

Security Operations Analyst

SOC Operations

Lesson Overview



Concepts, Definitions, and Incident Handling

Events, Event Handlers, and Incidents

Concepts, Definitions, and Incident Handling

Objectives

- Describe FortiAnalyzer SOC features
- Describe basic concepts and definitions related to FortiAnalyzer SOC features
- Analyze *NIST SP 800-61 Computer Security Incident Handling Guide*

FortiAnalyzer SOC Features

Incident Management



- Incident/case management
- Indicators attachment for incidents
- API to FortiSOAR for escalation

Automation



- Playbook templates and automation
- Connectors for playbooks
- Visual playbook editor
- Playbook execution
- Playbook monitor

Analytics



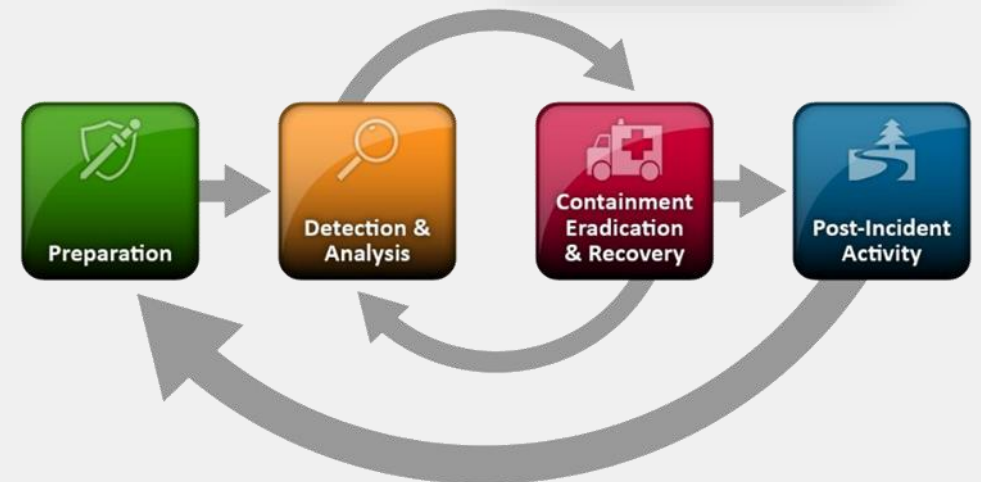
- Monitor and view log data with context of network activity
- Security Fabric analytics for devices within a Fabric ADOM

Concepts and Definitions

Concept	Definition
Security information and event management (SIEM)	Fabric (SIEM) logs are a licensed feature that enables the FortiAnalyzer SIEM capabilities to parse, normalize, and correlate logs from Fortinet products, as well as security event logs of Windows and Linux hosts (with Fabric Agent integration).
Indicators of compromise (IOC)	The IOC service on FortiAnalyzer downloads the threat database from FortiGuard. The FortiGuard threat database contains the blocklist and suspicious list. IOC detects suspicious events and potentially compromised network traffic using sophisticated algorithms on the threat database.
Security event	A record of an observed occurrence on a monitored information system. If an event is relevant from an information security perspective, it can be considered a security event. On FortiAnalyzer, events are generated using event handlers. Also, a Windows audit log entry indicating a successful user login can be considered a security event.
Security incident	An event that indicates a malicious or abnormal occurrence. On FortiAnalyzer, incidents are escalated from events.
Indicator enrichment	Querying threat intelligence sources about an indicator to obtain security context information. A form of enrichment that is frequently used is checking the reputation of an indicator. For example, you can verify if a given file hash is associated with known malware.

