SOC Operations Documentation Report

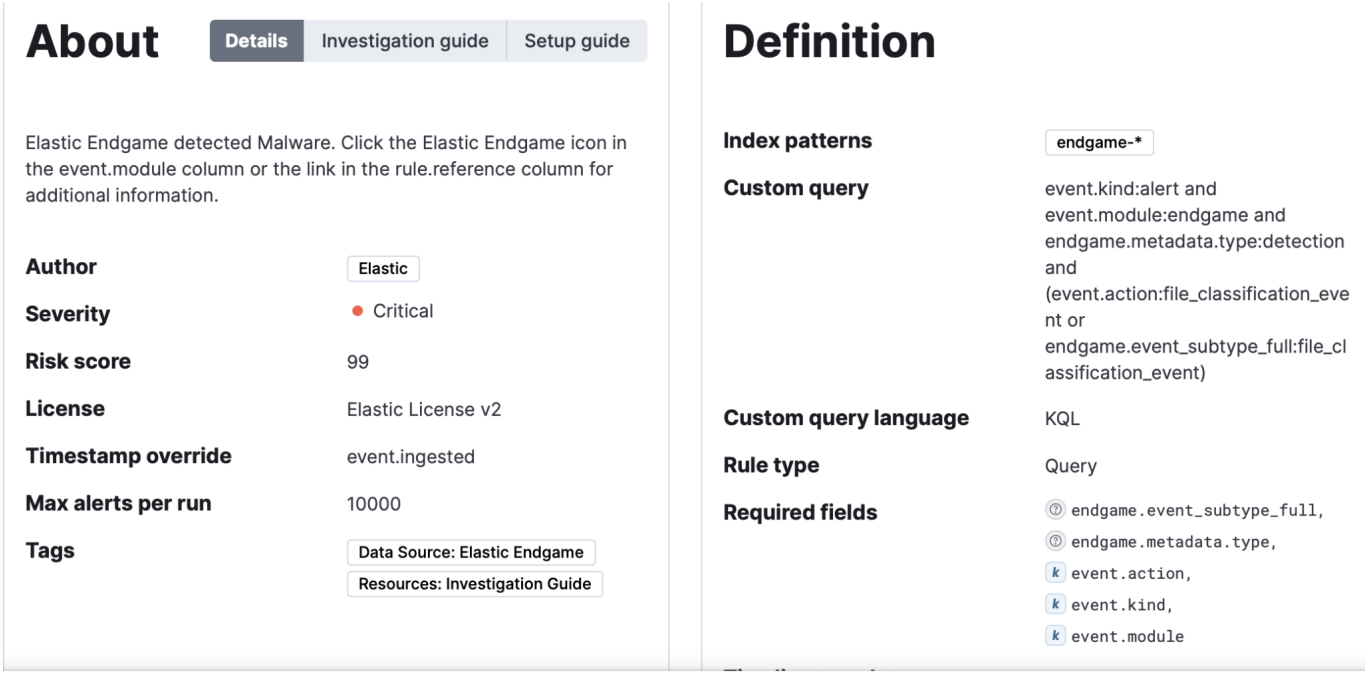
Introduction

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.



