SIEM IGURATION

ABSTRACT

This report provides an overview of configuring ELK (Elastic SIEM) to detect and analyze malware threats. It covers the setup process, integration of essential data sources, and the creation of custom rules for identifying malicious activities. The goal is to enhance real-time threat detection and response capabilities.

What is SIEM ?

A Security Information and Event Management (SIEM) solution is a software tool used by organizations to collect, analyze, and monitor security data from various sources such as firewalls, antivirus systems, servers, and applications. SIEM systems provide real-time threat detection by correlating security events and logs, identifying anomalies, and generating alerts based on predefined rules. They also assist in incident response and compliance reporting, helping organizations detect security incidents and mitigate potential threats more effectively.

How SIEM correlate with EDR, windows & linux logs ?

SIEM solutions correlate data from **Endpoint Detection and Response (EDR)** systems and **Windows/Linux logs** to provide comprehensive security monitoring and threat detection. Here's how they work together:

1. **Data Collection**:
    - SIEM collects logs from various sources, including EDR systems and operating systems like Windows and Linux. EDR provides detailed endpoint-level data on potential threats, such as malware infections, suspicious file executions, or lateral movement.
    - Windows logs (e.g., Event Viewer) and Linux logs (e.g., syslog) capture important system and security events, like user logins, file access, and system changes.
2. **Log Normalization**:
    - SIEM normalizes and categorizes logs from EDR and operating systems into a common format. This helps ensure that different types of logs are consistent and comparable for analysis.
3. **Correlation**:
    - The SIEM uses **correlation rules** to link related events from different sources, such as EDR alerts and OS logs. For example, an EDR alert about a suspicious process may be correlated with a Windows event log showing a login attempt or Linux logs showing unauthorized access.

- This multi-source correlation allows the SIEM to detect complex attacks or suspicious behaviors that might not be evident from a single source alone.

4. **Threat Detection & Response**:
    - By correlating EDR and OS logs, SIEM can detect patterns of malicious activity across the environment. For example, if an EDR detects a malware infection, SIEM can also review associated Windows or Linux logs for additional context, like lateral movement or privilege escalation attempts.
    - Based on these correlations, SIEM can generate actionable alerts for security teams to investigate and respond to.
5. **Incident Analysis**:
    - When investigating incidents, security analysts can use SIEM to review logs from both EDR and OS systems in a centralized dashboard, helping them understand the full scope of the attack and respond accordingly.

SIEM Products

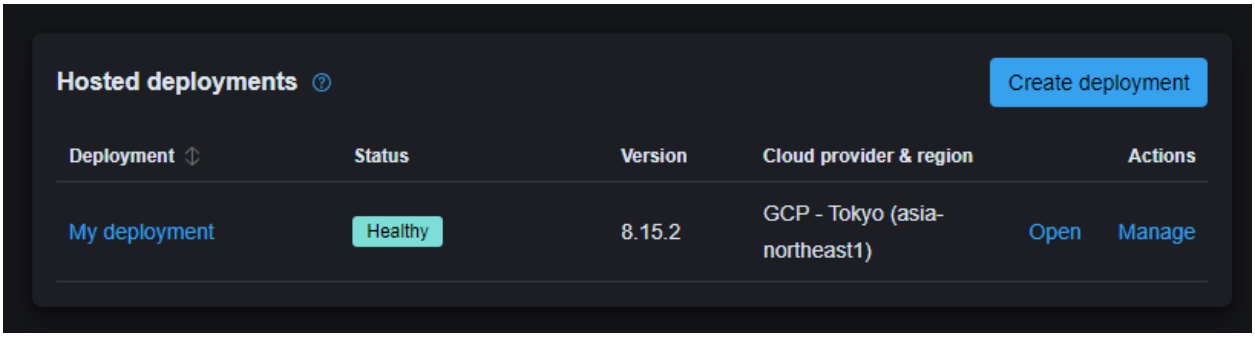
There are many SIEM products available in the market, each offering unique features, scalability, and integration capabilities EX: Splunk , IBM QRadar , ELK (Elastic) and Sophos .

We selected Elastic SIEM due to its cloud-based nature, which doesn't need local storage and high-performance hardware, unlike IBM QRadar. Additionally, Elastic SIEM's architecture is already pre-configured, saving us the hassle of building clusters and indices,required by Splunk SIEM. This makes Elastic SIEM the optimal choice for our needs.

