

SOC Operations Documentation Report

Introduction

This document demonstrates an understanding of key SOC (Security Operations Center) tools and operations, including SIEM systems, ticketing platforms, and monitoring solutions. It integrates screenshots from Elastic Security and documents workflows, shift transitions, and incident handling procedures.

Essential SOC Tools

****SIEM System:****

Elastic Security collects, analyzes, and correlates security data to detect threats.

AboutDetailsInvestigation guideSetup guide

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.

AuthorElastic

SeverityCritical

Risk score99

LicenseElastic License v2

Timestamp overrideevent.ingested

Max alerts per run10000

TagsData Source: Elastic EndgameResources: Investigation Guide

Definition

Index patternsendgame-*

Custom queryevent.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)

Custom query languageKQL

Rule typeQuery

Required fieldsendgame.event_subtype_full, endgame.metadata.type, event.action, event.kind, event.module

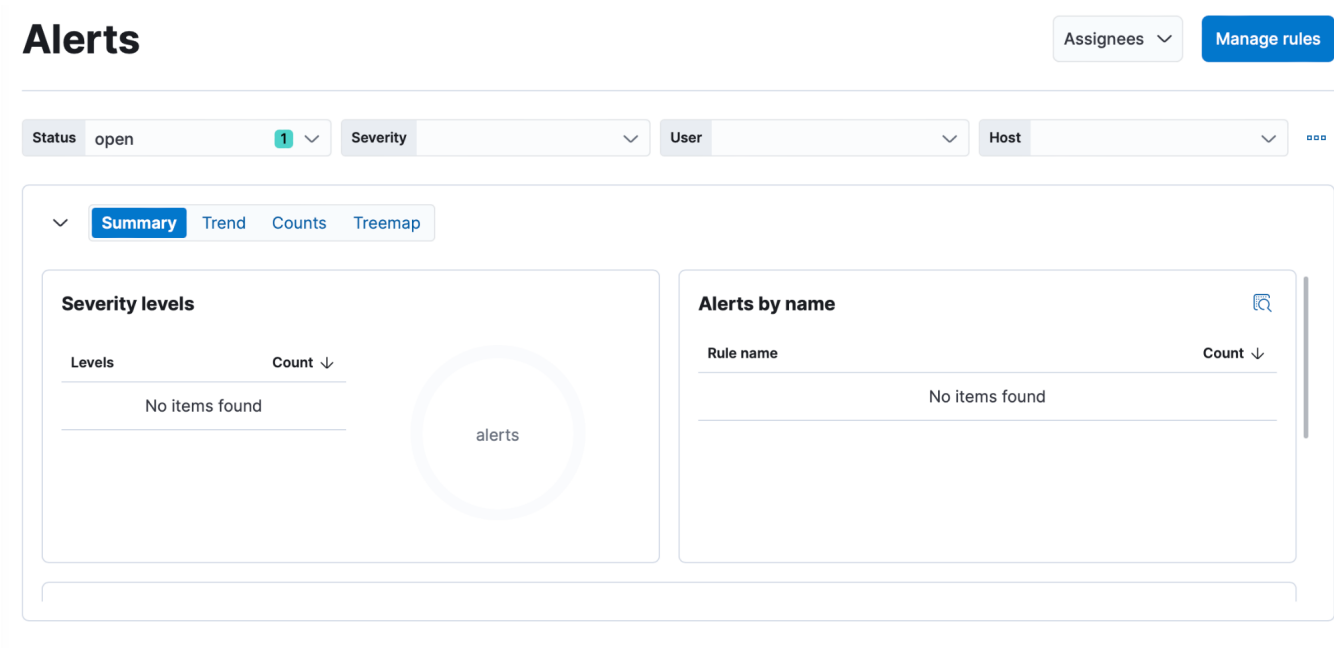
****Ticketing Platform:****

Simulated through Elastic's case management system to track incidents and responses.

****Monitoring Solution:****

Elastic Fleet manages endpoint agents ensuring continuous monitoring.

SOC Operations Documentation Report



SOC Operations Documentation Report

Fleet

Centralized management for Elastic Agents.