NIST SP 800-61 Incident Handling—Overview

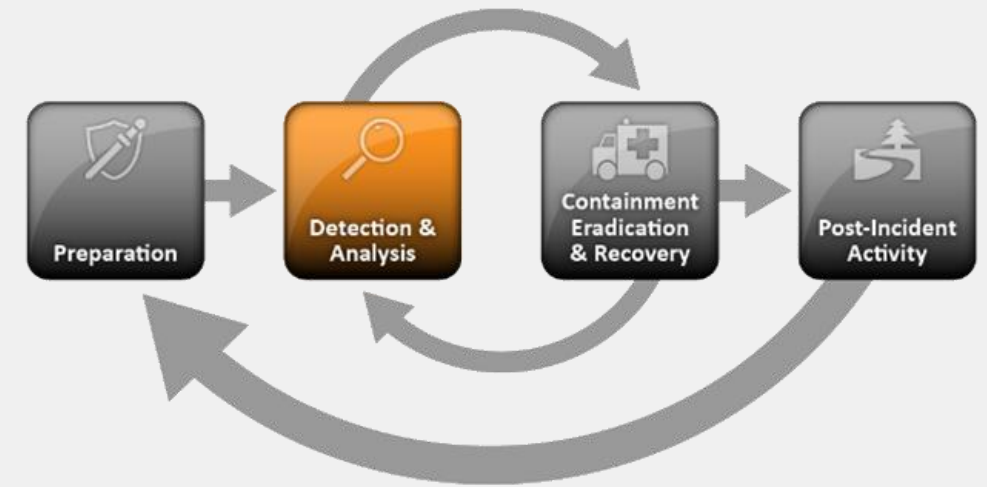
- Defines incident handling as a lifecycle with four phases
- Assists in
 - Establishing computer security incident response capabilities
 - Handling incidents efficiently and effectively
- Focuses on
 - Analyzing incident-related data
 - Determining appropriate response
- Agnostic and broad approach
 - Can be followed independently of particular hardware, OS, protocols, or applications
 - Recommended practices for handling any type of incident



The content of this slide is based on copyright material from the National Institute of Standards and Technology (NIST) available online at <https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final>.

NIST SP 800-61 Incident Handling—Detection and Analysis

- Prepare to handle any incident but focus on those that use common attack vectors, such as external and removable media, web, and email
- Signs of an incident
 - Precursors (relatively rare)—indicate an incident may occur in the future
 - Indicators (common)—indicate an incident may have occurred or may be occurring now
- Common sources of precursors and indicators
 - Intrusion detection and prevention systems (IDPSs)
 - Security information and event management (SIEM)
 - Antimalware and antispam
 - OS-level monitoring (file integrity, processes, and so on)
 - Logs (OS, services, applications, and network devices)
 - Network flows



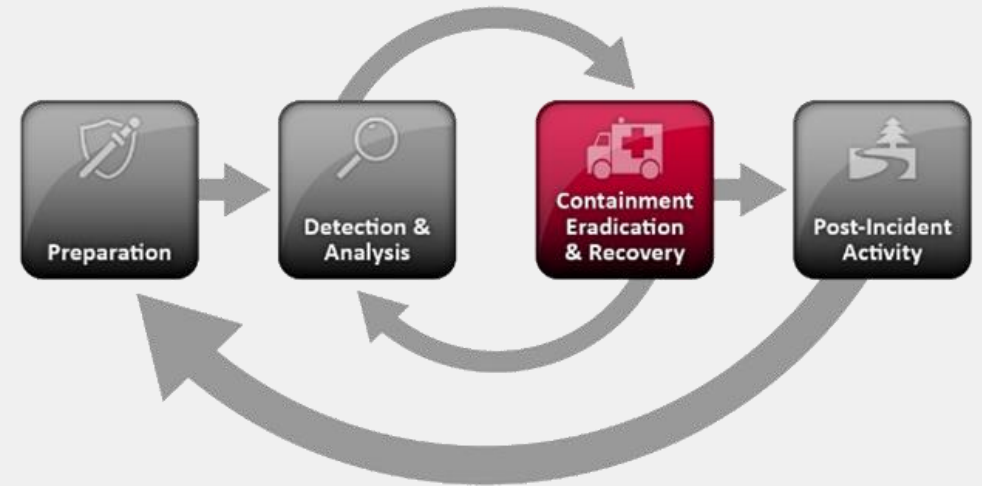
The content of this slide is based on copyright material from NIST available online at <https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final>.

NIST SP 800-61 Computer Security Incident Handling— Containment, Eradication and Recovery

- Containment
 - Often required and should be considered early
 - Decision-making is an essential part
 - Strategies vary per incident
- Eradication and Recovery
 - Identify affected resources, attacking resources, and communication channels
 - Eliminate components of the incident (delete malware, disable compromised accounts, remove persistence, and so on)
 - Restore systems to normal operations
 - Confirm systems are working normally
 - Remediate vulnerabilities (if applicable)

Recovery may involve actions, such as:

- Restore systems from clean backups and snapshots
- Rebuild systems from scratch
- Replace compromised files with clean and reliable versions
- Install patches
- Change passwords



The content of this slide is based on copyright material from NIST available online at <https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final>.