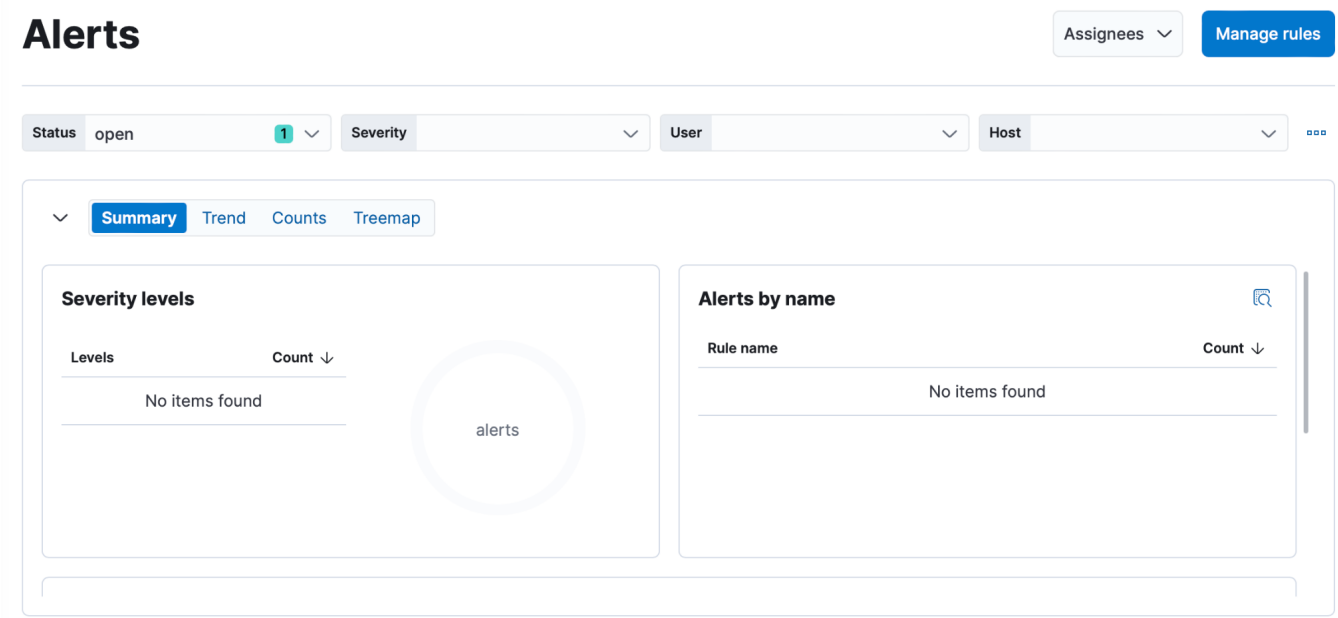
Ticketing Platform:

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 Workflows (Alert Handling and Escalation)

Alert detection, triage, incident creation, containment, investigation, escalation, and resolution are handled following structured paths (See workflow in the full document).

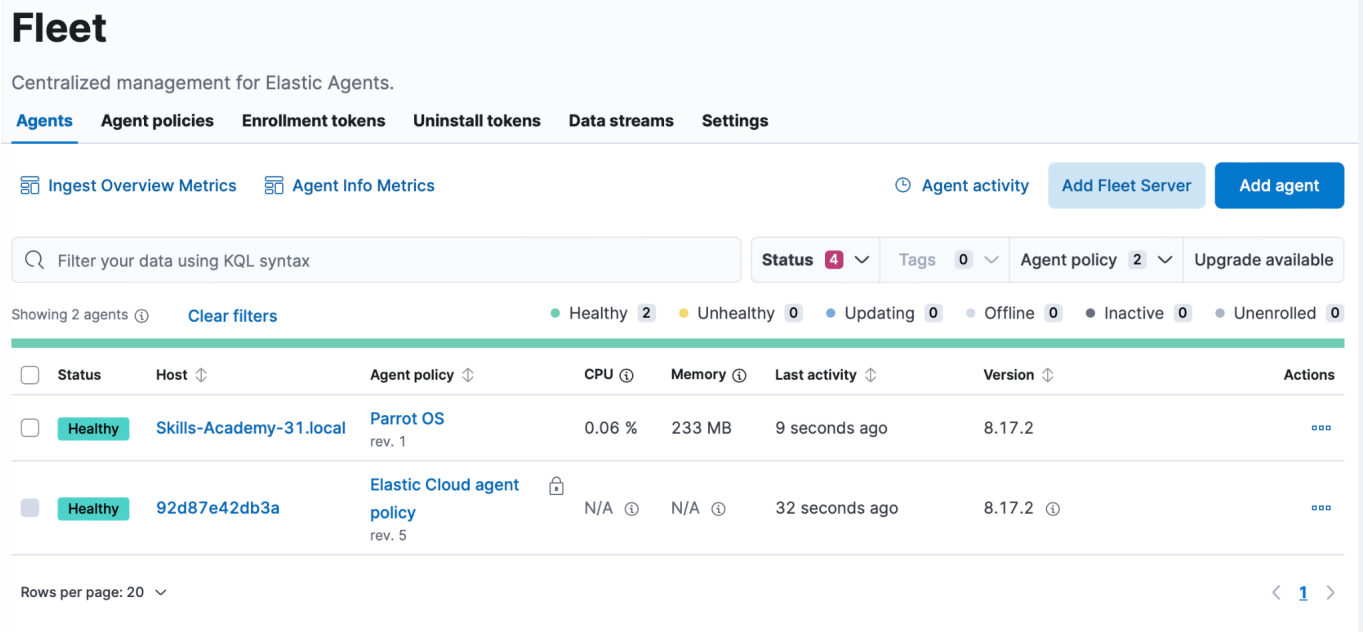
Shift Transition and Handover Procedures

