

# Security Operations Center (SOC) Operations Report

## Overview

This report documents the Security Operations Center (SOC) procedures using Elastic Security as the SIEM tool, supplemented by clear operational workflow diagrams and annotated screenshots of the SIEM system.

---

## Essential SOC Tools

### 1. Elastic Security (SIEM)

Elastic Security functions as our primary SIEM solution, allowing real-time threat detection, event correlation, malware detection, and centralized management via the Elastic Fleet.

### 2. Ticketing System

We use ticketing platforms to track, manage, and document security incidents, ensuring transparent and systematic handling.

### 3. Monitoring Solutions

Continuous asset and event monitoring through Elastic Security Discover and Fleet ensures rapid detection and response.

---

## SOC Workflow

The following Mermaid diagram illustrates the SOC workflow clearly, outlining alert handling and escalation paths:

- **Alert Detection:** Initial alerts detected via Elastic SIEM.
  - **Evaluation:** Determine if the alert is a false positive.
  - **Incident Logging:** Log real incidents into the ticketing platform.
  - **Severity Classification:** Assess severity level.
  - **Escalation Procedure:** If unresolved, escalate from Level 1 Analyst to Level 3 Analyst.
  - **Incident Resolution:** Document resolution and close ticket.
  - **Monitoring Updates:** Update rules based on incident learnings.
-

## Shift Transition and Handover Procedures

To maintain seamless SOC operations:

- Outgoing analysts summarize ongoing incidents, highlight critical alerts, and detail recent resolutions.
  - Incoming analysts confirm summaries, validate through Elastic Security dashboards, and formally acknowledge the handover.
- 

## Incident Handling Steps

### Incident Identification

- Alerts reviewed via Elastic Security dashboards.

### Incident Containment

- Isolate affected assets through Elastic Fleet.

### Incident Eradication

- Leverage Elastic Endgame for malware eradication.

### Incident Recovery

- Confirm system restoration through log analysis.

### Post-Incident Activities

- Document incidents comprehensively in the ticketing system.
  - Update SIEM detection rules accordingly.
- 

## Annotated Screenshots

- **Elastic Security Discover Dashboard:** Real-time monitoring and detailed logging of security events.
- **Elastic Fleet Dashboard:** Centralized agent monitoring, displaying agent health and system metrics.
- **Malware Detection Rules:** Elastic Endgame alerts, demonstrating critical alert configuration and active detection capabilities.
- **System Logs (securityd):** Provides detailed host-level security event monitoring.

These visuals reinforce clarity and comprehension of operational tools and processes within the SOC.

---

## **Conclusion**

This document clearly outlines SOC operations through the use of Elastic Security, robust procedural documentation, and illustrative workflow diagrams, ensuring structured, efficient incident handling and comprehensive monitoring across systems.

Use the Visual Editor in Mermaid Chart to design and build diagrams

Try now

Mermaid Live Editor

Playground - more features, no account required



Share

Save diagram

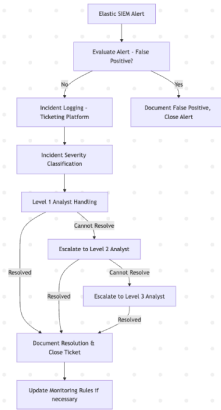
Code Config Docs

```
1 graph TD
2   A[Elastic SIEM Alert] --> B[Evaluate Alert - False Positive]
3   B -->|No| C[Incident Logging - Ticketing Platform]
4   B -->|Yes| D[Document False Positive, Close Alert]
5   C --> E[Incident Severity Classification]
6   E --> F[Level 1 Analyst Handling]
7   F -->|Cannot Resolve| G[Escalate to Level 2 Analyst]
8   F -->|Can Resolve| H[Escalate to Level 3 Analyst]
9   G --> I[Document Resolution & Close Ticket]
10  H --> I
```

Sample Diagrams

- Flow
- Sequence
- Class
- State
- ER
- Gantt
- User Journey
- Git
- Pie
- Mindmap
- ZenUML
- QuadrantChart
- XVChart
- Block
- Packet

Actions



v11.6.0

my-security-project-d6ed75.kb.us-east-1.aws.elastic.cloud/app/discover#/?\_g=(f...

Finish update

manga

Play Retro Games...

daily.dev | Where...

Humanize AI

All Bookmarks

My\_Security\_project

Discover

Give feedback

EE

Try ES|QL

Inspect

Alerts

+

Save

Data view

.alerts-security.alerts-default,apm-\*...

