



SIEM CONFIGURATION

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 .

Hosted deployments ⓘ					Create deployment
Deployment ⓘ	Status	Version	Cloud provider & region	Actions	
My deployment	Healthy	8.15.2	GCP - Tokyo (asia-northeast1)	Open	Manage

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 .

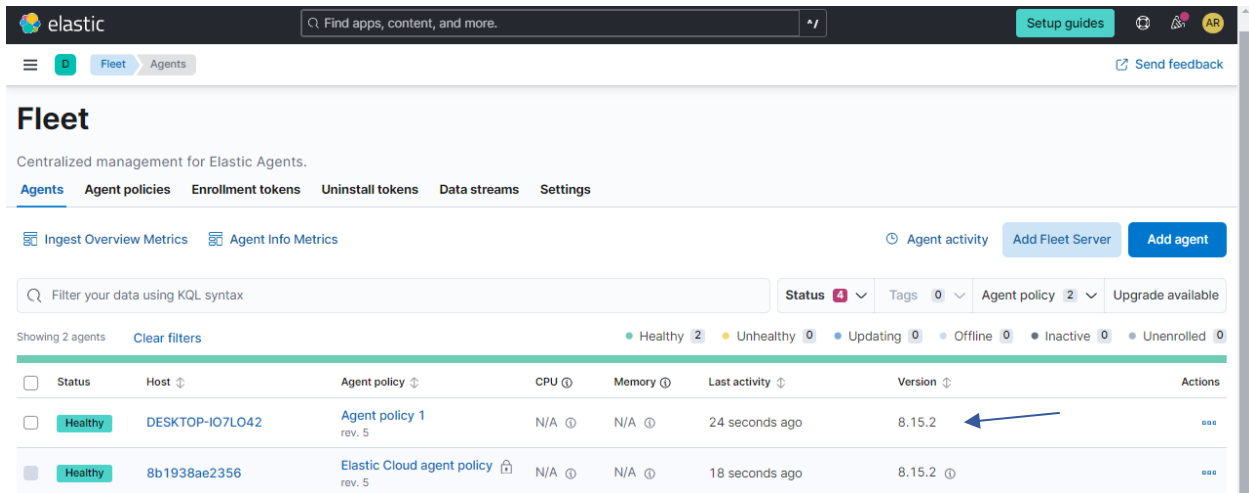
```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\WINDOWS\system32> $ProgressPreference = 'SilentlyContinue'
>> 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
>> Expand-Archive .\elastic-agent-8.15.2-windows-x86_64.zip -DestinationPath .
>> cd elastic-agent-8.15.2-windows-x86_64
>> .\elastic-agent.exe install --url=https://6fc8f71acac849af98f987124fdf5426.fleet.asia-northeast1.gcp.cloud.es.io:443 --enrollment-token=Z2k5N1haSUJTbk9vVh1Mlp501o6ZVp1dW1DcG5SSk9ESU1WR1BMc2dBUQ==
```

```
Elastic Agent will be installed at C:\Program Files\Elastic\Agent and will run as a service. Do you want to continue? [Y/n]:
[ === ] Service Started [7s] Elastic Agent successfully installed, starting enrollment.
[ == ] Waiting For Enroll... [8s] {"log.level":"info","@timestamp":"2024-10-08T10:03:17.605+0200","log.origin":{"function":"github.com/elastic/elastic-agent/internal/pkg/agent/cmd.(*enrollCmd).enrollWithBackoff","file.name":"cmd/enroll_cmd.go","file.line":518},"message":"Starting enrollment to URL: https://6fc8f71acac849af98f987124fdf5426.fleet.asia-northeast1.gcp.cloud.es.io:443/","ecs.version":"1.6.0"}
[====] Waiting For Enroll... [16s] {"log.level":"info","@timestamp":"2024-10-08T10:03:25.913+0200","log.origin":{"function":"github.com/elastic/elastic-agent/internal/pkg/agent/cmd.(*enrollCmd).daemonReloadWithBackoff","file.name":"cmd/enroll_cmd.go","file.line":481},"message":"Restarting agent daemon, attempt 0","ecs.version":"1.6.0"}
[====] Waiting For Enroll... [16s] {"log.level":"info","@timestamp":"2024-10-08T10:03:25.936+0200","log.origin":{"function":"github.com/elastic/elastic-agent/internal/pkg/agent/cmd.(*enrollCmd).Execute","file.name":"cmd/enroll_cmd.go","file.line":299},"message":"Successfully triggered restart on running Elastic Agent.","ecs.version":"1.6.0"}
Successfully enrolled the Elastic Agent.
[=== ] Done [16s]
Elastic Agent has been successfully installed.
