

Building a SIEM in My Home Lab with Elastic

A Personal Project in Configuring a SIEM for Network Monitoring and Security by Miguel K.

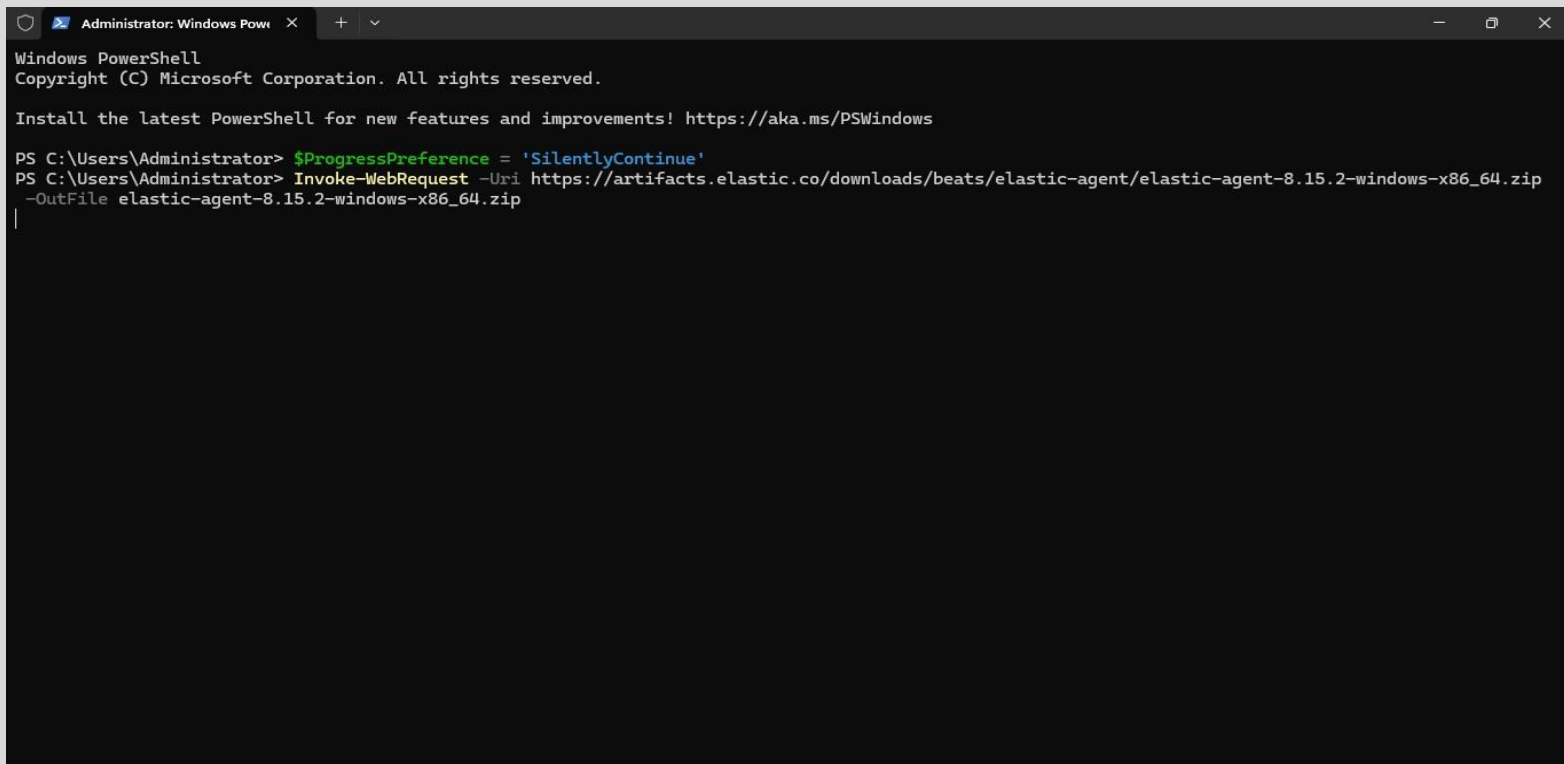
Configuring Elastic SIEM for Network Security Monitoring

In this project, I configured Elastic Defender through the Windows terminal on my local device, creating a secure conduit within my home lab to send logs to the cloud. These logs are then accessible in my SIEM instance, where I can analyze thousands of events.