Filter your data using KQL syntax

Today

Search field names

0

Auto interval

No breakdown

Available fields 49

@timestamp

agent.ephemeral\_id

agent.id

agent.name

agent.type

agent.version

component.binary

component.dataset

component.id

component.old\_state

component.state

component.type

data\_stream.dataset

data\_stream.namespace

data\_stream.type

ecs.version

elastic\_agent.id

elastic\_agent.snapshot

elastic\_agent.version

Add a field

200

150

100

50

0

00:00

March 3, 2025

06:00

12:00

18:00

Mar 3, 2025 @ 00:00:00.000 - Mar 3, 2025 @ 23:59:59.999 (interval: Auto - 30 minutes)

Documents (264)

Patterns

Field statistics

Sort fields 1

@timestamp

Summary

Mar 3, 2025 @ 17:42:22.252

@timestamp Mar 3, 2025 @ 17:42:22.25

2 agent.ephemeral\_id b477f282-5905-4c65-9f20-5fc1ccb61a

ae agent.id cbbec23e-1477-45cc-a70e-c0a56cc485a...

Mar 3, 2025 @ 17:42:14.000

@timestamp Mar 3, 2025 @ 17:42:14.00

0 agent.ephemeral\_id ee146342-a53d-4c65-b324-8d42084b9e

42 agent.id cbbec23e-1477-45cc-a70e-c0a56cc485a...

Mar 3, 2025 @ 17:37:28.645

@timestamp Mar 3, 2025 @ 17:37:28.64

5 agent.ephemeral\_id b477f282-5905-4c65-9f20-5fc1ccb61a

ae agent.id cbbec23e-1477-45cc-a70e-c0a56cc485a...

Mar 3, 2025 @ 17:37:28.644

@timestamp Mar 3, 2025 @ 17:37:28.64

4 agent.ephemeral\_id b477f282-5905-4c65-9f20-5fc1ccb61a

ae agent.id cbbec23e-1477-45cc-a70e-c0a56cc485a...

Mar 3, 2025 @ 17:36:43.524

@timestamp Mar 3, 2025 @ 17:36:43.52

4 agent.ephemeral\_id b477f282-5905-4c65-9f20-5fc1ccb61a

ae agent.id cbbec23e-1477-45cc-a70e-c0a56cc485a...

Rows per page: 100

< 1 2 3 >

🔍 Security

- Discover
- Dashboards
- Rules
- Alerts
- Attack discovery
- Findings
- Cases
- Investigations
- Intelligence
- Explore
- Assets
- Machine learning

- 🔗 Get started
- <> Developer tools
- ⚙️ Project Settings

Try ES|QL Inspect Alerts + 📄 📁 📌 Save

Data view .alerts-security.alerts-default,apm-\*... 🔍 Filter your data using KQL syntax 📅 Last 15 minutes 🔄 Refresh

🔍 Search field r 0

Available fields 49

- @timestamp
- agent.ephemeral\_id
- agent.id
- agent.name
- agent.type
- agent.version
- component.binary
- component.dataset
- component.id
- component.old\_state
- component.state
- component.type
- data\_stream.dataset
- data\_stream.namespace
- data\_stream.type
- ecs.version
- elastic\_agent.id
- elastic\_agent.snapshot
- elastic\_agent.version

Add a field

📅 Auto interval

📉 No breakdown

Mar 10, 2025 @ 16:23:13.924 - Mar 10, 2025 @ 16:38:13.924 (interval: Auto - 30 seconds)

Documents (6) Patterns Field statistics

📄 Sort fields 1 🔍 📄 🔄 📄

☐ @timestamp

Summary

☐ Mar 10, 2025 @ 16:33:37.721

@timestamp Mar 10, 2025 @ 16:33:37.721 agent.ephemeral\_id b477f282-5905-4c65-9f20-5fc1ccb61aae agent.id cbbec23e-1477-45cc-a70e-c0a56cc485a0 agent.name Skills-Academy-55.local agent.type filebeat agent.version 8.17.2 component.binary filebeat component.dataset elast...

☐ Mar 10, 2025 @ 16:30:27.860

@timestamp Mar 10, 2025 @ 16:30:27.860 agent.ephemeral\_id b477f282-5905-4c65-9f20-5fc1ccb61aae agent.id cbbec23e-1477-45cc-a70e-c0a56cc485a0 agent.name Skills-Academy-55.local agent.type filebeat agent.version 8.17.2 data\_stream.dataset elastic\_agen...

☐ Mar 10, 2025 @ 16:29:28.276

@timestamp Mar 10, 2025 @ 16:29:28.276 agent.ephemeral\_id b477f282-5905-4c65-9f20-5fc1ccb61aae agent.id cbbec23e-1477-45cc-a70e-c0a56cc485a0 agent.name Skills-Academy-55.local agent.type filebeat agent.version 8.17.2 data\_stream.dataset elastic\_agen...