PS C:\WINDOWS\system32> elastic-agent-8.15.2-windows-x86_64
PS C:\WINDOWS\system32> elastic-agent-8.15.2-windows-x86_64
PS C:\WINDOWS\system32> elastic-agent-8.15.2-windows-x86_64 $ProgressPreference = 'SilentlyContinue'
PS C:\WINDOWS\system32> elastic-agent-8.15.2-windows-x86_64 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 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.

The screenshot shows the Elastic Agent policy management interface. At the top, there's a search bar and navigation tabs for 'Fleet', 'Agent policies', and 'Agent policy 1'. Below this, a summary bar for 'Agent policy 1' shows 'Revision 5', 'Integrations 3', 'Agents 1 agent', and 'Last updated on Oct 06, 2024'. The 'Integrations' tab is active, displaying a table of installed integrations:

Name	Integration	Namespace	Actions
Elastic EDR	Elastic Defend v8.15.1	default	...
system-1	System v1.61.0	default	...
windows-1	Windows v2.1.0	default	...

Adding Linux OS device :

Adding linux device by running this command on Terminal .

```
(root@kali)~# curl -L -O https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.15.2-linux-x86_64.tar.gz
tar xzvf elastic-agent-8.15.2-linux-x86_64.tar.gz
cd elastic-agent-8.15.2-linux-x86_64
sudo ./elastic-agent install --url=https://6fc8f71acac849af98f987124fdf5426.fleet.asia-northeast1.gcp.cloud.es.io:443 --enrollment-token=bkRUSWFKSUJTbkW0VVhiMlgxWTK6WG5FQkt1cEdReDZkaWt4SWw1ZjRyZW==
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload   Total   Spent    Left   Speed
100 299M  100 299M    0     0  2200k      0  0:02:19  0:02:19 --:--:-- 2520k
elastic-agent-8.15.2-linux-x86_64/NOTICE.txt
