reports

Elements that Compromise a Report

An FAZ report is a set of data in organized charts

Chart



Defines what **data** from the SQL is displayed

Defines what **format** the data is displayed in

Dataset



Datasets are specific SQL SELECT queries

Format



Pie Chart



Bar Chart



Table

SELECT Statement

Select statement retrieves the log data

Must specify criteria using a recognized and supported clause

Clause	Definition
FROM	From which table(s) or view(s) the data will be extracted
WHERE	Sets the conditions (all rows that do not satisfy the condition are not shown in the output)
GROUP BY	Collects data across multiple records and groups the results by one or more columns
ORDER BY	Order the results by specific column(s), ascending or descending
LIMIT	Limits the number of records returned based on a limited value
OFFSET	Often used with the LIMIT clause to offset the results by a set value

Report WorkFlow

Select statement retrieves the log data

Must specify criteria using a recognized and supported clause



Reports and ADOMs

Each ADOM has its own reports, libraries, and advanced settings

Additional reports the FortiNet devices are available when ADOMs available

FortiAuthenticator

FortiCarrier

FortiClient

FortiDDos

FortiDeceptor

FortiManager

FortiMail

FortiNAC

FortiProxy

FortiSandbox

FortiWeb

Report Considerations

Audience

Level and type of information may vary

Purpose

What information is needed

Align with database query

Level of detail

To much detail can overwhelm

Keep reports short and concise

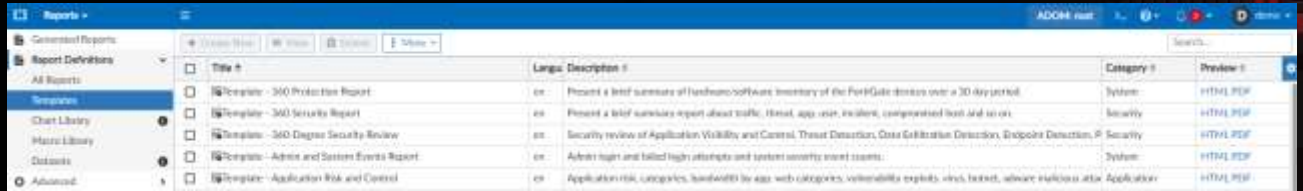
Too many charts very CPU intensive

Format

Best way to display information



Templates



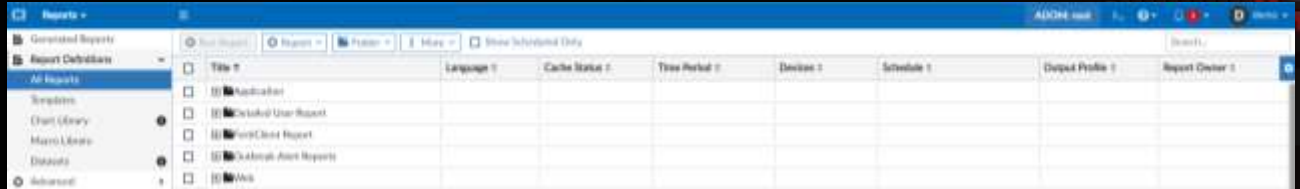
The screenshot shows the 'Reports' section of the StormWind interface. On the left, there is a navigation menu with categories: Generated Reports, Report Definitions, All Reports, Templates (selected), Chart Library, Macro Library, Outlook, and Advanced. The main area displays a table of report templates with columns for Title, Language, Description, Category, and Preview.

Title	Lang	Description	Category	Preview
Template - 360 Protection Report	en	Present a brief summary of hardware/software inventory of the FortiGate devices over a 30 day period.	System	HTML PDF
Template - 360 Security Report	en	Present a brief summary report about traffic, threat, app, user, incident, compromised host and so on.	Security	HTML PDF
Template - 360 Degree Security Review	en	Security review of Application Visibility and Control, Threat Detection, Cross Correlation Detection, Endpoint Detection, &	Security	HTML PDF
Template - Admin and System Events Report	en	Admin login and failed login attempts and system security event counts.	System	HTML PDF
Template - Application Risk and Control	en	Application risk categories, based on IP, web categories, vulnerability exploits, virus, botnet, malware, malicious sites	Application	HTML PDF

