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.

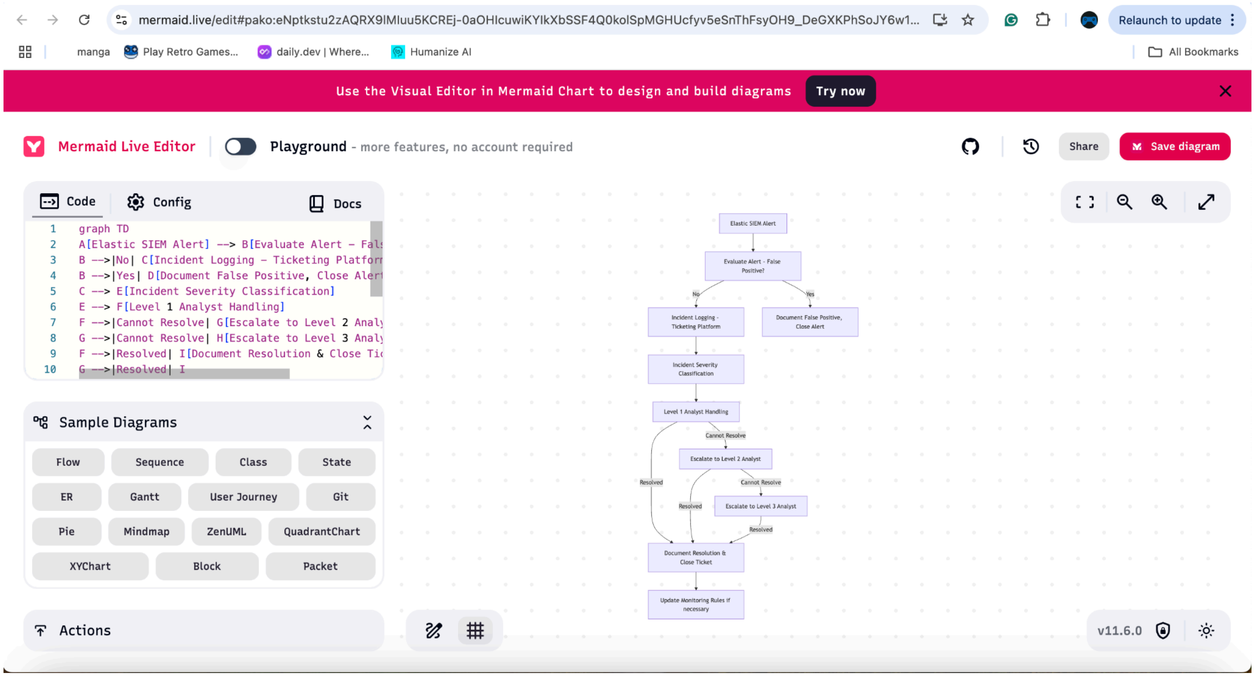
Annotated Screenshots

- **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.