Elk Configuration

1) Deployment of SIEM on cloud :

We deployed a SIEM on GCP (Google Cloud Provider) and chosen Tokyo to be the region of deployment .

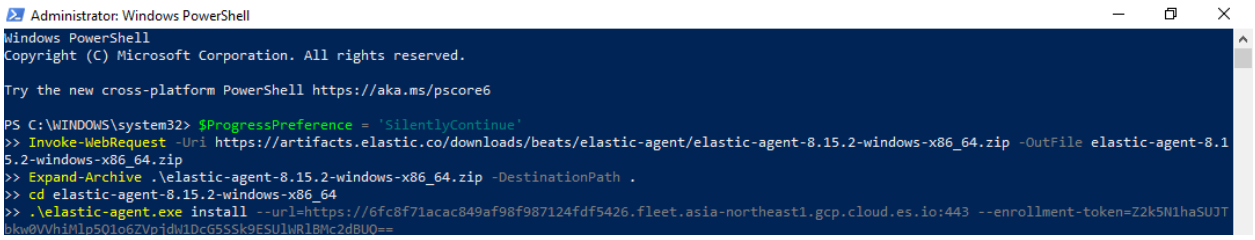


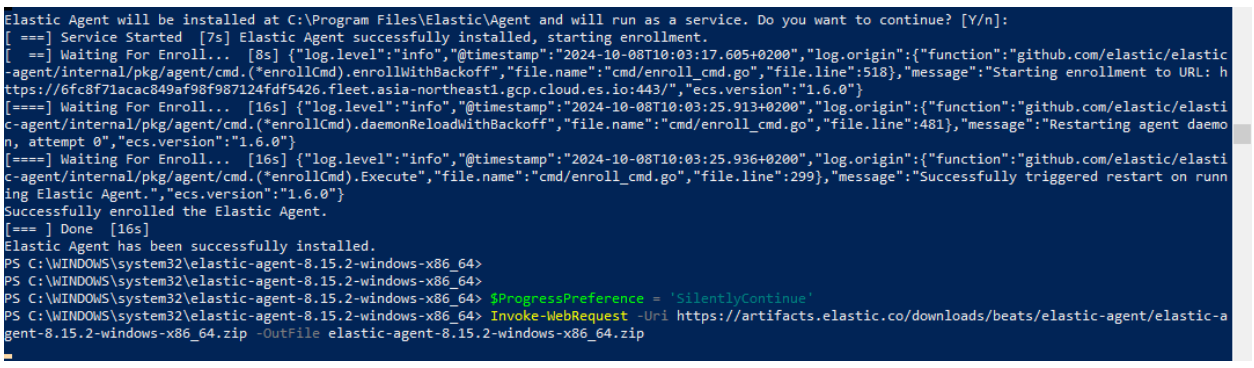
2) Connect End Points to SIEM :

Connecting devices to the SIEM by installing an ELK agent on the End Points .

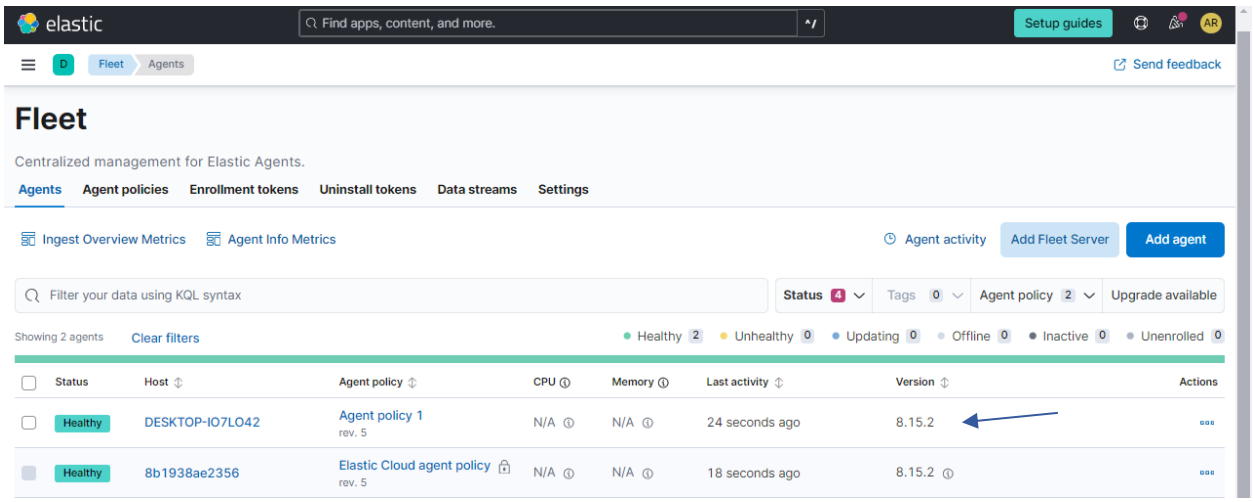
Windows OS devices :