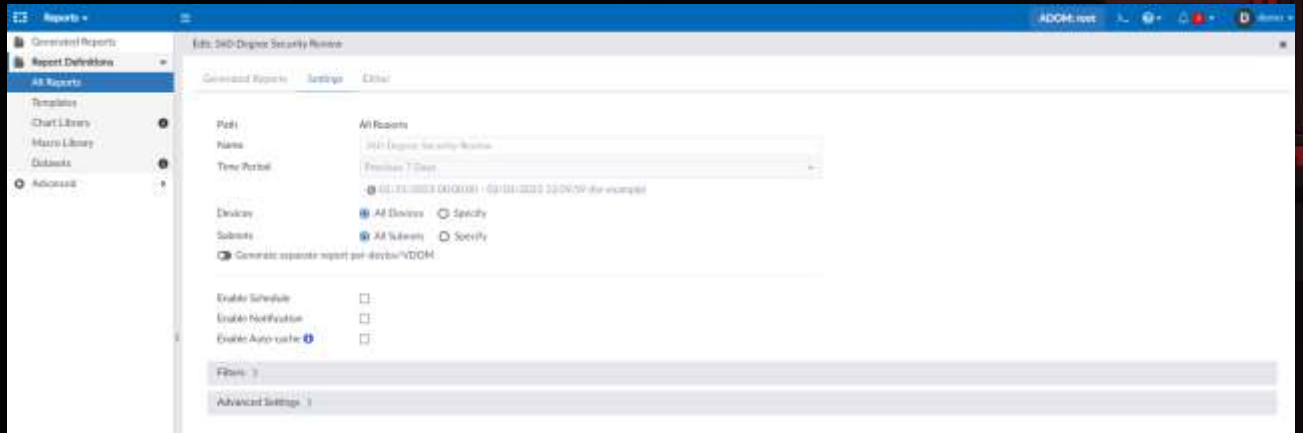
Running Predefined Reports

- Based on associate templates
 - Template Layout
 - Configured with basic default settings
- Configure basic report settings
 - Time Period
 - Devices
 - Types
- Run Report
 - On Demand
 - Scheduled
- Multiple Formats
 - HTML, PDF, XML, CSV, JSON

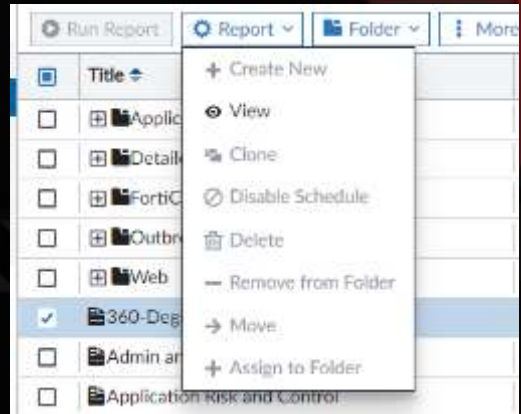
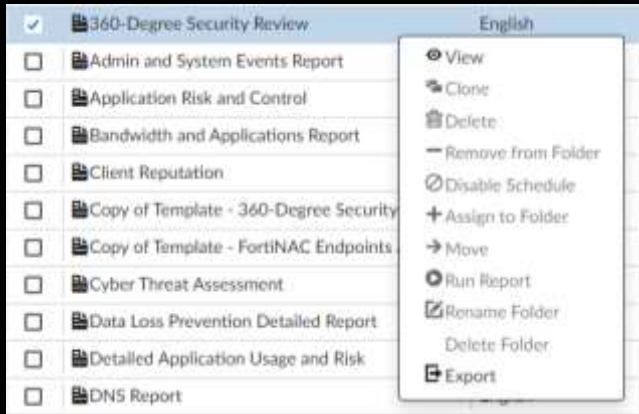
Running Predefined Reports



