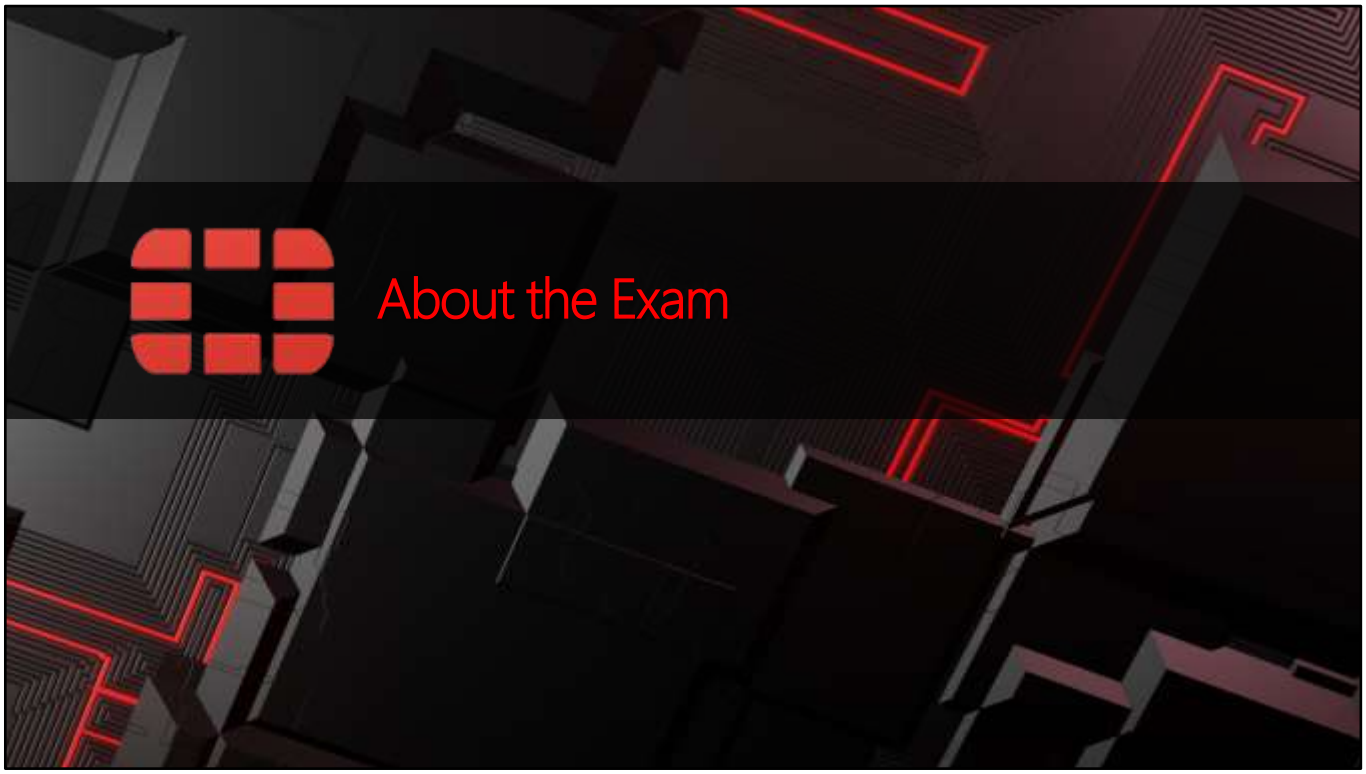
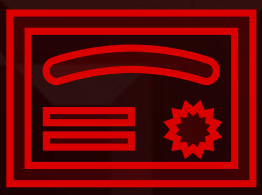


Program Requirements

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

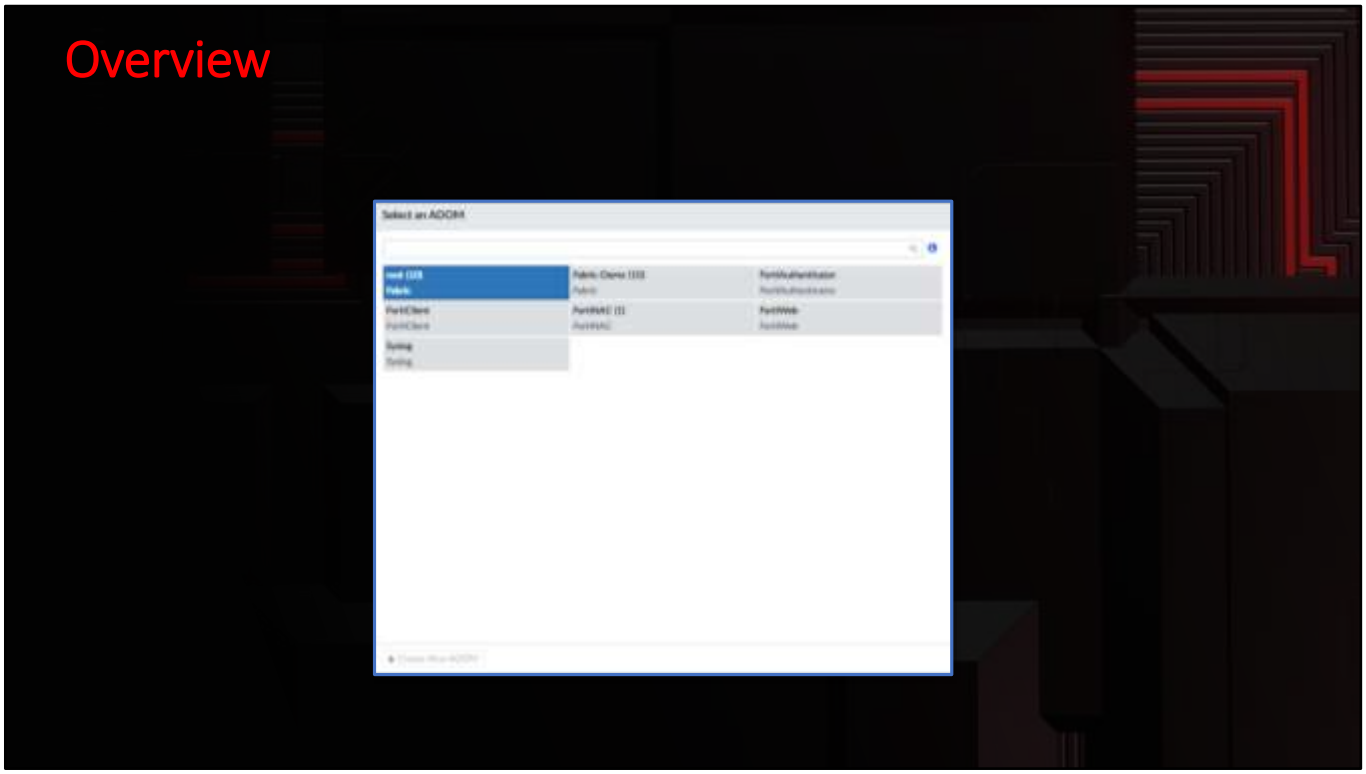
Exam

Demo Environment

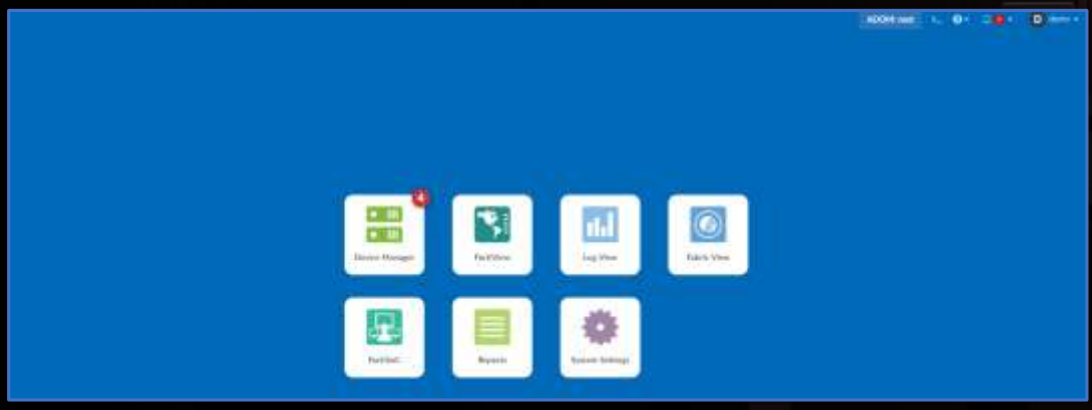
Overview

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

Overview

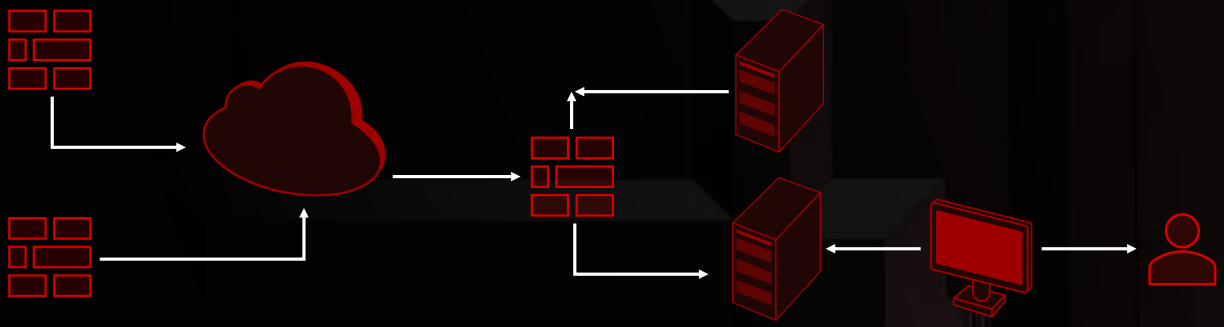


Overview



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 sore logs
- Admins
  - View and search logs
  - Configure, request, and view reports

FortiGate	FortiCarrier	FortiAnalyzer
FortiCache	FortiClient	FortiDDos
FortiMail	FortiManager	FortiSandBox
FortiWeb	Syslog	Chassis

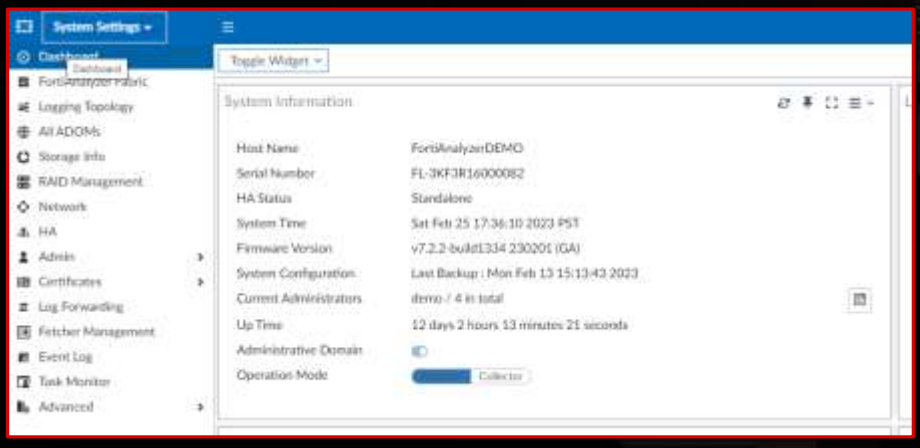
Reports, Events and Content Archiving

- 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

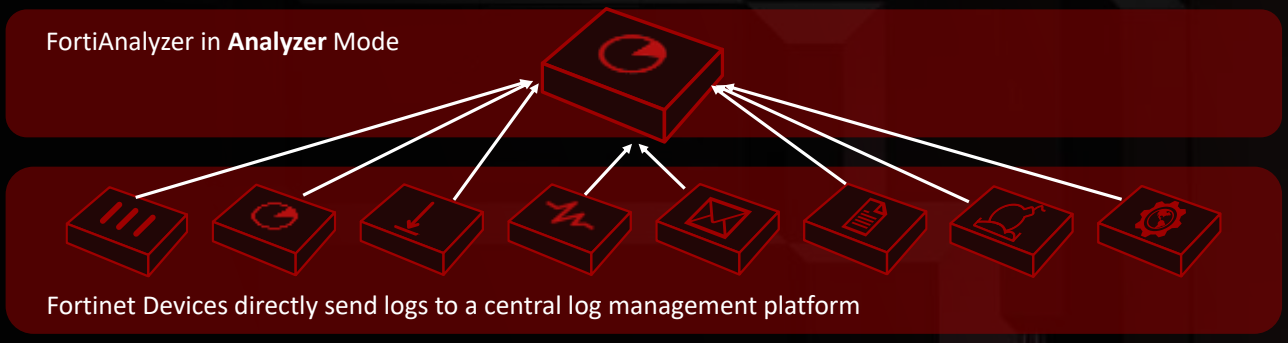
- Supports SQL for logging and reporting
- Inserts log data into SQL database for log view and report generation
- Uses a PostgreSQL database
- Advanced reporting does require SQL knowledge