Includes daily shift briefing, pending investigations review, active incident summaries, and critical alerts communication.

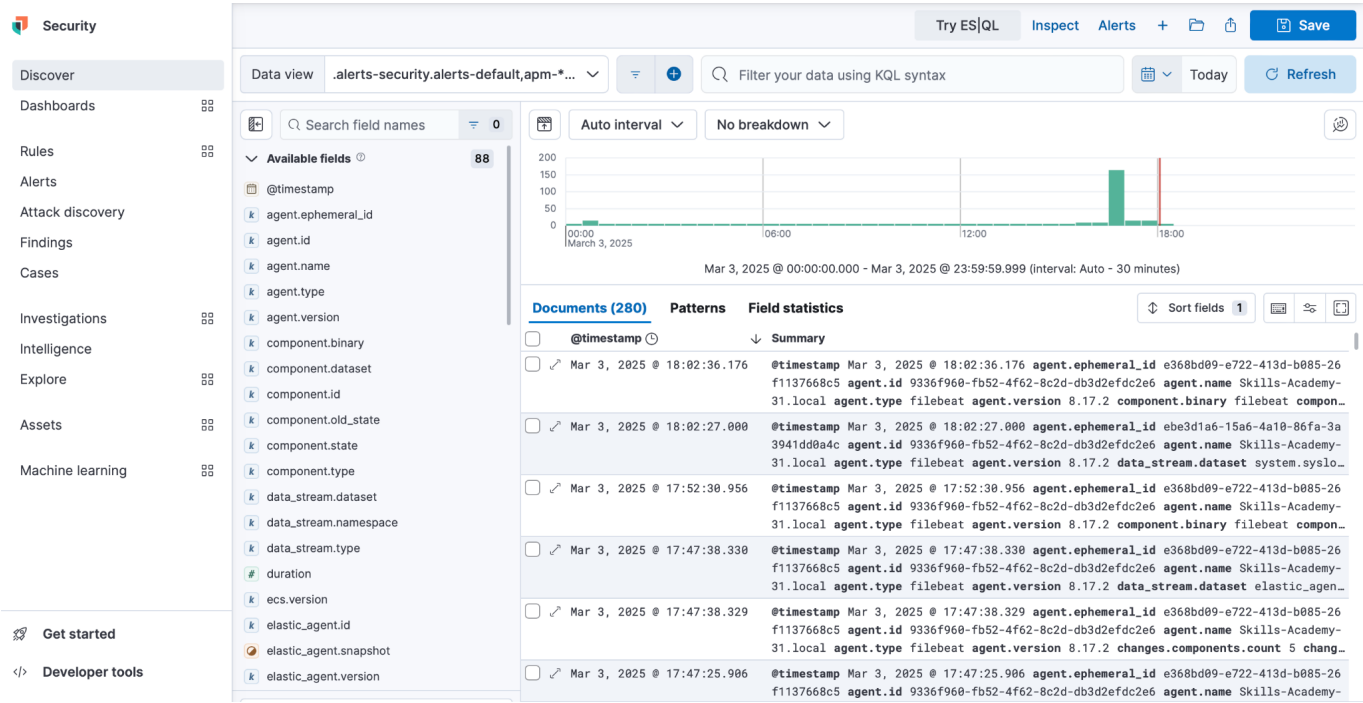
Detailed Incident Handling Steps

Malware detected by Elastic Endgame with critical severity and risk score 99.