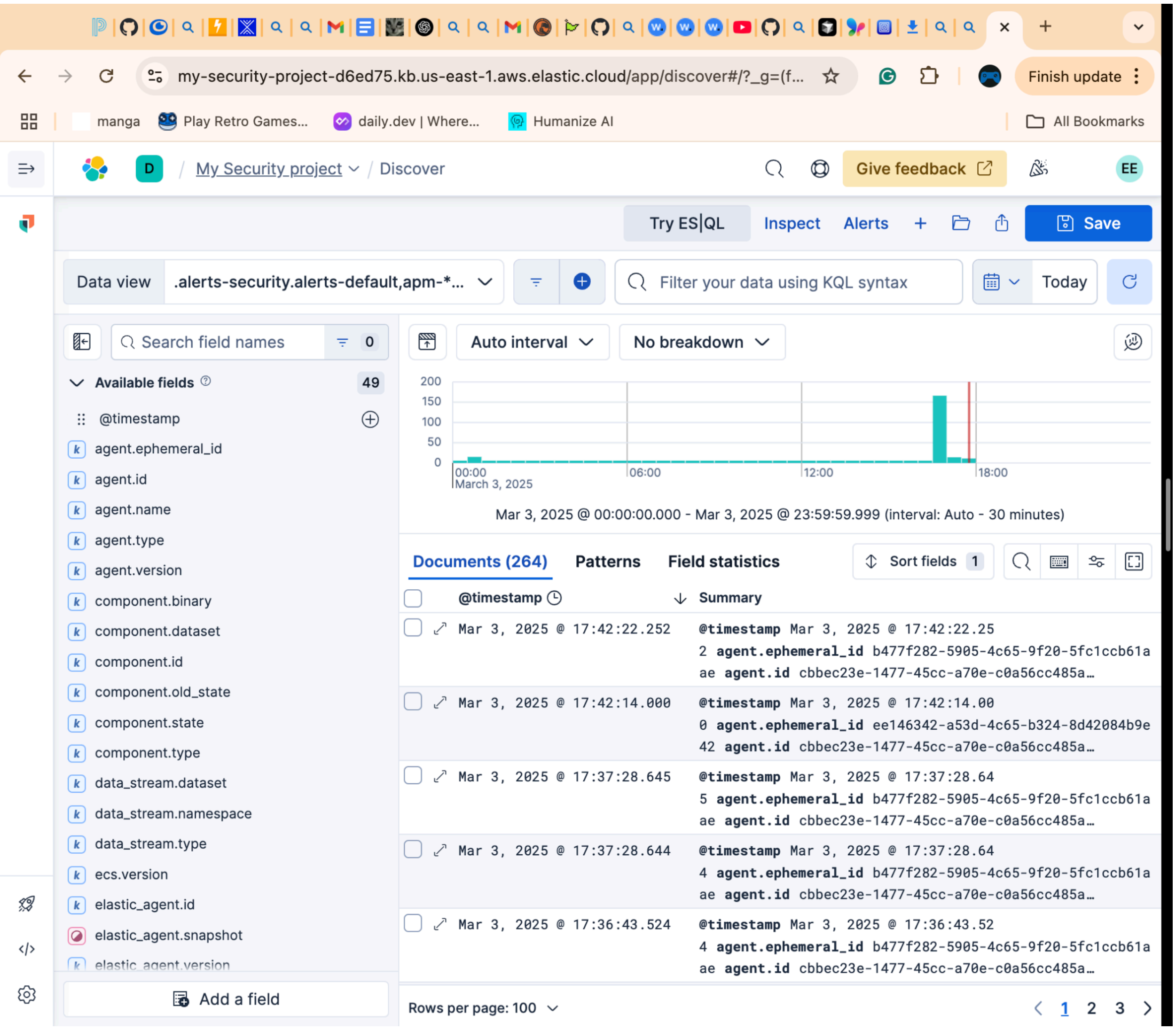
These visuals reinforce clarity and comprehension of operational tools and processes within the SOC.

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.


mermaid.live/edit#pako:eNptkstu2zAQRX9lMluu5KCREj-0aOHlcuwiKYIkXbSSF4Q0kolSpMGHUcfyv5eSnThFsyOH9_DeGXKPhSoJY6w...
Relaunch to update
manga
Play Retro Games...
daily.dev | Where...
Humanize AI
All Bookmarks
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
Sample Diagrams
Flow
Sequence
Class
State
ER
Gantt
User Journey
Git
Pie
Mindmap
ZenUML
QuadrantChart
XYChart
Block
Packet
Actions
v11.6.0
Elastic SIEM Alert
Evaluate Alert - False Positive?
No
Yes
Incident Logging - Ticketing Platform
Document False Positive, Close Alert
Incident Severity Classification
Level 1 Analyst Handling
Cannot Resolve
Escalate to Level 2 Analyst
Resolved
Resolved
Cannot Resolve
Escalate to Level 3 Analyst
Resolved
Document Resolution & Close Ticket
Update Monitoring Rules if necessary