go to fleet page and press add agent copy windows command and paste it in power shell as an administrator .





After that the device will appear on the SIEM .



The next step is to download SYSMON (is a system monitoring tool for Windows that provides detailed event logging for processes, network connections, and system changes.)

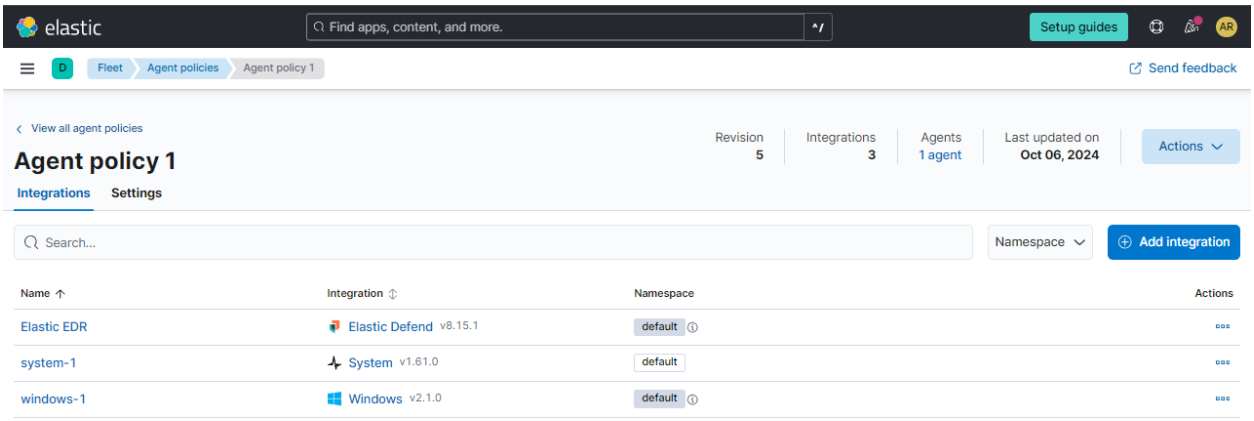
After downloading Sysmon we need to add some integration to the agent policies at the end point device .

1) **Elastic Defend (EDR) :** Elastic Defend provides organizations with prevention, detection, and response capabilities with deep visibility for EPP, EDR, SIEM, and Security Analytics use cases across Windows, macOS, and Linux operating systems running on both traditional endpoints and public cloud environments. Use Elastic Defend to:

   Prevent complex attacks - Prevent malware (Windows, macOS, Linux) and ransomware (Windows) from executing, and stop advanced threats with malicious behavior (Windows, macOS, Linux), memory threat (Windows, macOS, Linux), and credential hardening (Windows) protections. All powered by Elastic Labs and our global community.
   Alert in high fidelity - Bolster team efficacy by detecting threats centrally and minimizing false positives via extensive corroboration.
   Detect threats in high fidelity - Elastic Defend facilitates deep visibility by instrumenting the process, file, and network data in your environments with minimal data collection overhead.