To demonstrate a practical use case, I created a rule that sends me an email alert whenever an Nmap scan is performed on my IP address. I successfully tested this by running an Nmap scan, and the SIEM sent the expected email alert, confirming that the rule was functioning as intended. This exemplifies how a SIEM can be effectively leveraged to enhance network protection.

The screenshot shows the Elastic Cloud console interface. At the top, there's a navigation bar with the Elastic logo, a search bar, and links for 'Setup guides' and 'Endpoints & API keys'. Below this is a sidebar with a 'Manage this deployment' header and a list of navigation items: Home, Analytics (with a dropdown arrow), Discover, Dashboards, Canvas, Maps, Machine Learning, Graph, Visualize Library, Search (with a dropdown arrow), and Overview. A red arrow points to the 'Add integrations' button at the bottom of the sidebar. The main content area features a large banner titled 'Improve search relevance with AI' with three icons: a blue arrow, a line graph, and a laptop. Below the banner, text describes building AI search-powered applications using the Elastic platform, including the ELSER model. A section titled 'Semantic search with ELSER' is partially visible at the bottom.

I accessed Elastic Cloud [here](#) to obtain the software necessary to build out the SIEM.

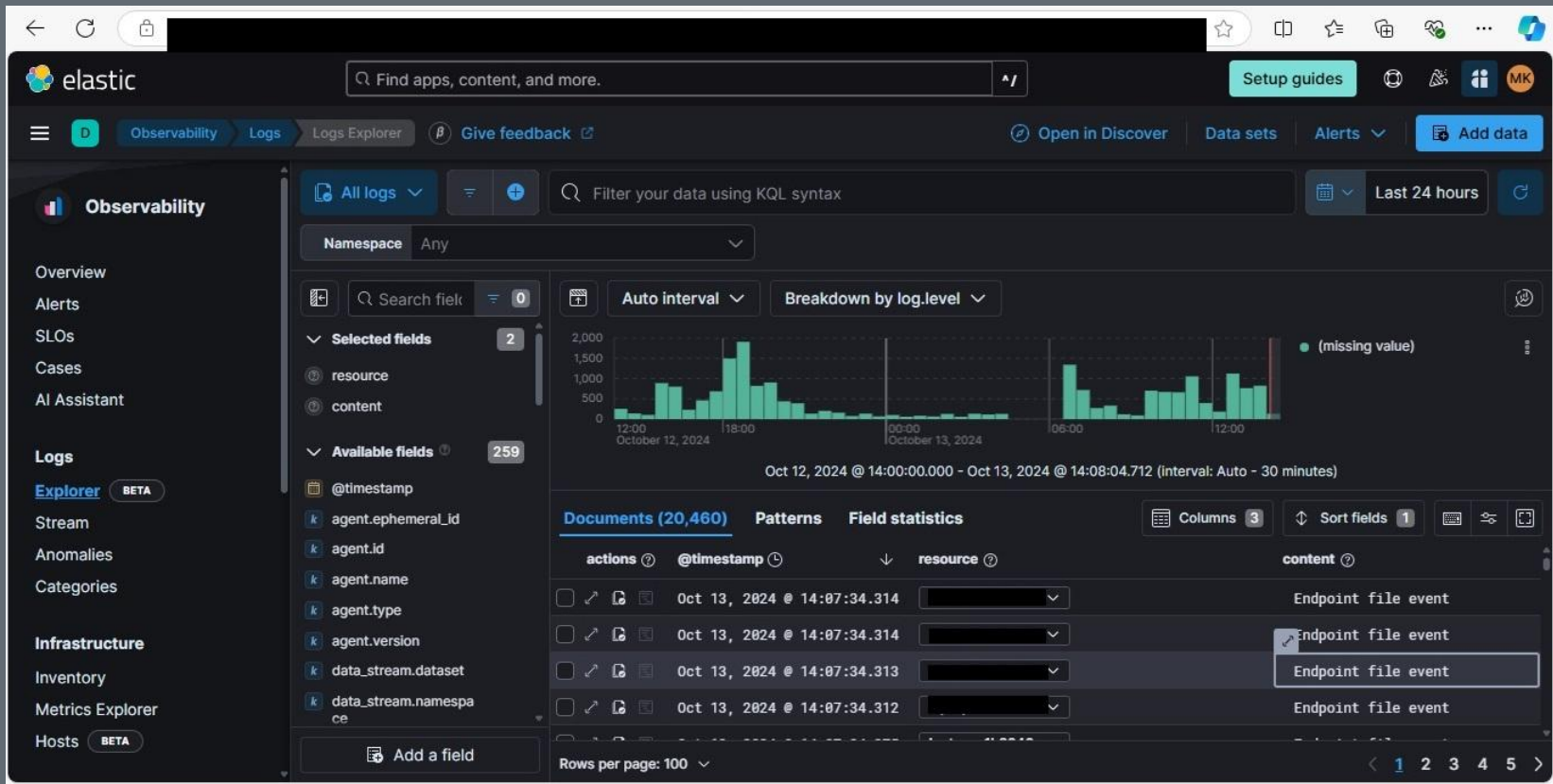


```
Administrator: Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\Administrator> $ProgressPreference = 'SilentlyContinue'
PS C:\Users\Administrator> Invoke-WebRequest -Uri https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.15.2-windows-x86_64.zip
-OutFile elastic-agent-8.15.2-windows-x86_64.zip
```