Fine-tuning Predefined Reports

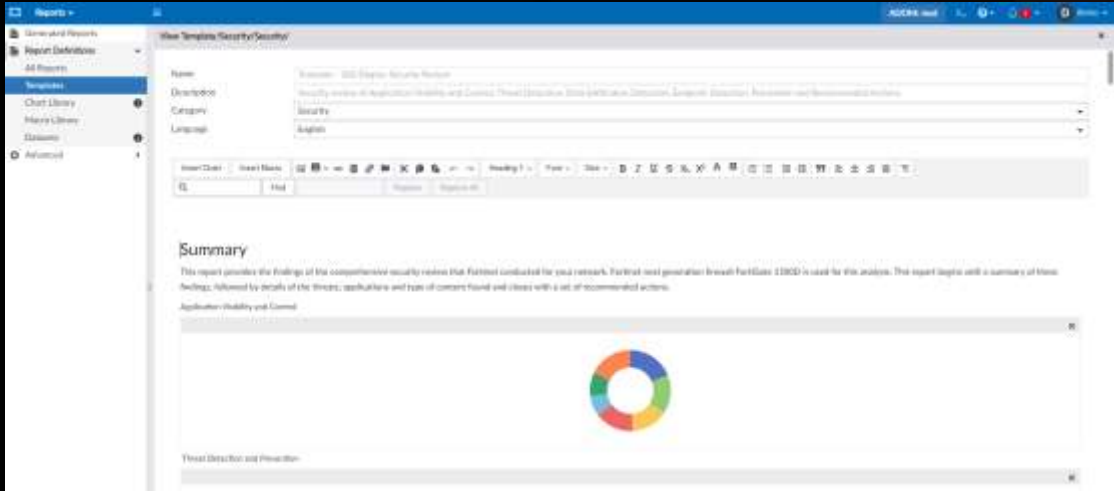


Customization Options

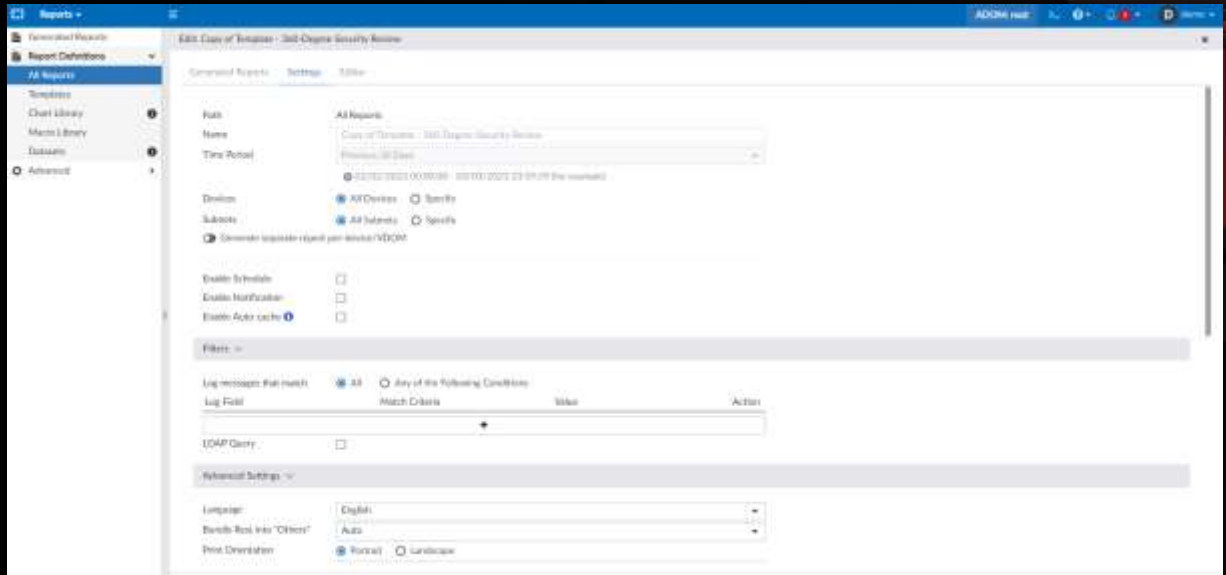


Customization: Template vs Report

Templates only include the layout of the report – they do NOT include report settings



Edit: Copy of Template



Inserting Macros as Abbreviated Dataset Queries

Macros specify what data to extract from the logs

Represent a sequence of instructions in abbreviated form

Can insert into templates and reports without having to use a chart to display data

Predefined and custom

ADOM-Specific



The screenshot shows the ADOM console interface. On the left, there is a navigation pane with 'Macros Library' selected. The main area displays a table of macros with columns for Name, Description, Device Type, and Category.

Name	Description	Device Type	Category
ADOM Security Total Malware Detected	ADOM Security Total Malware Detected	FortiGate	View
ADOM Account Disabled Count	A Patched Endpoint Count	FortiGate	Application Control
ADOM Analyzed Security Event Count	Analyzed Security Event Count	FortiGate	Application Control
ADOM App Count of Self-Harm Risky Terms	App Count of Self-Harm Risky Terms	FortiGate	Application Control
ADOM Application Categories with Highest Bandwidth	Application Categories with Highest Bandwidth	FortiGate	Subs

Chart / Dataset Requirements

If Predefine charts/Datasets do not meet requirements

Chart Library contains more than 700 predefine charts

Can't be edited

Datasets library contains more than 800 datasets

Can't be edited

Can clone and modify both charts and datasets or create new ones

External Storage of Generated Reports

Send or store reports for offline purposes

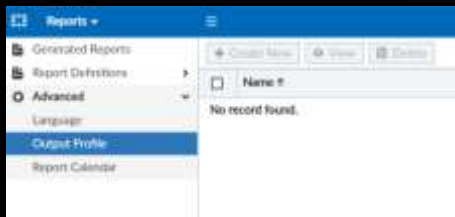
Configured per ADOM

Email or upload to server – PDF HTML XML and CVS formats

Must configure back-end configuration

Mail-Server

Output Profile



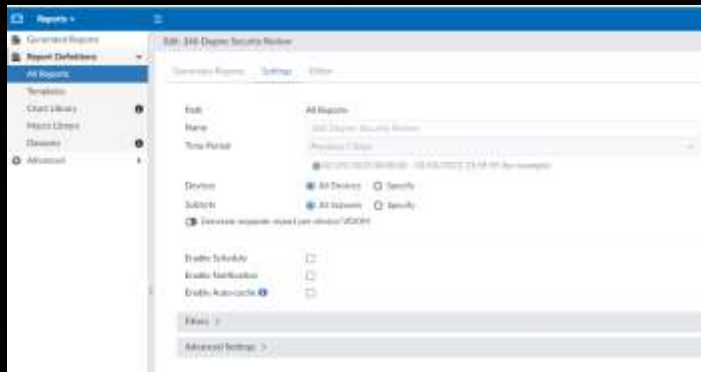
SQL Hard Cache

Must be built before the FAZ can build the report

Increases report generation time

If no new log hcache does not need to rebuild

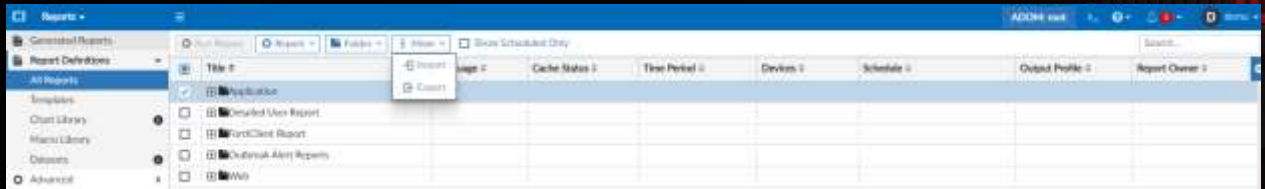
To reduce report generation time enable auto-cache from report settings