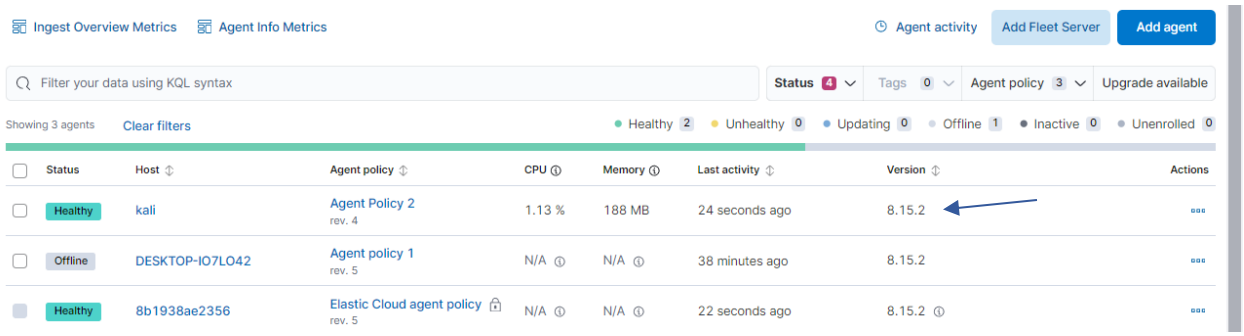
2) **System Integration :** The System integration allows you to monitor servers, personal computers,Use the System integration to collect metrics and logs machines. Then visualize that data in Kibana, create alerts to notify if something goes wrong, and reference data when troubleshooting an issue.

3) **Windows Integration :** to collect metrics and logs from your machine. Then visualize that data in Kibana, create alerts to notify you if something goes wrong, and reference data when troubleshooting an issue.

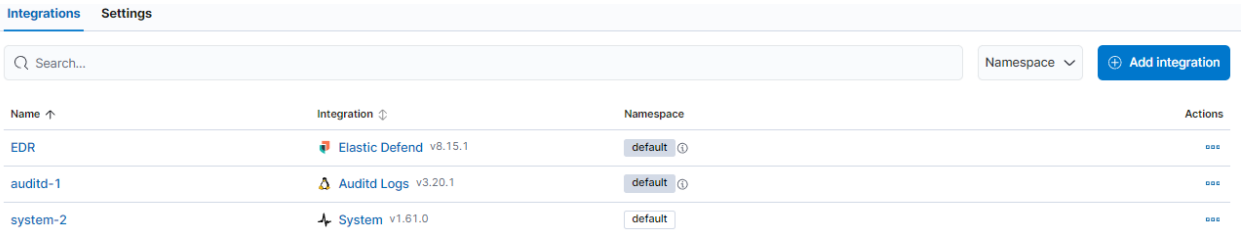


Adding Linux OS device :

Adding linux device by running this command on Terminal .



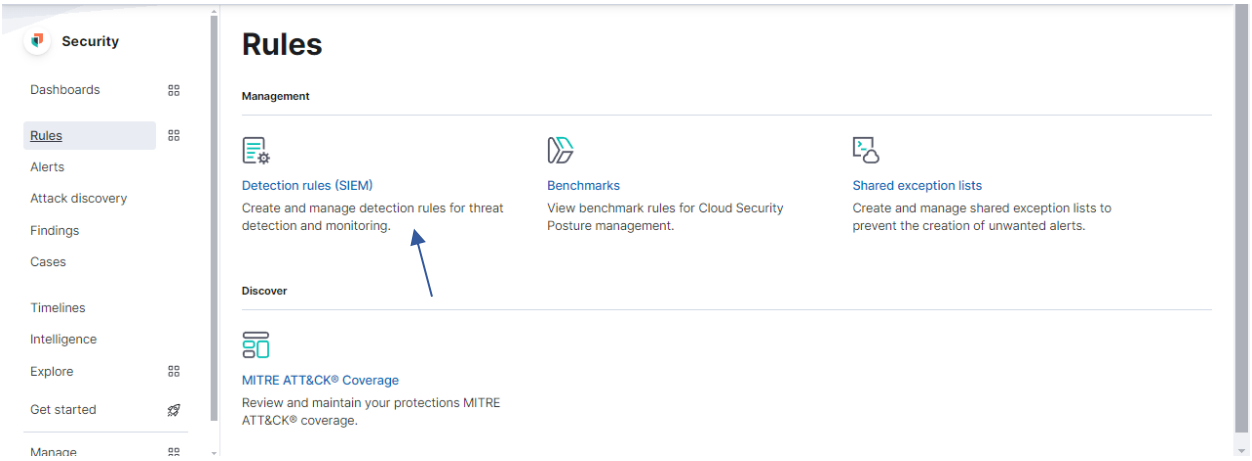
After that add integrations to Agent Policies :