FortiAnalyzer Operating Modes



FortiAnalyzer Operating Modes

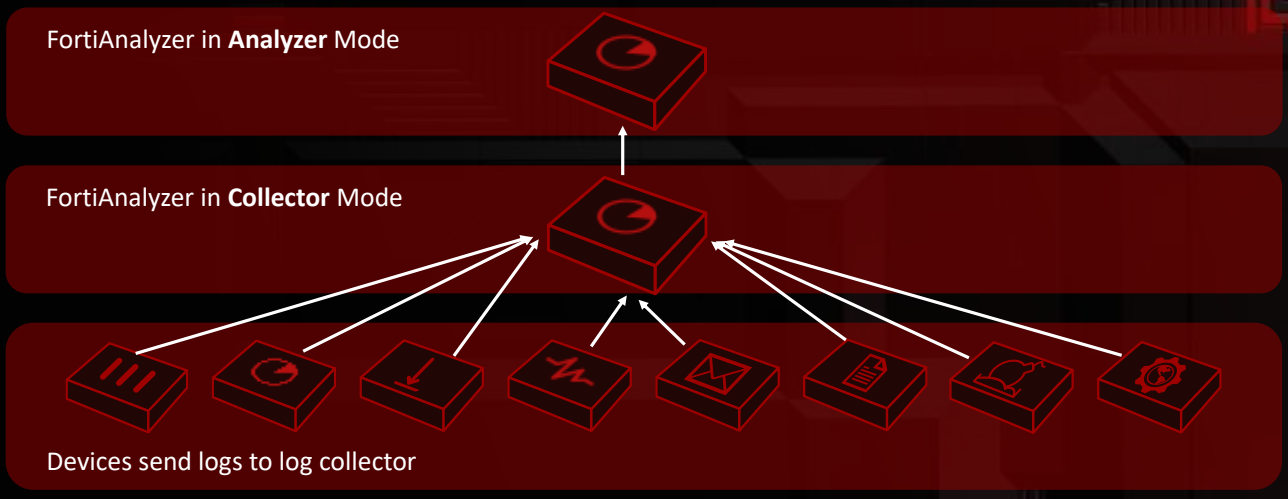
- Analyzer
  - Default Mode
  - Central log for one or more devices in collector mode
    - Can still forward logs to another FortiAnalyzer of syslog/CEF server



FortiAnalyzer Operating Modes

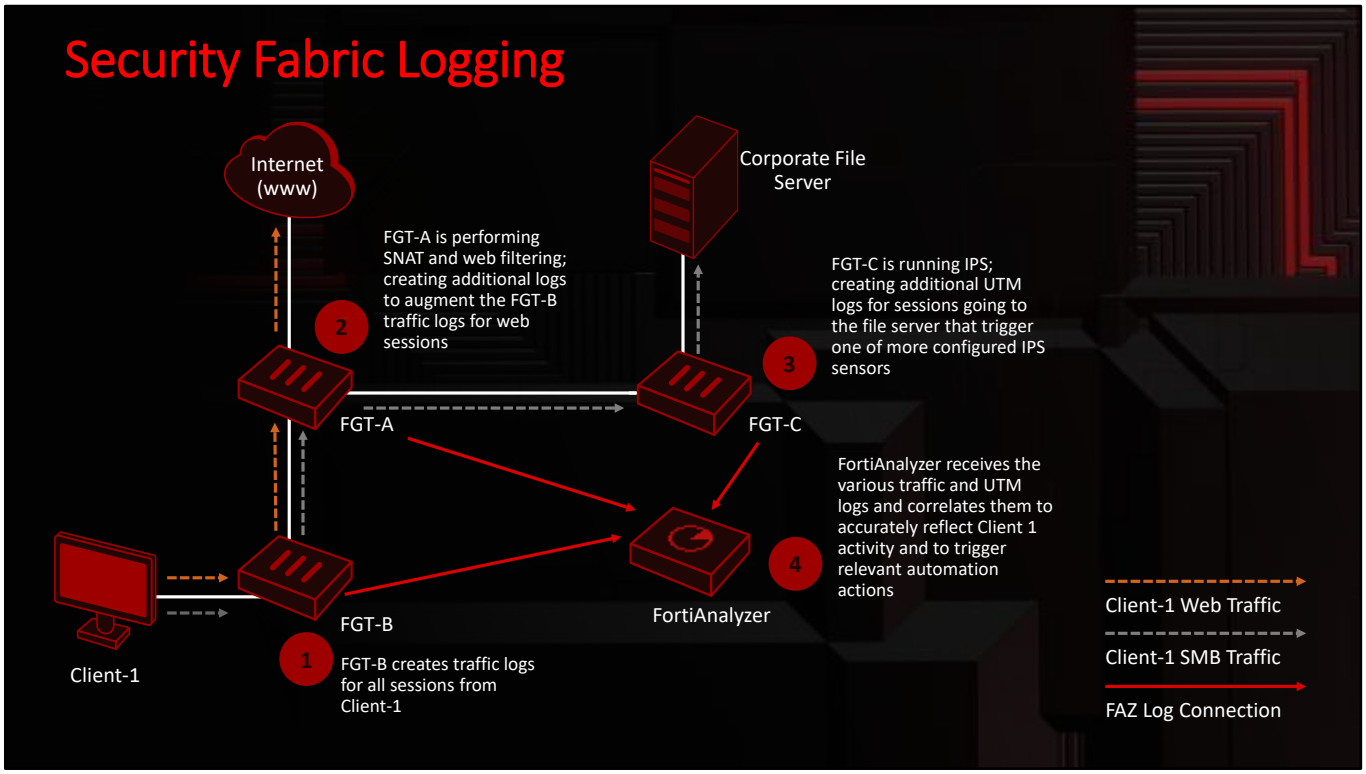
Collects logs from multiple devices and forwards to FortiAnalyzer in analyzer mode

Can forward to syslog/CEF server in real-time forward mode only



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



FortiAnalyzer Fabric

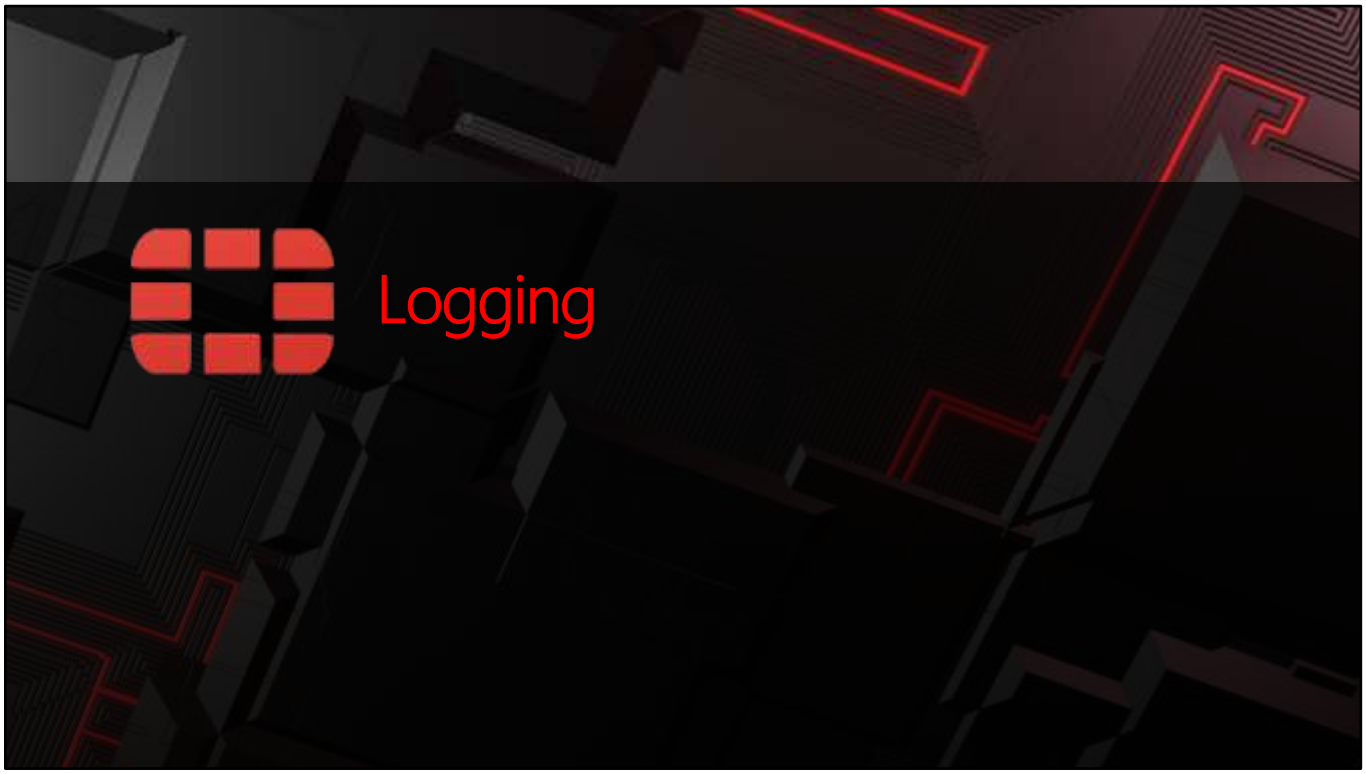
- Enables centralized viewing of devices, incidents, and events across multiple FortiAnalyzers
- Ideal for environments with many FortiAnalyzers and high log volume
- 2 Operations modes
  - Supervisor – one per fabric acts as root
  - Member – Sends information to supervisor
- Must be configured in same 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



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

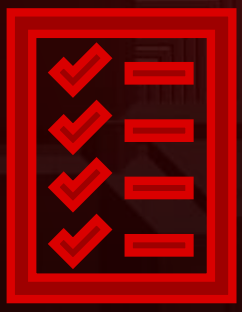
Track services used

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

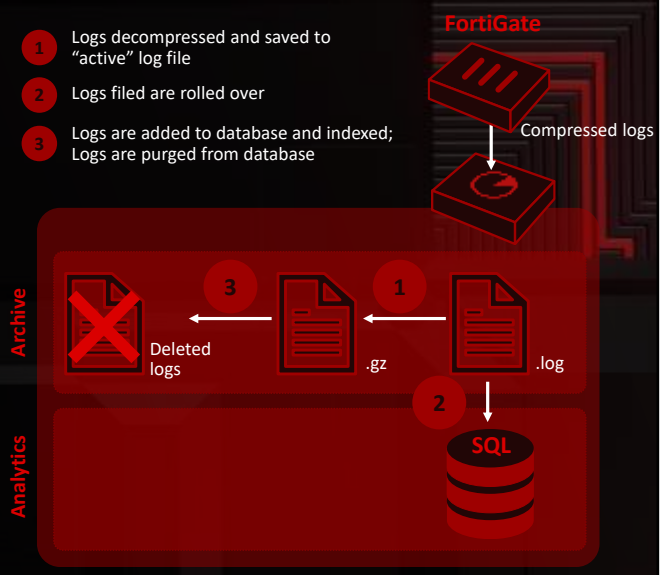


Log Type by Device

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)