Moving Reports Between ADOMs



Each ADOM has its own reports, libraries, and advanced settings



Attach Reports to Incidents

● Add reports for historical data to incidents

● 3 ways to attach

1. Manually, from existing report
2. Manually, from existing incident
3. Automatically by use of playbooks

Viewing Scheduled Reports Through Calendar



Troubleshooting Report Generation Run Time

The screenshot displays a web application interface for report management. The main table lists reports with columns for Report Name, Format, Time Range, Device, and Status. A detailed view of a report is shown in a pop-up window, listing various categories and their corresponding run times.

Report Name	Format	Time Range	Device	Status
Cyber Threat Assessment FTNT-D	HTML PDF XML CSV JSON	2023-03-04 - 2023-03-04	FTNT-DEMO	7s
Threat Report-FTNT-DEMO-2023		2023-03-04	FTNT-DEMO	2s
Threat Report-FTNT-DEMO-2023		2023-03-01	FTNT-DEMO	2s
Threat Report-FTNT-DEMO-2023		2023-03-02	FTNT-DEMO	2s
Cyber Threat Assessment FTNT-D		2023-03-03	FTNT-DEMO	6s
Threat Report-FTNT-DEMO-2023		2023-03-03	FTNT-DEMO	2s
Threat Report-FTNT-DEMO-2023		2023-03-03	FTNT-DEMO	2s
Cyber Threat Assessment FTNT-D		2023-03-03	FTNT-DEMO	4s
Threat Report-FTNT-DEMO-2023		2023-03-03	FTNT-DEMO	2s
Threat Report-FTNT-DEMO-2023		2023-03-03	FTNT-DEMO	2s
Threat Report-Demo-DCFW-Insta		2023-03-03	Demo-DCFW-Insta	2s
Threat Report-IPFW_BSDG-Front		2023-03-03	IPFW_BSDG-Front	2s
Threat Report-IPFW_BSDG-Rear		2023-03-03	IPFW_BSDG-Rear	2s
Threat Report-IPFW_BSDG-Front		2023-03-03	IPFW_BSDG-Front	2s
Threat Report-IPFW_BSDG-Rear		2023-03-03	IPFW_BSDG-Rear	2s
Cyber Threat Assessment FTNT-D		2023-03-03	FTNT-DEMO	6s
Cyber Threat Assessment Demo L		2023-03-03	Demo-DCFW-Insta	6s
Cyber Threat Assessment GFW-R		2023-03-03	IPFW_BSDG-Front	7s

Report Name	Format	Time Range	Device	Status
Cyber Threat Assessment FTNT-D	HTML PDF XML CSV JSON	2023-03-04 - 2023-03-04	FTNT-DEMO	7s
Threat Report-FTNT-DEMO-2023		2023-03-04	FTNT-DEMO	2s
Threat Report-FTNT-DEMO-2023		2023-03-01	FTNT-DEMO	2s
Threat Report-FTNT-DEMO-2023		2023-03-02	FTNT-DEMO	2s
Cyber Threat Assessment FTNT-D		2023-03-03	FTNT-DEMO	6s
Threat Report-FTNT-DEMO-2023		2023-03-03	FTNT-DEMO	2s
Threat Report-FTNT-DEMO-2023		2023-03-03	FTNT-DEMO	2s
Cyber Threat Assessment FTNT-D		2023-03-03	FTNT-DEMO	4s
Threat Report-FTNT-DEMO-2023		2023-03-03	FTNT-DEMO	2s
Threat Report-FTNT-DEMO-2023		2023-03-03	FTNT-DEMO	2s
Threat Report-Demo-DCFW-Insta		2023-03-03	Demo-DCFW-Insta	2s
Threat Report-IPFW_BSDG-Front		2023-03-03	IPFW_BSDG-Front	2s
Threat Report-IPFW_BSDG-Rear		2023-03-03	IPFW_BSDG-Rear	2s
Threat Report-IPFW_BSDG-Front		2023-03-03	IPFW_BSDG-Front	2s
Threat Report-IPFW_BSDG-Rear		2023-03-03	IPFW_BSDG-Rear	2s
Cyber Threat Assessment FTNT-D		2023-03-03	FTNT-DEMO	6s
Cyber Threat Assessment Demo L		2023-03-03	Demo-DCFW-Insta	6s
Cyber Threat Assessment GFW-R		2023-03-03	IPFW_BSDG-Front	7s

Report Troubleshooting CLI Commands

What to Investigate	CLI Command to Use
What is SQL Insertion Status? What are the SQL query connections and hcache status?	<pre># diagnose sql status sqlplugind # diagnose sql status sqlreportd</pre>
Is the hcache creation able to catch up? What are the log file-related activities rolled/deleted/uploaded) (file	<pre># diagnose test application logfiled 2</pre>
What are the current SQL processes running (any log queries)?	<pre># diagnose sql process list</pre>
What is the configuration status of all configured reports?	<pre># execute sql-report list-schedule <ADOM></pre>
What is the state of the hcache?	<pre># diagnose test application sqlrptcached <level></pre>
What is the hcache size on the file system?	<pre># diagnose sql show hcache-size</pre>