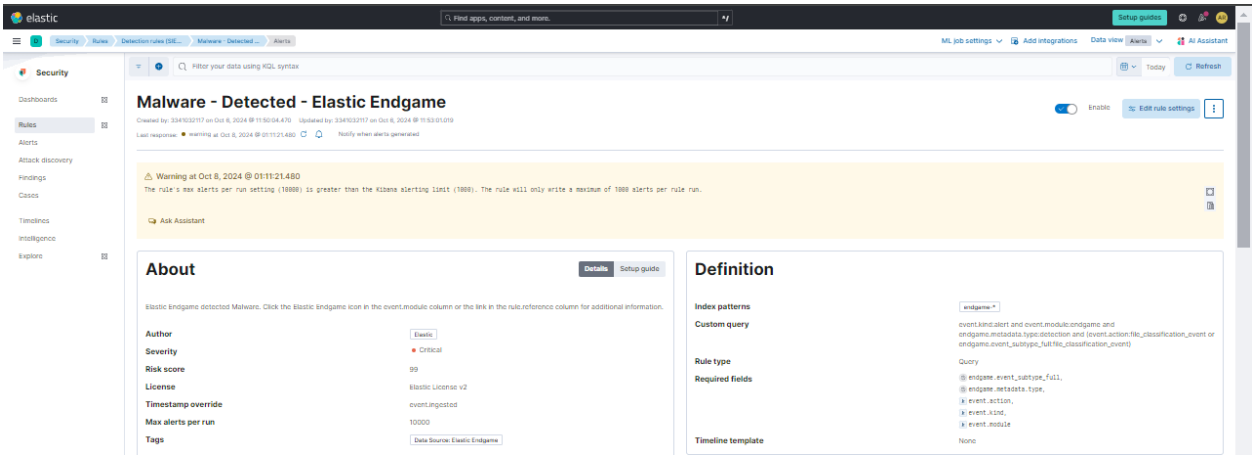
- The Auditd Logs integration collects and parses logs from the audit daemon
- Also add Journalctl (journalctl is a command-line utility used on Linux systems to view and query the systemd journal. The systemd journal is a logging system that collects and manages system logs, service logs, kernel messages, and other relevant events on the system.)

Setting Rules

From Security page click on Rules after that Detection rules SIEM



After that adding a Malware Detection Rule

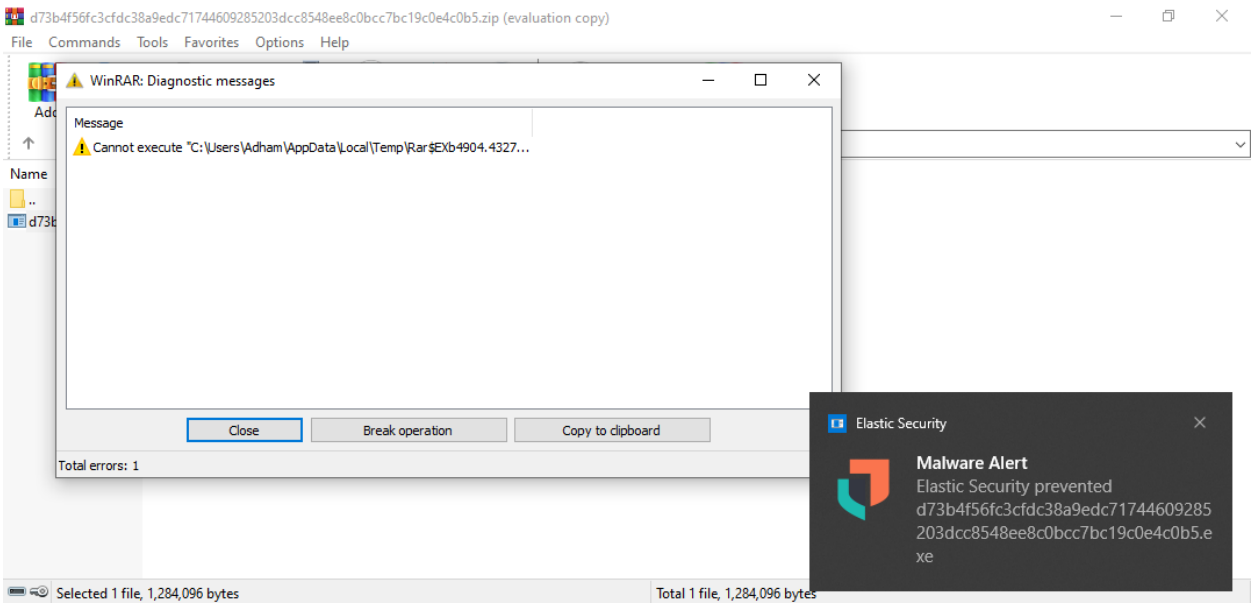


Malware Download & Detection

Download a malware sample from malware bazzar on a device.