Knowledge Check

1. Which part of containment, eradication, and recovery does quarantining an infected host fall under?

- ✓ A. Containment
- B. Eradication
- C. Recovery

2. On FortiAnalyzer, what is an incident?

- A. A record of an observed occurrence on a monitored system
- ✓ B. A security event that has been escalated

Lesson Overview



Concepts, Definitions, and Incident Handling

Events, Event Handlers, and Incidents



Events, Incidents, and Handlers



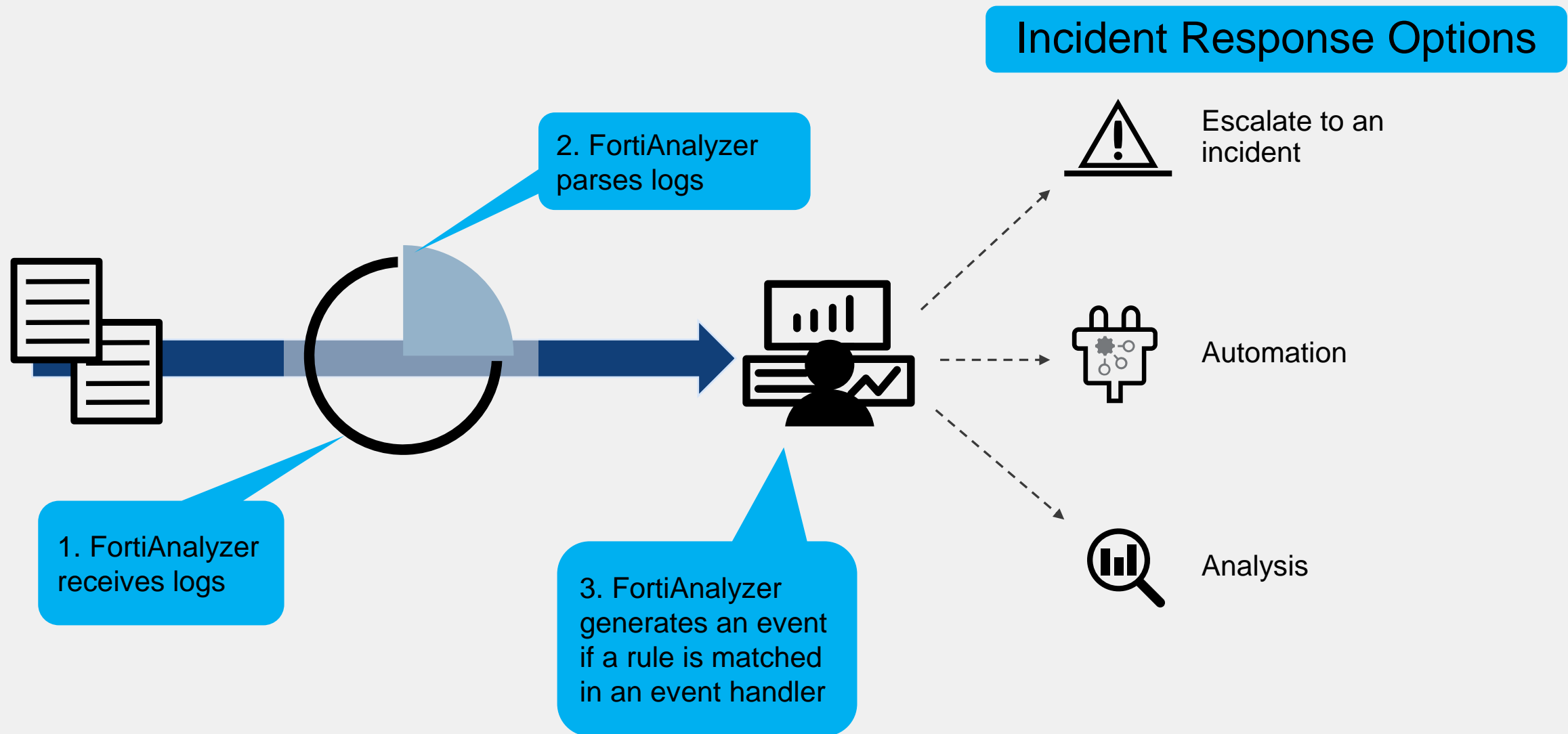
Objectives

- Analyze and manage events and event handlers
- Customize event handlers
- Analyze and create incidents

Events and Event Handlers

- Events are generated by event handlers
- FortiAnalyzer is preconfigured with many event handlers
- You can create custom event handlers to generate events
- FortiAnalyzer filters all incoming logs using event handlers
- If logs match the conditions configured in an event handler, FortiAnalyzer generates an event
- All the events that are generated can be viewed on the **Events Monitor** page





How Are Events Generated?