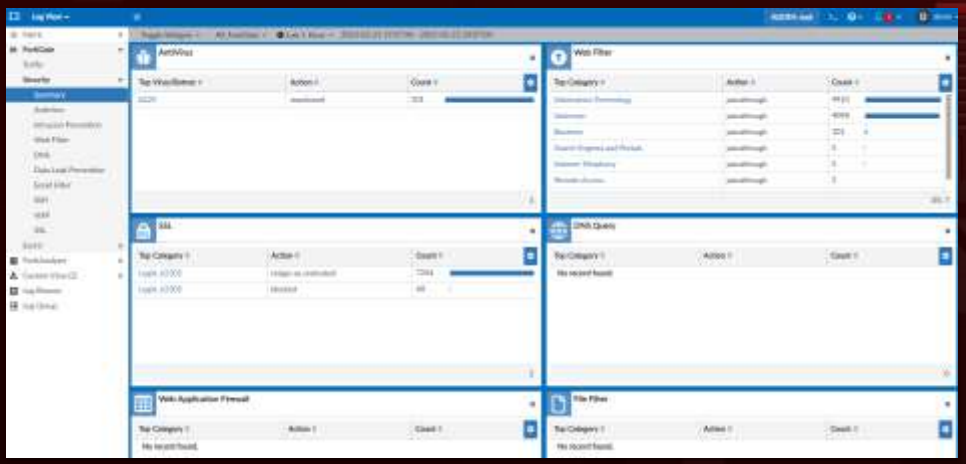


Log View

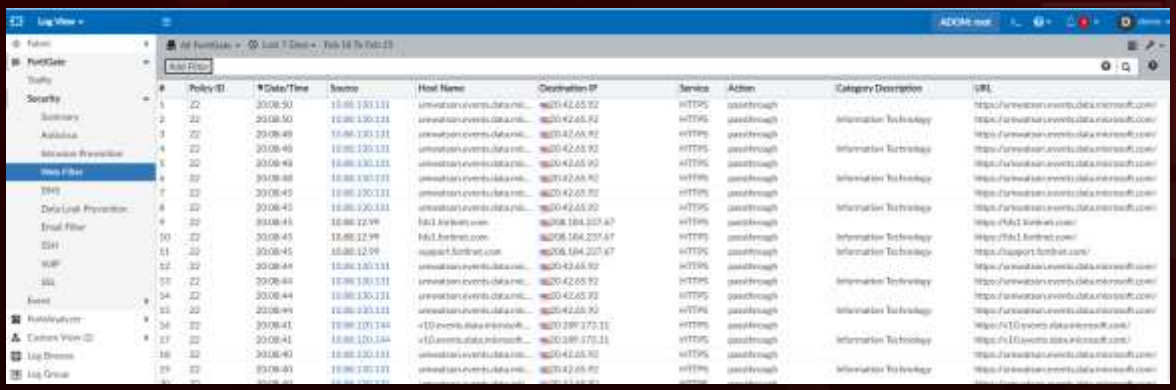
View all logs in each ADOM

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

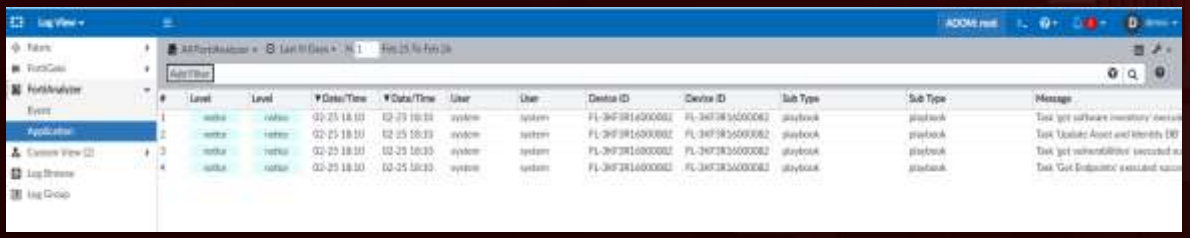
Summary Dashboard



Searching



Application Logs



FortiView

FortiView has two panes

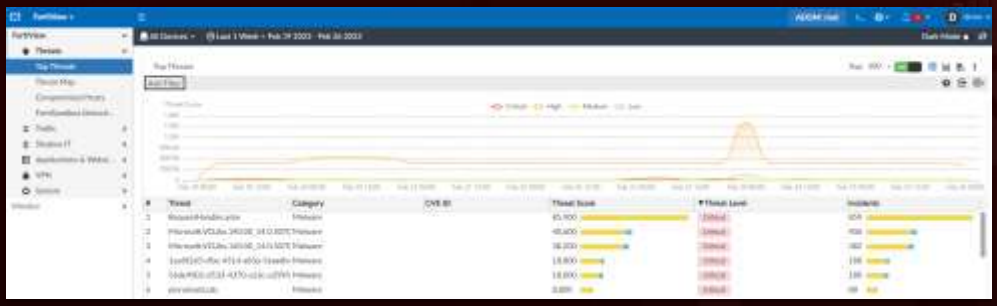
1. FortiView: Comprehensive monitoring system that displays real-time and historical data
2. Monitors: designed for NOC/SOC with big monitors displaying in dashboards

Each ADOM has its own data in FortiView

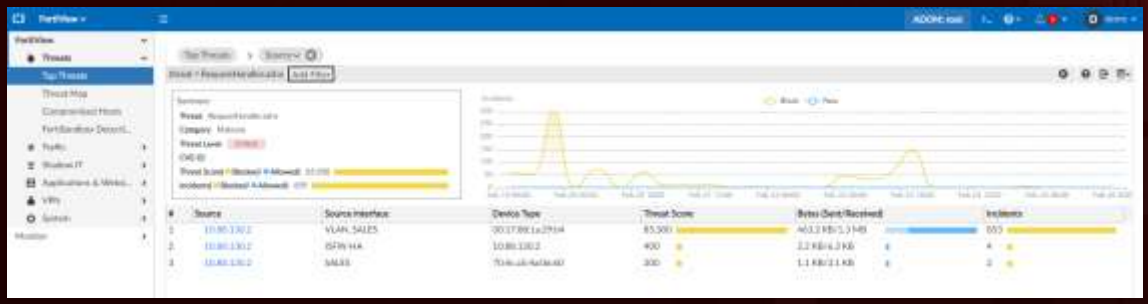
FortiView Pane

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

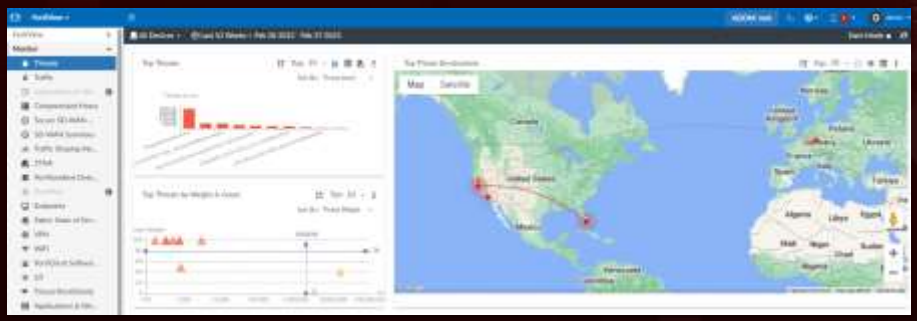
Branch Detection engine parses logs into categories

1. Infected
2. Highly Suspicious

Monitors Pane

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

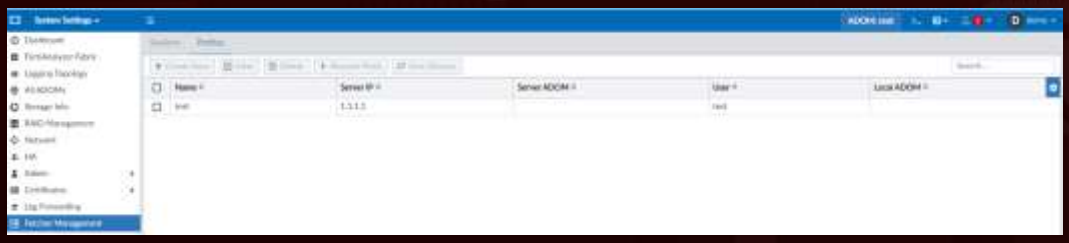
Dashboards contained customizable widgets



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



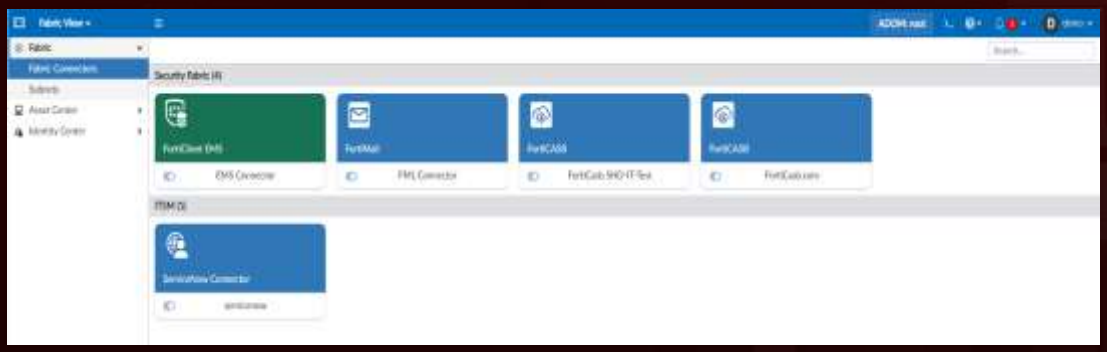
Log Fetching

- 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

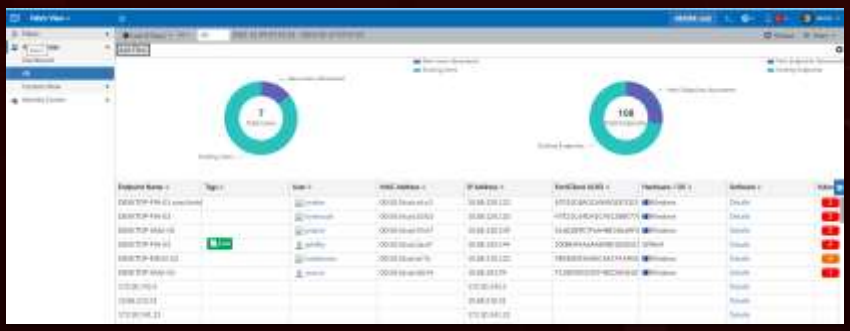
Fabric View Screen Cap



Asset Center

Pane provides endpoint and user information grouped by endpoint

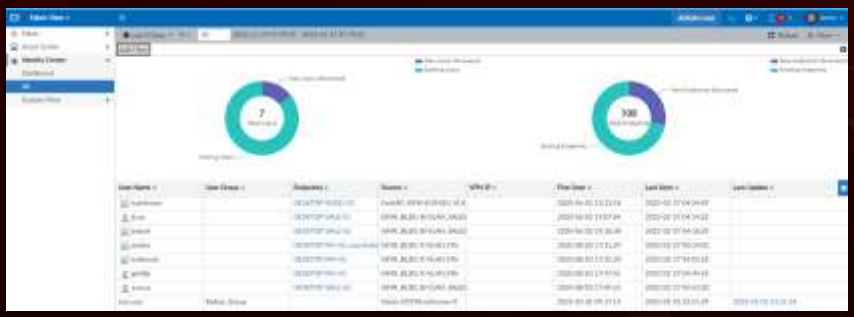
Useful in compliance and incident response investigation