Conclusions

Report Concepts

Generating and Customizing Reports

Customizing Charts and Datasets

Managing Reports

Troubleshooting Reports



Working with Playbooks

Overview

FAZ automation capabilities

Playbook concepts

Trigger Types and Characteristics

Connector Types

Playbook Tasks

Why Automation

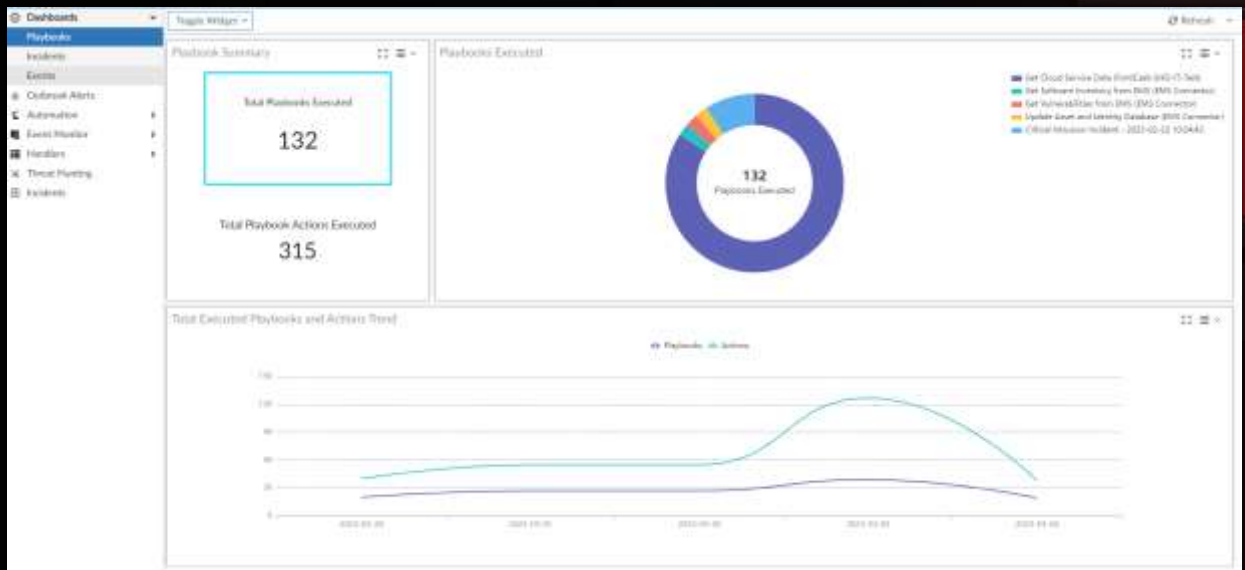
General Benefits

- Improves Productivity
- Reduces cost
- Increase efficiency
- Reduces human error