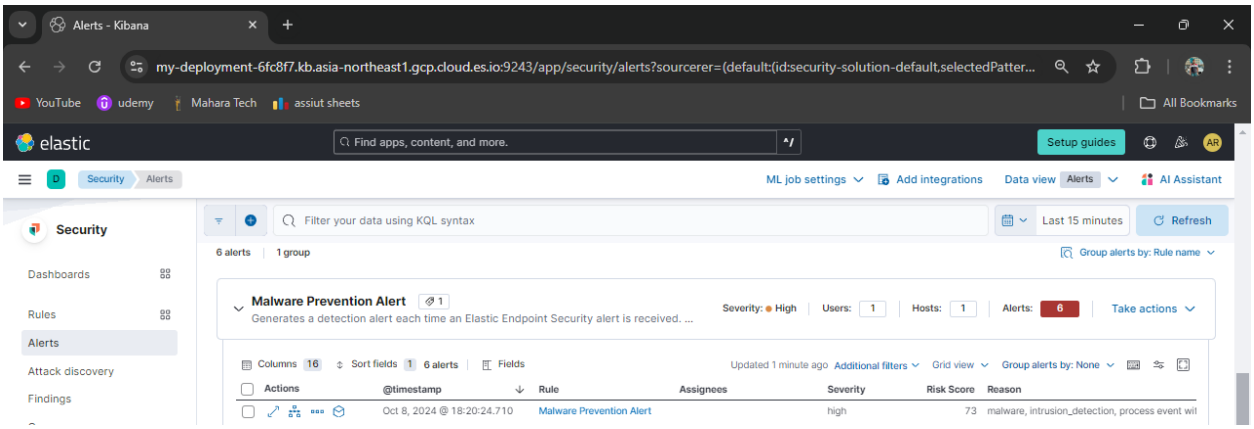
Malware reference on malware bazzar : https://bazaar.abuse.ch/sample/d73b4f56fc3cfdc38a9edc71744609285203dcc8548ee8c0bcc7bc19c0e4c0b5/

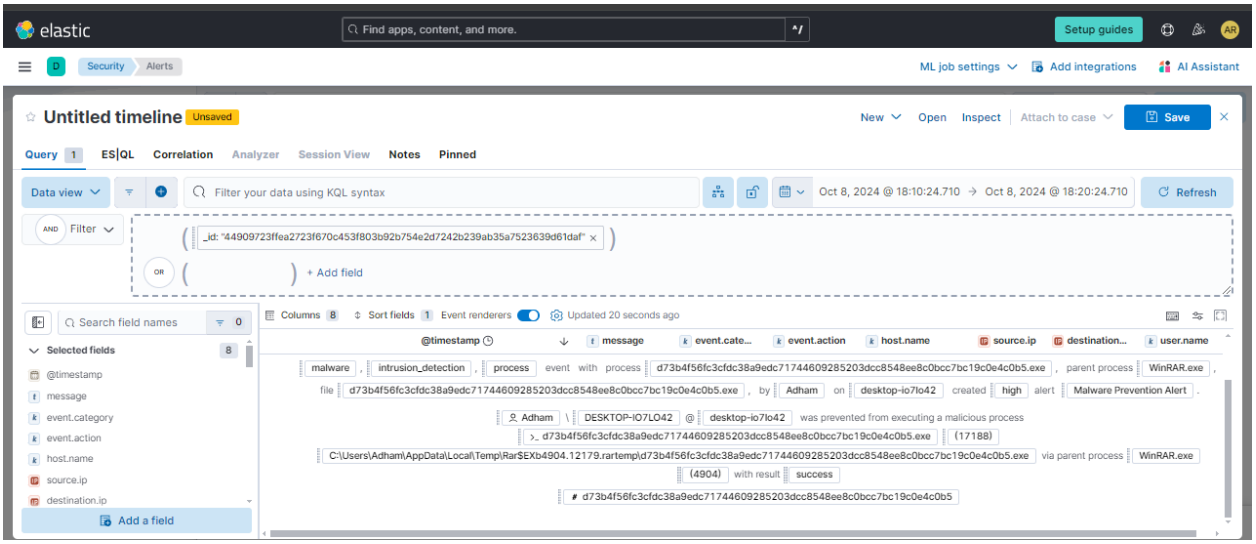
EDR Prevented the malware and send the process logs to SIEM an alert Fired .