Managing Event Handlers

- Event handlers look for specific conditions in logs
- Enable or disable event handlers as needed
- Disabled handlers do *not* generate events

Incidents & Events > Handlers

<div><div>+ Create New</div><div>Edit</div><div>Delete</div><div>Clone</div><div>More</div></div> <div>Search...</div>					
<input type="checkbox"/>	Status	Name	Rules	Events	MITRE Tech ID
<input type="checkbox"/>		Default-Windows-Registry-Modification-Block...	Rule-1 Windows Registry or File Modification Blocked		T1112
<input type="checkbox"/>		Default-Web-Server-URL-Scanning-Detected	Rule-1 Web Server Scanning: (Default,Reconnaissance		T1595.003
<input type="checkbox"/>		Default-Risky-Destination-Detection-By-Threat	Rule-1 Web request to malicious destination detected Rule-2 Web request to malicious destination blocked: Rule-3 DNS request to malicious destination detected Rule-4 DNS request to malicious destination blocked: <div>+11</div>	33	T1102,T1071.001,T1071.004,T1021.00
<input type="checkbox"/>		Default-Risky-Destination-Detection-By-Endpoi...	Rule-1 Web request to malicious destination blocked: Rule-2 Web request to malicious destination detected Rule-3 Web request to suspicious destination detecte Rule-4 DNS request to malicious destination detected <div>+10</div>	7	T1102,T1071.001,T1071.004,T1021

Disabled handlers don't generate events

Enable only the event handlers you need

This handler has 15 rules and has generated 33 events

Event Handlers—Configuration

- The configuration for each event handler can include:

- MITRE attributes
- Data selectors (exclusion filters)
- Automation stitches
- Notifications
- Rules

Set MITRE ATT&CK domain and technique ID(s) the event handler provides coverage for

- Rules are granular conditions

- Event handlers can have one or more rules
- Basic event handlers use OR logic
- Correlation event handlers have many operator logic options

Get notified when an event handler is triggered

Incidents & Events > Handlers > Basic Handlers

The screenshot displays the configuration page for a 'SOC SMTP Enumeration Data Handler'. The 'MITRE Tech ID' field is active, showing a search bar and a list of selected techniques: 'T1589 Gather Victim Identity Information' and 'T1589.002 Email Addresses'. The 'Rules' section shows 'SOC Antispam Rule 1' is enabled. The 'Notifications' field is set to 'SOC SMTP Enumeration Alert'.

Selected 2 (Total: 716)
<input type="checkbox"/> Enterprise Domain
<input type="checkbox"/> Reconnaissance
<input checked="" type="checkbox"/> T1589 Gather Victim Identity Information
<input type="checkbox"/> T1589.001 Credentials
<input checked="" type="checkbox"/> T1589.002 Email Addresses
<input type="checkbox"/> T1589.003 Employee Names
<input type="checkbox"/> T1590 Gather Victim Network Information
<input type="checkbox"/> T1590.001 Domain Properties

Event Handlers—Rule Configuration

- Rules have many customizable fields
 - Not every field is required

Note: The fields available in the rules depend on the **Log Device Type** value

Incidents & Events > Handlers > Basic Handlers

Status	<input checked="" type="checkbox"/>		
Name	Antispam Rule 1		
Event Severity	High		
Choose Your Logs			
Start by selecting the device and log type that you want to monitor for events.			
Log Device Type	FortiMail		
Log Type	Anti-Spam Log (spam)		
The system will categorize logs into smaller groups based on the chosen log fields.			
Log Field <i>i</i>	Device Name (devname)	From (from)	Device ID (device_id)
Log Filters	All Filters Any One of the Filters		
	Log Field	Match Criteria	Value
			Action
		+	
Log Filter by Text <i>i</i>	type==spam		

Supports most Fortinet products and third-party devices through syslog

Use the generic text filter to search using wildcard expressions or regular expressions

Event Handlers—Rule Configuration (Contd)