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?
What are the log receive rate totals?
What is the device log rate?
What is the log rate for each log type?
	`# diagnose fortilogd lograte`
	`# diagnose fortilogd lograte-total`
	`# diagnose fortilogd lograte-device`
	`# 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?	`# diagnose fortilogd lograte-adom {all | adom-name}`
Log volume for all, or a specific ADOM?	`# diagnose fortilogd logvol-adom {all | adom-name}`

Conclusions

Purpose of Collecting and storing logs

Log file workflow

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

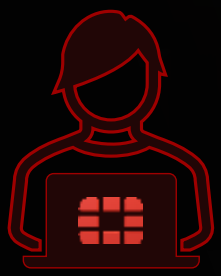
SOC Automation

- FortiSOC Module
- Playbook Templates and Automation
- Connectors for Playbooks
- Visual Playbook Editor
- Playbook Execution
- Playbook Monitor

Fabric Analytics

- SOC Analytics

FortiSoc Features

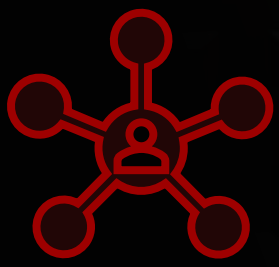


FortiSOC capabilities

- 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

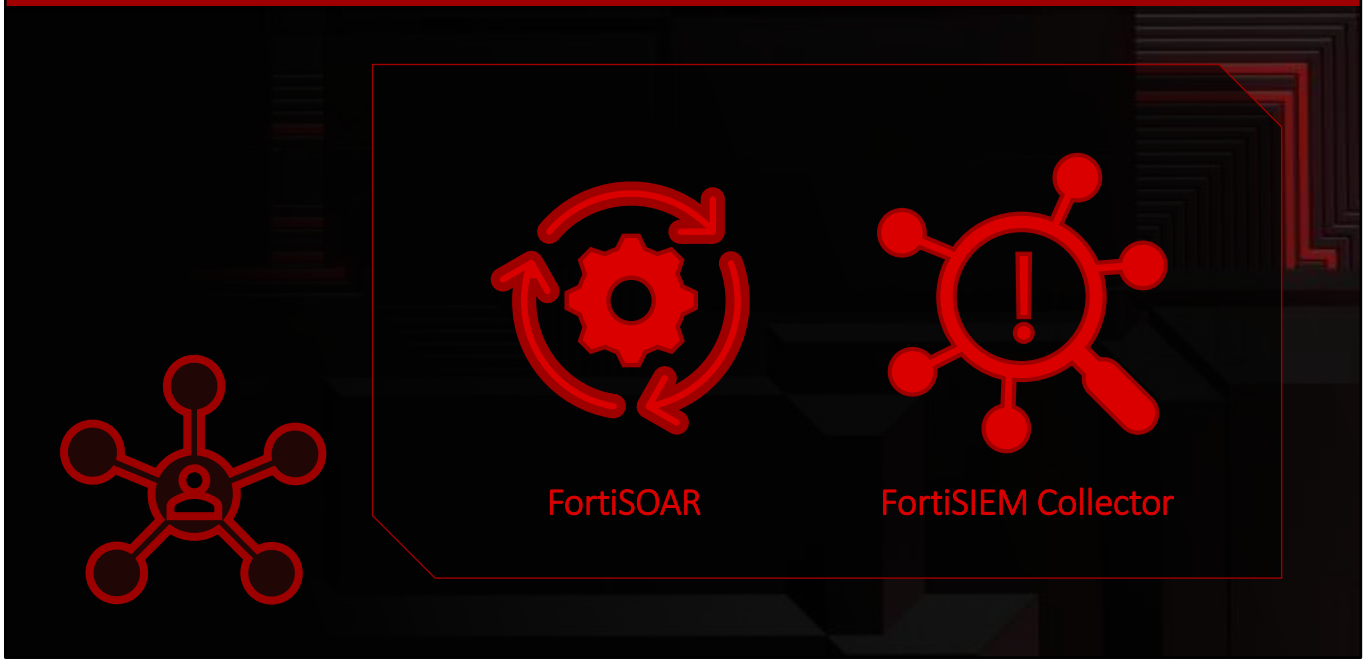
Management extensions are full-fledged running instances of a product in the form of a docker container

- 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

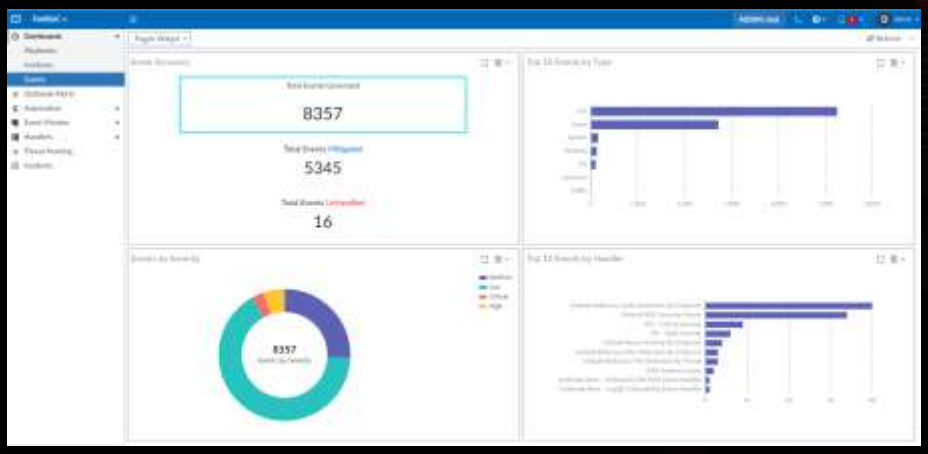


Dashboards

FortiSOC includes 3 dashboards

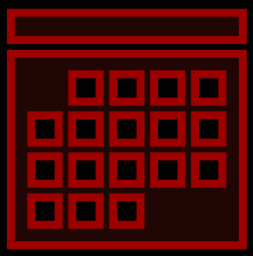
1. PlayBooks
2. Incidents
3. Events

Events Dashboards



Incident Dashboards

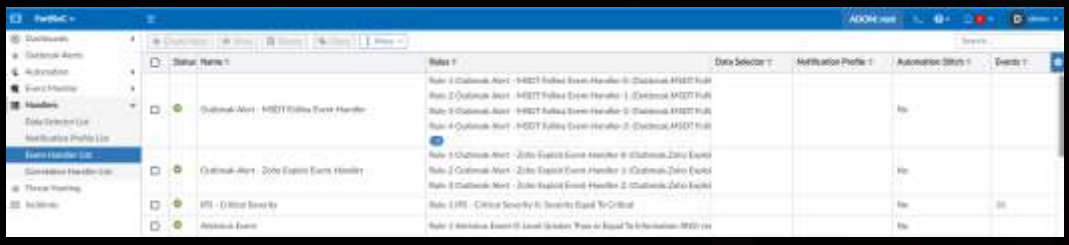
Events Generated



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



Matching Filters

Match Criteria

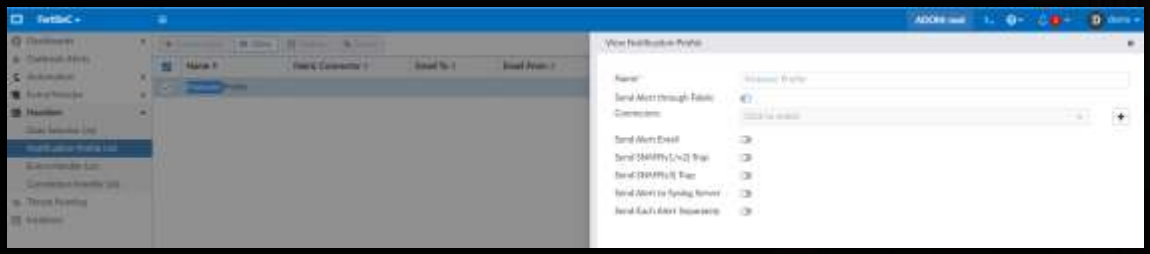
- Device (By name)
- Subnets
- Pre-Filters
- Device Type
- Log Type
- Log Match
- Log Field
- Generic