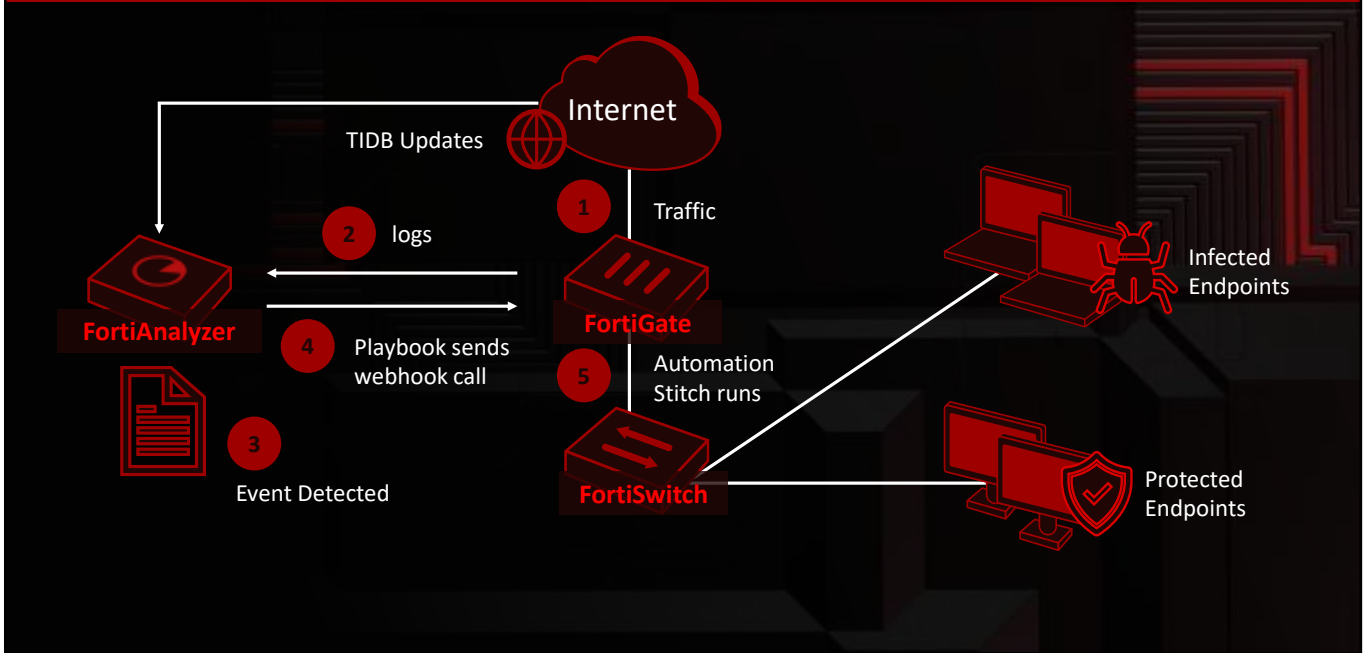
SOC Advantages

- Faster incident response time
- Faster data analysis
- Better use of analysis time
- Better compliance management
- Consistent security posture

Why Automation



Example Automation



Playbook Concepts

Automate common SOC tasks

Created per ADOM

Each playbook has only 1 trigger

Have 1 or more tasks

Actions can be performed depending upon connector used

Built-in or newly created

Created using an intuitive playbook designer

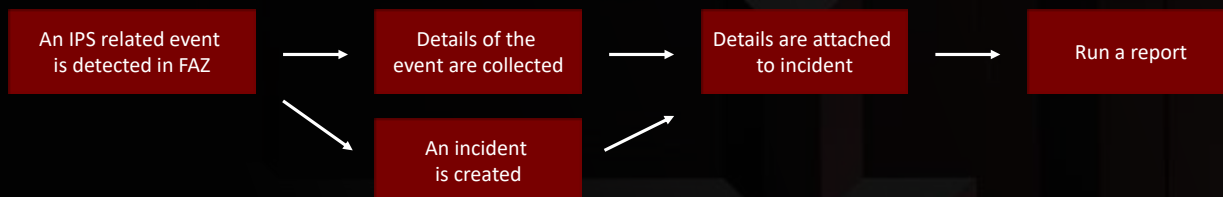
Playbook Concepts

A simple playbook execution sequence

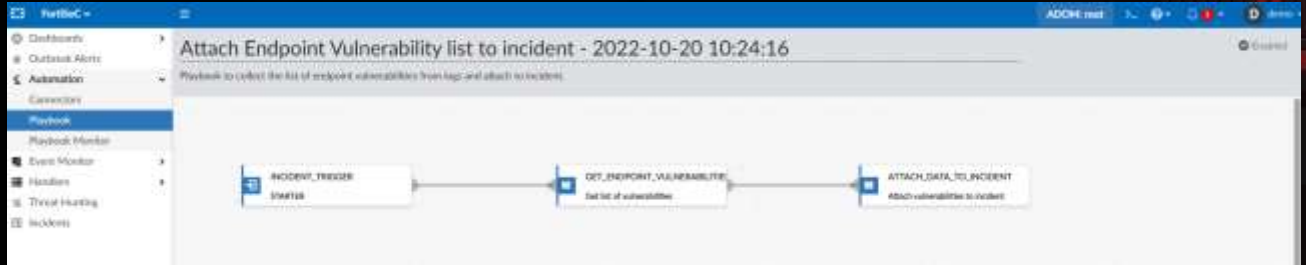


Multiple tasks can be triggered

Tasks can be sequential, or run in parallel



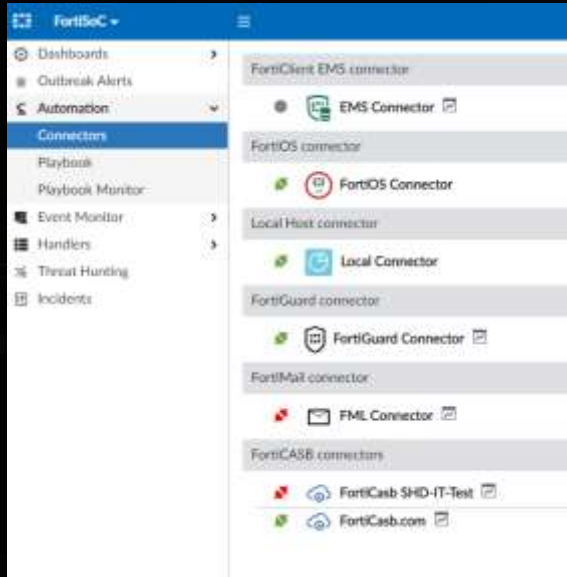
Playbook Concepts



Triggers

Trigger Type	Description
EVENT_TRIGGER	The playbook is run when an event is created that matches the configured filters When no filters are set, all events will trigger the playbook
INCIDENT_TRIGGER	The playbook is run when an incident is created that matches the configured filters When no filters are set, all incidents will trigger the playbook
ON_SCHEDULE	The playbook is run during the configured schedule You can define the start time, end time, interval type, and interval frequency for the schedule
ON_DEMAND	The playbook is run when manually started by an administrator