SOC Operations Documentation Report



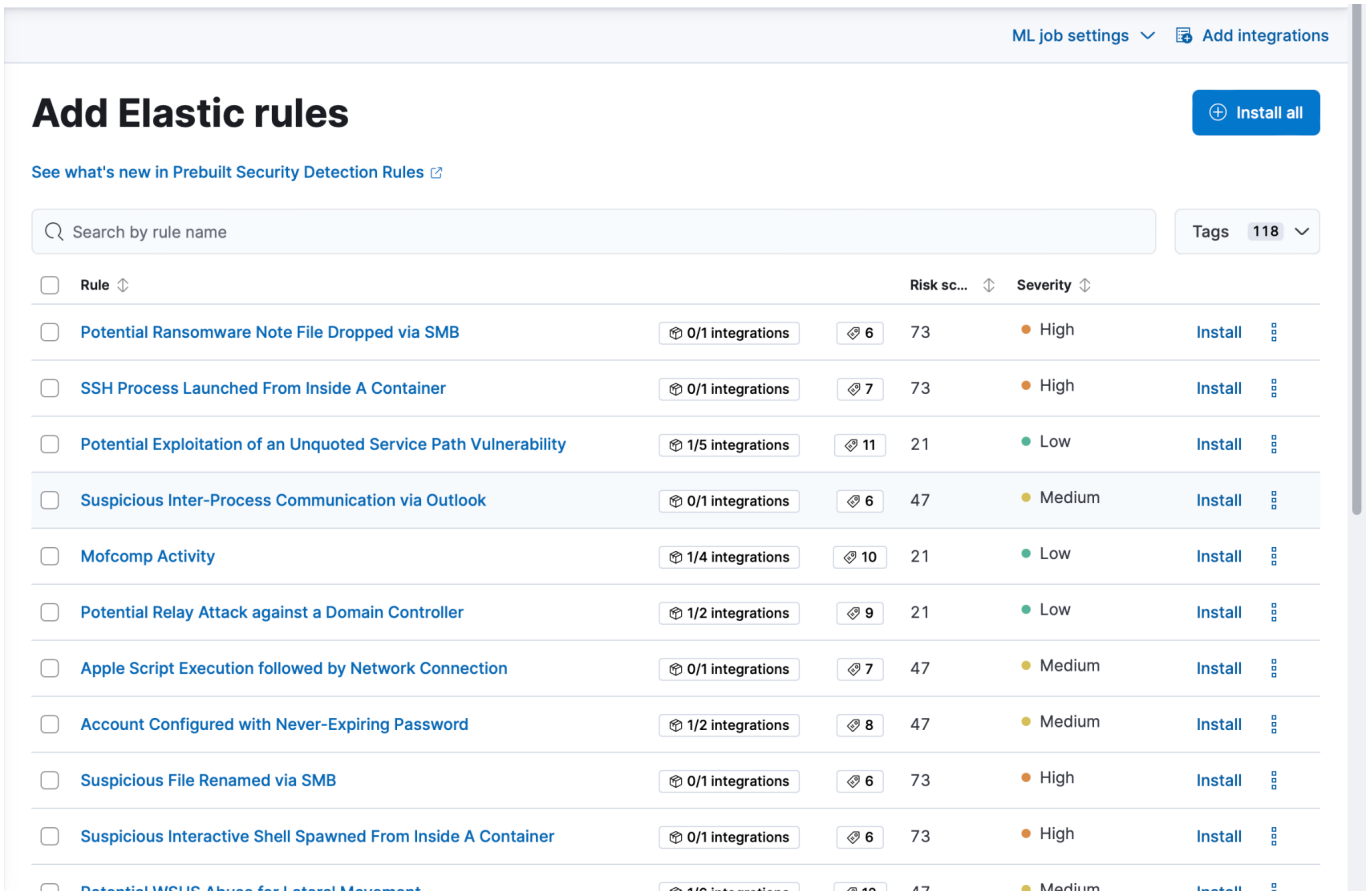
Log investigation performed through Discover view, analyzing correlated events.



Elastic Rules Overview

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

SOC Operations Documentation Report



Conclusion

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