Can user 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

Event Notifications



Event Status

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

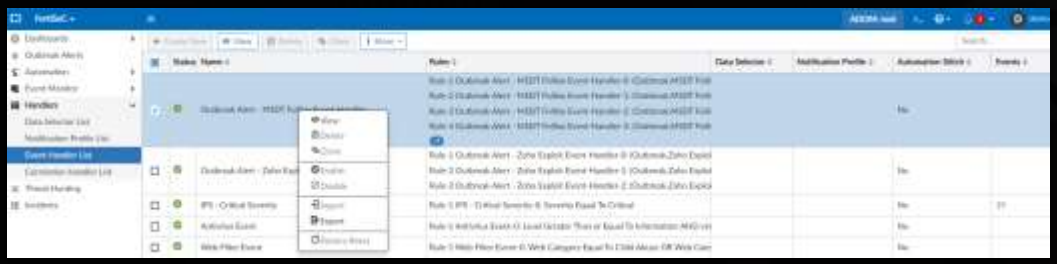
Exporting and Importing Event Handlers

Event handlers are configured per ADOM

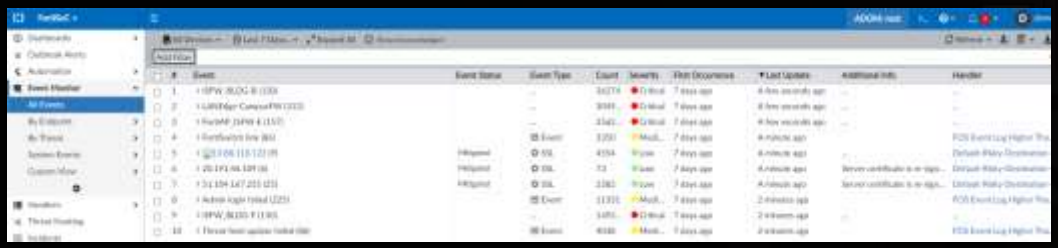
Can export from one ADOM to another

- If name conflict a time stamp will be added to the name

Use JSON format



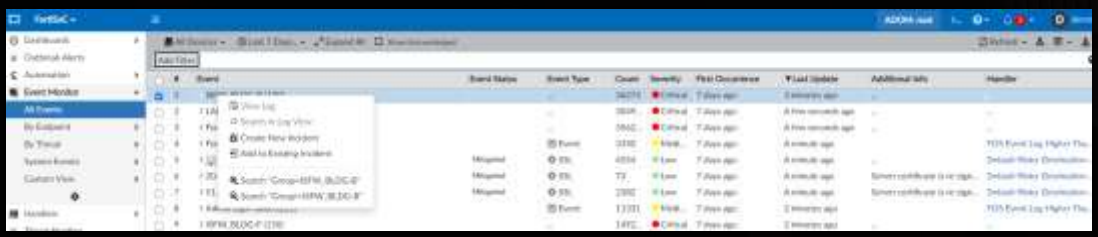
Managing Events



Creating an Incident

Created when an event needs further investigation

Can be created manually or automatically vis a playbook

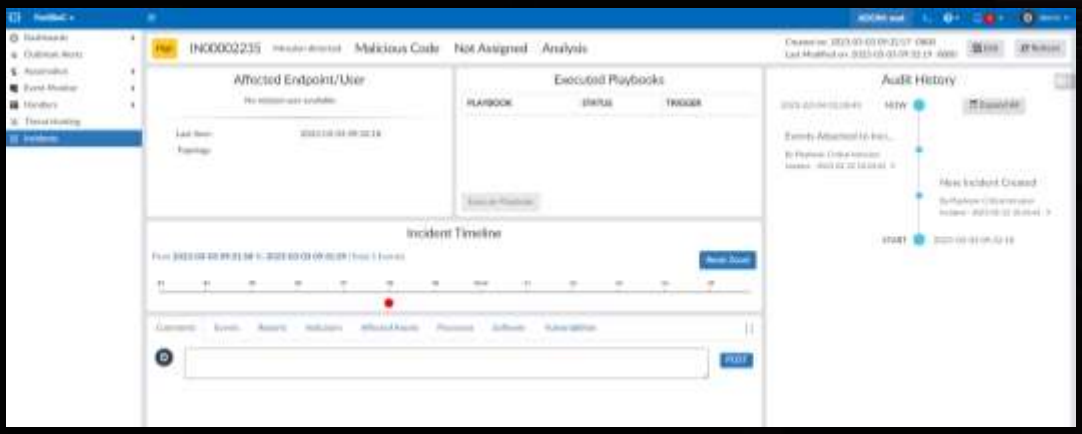


Creating an Incident

Created when an event needs further investigation

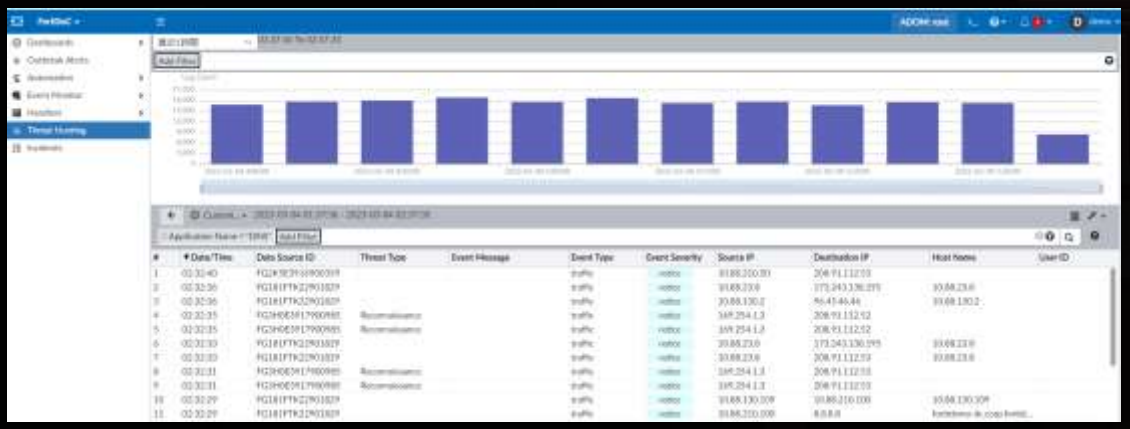
Can be created manually or automatically vis a playbook

Analyzing an Incident



Editing an Incident

Threat Hunting

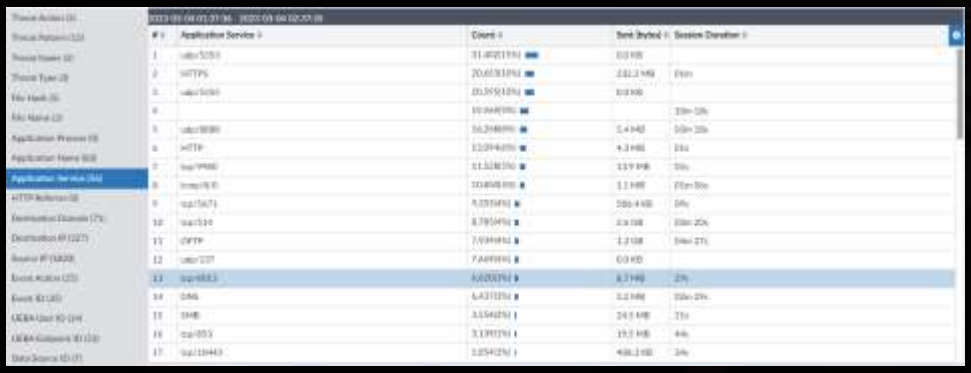


Log Count Chart

SIEM Log Analytics

Table contains may elements to gain insights in SOC

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



Outbreak Detection Service

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

Conclusions

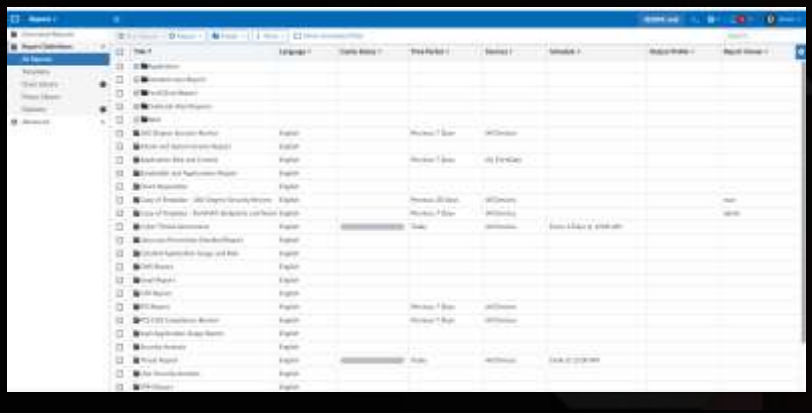
- Understand FortiSOC features
- Understand management extension applications
- Summarize FortiSOC dashboards information

Purpose of Reports

Summarize large amount of log data

FAZ retrieves information collected logs of managed devices

Quick and details analysis of activity



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 us displayed in

Dataset

Datasets are specific SQL `SELECT` queries

Format

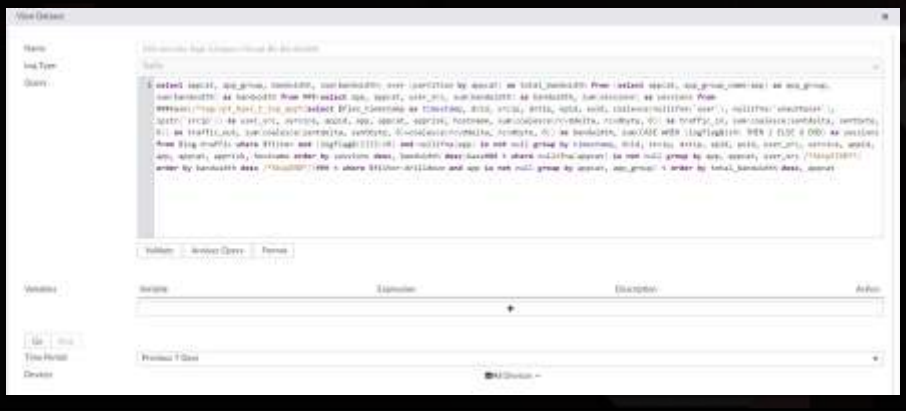
Pie Chart

Bar Chart

Table

How do Charts Extract Data

Datasets are SQL queries to the database
Data populates the chart
FAZ only uses the select SQL statement for reports
Read-Only statement retrieves data



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

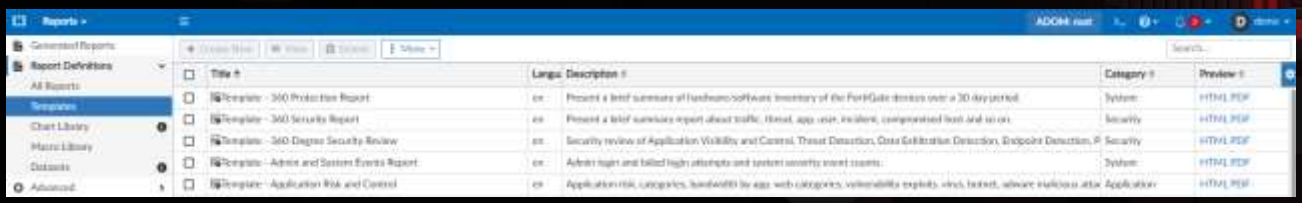
Additional reports the FortiNet devices are available when ADOMs available

- FortiAuthenticator
- FortiCarrier
- FortiClient
- FortiDDos
- FortiDeceptor
- FortiManager
- FortiMail
- FortiNAC
- FortiProxy
- FortiSandbox
- FortiWeb