After adding the Elastic Defender integration, I configured Elastic to run on Windows by executing the command displayed in the image.



After configuration, the SIEM has begun collecting data. I can now utilize queries to search for specific information and sort and filter results according to my preferences.

The screenshot displays the Elastic Security console's 'Create new rule' page. The left sidebar contains navigation links for Dashboards, Rules, Alerts, Attack discovery, Findings, Cases, Timelines, Intelligence, Explore, Get started, and Manage. The main content area is titled 'Create new rule' and features a 'Rule preview' button. Under the '1 Define rule' section, six rule types are presented in a grid:

- Custom query** (circled in red): Use KQL or Lucene to detect issues across indices. A green 'Selected' button is at the bottom.
- Machine Learning**: Select ML job to detect anomalous activity. A 'Select' button is at the bottom.
- Threshold**: Aggregate query results to detect when number of matches exceeds threshold. A 'Select' button is at the bottom.
- Event Correlation**: Use Event Query Language (EQL) to match events, generate sequences, and stack data. A 'Select' button is at the bottom.
- Indicator Match**: Use indicators from intelligence sources to detect matching events and alerts. A 'Select' button is at the bottom.
- New Terms**: Find documents with values appearing for the first time. A 'Select' button is at the bottom.

At the bottom of the grid is an 'ESQL' section. On the right, the 'Rule preview' section explains that the preview reflects the current configuration and includes a 'Select a preview timeframe' dropdown set to 'Last 1 hour' and a 'Refresh' button. The bottom status bar shows '+ Untitled timeline' and 'Unsaved'.

I created a custom rule to illustrate how a SIEM can generate alerts in response to specified events.

The screenshot displays the Elastic Security console interface. The left sidebar shows the navigation menu with 'Security' selected. The main content area is titled 'Nmap Scan Detected' and includes a table with rule details, a definition section, and an actions section.