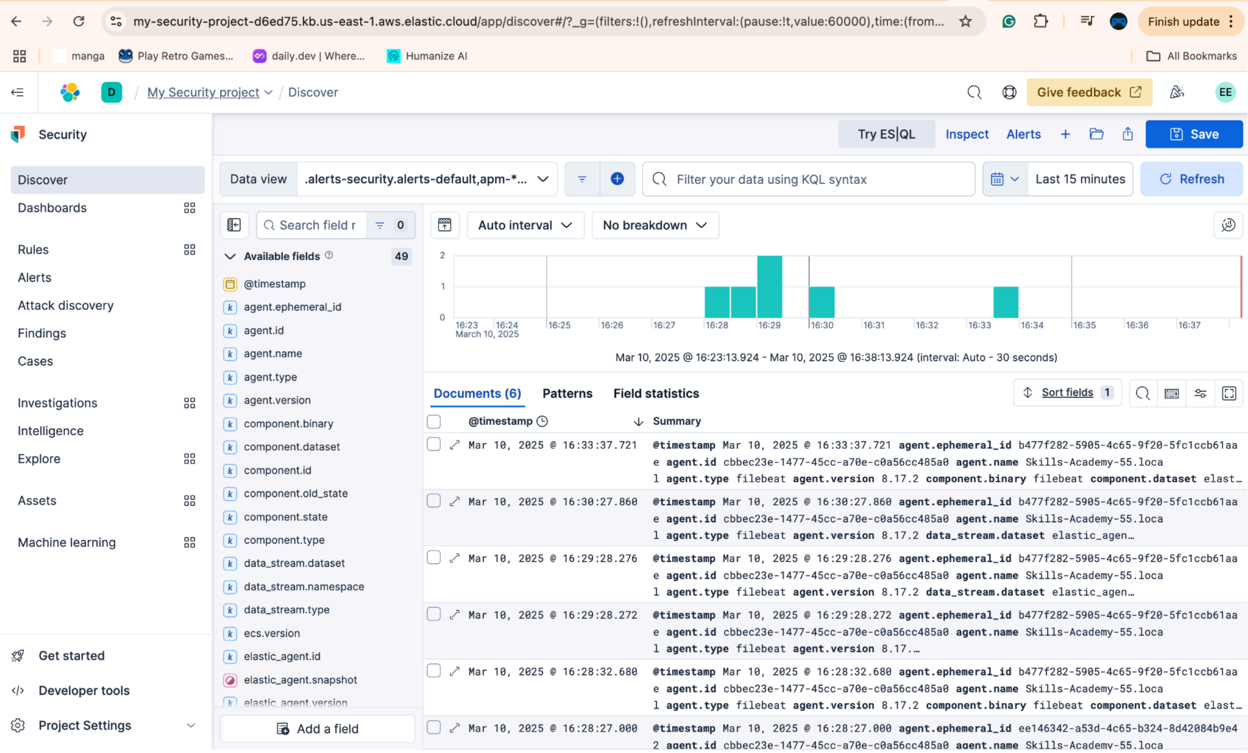
```
graph TD
A[Elastic SIEM Alert] --> B[Evaluate Alert - Fals
B -->|No| C[Incident Logging - Ticketing Platforr
B -->|Yes| D[Document False Positive, Close Alert
C --> E[Incident Severity Classification]
E --> F[Level 1 Analyst Handling]
F -->|Cannot Resolve| G[Escalate to Level 2 Analy
G -->|Cannot Resolve| H[Escalate to Level 3 Analy
F -->|Resolved| I[Document Resolution & Close Tic
G -->|Resolved| I
```



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

- @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

```
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…
```



my-security-project-d6ed75.kb.us-east-1.aws.elastic.cloud/app/discover#/?_g=(filters:!(),refreshInterval:(pause:!t,value:60000),time:(from...

Data view .alerts-security.alerts-default,apm-*...