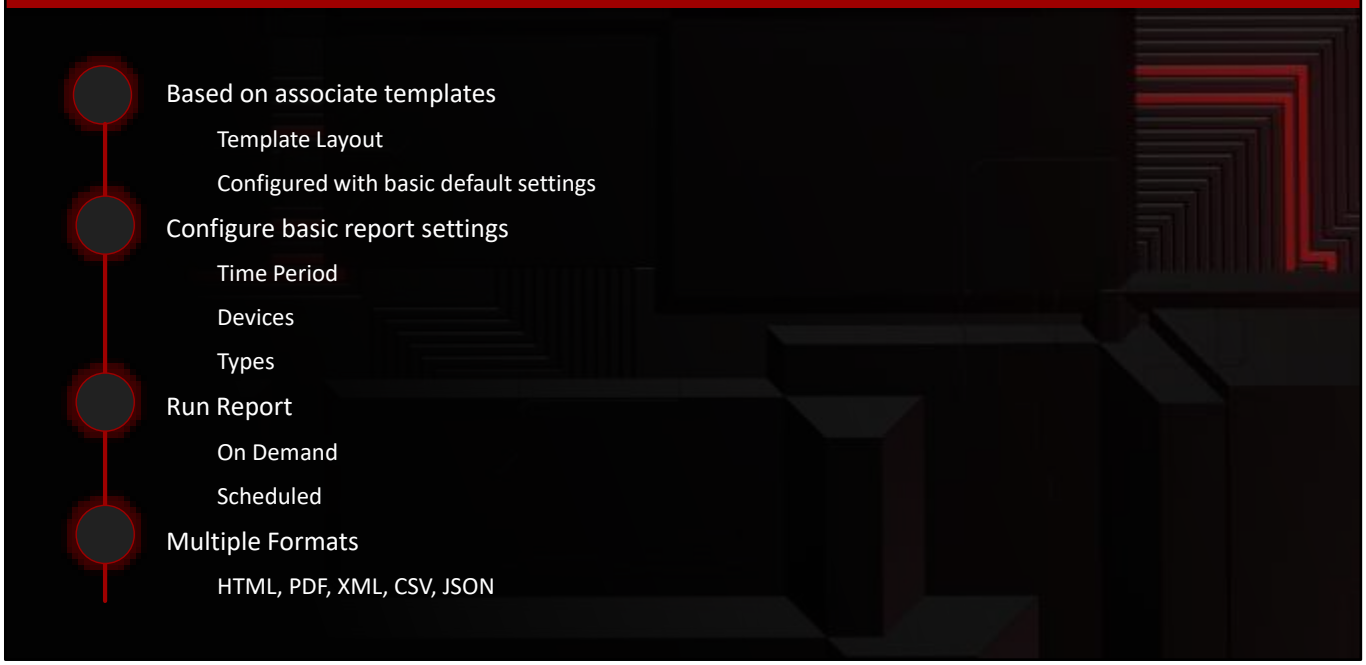
Report Considerations

- 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



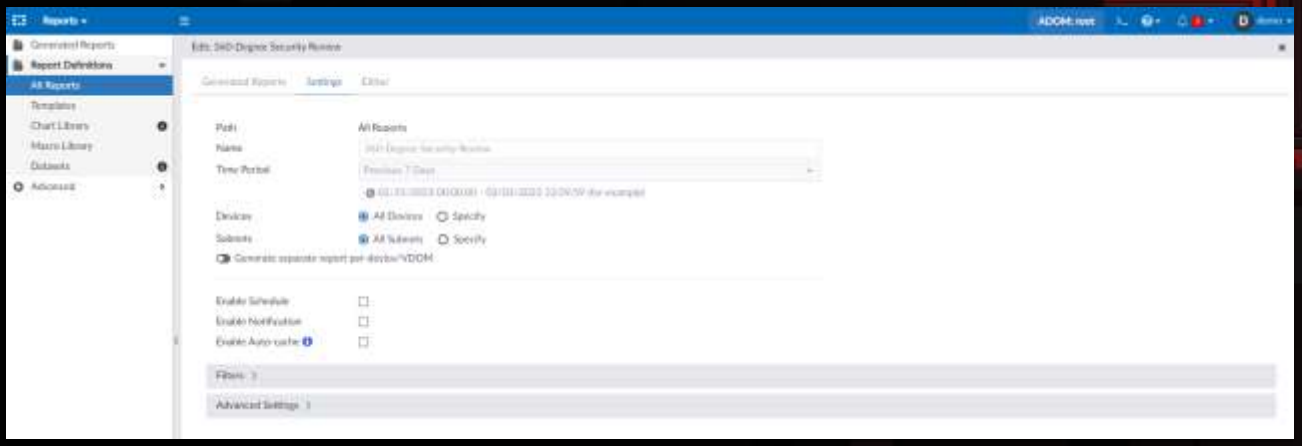
Running Predefined Reports



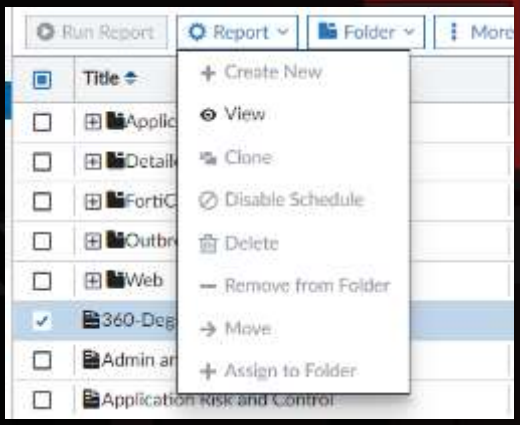
- Based on associate templates
  - Template Layout
  - Configured with basic default settings
- Configure basic report settings
  - Time Period
  - Devices
  - Types
- Run Report
  - On Demand
  - Scheduled
- Multiple Formats
  - HTML, PDF, XML, CSV, JSON

Running Predefined Reports

Fine-tuning Predefined Reports

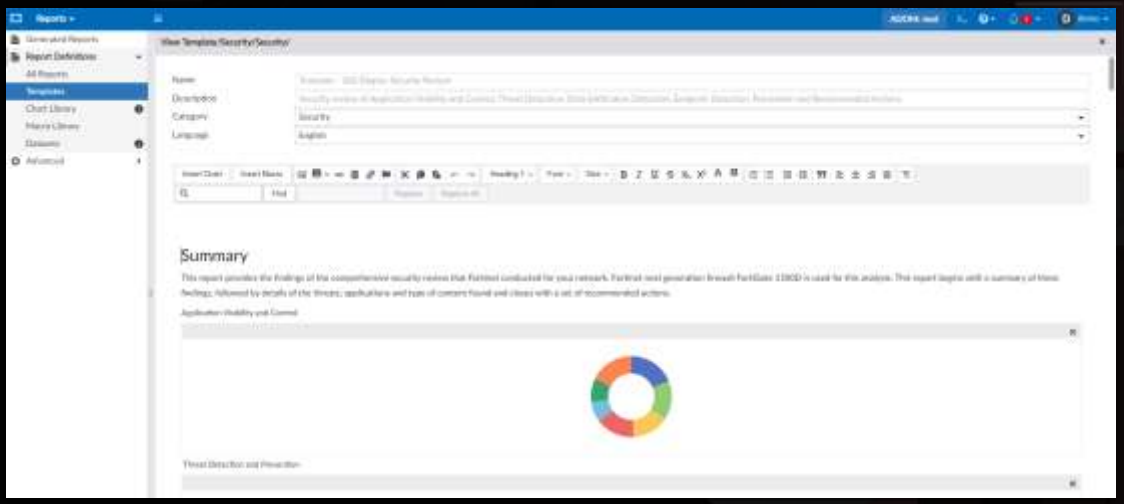


Customization Options

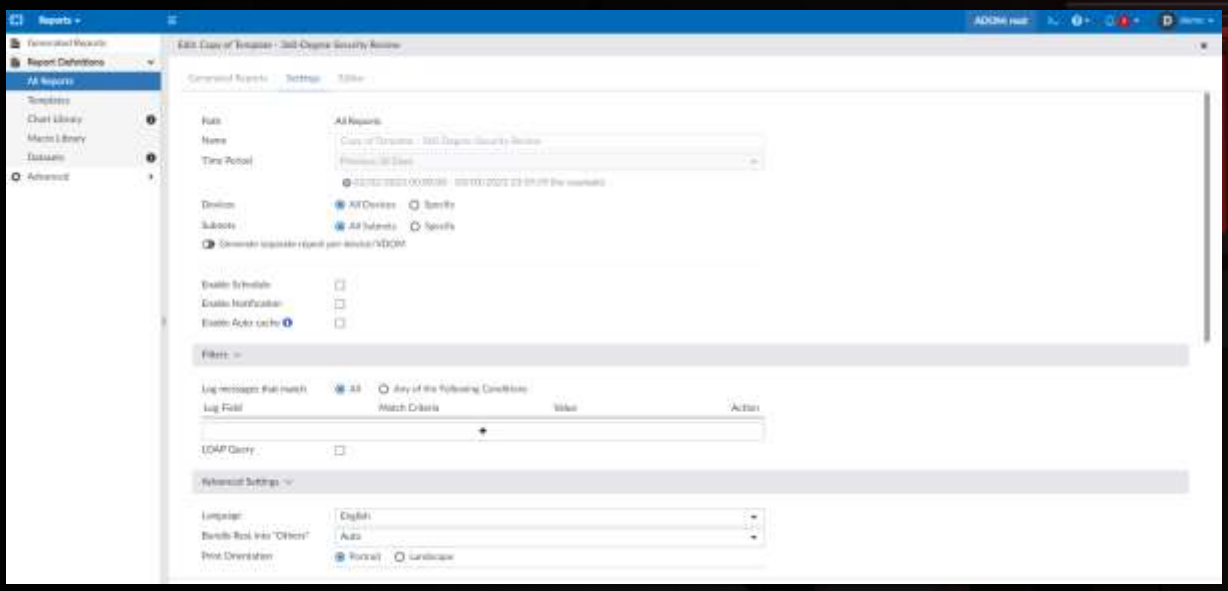


Customization: Template vs Report

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

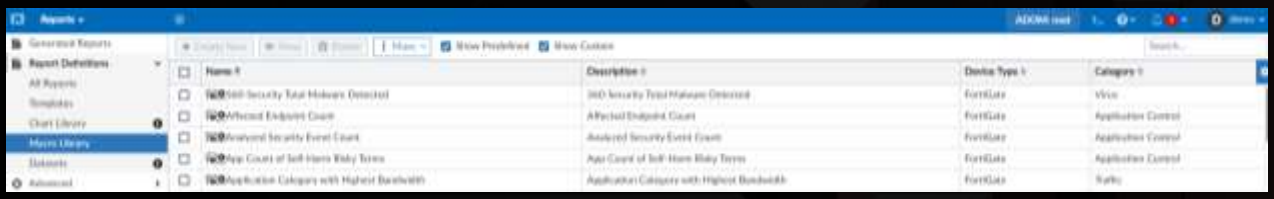
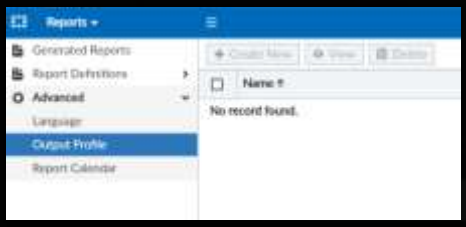


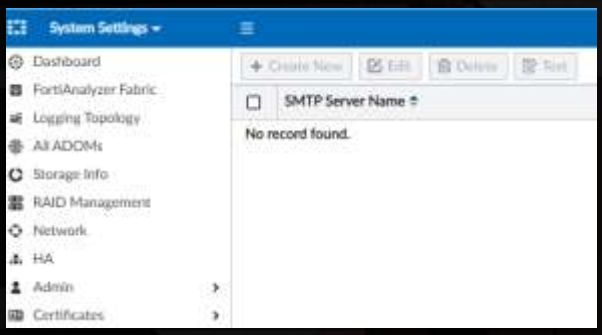
Chart / Dataset Requirements

- 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

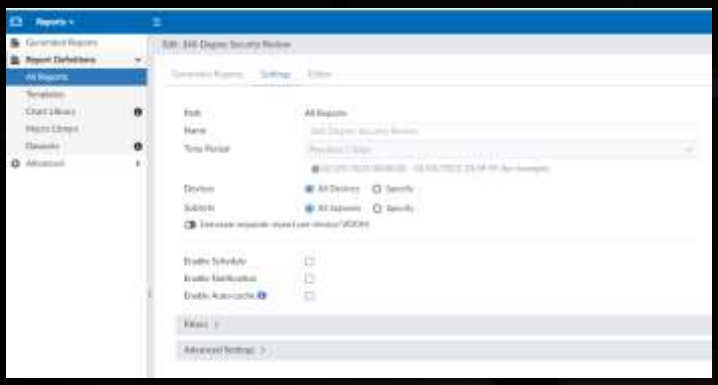
- Send or store reports for offline purposes
  - Configured per ADOM
- Email or upload to server – PDF HTML XML and CVS formats
- Must configure back-end configuration
  - Mail-Server
  - Output Profile





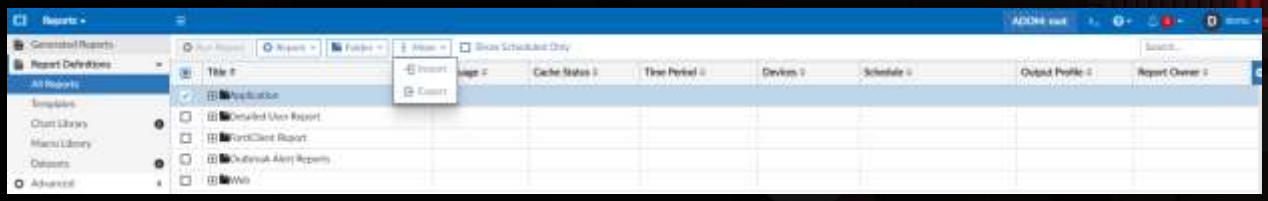
SQL Hard Cache

- 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

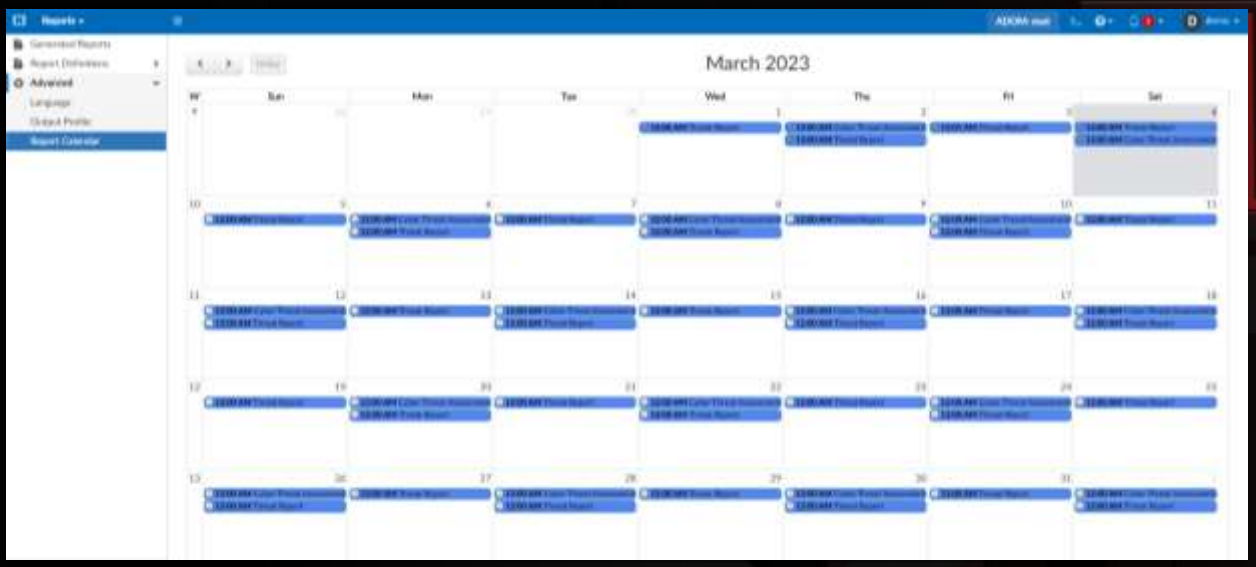
- Each ADOM has its own reports, libraries, and advanced settings