Property	Value
Severity	High
Risk score	73
Max alerts per run	100

Definition

Index patterns: `apm-* transaction*`, `auditbeat-*`, `endgame-*`, `elastic-*`, `logs-*`, `packetbeat-*`, `traces-apm*`, `windowsbeat-*`, `*elastic-cloud-logs*`

Custom query (circled in red): `process.args:"nmap"`

Rule type: Query

Timeline template: None

Schedule

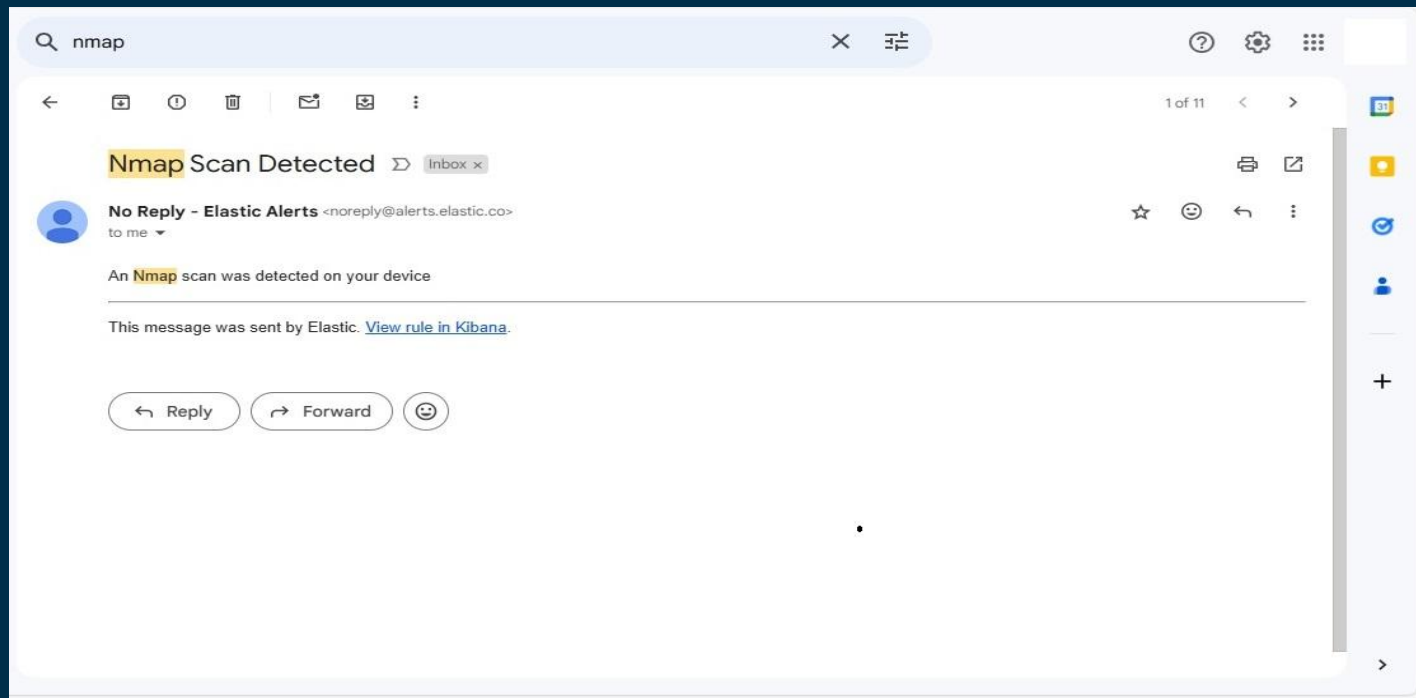
Runs every: 5m

Additional look-back time: 1m

Actions

Notification actions (circled in red): Elastic-Cloud-SMTP (Summary of alerts. Per rule run.)

I developed a custom query using `process.args: "nmap"`, designed to detect any logs associated with "nmap" on the system. Additionally, I configured the alert to be sent to my email whenever Nmap activity is detected.



After executing an Nmap scan on the system, I received an alert from the SIEM in accordance with the established rules. This successful alerting process highlights the effectiveness of the SIEM in monitoring and responding to network activities.

In conclusion, this project demonstrates how SIEMs serve as powerful tools for enhancing security monitoring by aggregating and analyzing log data to detect and respond to potential threats in real time.