Connectors



Tasks

Tasks are actions that are executed when playbook runs

Available actions depend on connector chosen

You can chain actions together

Output of a task can be used as an input for the next tasks

Customizing Playbooks Settings

The screenshot displays the FortiGate GUI for configuring a playbook. The main window is titled "Run AV Scan on Endpoint - 2022-10-20 10:23:41". The left sidebar shows navigation options: Dashboard, Outlook Alerts, Automation, Connectors, Playbook, Playbook Monitor, Event Monitor, Handlers, Threat Hunting, and Incidents. The "Automation" section is expanded to show "Connectors" and "Playbook". The "Playbook" section is selected, showing a flowchart with two steps: "ON_DESIGNER" (START) and "AV_QUICK_SCAN" (Run AV Scan). The "AV_QUICK_SCAN" step is highlighted with a blue border. The right pane shows the configuration for the "AV_QUICK_SCAN" action, titled "EMS_AV_QUICK_SCAN". The configuration fields are:

- Name: Run AV Scan
- Description: (empty)
- Connector: EMS Connector
- Action: AV Quick Scan
- Use ID: No Data / Yes
- Endpoint ID: Playbook Starter / epid
- FeedName ID: (empty)

Using Variable in Tasks

Can use output variables and Trigger variables in playbook tasks

Output variables: Output of previous tasks is input of current tasks

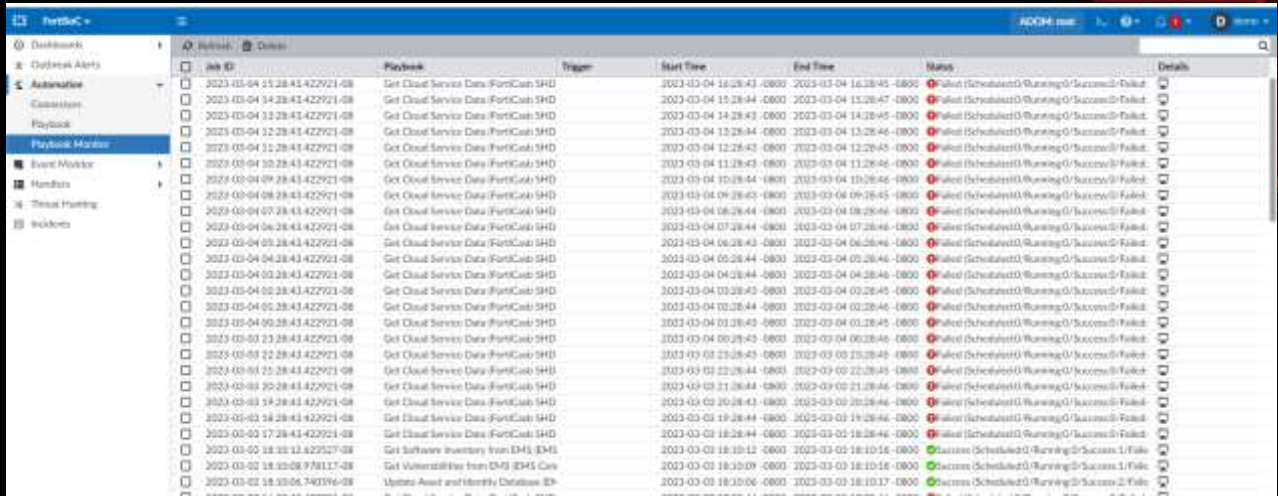
Format `${task_id.output}`

Previous task ID is needed

Trigger variables: Use some information from the trigger to filter the action tasks