- Define the condition that triggers an event
- There are three options:
 - Count: A minimum threshold count of matching logs
 - Log field value: Within a group, the log field <log field> has <integer> or more unique values
 - Sum: Multiple options such as duration, sent/received bytes, and sent/received packets
- Additionally, configure the following in relation to your selection:
 - Time: All logs were generated within <integer> minutes

Incidents & Events > Handlers > Basic Handlers

Trigger an event when:

☒ A group contains or more log occurrences

☐ Within a group, the log field has or more unique values ↺

☐ The sum of is greater than or equal to

All logs were generated within minutes

Advanced Settings ▾

Event Type Override

Event Message ⓘ

Event Status

☒ Allow FortiAnalyzer to choose

Tags

Indicators

Log Field	Indicator Type	Count	Action
<div>+</div>			

Additional Info

☐ Use system default

☒ Use custom message ⓘ

Used for data exfiltration and is only for log device type **Fabric**

Event Handlers—Data Selectors

- Data selectors help narrow down events generated by devices, subnets, and filters:
 - Devices (by name)
 - Subnets (created in Fabric View)
 - Filters (OR logic)
- Filters are granular conditions within data selectors:
 - Log device type
 - Log type/subtype
 - Matching logic (AND/OR logic)
 - Generic text filter (for more precise filtering)

Incidents & Events > Handlers > Data Selectors

Edit Data Selector

Name* SOC SMTP Enumeration Data Selector

Devices **All Devices** Specify Local Device

Subnets **All Subnets** Specify

Filters **Any of the following conditions**

SMTP Enumeration [x] [+]

SMTP Enumeration

Name SMTP Enumeration

Log Device Type FortiMail

Log Type Anti-Spam Log (spam)

Logs match **All** **Any of the following conditions**

Log Field	Match Criteria	Value	Action
Subject (subject)	Equal To	Urgent!	[x] [+]

Generic Text Filter

Event Status

- Events can be set to one of four statuses

Incidents & Events > Event Monitor

10.0.3.20 (115)	Unhandled
Compromised host detected	Unhandled
Web request to Unrated detected	Unhandled
Web request to Malicious Websites blocked	Mitigated
Compromised host detected	Unhandled
Compromised host detected	Unhandled
Web request to Malicious Websites blocked	Mitigated

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

Note: You can configure the desired event status manually in the handler settings, or let FortiAnalyzer choose it automatically

Event Handlers—Generic Text Filters

- Generic text filters allow more precise and flexible control over which logs trigger an event
 - Multiple operators and logic are supported
- Supported operators:

Operator	Meaning
==	Equal (exact match)
!=	Not equal (not matching)
<	Smaller than
<=	Smaller than or equal to
>	Greater than
>=	Greater than or equal to
~	Contains the regular expression
!~	Does not contain the regular expression

Tokens: '(', ')', '&', '|', 'and', 'or', 'not'

Generic text format:

- Tokens: '(', ')', '&', '|', 'and', 'or'
- Operators: '==', '!=', '<', '<=', '>', '>=', '~', '!~'

Examples:

```
dstip==192.168.1.168 and hostname ~ "facebook" dstip==192.168.1.168 and ( dstport == 514 or dstport == 515 )
```

Log Filter by Text











Hover over this icon to see the tooltip in the GUI

Tip: Identify the logs that you want to generate events for, and from the raw view, copy the strings you want to match

Managing Events

- **Event Monitor** displays events generated by the configured event handlers

Incidents & Events > Event Monitor

All Events		By Endpoint	By Threat	System Events	Toggle Views				
 All Devices		 Last 5 Minutes		<input type="checkbox"/> Show Acknowledged		 Expand All			
Search or type filters...									
<input type="checkbox"/>	Event	Event Status	Event Type	Count	Severity	First Occurrence	Last Update	Additional Info	Handler
<input type="checkbox"/>	 FortiMail (1)	Unhandled	 Email Filter	11	 Critical	a minute ago	a minute ago	Malware:\$(mname) with se	SMTP Enumeration Data Handler
<input type="checkbox"/>	FortiMail Detected Spam from email@mail.com	Unhandled	 Email Filter	11	 Critical	2024-03-05 16:22:57	2024-03-05 16:23:07	Malware:\$(mname) with se	SMTP Enumeration Data Handler

Critical severity and marked as unhandled
Double-click to see the originating log

This is a snippet of **Log View** of correlated logs with the event

This is the event handler that generated this event

Note: If you are receiving unexpected events, check that the handler is configured correctly