Filter your data using KQL syntax

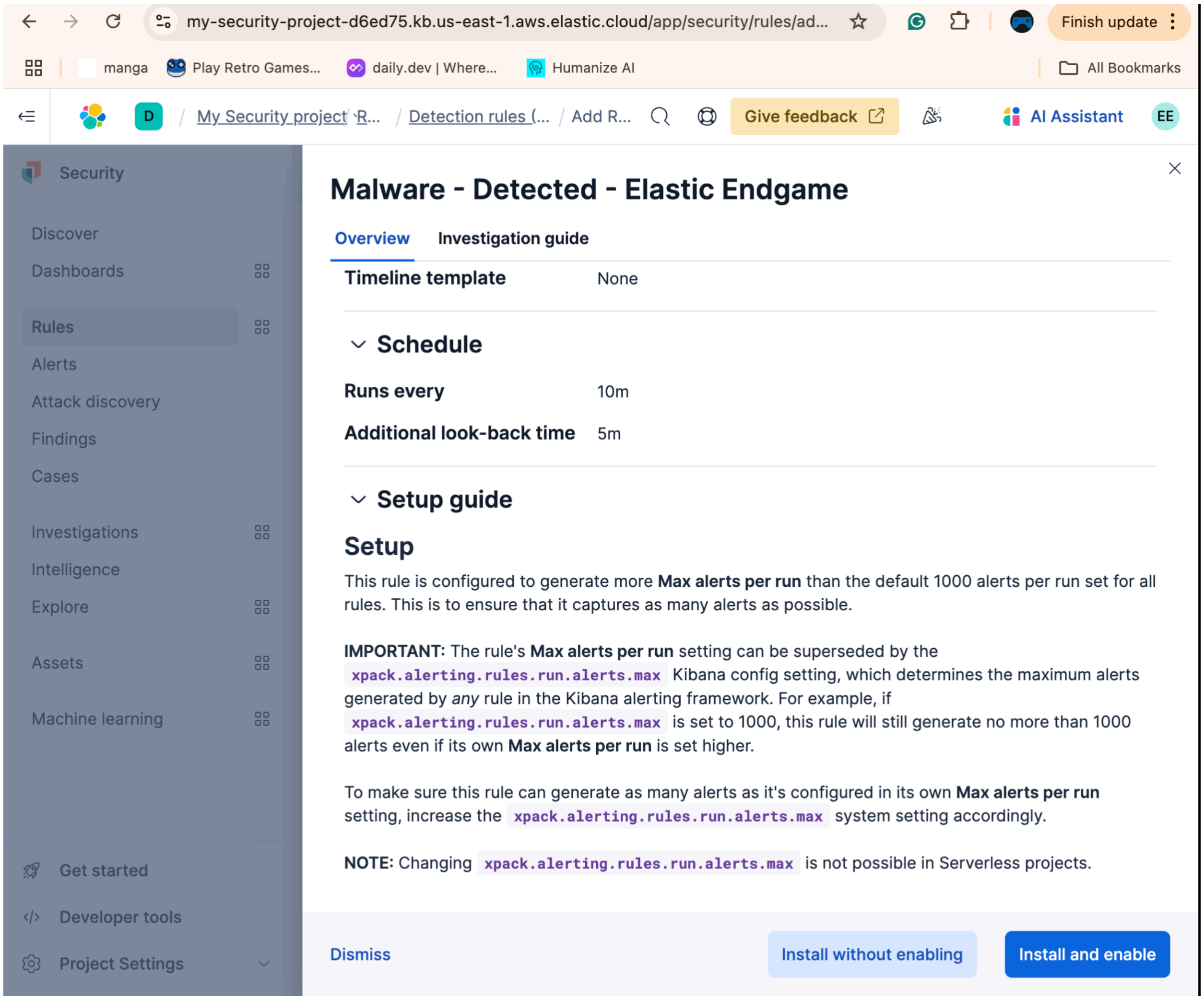
Last 15 minutes

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

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

@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.…
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.loca