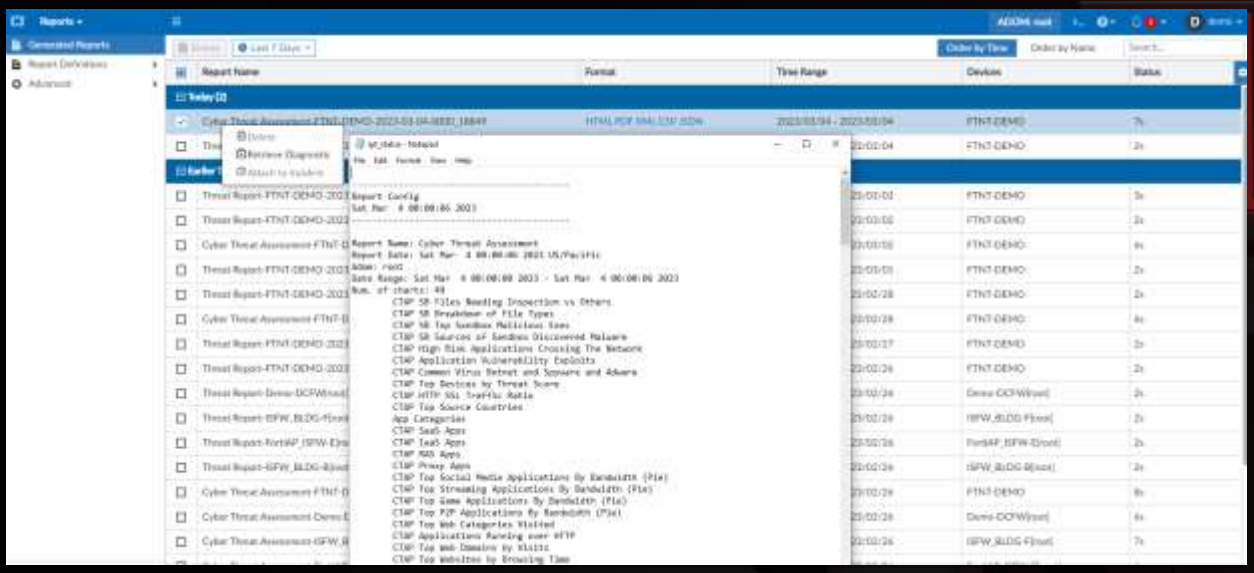
Attach Reports to Incidents

- 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

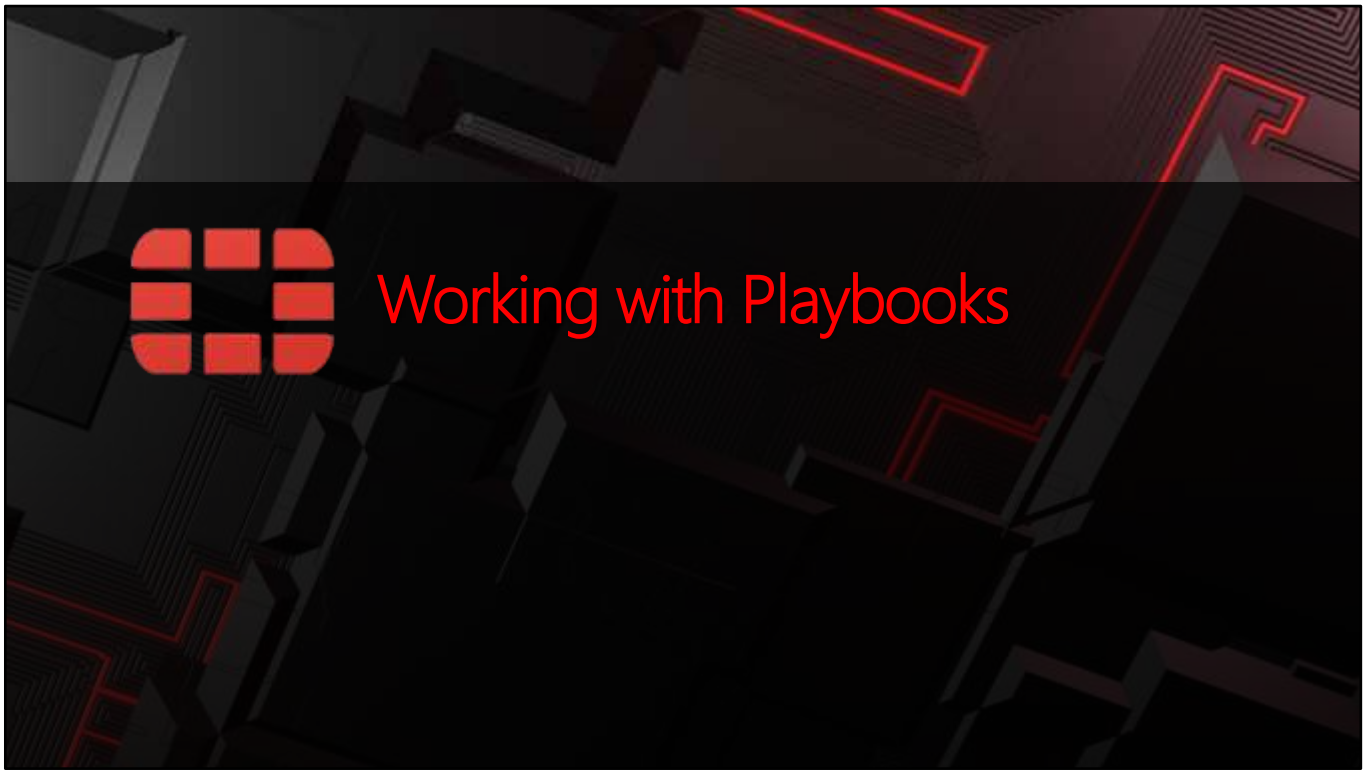


Report Troubleshooting CLI Commands

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

Conclusions

- Report Concepts
- Generating and Customizing Reports
- Customizing Charts and Datasets
- Managing Reports
- Troubleshooting Reports



Overview

- FAZ automation capabilities
- Playbook concepts
- Trigger Types and Characteristics
- Connector Types
- Playbook Tasks