View Correlated Logs									
Search or type filters...									
#	Date/Time	Device ID	Session ID	Client Name	Destination IP	From	To	Subject	Message
1	16:22:57	FEVMSLTM22000111	4260MsDw006655-4260MsDx00665		10.200.200.100	email@mail.com	2002@acmecorp.net		<2002@acmecorp.net>... User unknown

Available Management Actions for Events

- You can acknowledge an event, add a comment, assign it to an administrator, or create an incident from it

Incidents & Events > Event Monitor

All Events | By Endpoint | By Threat | System Events | Toggle Views

All Devices All ☐ Show Acknowledged Expand All

Search or type filters...

Event	Event Status	Event Type	Count	Severity	First C
198.50.152.88 (2)	Unhandled	Traffic	2	Critical	a day
Traffic to C&C from 10.0.3.20 detected	Unhandled	Traffic			2023-
Traffic to C&C from 10.0.1.200 detected	Unhandled	Traffic			2023-0
192.169.69.25 (2)	Unhandled	Traffic			a day
178.162.203.226 (2)	Unhandled	Traffic			day
66.45.245.150 (2)	Unhandled	Traffic			2 da
178.162.217.107 (4)	Unhandled	Traffic			2 da
5.79.71.205 (4)	Unhandled	Traffic			
193.166.255.171 (2)	Unhandled	Traffic			2 days ago

Right-click an event to see the list of available actions

Acknowledged events are not shown by default

Create incidents from events that require further investigation

Filter based on the column values to display events of interest only

- Acknowledge
- Comment
- Assign To
- View Log
- Search in Log View
- Create New Incident
- Add to Existing Incident
- Filter by Event Type = Traffic
- Filter by Event Type != Traffic

Creating an Incident

- Create an incident when an event needs further analysis
- Can create manually or automatically (playbooks)

Incidents & Events > Event Monitor

<input type="checkbox"/>	WIN-CLIENT (4)	Unhandled
<input checked="" type="checkbox"/>	IP scanning on Port: 443 detected	Unhandled
<input type="checkbox"/>	IP scanning on	
<input type="checkbox"/>	IP scanning on	
<input type="checkbox"/>	IP scanning on	
<input type="checkbox"/>	Delete report (1)	
<input type="checkbox"/>	desc:Delete rep	
<input type="checkbox"/>	WIN-AD (3)	
<input type="checkbox"/>	IP scanning on	
<input type="checkbox"/>	IP scanning on	

☒ Acknowledge
☒ Comment
☐ Assign To
☐ View Logs
☐ Search in Log View
☒ Create New Incident
☐ Add to Existing Incident
 Search

Create New Incident

Incident Category

Scans/Probes/Attempted Access

MITRE Tech ID

T1590 Gather Victim Network Information ☒

T1595.001 Scanning IP Blocks ☒

2 entries selected

Severity

Medium

Status

New

Affected Endpoint

10.200.3.219 (WIN-CLIENT)

Description

Default-Recon-Activity-By-Endpoint happened at WIN-CLIENT

Assigned To

admin (Super_User)

Must create accounts for party responsible for handling incidents

Incidents & Events > Incidents

<input type="checkbox"/>	Incident Number ▾	Incident Date / Time ▾	Incident Reporter ▾	Incident Category ▾	Severity ▾	Status ▾	Affected Endpoint ▾
<input type="checkbox"/>	IN00000012	2024-08-13 15:15:22	admin	Scans / Probes / Attempted	Medium	New	10.200.3.219 (WIN-CLIENT)

Analyzing an Incident

Incidents & Events > Incidents

Incident #, description, category, assignee, and incident status

<

Medium

IN00000012

Default-Recon-Activity-By-Endpoint happened at WIN-CLIENT

Scans / Probes / Attempted Access

Assigned to:admin

New


Created on: 2024-08-13 15:15:22 -0700

Last Modified on: 2024-08-13 15:15:23 -0700

Edit

Refresh

Affected Endpoint/User



bob

Last Seen

2024-08-13 15:15:23

Topology

WIN-CLIENT

Addresses

MAC: 00:0c:29:eb:74:13

IP: 10.200.3.219

Executed Playbooks

Playbook	Status	Trigger
<div>Execute Playbook</div>		

Audit History

2024-08-13 15:17:...

Now

Expand All

Events Attached to I...