Malware - Detected - Elastic Endgame

Timeline template	None

Schedule

Runs every	10m
Additional look-back time	5m

Setup guide

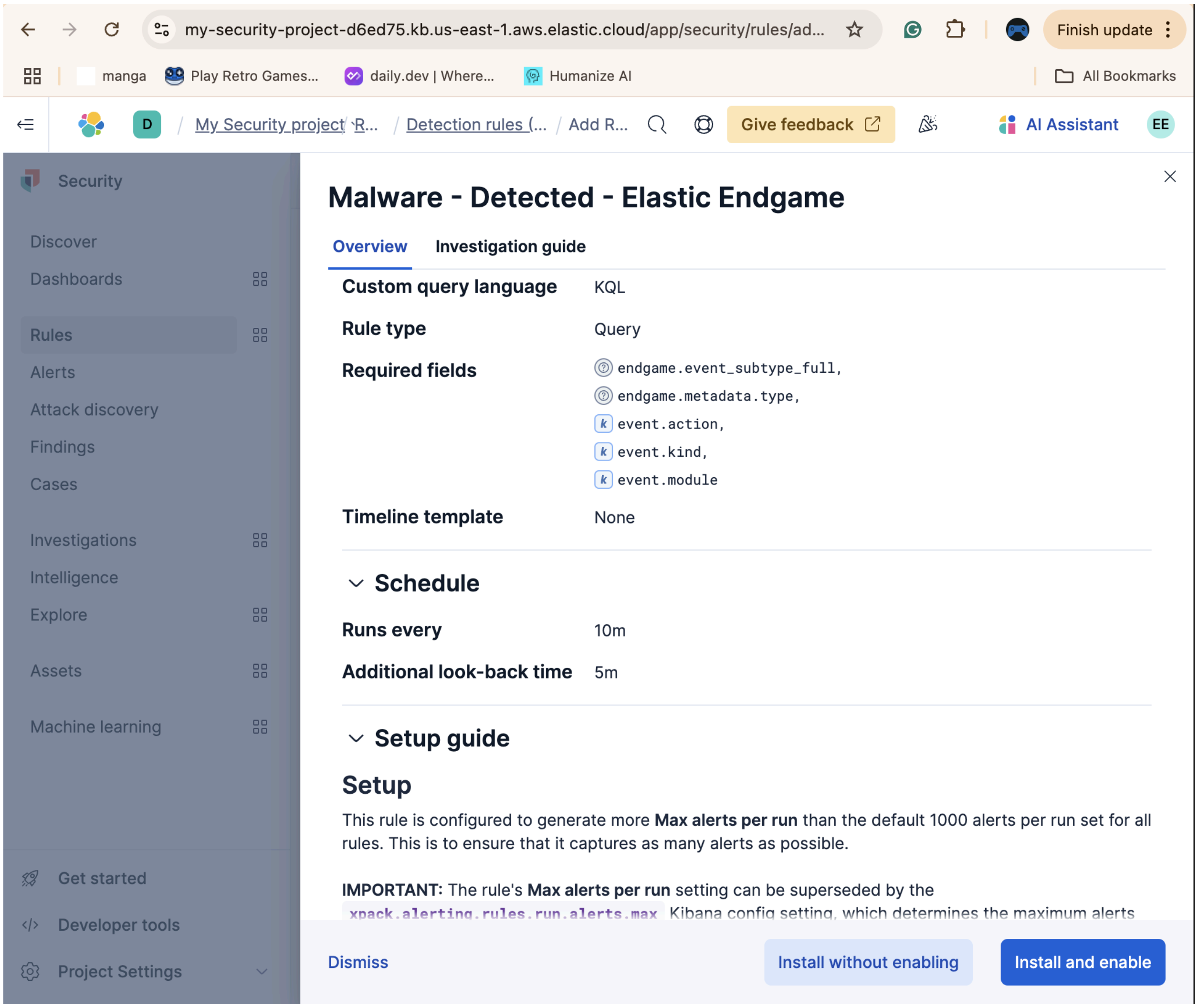
Setup

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.



Malware - Detected - Elastic Endgame

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

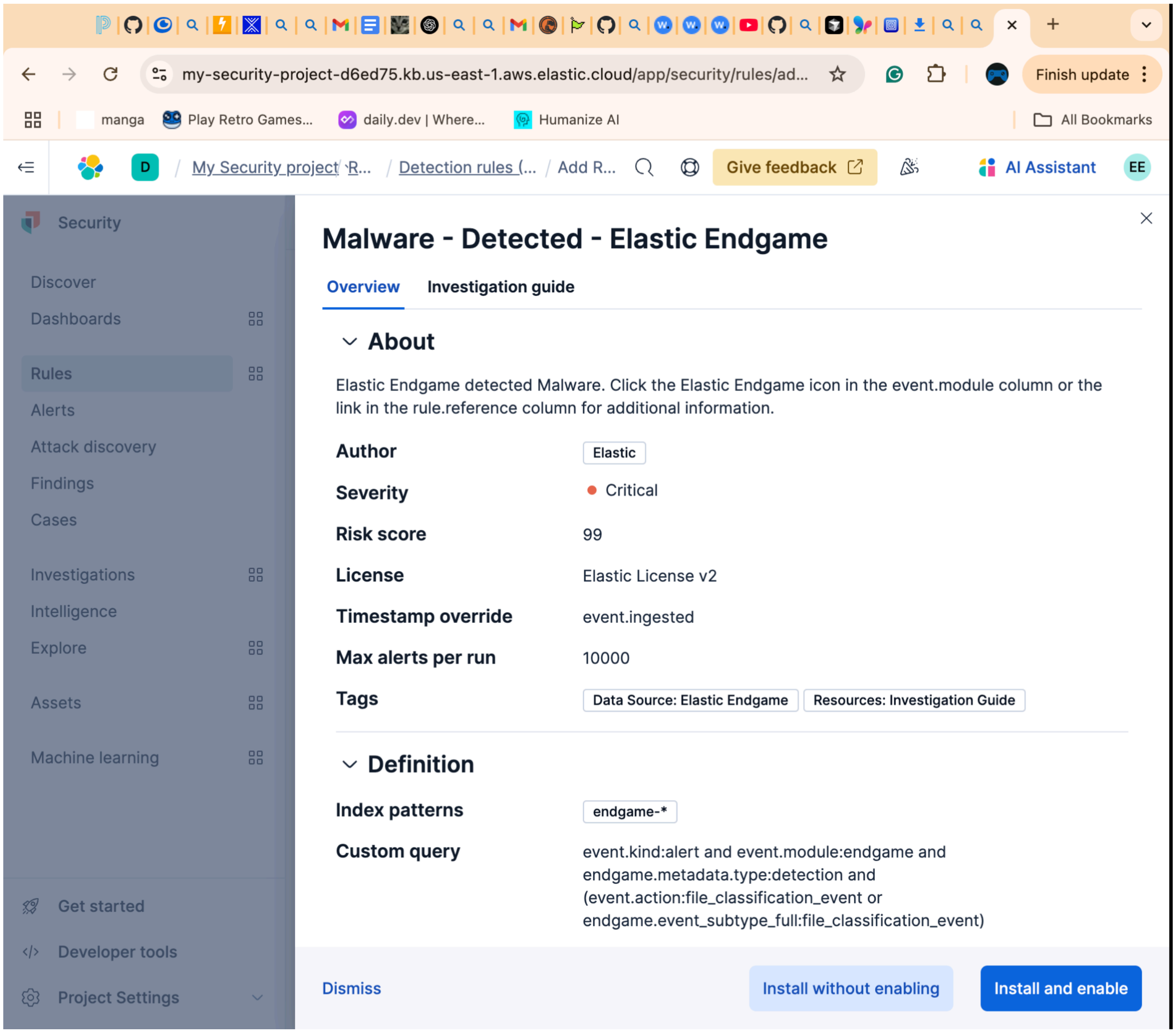
Runs every	10m
Additional look-back time	5m