elastic-agent-8.15.2-linux-x86_64/LICENSE.txt
```

The screenshot shows the Elastic Agent activity monitoring interface. It includes a search bar, filters for 'Status' (4), 'Tags' (0), 'Agent policy' (3), and 'Upgrade available'. A summary bar shows 'Showing 3 agents' with status counts: Healthy (2), Unhealthy (0), Updating (0), Offline (1), Inactive (0), and Unenrolled (0). The main table lists the agents:

Status	Host	Agent policy	CPU	Memory	Last activity	Version	Actions
Healthy	kali	Agent Policy 2 rev. 4	1.13 %	188 MB	24 seconds ago	8.15.2	...
Offline	DESKTOP-IO7LO42	Agent policy 1 rev. 5	N/A	N/A	38 minutes ago	8.15.2	...
Healthy	8b1938ae2356	Elastic Cloud agent policy rev. 5	N/A	N/A	22 seconds ago	8.15.2	...

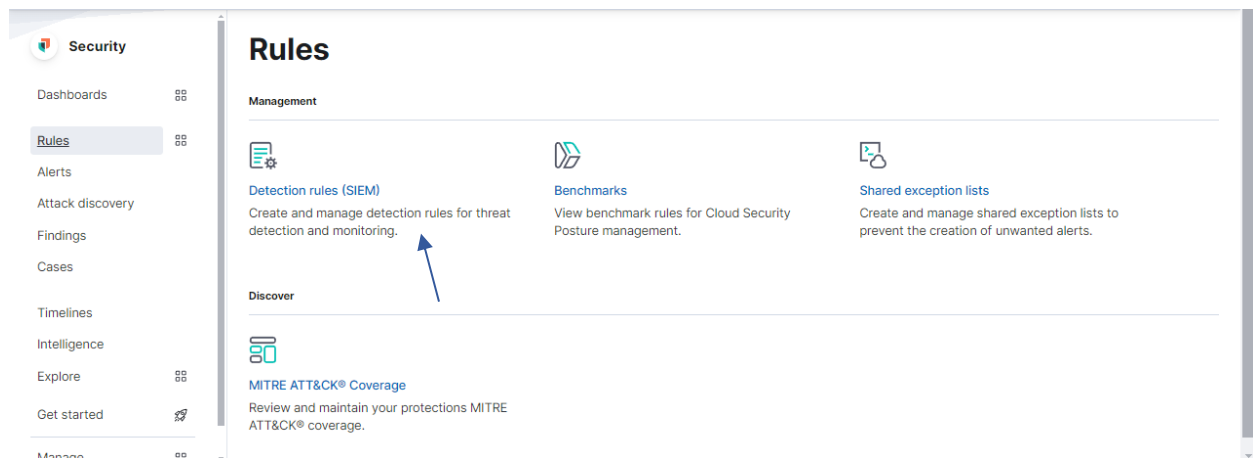
After that add integrations to Agent Policies :

Integrations Settings			
<input type="text" value="Search..."/>			Namespace ▼ ➕ Add integration
Name ↑	Integration ⬇	Namespace	Actions
EDR	Elastic Defend v8.15.1	default ⓘ	⋮
auditd-1	Auditd Logs v3.20.1	default ⓘ	⋮
system-2	System v1.61.0	default	⋮

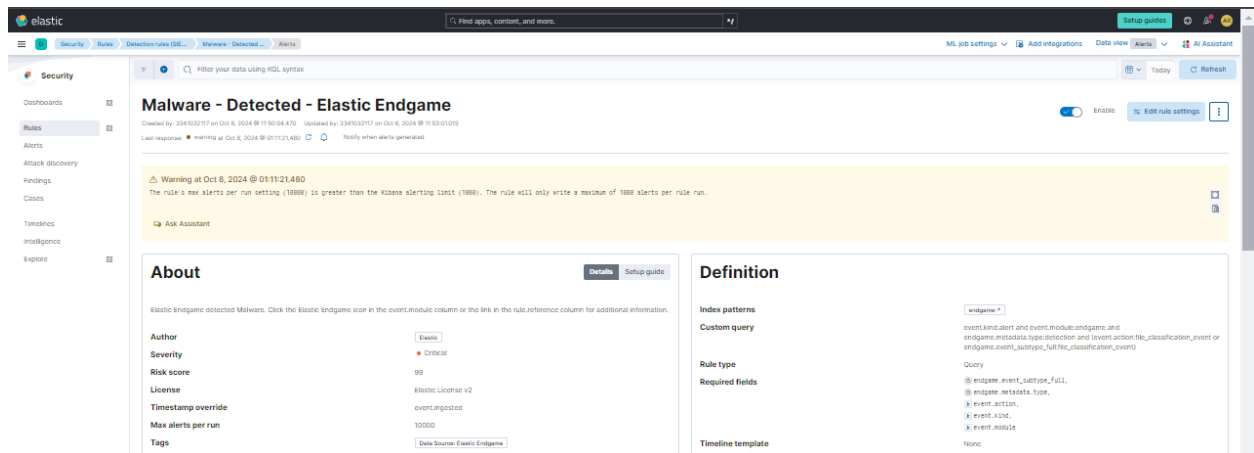
- The Auditd Logs integration collects and parses logs from the audit daemon
- Also add Journalctl (journalctl is a command-line utility used on Linux systems to view and query the systemd journal. The systemd journal is a logging system that collects and manages system logs, service logs, kernel messages,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



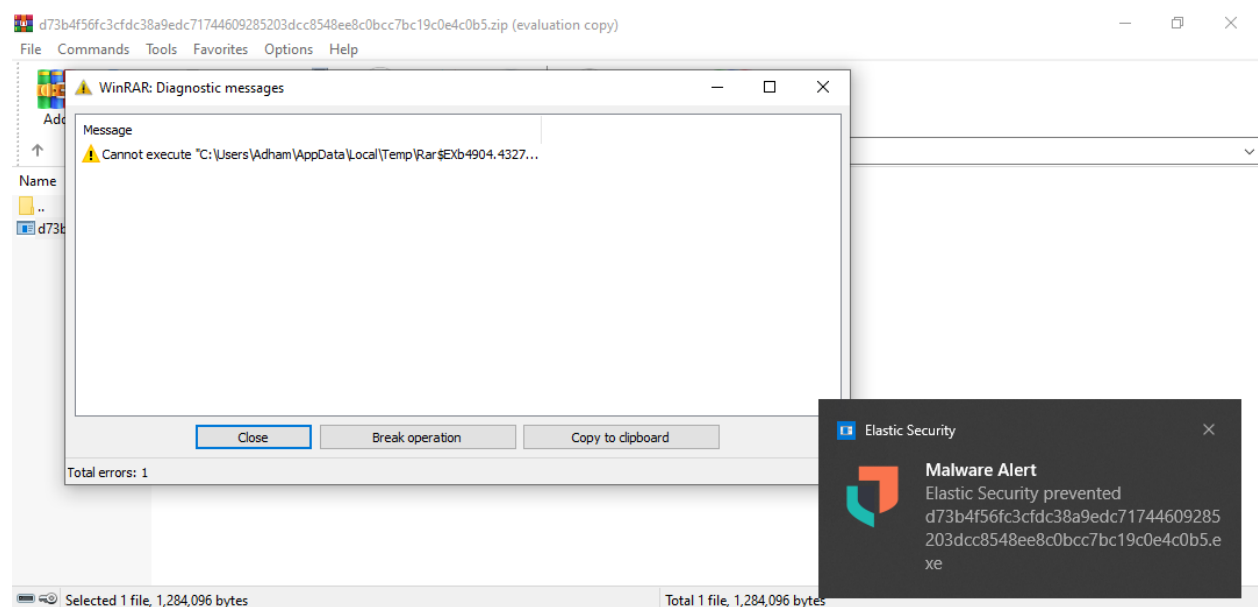
Malware Download & Detection

Download a malware sample from malware bazaar on a device.