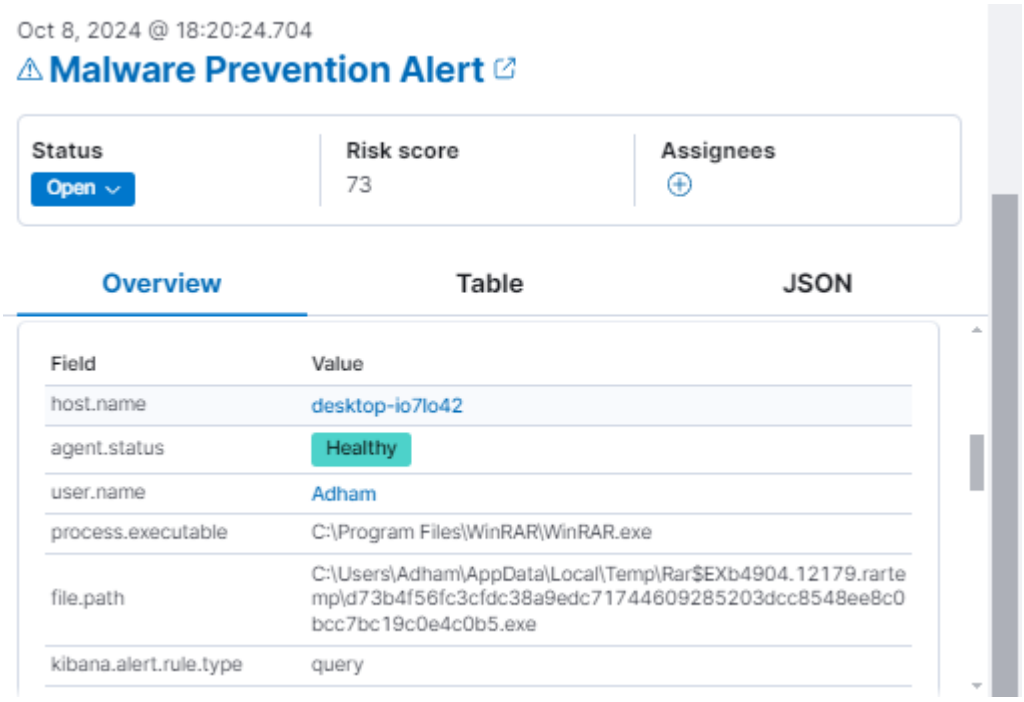


Process Logs :

SIEM Alerts:






Oct 8, 2024 @ 18:20:24.704
Malware Prevention Alert
Status
Open
Risk score
73
Assignees
Overview
Table
JSON
Field
Value
host.name
desktop-io7lo42
agent.status
Healthy
user.name
Adham
process.executable
C:\Program Files\WinRAR\WinRAR.exe
file.path
C:\Users\Adham\AppData\Local\Temp\Rar$EXb4904.12179.rartemp\d73b4f56fc3cfdc38a9edc71744609285203dcc8548ee8c0bcc7bc19c0e4c0b5.exe
kibana.alert.rule.type
query


Overview
Table
JSON
file.name
d73b4f56fc3cfdc38a9edc71744609285203dcc8548ee8c0bcc7bc19c0e4c0b5.exe
file.hash.sha256
d73b4f56fc3cfdc38a9edc71744609285203dcc8548ee8c0bcc7bc19c0e4c0b5
file.directory
C:\Users\Adham\AppData\Local\Temp\Rar$EXb4904.12179.rartemp
process.name
WinRAR.exe
quarantined.path
C:\.equarantine\c019041d-7f29-46d8-8b59-b0e47a59aef7