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



Malware - Detected - Elastic Endgame

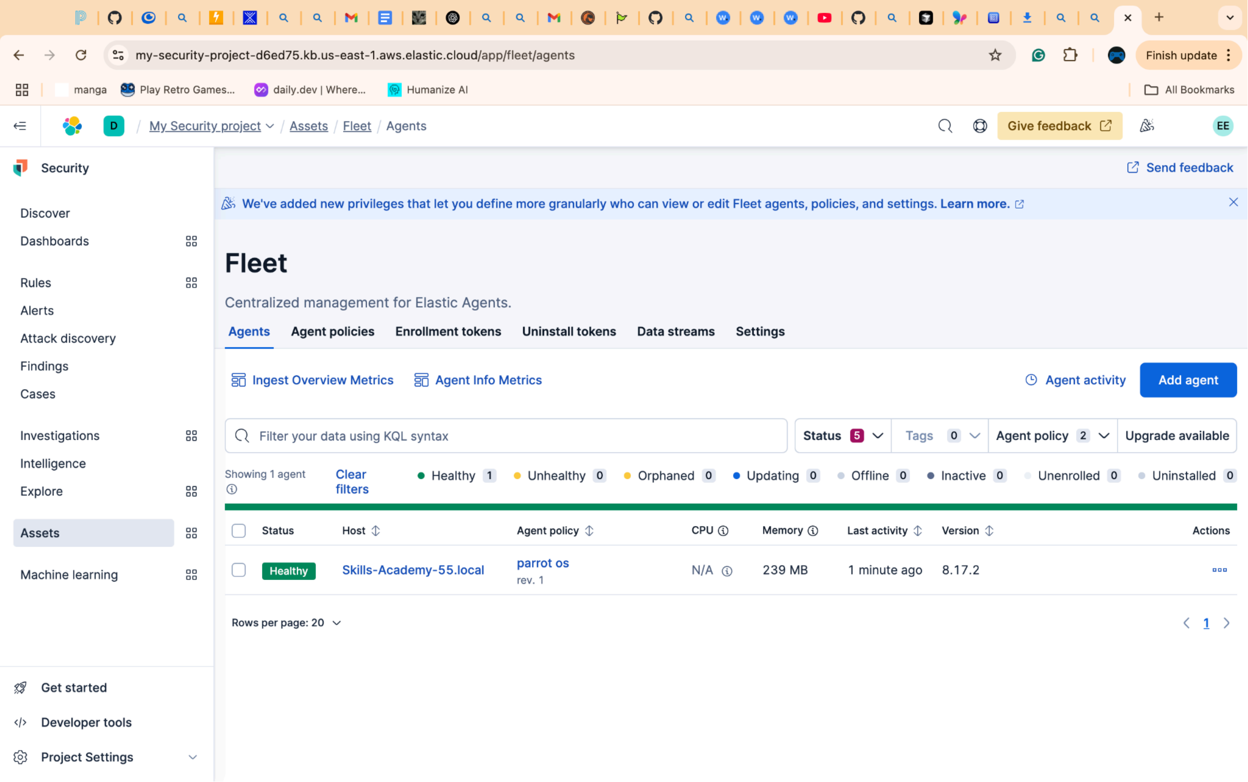
About

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)



We've added new privileges that let you define more granularly who can view or edit Fleet agents, policies, and settings. Learn more.