Format `${trigger.variable}`

Managing Playbooks



Job ID	Playbook	Trigger	Start Time	End Time	Status	Details
2023-03-04 11:28:43 422921-08	Get Cloud Service Data-FortiGate SHD		2023-03-04 11:28:43 -0800	2023-03-04 11:28:45 -0800	Failed (Scheduled) Running 0 Success 0 Failed	
2023-03-04 14:28:43 422921-08	Get Cloud Service Data-FortiGate SHD		2023-03-04 14:28:44 -0800	2023-03-04 14:28:47 -0800	Failed (Scheduled) Running 0 Success 0 Failed	
2023-03-04 17:28:43 422921-08	Get Cloud Service Data-FortiGate SHD		2023-03-04 17:28:43 -0800	2023-03-04 17:28:45 -0800	Failed (Scheduled) Running 0 Success 0 Failed	
2023-03-04 12:28:43 422921-08	Get Cloud Service Data-FortiGate SHD		2023-03-04 12:28:44 -0800	2023-03-04 12:28:46 -0800	Failed (Scheduled) Running 0 Success 0 Failed	
2023-03-04 12:28:43 422921-08	Get Cloud Service Data-FortiGate SHD		2023-03-04 12:28:43 -0800	2023-03-04 12:28:45 -0800	Failed (Scheduled) Running 0 Success 0 Failed	
2023-03-04 09:28:43 422921-08	Get Cloud Service Data-FortiGate SHD		2023-03-04 09:28:44 -0800	2023-03-04 09:28:46 -0800	Failed (Scheduled) Running 0 Success 0 Failed	
2023-03-04 08:28:43 422921-08	Get Cloud Service Data-FortiGate SHD		2023-03-04 08:28:44 -0800	2023-03-04 08:28:46 -0800	Failed (Scheduled) Running 0 Success 0 Failed	
2023-03-04 07:28:43 422921-08	Get Cloud Service Data-FortiGate SHD		2023-03-04 07:28:44 -0800	2023-03-04 07:28:46 -0800	Failed (Scheduled) Running 0 Success 0 Failed	
2023-03-04 06:28:43 422921-08	Get Cloud Service Data-FortiGate SHD		2023-03-04 06:28:43 -0800	2023-03-04 06:28:46 -0800	Failed (Scheduled) Running 0 Success 0 Failed	
2023-03-04 05:28:43 422921-08	Get Cloud Service Data-FortiGate SHD		2023-03-04 05:28:44 -0800	2023-03-04 05:28:46 -0800	Failed (Scheduled) Running 0 Success 0 Failed	
2023-03-04 04:28:43 422921-08	Get Cloud Service Data-FortiGate SHD		2023-03-04 04:28:44 -0800	2023-03-04 04:28:46 -0800	Failed (Scheduled) Running 0 Success 0 Failed	
2023-03-04 03:28:43 422921-08	Get Cloud Service Data-FortiGate SHD		2023-03-04 03:28:43 -0800	2023-03-04 03:28:45 -0800	Failed (Scheduled) Running 0 Success 0 Failed	
2023-03-04 02:28:43 422921-08	Get Cloud Service Data-FortiGate SHD		2023-03-04 02:28:44 -0800	2023-03-04 02:28:46 -0800	Failed (Scheduled) Running 0 Success 0 Failed	
2023-03-04 01:28:43 422921-08	Get Cloud Service Data-FortiGate SHD		2023-03-04 01:28:43 -0800	2023-03-04 01:28:45 -0800	Failed (Scheduled) Running 0 Success 0 Failed	
2023-03-04 00:28:43 422921-08	Get Cloud Service Data-FortiGate SHD		2023-03-04 00:28:43 -0800	2023-03-04 00:28:46 -0800	Failed (Scheduled) Running 0 Success 0 Failed	
2023-03-03 23:28:43 422921-08	Get Cloud Service Data-FortiGate SHD		2023-03-03 23:28:43 -0800	2023-03-03 23:28:45 -0800	Failed (Scheduled) Running 0 Success 0 Failed	
2023-03-03 22:28:43 422921-08	Get Cloud Service Data-FortiGate SHD		2023-03-03 22:28:44 -0800	2023-03-03 22:28:45 -0800	Failed (Scheduled) Running 0 Success 0 Failed	
2023-03-03 21:28:43 422921-08	Get Cloud Service Data-FortiGate SHD		2023-03-03 21:28:44 -0800	2023-03-03 21:28:46 -0800	Failed (Scheduled) Running 0 Success 0 Failed	
2023-03-03 20:28:43 422921-08	Get Cloud Service Data-FortiGate SHD		2023-03-03 20:28:43 -0800	2023-03-03 20:28:46 -0800	Failed (Scheduled) Running 0 Success 0 Failed	
2023-03-03 19:28:43 422921-08	Get Cloud Service Data-FortiGate SHD		2023-03-03 19:28:44 -0800	2023-03-03 19:28:46 -0800	Failed (Scheduled) Running 0 Success 0 Failed	
2023-03-03 18:28:43 422921-08	Get Cloud Service Data-FortiGate SHD		2023-03-03 18:28:44 -0800	2023-03-03 18:28:46 -0800	Failed (Scheduled) Running 0 Success 0 Failed	
2023-03-03 18:10:12 829527-08	Get Software Inventory from EMS (EMS)		2023-03-03 18:10:12 -0800	2023-03-03 18:10:16 -0800	Success (Scheduled) Running 0 Success 1 Failed	
2023-03-03 18:10:09 778117-08	Get Vulnerability from EMS (EMS Core)		2023-03-03 18:10:09 -0800	2023-03-03 18:10:16 -0800	Success (Scheduled) Running 0 Success 1 Failed	
2023-03-03 18:10:06 740396-08	Update Asset and Monthly Database ID		2023-03-03 18:10:06 -0800	2023-03-03 18:10:17 -0800	Success (Scheduled) Running 0 Success 2 Failed	

Managing Playbooks

Playbook Tasks

Refresh View Raw Log

Task ID	Task	Start Time	End Time	Status	Raw Log
get_software_inventory	get software inventory	2023-03-03 18:10:14 -0800	2023-03-03 18:10:18 -0800	Success	View Log

Managing Playbooks

Playbook Tasks

task, id: 'get_software_inventory'

#	Level	Level	Date/Time	Date/Time	User	User	Device ID	Device ID	Sub Type	Sub Type	Message
1	notice	notice	03-03 18:10	03-03 18:10	system	system	FL-38F381A0000002	FL-38F381A0000002	playbook	playbook	Task get software inventory succeeded

Exporting Playbooks

Playbooks are defined per ADOM

Export to be used in different ADOMs

Connectors can be used in the exported file

Uses JSON format

Can compress the file

Conclusions

FAZ automation capabilities

Playbook concepts

Trigger Types and Characteristics

Connector Types

Playbook Tasks