By: admin

>

New Incident Created

By: admin

>

Start

2024-08-13 15:15:23

Incident Timeline

From 2024-06-12 14:26:10 To 2024-06-12 14:27:55 (Total 1 Event)

Reset Zoom

14:00

14:05

14:10

14:15

14:20

14:25

14:30

14:35

14:40

14:45

14:50

14:55

15:00

15:05

15:10

15:15

15:20

15:25

14:26:10

Comments

Events

Reports

Indicators

Affected Assets

Processes



Software

Vulnerabilities

Delete

Search in Log View

Search...

<input type="checkbox"/>	#	Event	Event Status	Event Type	Count	Severity	First Occurrence	
<input type="checkbox"/>		 IP scanning on Port: 443 detected	Unhandled	 Traffic	414	Medium	2024-06-12 13:48:35	202

Important details to help you investigate the threat, with the option to add or delete entries

Editing an Incident

- Update each incident setting while working in it
- Close any solved incident
- Once closed, you can delete the incident from the list
- Notifications can be configured for each status change

Note: You should update incident details according to the progress of the investigation. Every incident should reach the **Closed** status.

Incidents & Events > Incidents

Edit Incident

Incident Number: IN00000012

Incident Date / Time: 2024-08-13 15:15:22

Incident Category: Scans/Probes/Attempted Access

MITRE Tech ID: T1590 Gather Victim Network Information, T1595.001 Scanning IP Blocks (2 entries selected)

Severity: Medium

Status: New

Affected Endpoint:

Description:

Assigned To:

Keep the incident status up to date



Configure Incidents Settings

Incidents & Events > Incidents

+ Create New	Edit	Delete All	Analysis	Settings	All ▾
<input type="checkbox"/>	Incident Number ▾	Incident Date / Time ▾	Last Update	Date / Time ▾	
<input type="checkbox"/>	IN00000007	2023-09-07 10:53:35	2023-09-07	10:56:54	
<input type="checkbox"/>	IN00000006	2023-09-07 10:48:10	2023-09-07	10:48:11	

Notifications


[+ Create New](#)

Fabric Connector 1  MS_Teams_Connect ▾ 

☒ Send notification when an incident is created ⓘ

☒ Send notification when an incident is updated

☒ Send notification when an incident is deleted


Fabric Connector 2  ServiceNow_Connect ▾

☐ Send notification when an incident is created ⓘ

☒ Send notification when an incident is updated

☐ Send notification when an incident is deleted

First create the connectors in **Fabric View**

 FAZ_Notification 1:23 PM

```
fortianalyzer_notification: {
  type: incident
  adom: ADOM1
  from: FAZ-VM0000065040
  timestamp: 1694118176
  apiver: 1
  data: [
    {
      incid: IN00000007
      change_type: update
      revision: 1
      attach_revision: 3
    }
  ]
}
```

Notification example

Use Case—Healthcare Sector



Your organization is a hospital targeted by cybercriminals through a phishing attack to ransom private data

Threat: Potential breach exposing thousands of patients' data and putting patients at risk

Our goal: *Configure event handlers to detect the tactics and techniques used by Group ABC*

Domain: Enterprise

Attacker: Group ABC



Blue Team Plan of Action—Detection Capabilities



- Configure custom event handlers and data selectors to identify:
 - Probing attacks that target email systems in search of valid email accounts
 - Spearphishing emails with attached malicious macro-enabled files
 - Operating system service creation
 - Network scans that identify high-priority targets
 - Defense evasion (clearing security audit logs on the compromised host)
 - Lateral movement and exploiting remote access
 - Data exfiltration



Mock Attack Example

Incidents & Events > Event Monitor

<input type="checkbox"/>	Event	Event Status	Event Type	Count	Severity	First Occurrence	Last Update	Additional Info	Handler
<input type="checkbox"/>	MSOffice/Agent.NUOSZNItr (1)	Unhandled	Malware	1	Critical	a few seconds ago	a few seconds ago		Spearphishing handler
<input type="checkbox"/>	FortiSandbox Detected Malware from 100.64.1.20	Unhandled	Malware	1	Critical	2024-03-07 12:35:19	2024-03-07 12:35:39		Spearphishing handler
<input type="checkbox"/>	FortiMail (2)	Unhandled	Email Filter	4955	Critical	4 hours ago	4 hours ago	Malware:\$(mname) with s	SMTP Enumeration Data Handler
<input type="checkbox"/>	FortiMail Detected Spam from email@mail.com	Unhandled	Email Filter	3303	Critical	2024-03-07 08:39:49	2024-03-07 08:42:33	Malware:\$(mname) with s	SMTP Enumeration Data Handler
<input type="checkbox"/>	FortiMail Detected Spam from email@mail.com	Unhandled	Email Filter	1652	Critical	2024-03-07 08:15:36	2024-03-07 08:16:51	Malware:\$(mname) with s	SMTP Enumeration Data Handler