Malware reference on malware bazaar :

<https://bazaar.abuse.ch/sample/d73b4f56fc3cfdc38a9edc71744609285203dcc8548ee8c0bcc7bc19c0e4c0b5/>

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



Process Logs :

✓	<input type="checkbox"/>	Oct 8, 2024 @ 18:20:24.710	file.hash.sha256 873b4f56fc3fdc38a9edc71744609285203dcc8548ee8c0bcc7bc19c0e4c0b5 process.hash.sha256 873b4f56fc3fdc38a9edc71744609285203dcc8548ee8c0bcc7bc19c0e4c0b5 @timestamp Oct 8, 2024 @ 18:20:24.710 agent.build.original version: 8.15.2, compiled: Tue Sep 17 23:08:08 2024, branch: HEAD, commit: b4d61a7079c66492513f98f541621f2ec028a46d agent.id 9d57128e-764e-4132-b1ca-5f29af6079e agent.type endpoint agent.version 8.15.2 data_stream.dataset endpoint.alerts data_stream.namespace default data_stream.type logs ecs.version 8.10...
✓	<input type="checkbox"/>	Oct 8, 2024 @ 18:20:24.704	file.hash.sha256 873b4f56fc3fdc38a9edc71744609285203dcc8548ee8c0bcc7bc19c0e4c0b5 @timestamp Oct 8, 2024 @ 18:20:24.704 agent.build.original version: 8.15.2, compiled: Tue Sep 17 23:08:08 2024, branch: HEAD, commit: b4d61a7079c66492513f98f541621f2ec028a46d agent.id 9d57128e-764e-4132-b1ca-5f29af6079e agent.type endpoint agent.version 8.15.2 data_stream.dataset endpoint.alerts data_stream.namespace default data_stream.type logs ecs.version 8.10.0 elastic.agent.id 9d57128e-764e-4132-b1ca-5f29af6079e...

SIEM Alerts:

The screenshot shows the Elastic Security Alerts page. The left sidebar contains navigation links for Dashboards, Rules, Alerts, Attack discovery, and Findings. The main content area displays a 'Malware Prevention Alert' with a severity of High. The alert details include: Generates a detection alert each time an Elastic Endpoint Security alert is received. The alert is associated with 1 user, 1 host, and 6 alerts. A table below the alert shows the following data:

Columns	Sort fields	6 alerts	Fields
Actions	@timestamp	Rule	Assignees
	Oct 8, 2024 @ 18:20:24.710	Malware Prevention Alert	Severity
			Risk Score
			Reason

The screenshot shows the Elastic Security Timeline view. The left sidebar contains navigation links for Query, ES|QL, Correlation, Analyzer, Session View, Notes, and Pinned. The main content area displays a timeline of events. The timeline is filtered by the query: (_id: "44909723f6e2723f670c453f803b92b754e2d7242b239ab35a7523639d61daf" x). The timeline shows a sequence of events related to a malware detection. The events are as follows:

- Event 1: malware, intrusion_detection, process event with process [d73b4f56fc3fdc38a9edc71744609285203dcc8548ee8c0bcc7bc19c0e4c0b5.exe], parent process [WinRAR.exe], file [d73b4f56fc3fdc38a9edc71744609285203dcc8548ee8c0bcc7bc19c0e4c0b5.exe], by [Adham] on [desktop-io7lo42] created [high] alert [Malware Prevention Alert].
- Event 2: [Adham] \ [DESKTOP-IO7LO42] @ [desktop-io7lo42] was prevented from executing a malicious process [d73b4f56fc3fdc38a9edc71744609285203dcc8548ee8c0bcc7bc19c0e4c0b5.exe] (17188).
- Event 3: [C:\Users\Adham\AppData\Local\Temp\Rar\$EXB4904.121717.rartemp\d73b4f56fc3fdc38a9edc71744609285203dcc8548ee8c0bcc7bc19c0e4c0b5.exe] via parent process [WinRAR.exe] (4904) with result [success].
- Event 4: [d73b4f56fc3fdc38a9edc71744609285203dcc8548ee8c0bcc7bc19c0e4c0b5].

Oct 8, 2024 @ 18:20:24.704

⚠️ **Malware Prevention Alert** [🔗](#)

Status	Risk score	Assignees
Open ▾	73	+

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\$XB4904.12179.rar\temp\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\$XB4904.12179.rar\temp	
process.name	WinRAR.exe	
quarantined.path	C:\.equarantine\c019041d-7f29-46d8-8b59-b0e47a59aef7	