Fleet

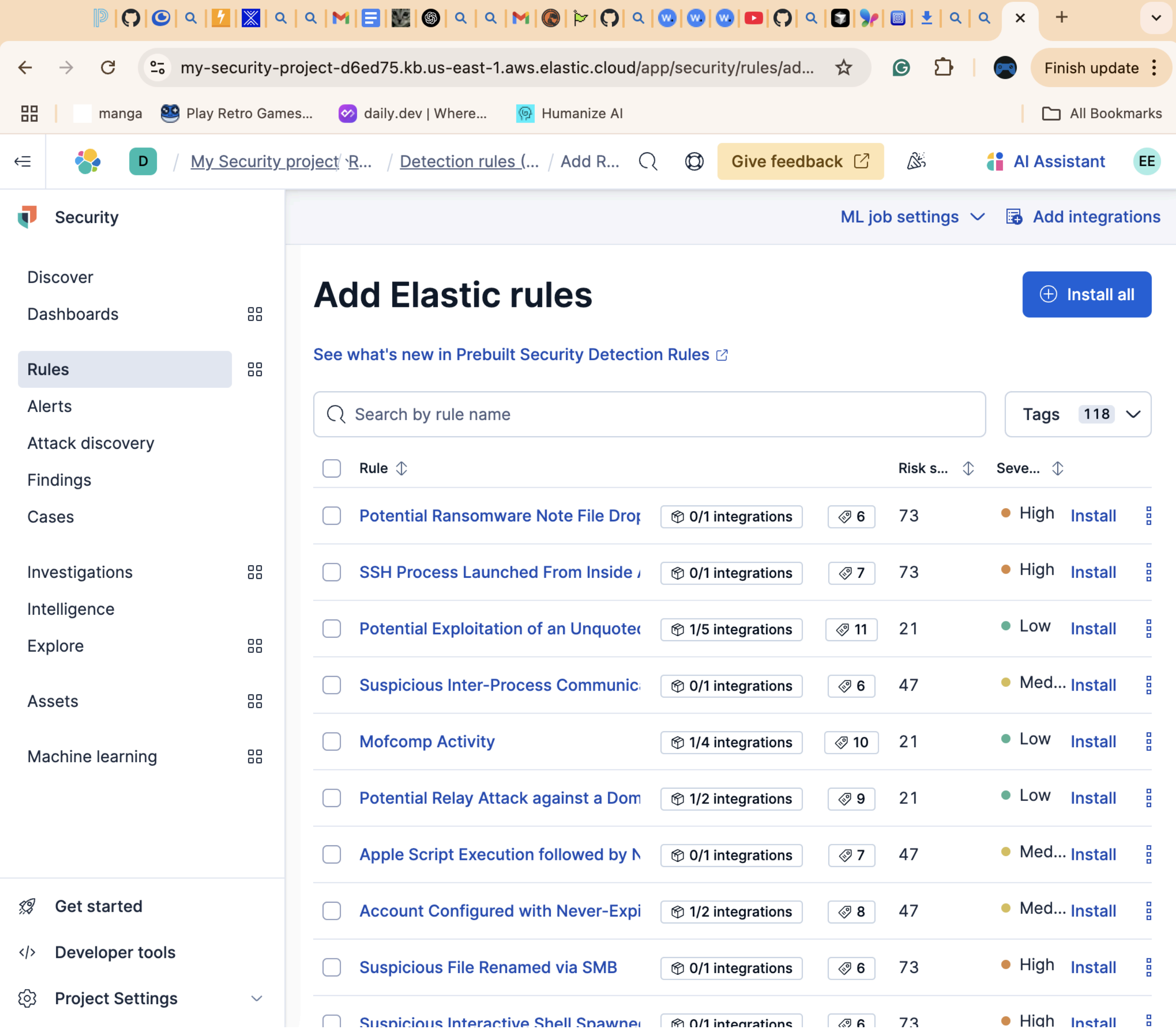
Centralized management for Elastic Agents.