Events generated by custom event handlers configured by the blue team

Incidents & Events > Incidents

+ Create New

Edit

Delete All

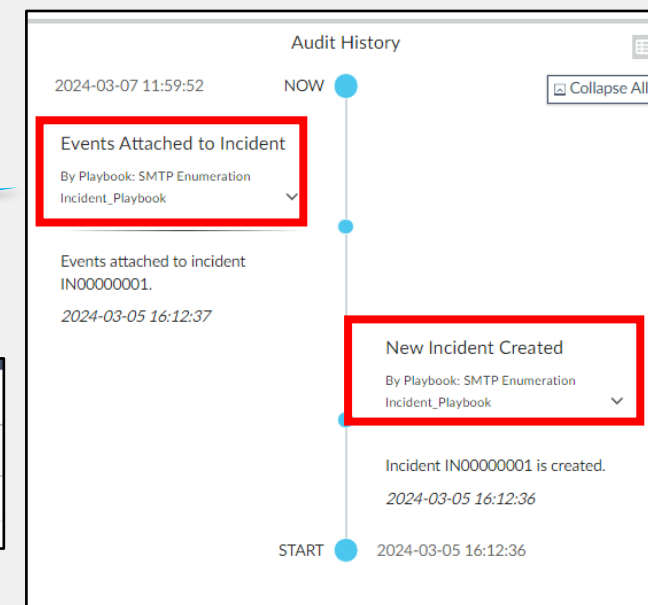
Analysis

Settings

All

<input type="checkbox"/>	Incident Number	Incident Date / Time	Last Update Date / Time	Incident Reporter	Incident Category	Severity	Status
<input type="checkbox"/>	IN00000001	2024-03-05 16:12:36	2024-03-05 16:12:37	SMTP Enumeration Incident_Playbook	Denial of Service (DoS)	High	New

Incident created on FortiAnalyzer to monitor the event



Mock Attack Example (Contd)

Incidents & Events > MITRE ATT&CK

Attack	Coverage			
Refresh	Last 4 Hours	2024-03-07 08:37:11 - 2024-03-07 12:37:11		
Reconnaissance	Resource Development	Initial Access	Execution	Persistence
10 techniques	8 techniques	9 techniques	14 techniques	19 techniques
Active Scanning ✓ Covered	Acquire Access	Drive-by Compromise	Cloud Administration Command	Account Manipulation
Gather Victim Host Information ✓ Covered	Acquire Infrastructure ✓ Covered	Exploit Public-Facing Application ✓ Covered	Command and Scripting Interpreter ✓ Covered	BITS Jobs ✓ Covered
Gather Victim Identity Information 1	Compromise Accounts	External Remote Services ✓ Covered	Container Administration Command	Boot or Logon Autostart Execution ✓ Covered
Gather Victim Network	Compromise Infrastructure ✓ Covered	Hardware Additions ✓ Covered	Deploy Container	Boot or Logon Initialization Scripts ✓ Covered
Gather Victim Org Information	Develop Capabilities	Phishing 1	Exploitation for Client Execution ✓ Covered	Browser Extensions
Phishing for Information ✓ Covered	Establish Accounts	Replication Through Removable Media ✓ Covered	Inter-Process Communication	Compromise Client Software Binary
	Obtain Capabilities ✓ Covered		Native API	

The attack is covered on FortiAnalyzer based on the **MITRE ATT&CK** page

Knowledge Check

1. Which FortiAnalyzer feature generates events?

A. Playbooks

✓ B. Event handlers

2. What does the *mitigated* event status mean?

✓ A. The risk source is being blocked.

B. The risk source is being quarantined.

Lesson Overview



Concepts, Definitions, and Incident Handling



Events, Event Handlers, and Incidents

Review

- ✓ Describe basic FortiAnalyzer SOC concepts, definitions, and features
- ✓ Analyze and manage events, and customize event handlers
- ✓ Analyze and create incidents