☐ Mar 10, 2025 @ 16:29:28.272

@timestamp Mar 10, 2025 @ 16:29:28.272 agent.ephemeral\_id b477f282-5905-4c65-9f20-5fc1ccb61aae agent.id cbbec23e-1477-45cc-a70e-c0a56cc485a0 agent.name Skills-Academy-55.local agent.type filebeat agent.version 8.17.2

☐ Mar 10, 2025 @ 16:28:32.680

@timestamp Mar 10, 2025 @ 16:28:32.680 agent.ephemeral\_id b477f282-5905-4c65-9f20-5fc1ccb61aae agent.id cbbec23e-1477-45cc-a70e-c0a56cc485a0 agent.name Skills-Academy-55.local agent.type filebeat agent.version 8.17.2 component.binary filebeat component.dataset elast...

☐ Mar 10, 2025 @ 16:28:27.000

@timestamp Mar 10, 2025 @ 16:28:27.000 agent.ephemeral\_id ee146342-a53d-4c65-b324-8d42084b9e42 agent.id cbbec23e-1477-45cc-a70e-c0a56cc485a0 agent.name Skills-Academy-55.local

←

→

↺

🌐 my-security-project-d6ed75.kb.us-east-1.aws.elastic.cloud/app/security/rules/ad...

☆

🗄️

🎮

Finish update ⋮

🗄️

manga

🎮 Play Retro Games...

🔗 daily.dev | Where...

🧠 Humanize AI

📁 All Bookmarks

≡

🌈

D

/ My\_Security\_project · R...

/ Detection rules (...

/ Add R...

🔍

🌐

Give feedback 📧

🔔

AI Assistant

EE

Security

Discover

Dashboards 🗄️

Rules 🗄️

Alerts

Attack discovery

Findings

Cases

Investigations 🗄️

Intelligence

Explore 🗄️

Assets 🗄️

Machine learning 🗄️

🚀 Get started

🔧 Developer tools

⚙️ Project Settings ▾

Malware - Detected - Elastic Endgame

✕

Overview

Investigation guide

Timeline template

None

📅 Schedule

Runs every

10m

Additional look-back time

5m

📖 Setup guide

Setup

This rule is configured to generate more **Max alerts per run** than the default 1000 alerts per run set for all rules. This is to ensure that it captures as many alerts as possible.

**IMPORTANT:** The rule's **Max alerts per run** setting can be superseded by the `xpack.alerting.rules.run.alerts.max` Kibana config setting, which determines the maximum alerts generated by *any* rule in the Kibana alerting framework. For example, if `xpack.alerting.rules.run.alerts.max` is set to 1000, this rule will still generate no more than 1000 alerts even if its own **Max alerts per run** is set higher.

To make sure this rule can generate as many alerts as it's configured in its own **Max alerts per run** setting, increase the `xpack.alerting.rules.run.alerts.max` system setting accordingly.

**NOTE:** Changing `xpack.alerting.rules.run.alerts.max` is not possible in Serverless projects.

Dismiss

Install without enabling

Install and enable

←

→

↺

my-security-project-d6ed75.kb.us-east-1.aws.elastic.cloud/app/security/rules/ad...

☆

🌐

📁

🔒

Finish update

⋮

🗃️

manga

🎮 Play Retro Games...

💻 daily.dev | Where...

🧠 Humanize AI

📁 All Bookmarks

⏪

🌐

D

/

My Security project

'R...

/

Detection rules (...)

/

Add R...

🔍

🔄

Give feedback

📧

AI Assistant

EE

🛡️ Security

Discover

Dashboards

Rules

Alerts

Attack discovery

Findings

Cases

Investigations

Intelligence

Explore

Assets

Machine learning

🚀 Get started

🔧 Developer tools

⚙️ Project Settings

Malware - Detected - Elastic Endgame

✕

Overview

Investigation guide

Custom query language

KQL

Rule type

Query

Required fields

Ⓢ endgame.event\_subtype\_full,

Ⓢ endgame.metadata.type,

Ⓚ event.action,

Ⓚ event.kind,

Ⓚ event.module

Timeline template

None

📅 Schedule

Runs every

10m

Additional look-back time

5m

📖 Setup guide

Setup

This rule is configured to generate more **Max alerts per run** than the default 1000 alerts per run set for all rules. This is to ensure that it captures as many alerts as possible.

**IMPORTANT:** The rule's **Max alerts per run** setting can be superseded by the `xpack.alerting.rules.run.alerts.max` Kibana config setting, which determines the maximum alerts

Dismiss

Install without enabling

Install and enable



my-security-project-d6ed75.kb.us-east-1.aws.elastic.cloud/app/security/rules/ad...

manga Play Retro Games... daily.dev | Where... Humanize AI

All Bookmarks

My Security project R... Detection rules (... Add R...