Agents Agent policies Enrollment tokens Uninstall tokens Data streams Settings

Ingest Overview Metrics Agent Info Metrics

Agent activity Add Fleet Server Add agent

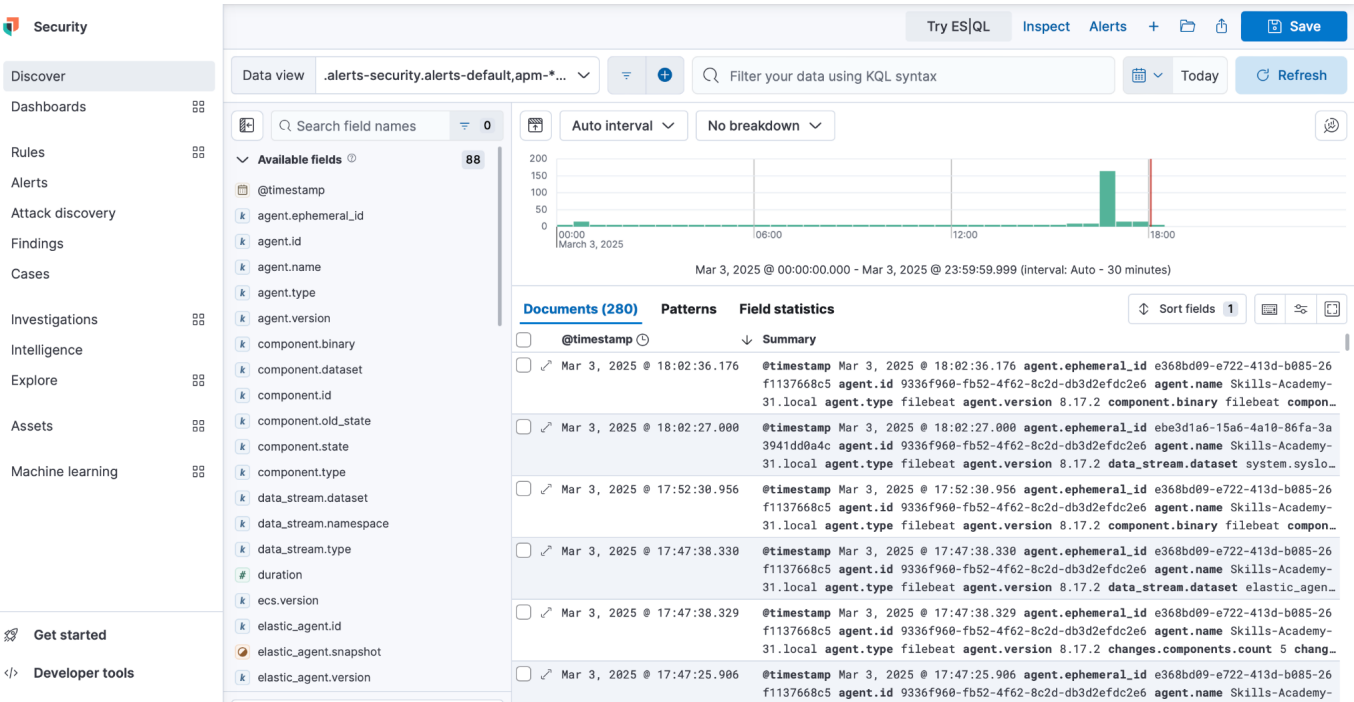
Filter your data using KQL syntax Status 4 Tags 0 Agent policy 2 Upgrade available

Showing 2 agents Clear filters Healthy 2 Unhealthy 0 Updating 0 Offline 0 Inactive 0 Unenrolled 0

Status	Host	Agent policy	CPU	Memory	Last activity	Version	Actions
Healthy	Skills-Academy-31.local	Parrot OS rev. 1	0.06 %	233 MB	9 seconds ago	8.17.2	
Healthy	92d87e42db3a	Elastic Cloud agent policy rev. 5	N/A	N/A	32 seconds ago	8.17.2	

Rows per page: 20 < 1 >

Log investigation performed through Discover view, analyzing correlated events.



Elastic Rules Overview

Elastic provides prebuilt detection rules classified by severity and risk score.

SOC Operations Documentation Report

ML job settingsAdd integrations

Add Elastic rules

See what's new in Prebuilt Security Detection Rules

Search by rule name

Tags118

Rule		Risk score	Severity	
<input type="checkbox"/> Potential Ransomware Note File Dropped via SMB	0/1 integrations6	73	High	Install
<input type="checkbox"/> SSH Process Launched From Inside A Container	0/1 integrations7	73	High	Install
<input type="checkbox"/> Potential Exploitation of an Unquoted Service Path Vulnerability	1/5 integrations11	21	Low	Install
<input type="checkbox"/> Suspicious Inter-Process Communication via Outlook	0/1 integrations6	47	Medium	Install
<input type="checkbox"/> Mofcomp Activity	1/4 integrations10	21	Low	Install
<input type="checkbox"/> Potential Relay Attack against a Domain Controller	1/2 integrations9	21	Low	Install
<input type="checkbox"/> Apple Script Execution followed by Network Connection	0/1 integrations7	47	Medium	Install
<input type="checkbox"/> Account Configured with Never-Expiring Password	1/2 integrations8	47	Medium	Install
<input type="checkbox"/> Suspicious File Renamed via SMB	0/1 integrations6	73	High	Install
<input type="checkbox"/> Suspicious Interactive Shell Spawned From Inside A Container	0/1 integrations6	73	High	Install
<input type="checkbox"/> Potential WMI Abuse for Lateral Movement	0/1 integrations6	47	Medium	Install

Conclusion

This project integrates SOC operations by monitoring agents, managing security alerts, and documenting incident response processes using Elastic Security.