Showing 1 agent

● Healthy 1 ● Unhealthy 0 ● Orphaned 0 ● Updating 0 ● Offline 0 ● Inactive 0 ● Unenrolled 0 ● Uninstalled 0

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

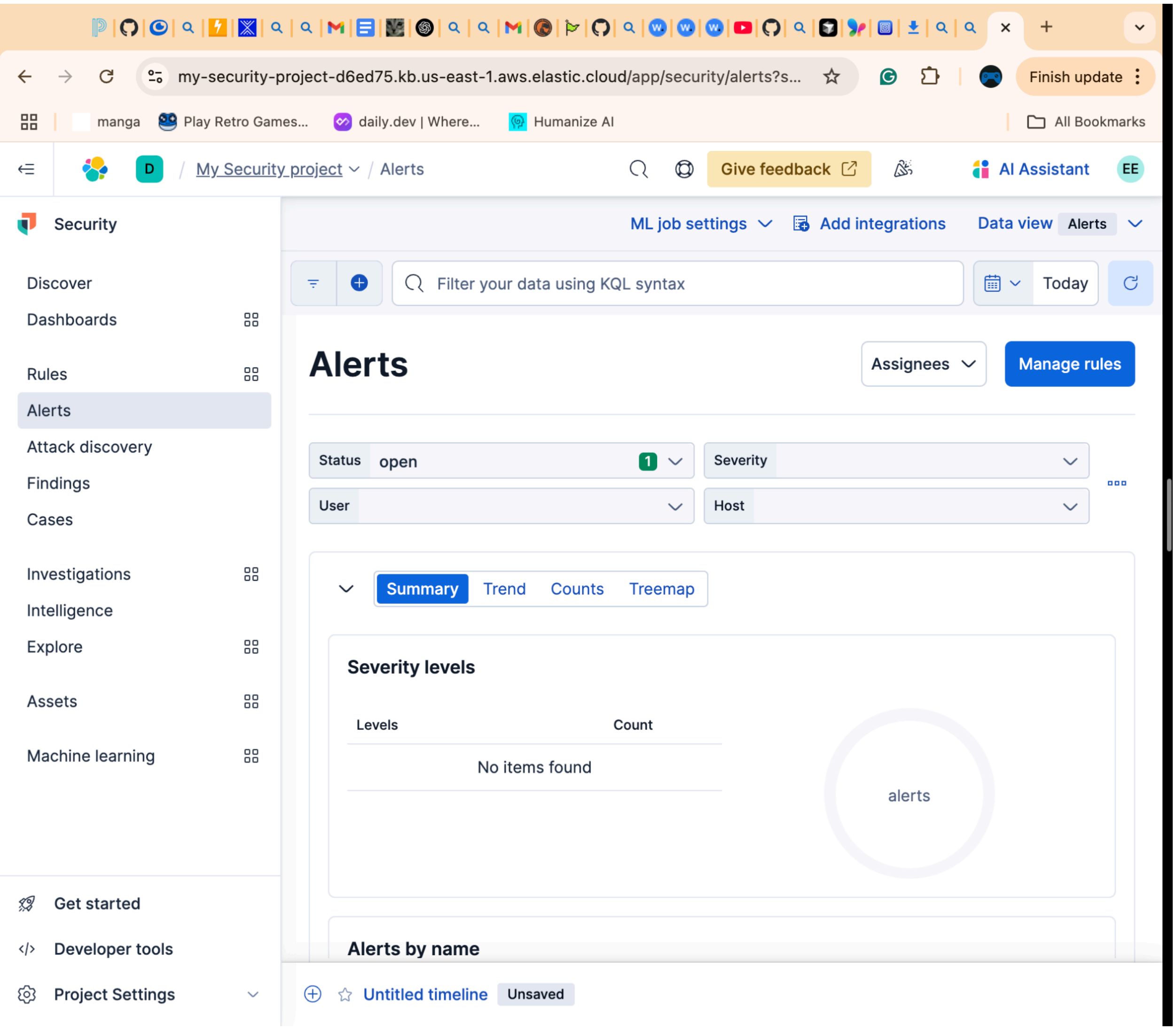
Rows per page: 20



Add Elastic rules

See what's new in Prebuilt Security Detection Rules

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



Alerts

Status open 1

Severity

User

Host

Severity levels

Levels	Count
No items found	

alerts

Alerts by name