Why Automation

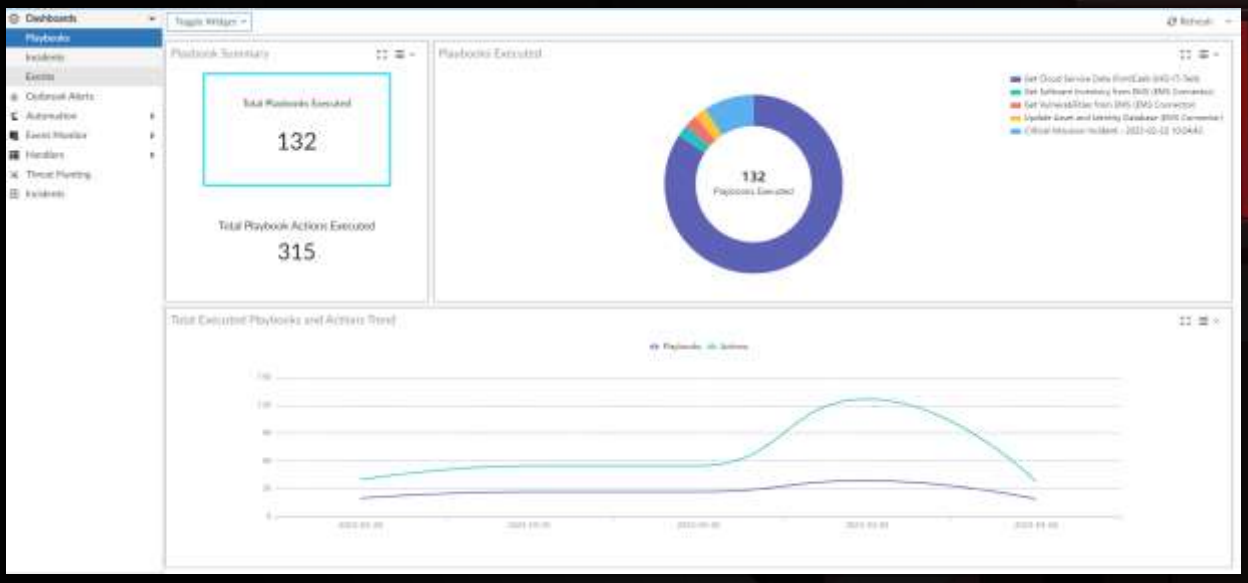
General Benefits

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

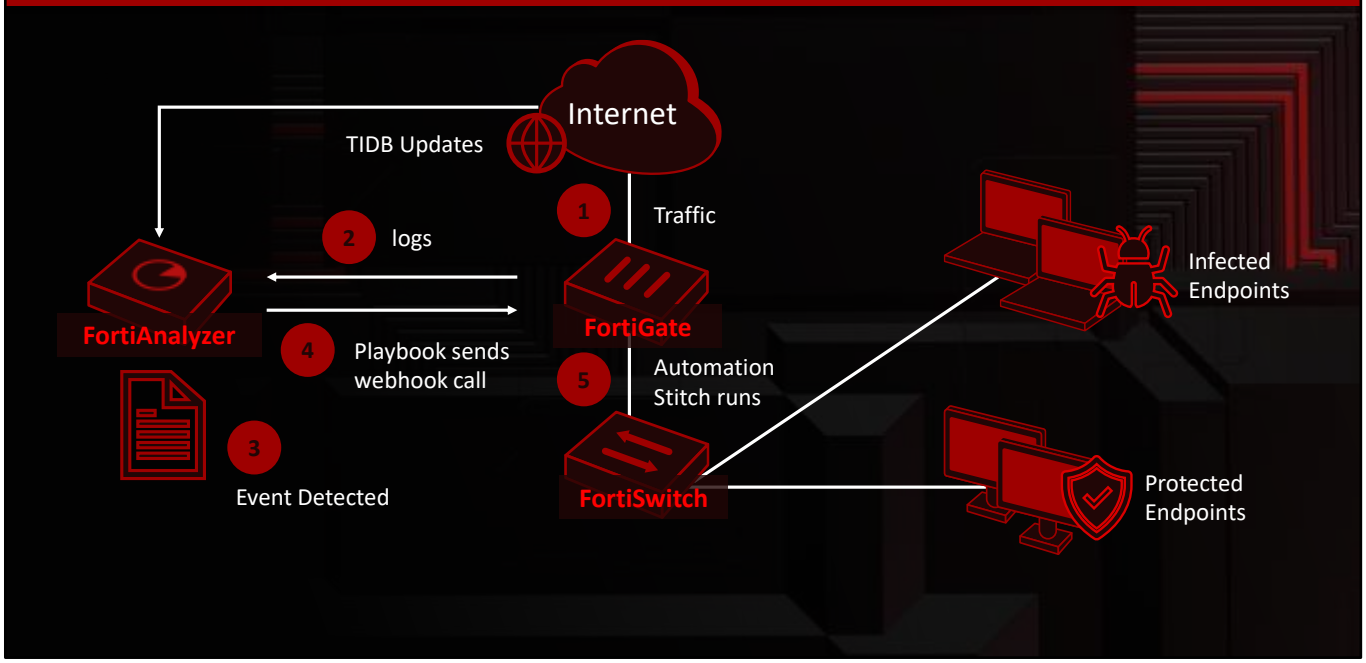
SOC Advantages

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

Why Automation



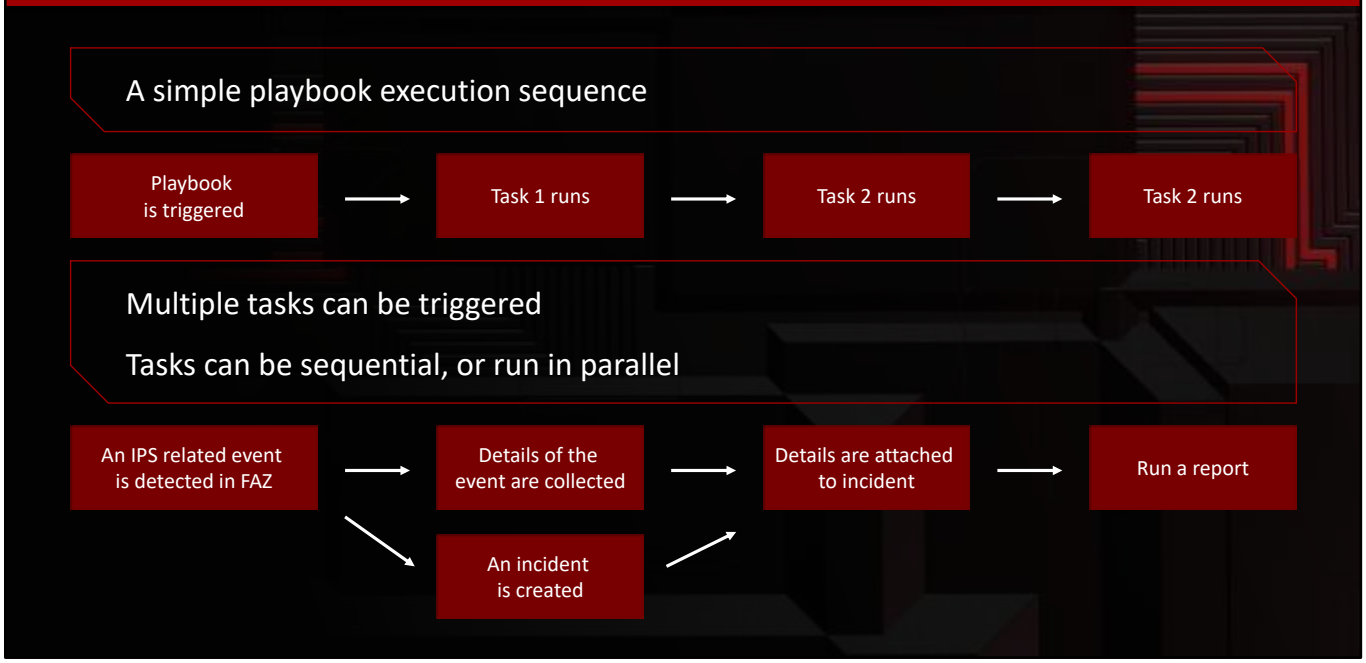
Example Automation



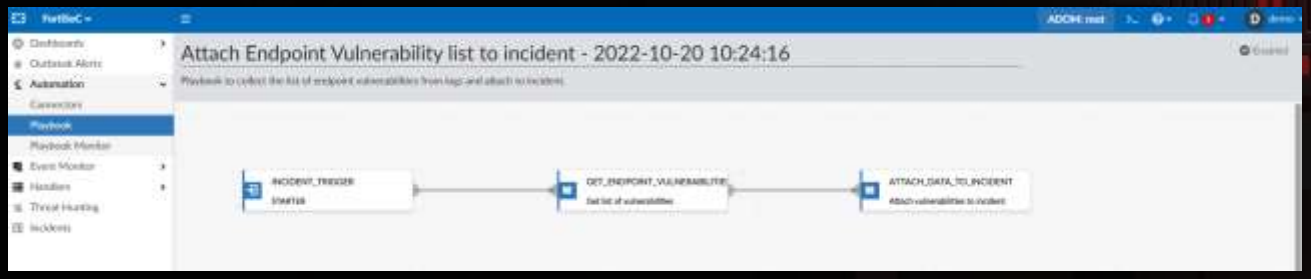
Playbook Concepts

- 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



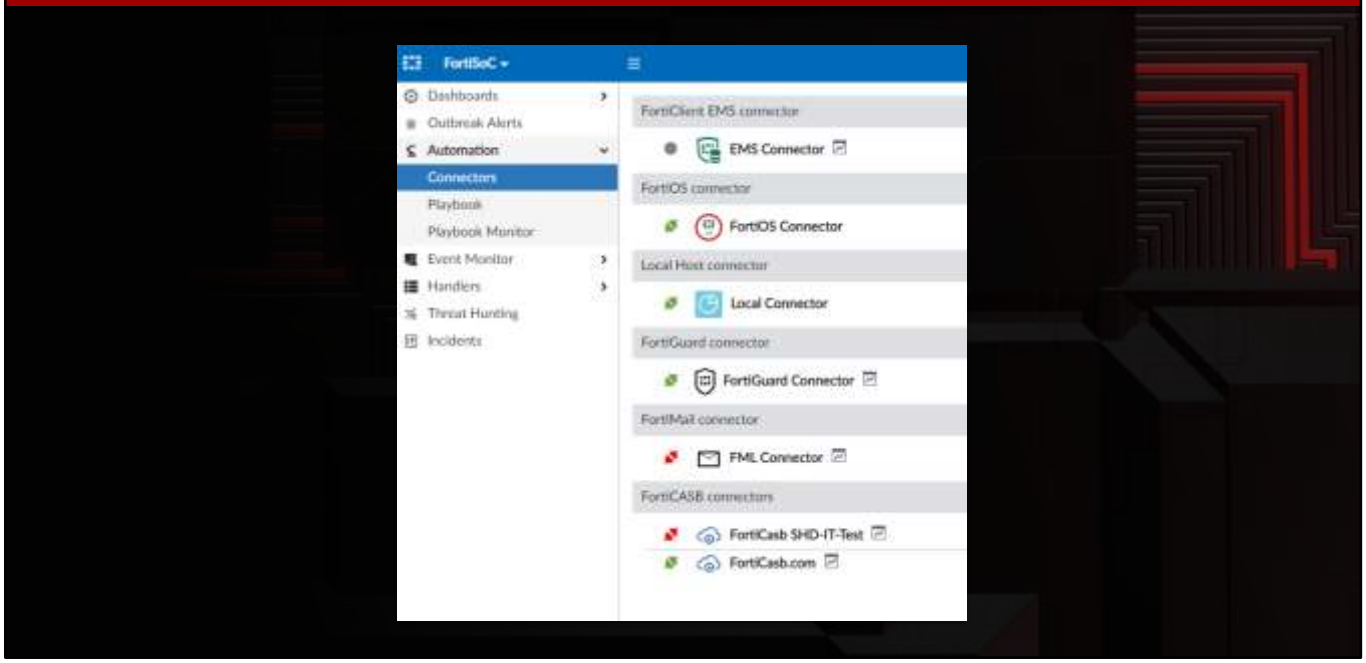
Playbook Concepts



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

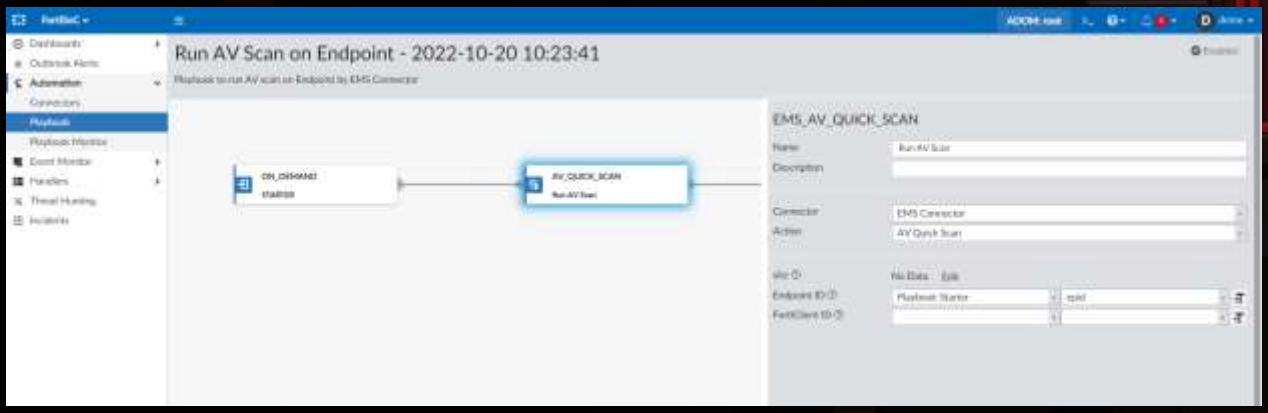
Tasks are actions that are executed when playbook runs

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



Using Variable in Tasks

Can use output variables and Trigger variables in playbook tasks

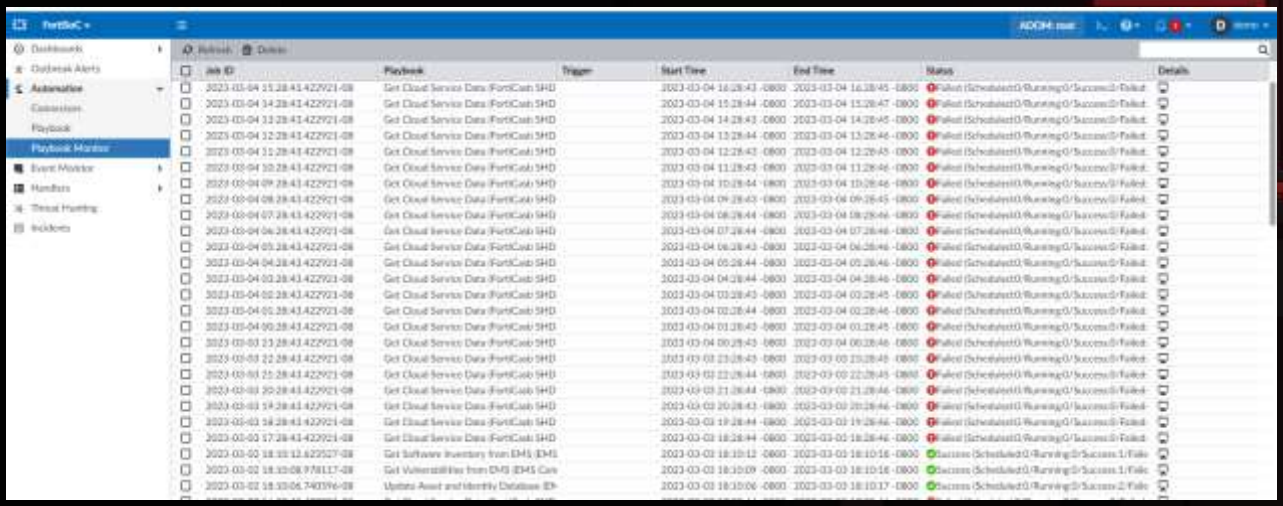
Output variables: Output of previous tasks is input of current tasks

- 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



Managing Playbooks

Managing Playbooks

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