Give feedback

AI Assistant EE

Security

Discover

Dashboards

Rules

Alerts

Attack discovery

Findings

Cases

Investigations

Intelligence

Explore

Assets

Machine learning

Get started

Developer tools

Project Settings

Malware - Detected - Elastic Endgame

Overview Investigation guide

About

Elastic Endgame detected Malware. Click the Elastic Endgame icon in the event.module column or the link in the rule.reference column for additional information.

Author

Elastic

Severity

Critical

Risk score

99

License

Elastic License v2

Timestamp override

event.ingested

Max alerts per run

10000

Tags

Data Source: Elastic Endgame

Resources: Investigation Guide

Definition

Index patterns

endgame-\*

Custom query

event.kind:alert and event.module:endgame and endgame.metadata.type:detection and (event.action:file\_classification\_event or endgame.event\_subtype\_full:file\_classification\_event)

Dismiss

Install without enabling

Install and enable

The screenshot shows the AWS Security console's Fleet page. The left sidebar contains navigation links: Security, Discover, Dashboards, Rules, Alerts, Attack discovery, Findings, Cases, Investigations, Intelligence, Explore, Assets (selected), Machine learning, Get started, Developer tools, and Project Settings. The main content area has a header with 'Fleet' and a sub-header 'Centralized management for Elastic Agents.' Below this are tabs for 'Agents' (selected), 'Agent policies', 'Enrollment tokens', 'Uninstall tokens', 'Data streams', and 'Settings'. A summary bar shows 'Showing 1 agent' and various status counts: 1 Healthy, 0 Unhealthy, 0 Orphaned, 0 Updating, 0 Offline, 0 Inactive, 0 Unenrolled, and 0 Uninstalled. A table lists the agent details:

Status	Host	Agent policy	CPU	Memory	Last activity	Version	Actions
Healthy	Skills-Academy-55.Jocal	parrot os rev. 1	N/A	239 MB	1 minute ago	8.17.2	...

At the bottom, it indicates 'Rows per page: 20' and a pagination link '< 1 >'.

Security

Discover

Dashboards

Rules

Alerts

Attack discovery

Findings

Cases

Investigations

Intelligence

Explore

Assets

Machine learning

Get started

Developer tools

Project Settings

ML job settings

Add integrations

Add Elastic rules

See what's new in Prebuilt Security Detection Rules

Search by rule name

Tags 118

<input type="checkbox"/>	Rule	<div>0/1 integrations</div>	<div>6</div>	Risk s... 73	Seve... High	Install
<input type="checkbox"/>	Potential Ransomware Note File Dro	<div>0/1 integrations</div>	<div>6</div>	73	High	Install
<input type="checkbox"/>	SSH Process Launched From Inside	<div>0/1 integrations</div>	<div>7</div>	73	High	Install
<input type="checkbox"/>	Potential Exploitation of an Unquote	<div>1/5 integrations</div>	<div>11</div>	21	Low	Install
<input type="checkbox"/>	Suspicious Inter-Process Communic	<div>0/1 integrations</div>	<div>6</div>	47	Med...	Install
<input type="checkbox"/>	Mofcomp Activity	<div>1/4 integrations</div>	<div>10</div>	21	Low	Install
<input type="checkbox"/>	Potential Relay Attack against a Dom	<div>1/2 integrations</div>	<div>9</div>	21	Low	Install
<input type="checkbox"/>	Apple Script Execution followed by N	<div>0/1 integrations</div>	<div>7</div>	47	Med...	Install
<input type="checkbox"/>	Account Configured with Never-Expi	<div>1/2 integrations</div>	<div>8</div>	47	Med...	Install
<input type="checkbox"/>	Suspicious File Renamed via SMB	<div>0/1 integrations</div>	<div>6</div>	73	High	Install
<input type="checkbox"/>	Suspicious Interactive Shell Spawne	<div>0/1 integrations</div>	<div>6</div>	73	High	Install

my-security-project-d6ed75.kb.us-east-1.aws.elastic.cloud/app/security/alerts?s...

Finish update

manga

Play Retro Games...

daily.dev | Where...

Humanize AI

All Bookmarks

My\_Security\_project

Alerts

Give feedback

AI Assistant

EE

Security

Discover

Dashboards

Rules

Alerts

Attack discovery

Findings

Cases

Investigations

Intelligence

Explore

Assets

Machine learning

Get started

Developer tools

Project Settings

ML job settings

Add integrations

Data view

Alerts

Filter your data using KQL syntax

Today

Alerts

Assignees

Manage rules

Status

open

Severity

User

Host

Summary

Trend

Counts

Treemap

Severity levels

Levels

Count

No items found

alerts

Alerts by name

Untitled timeline

Unsaved