Elastic SIEM Home Lab (Kali Linux)

End-to-end guide on setting up Elastic Agent, forwarding logs, detecting attacker activity (Nmap scans, suspicious processes), and creating custom detection rules with alerting.

1. Introduction

This project demonstrates how to build a blue team SOC simulation using Elastic Security.
We:

- Installed and configured Elastic Agent on a Kali VM
- Forwarded logs into Elastic Cloud
- Created detection rules for attacker activity (e.g., Nmap scans)
- Configured alert notifications
- Tested with simulated attacks

The goal:- replicate a **SOC analyst workflow: collect logs → detect threats → generate alerts.**

2. Environment Setup

- Operating System: Kali Linux (VirtualBox VM)
- Elastic Cloud: Free trial account (Elastic Security & Observability enabled)
- Tools Used:
    - Elastic Agent
    - Kibana (UI for Elastic Security)
    - Kali commands (nmap, curl, wget)

3. Installing Elastic Agent on Kali

1. Download the Elastic Agent package from Elastic Cloud. Example:
2. curl -L -O https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.13.2-linux-x86_64.tar.gz
3. Extract the package:
4. tar xzvf elastic-agent-8.13.2-linux-x86_64.tar.gz
5. cd elastic-agent-8.13.2-linux-x86_64
6. Enroll the agent (replace ENROLL_TOKEN and URL with values from Elastic Cloud):

7. sudo ./elastic-agent install \
8. --url=https://<CLOUD-ID>.fleet.apm.elstc.co:443 \
9. --enrollment-token=<ENROLL_TOKEN>
10. Verify status:
11. sudo elastic-agent status

✅ Expected: Agent is healthy and connected to Elastic.

4. Validating Log Ingestion

- Go to Kibana → Discover
- Select the *logs- index**
- Run commands in Kali (like ls, whoami) and confirm they appear as logs.

5. Generating Logs (Attacker Simulation)

🔷 **Nmap Scan**

nmap -sS -p 1-1000 127.0.0.1

- This creates network scanning logs that Elastic Agent forwards.

🔷 **Curl/Wget Requests**

curl http://example.com

wget http://testphp.vulnweb.com

- These mimic basic reconnaissance and exploitation attempts.

6. Creating Detection Rules

🛡️ **Rule 1: Nmap Scan Detection**

- Go to Elastic Security → Rules → Create Rule
- Define:
    - Index: logs-*
    - KQL Query:
    - process.args : "nmap"
- Add action: Send Email Alert

Rule 2: Suspicious Process Detection

- Query for suspicious binaries:
- process.name : ("curl" or "wget" or "nc" or "ncat")

7. Alerting Setup (Email Notifications)

1. In Kibana → Stack Management → Connectors
2. Configure SMTP email connector (e.g., Gmail/Outlook SMTP).
3. Attach connector to rules created earlier.
4. Test by triggering an alert → check email inbox.

8. Testing & Results

- Ran multiple nmap, curl, and wget commands.
- Verified alerts triggered in Elastic Security.
- Verified email notifications received.
- Simulated high-volume scans to generate 100+ alerts for testing scalability.

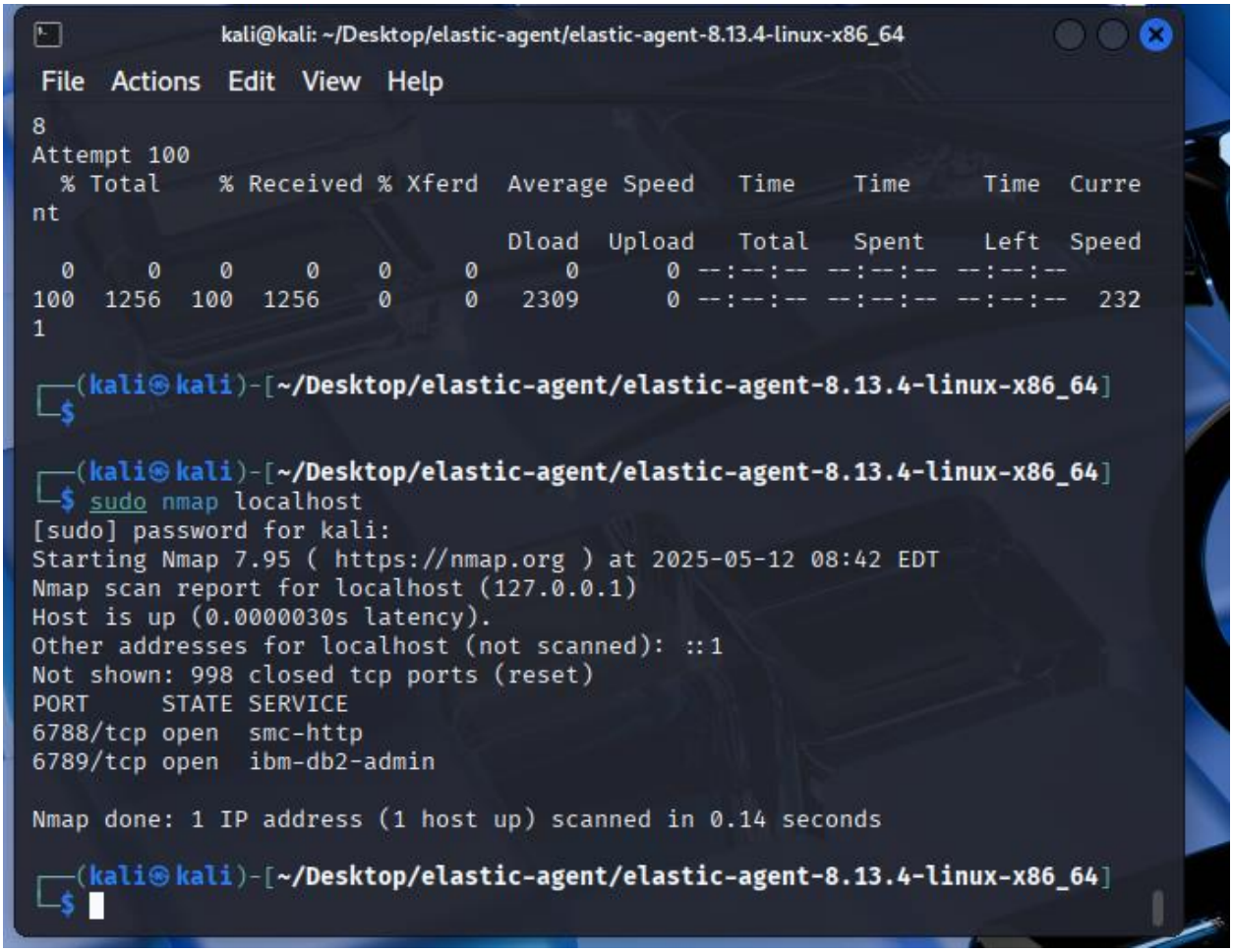
9. Conclusion

This project successfully replicated a SOC monitoring environment.
We showed:

- End-to-end Elastic Security setup
- Realistic attacker simulation
- Detection rules and automated alerts

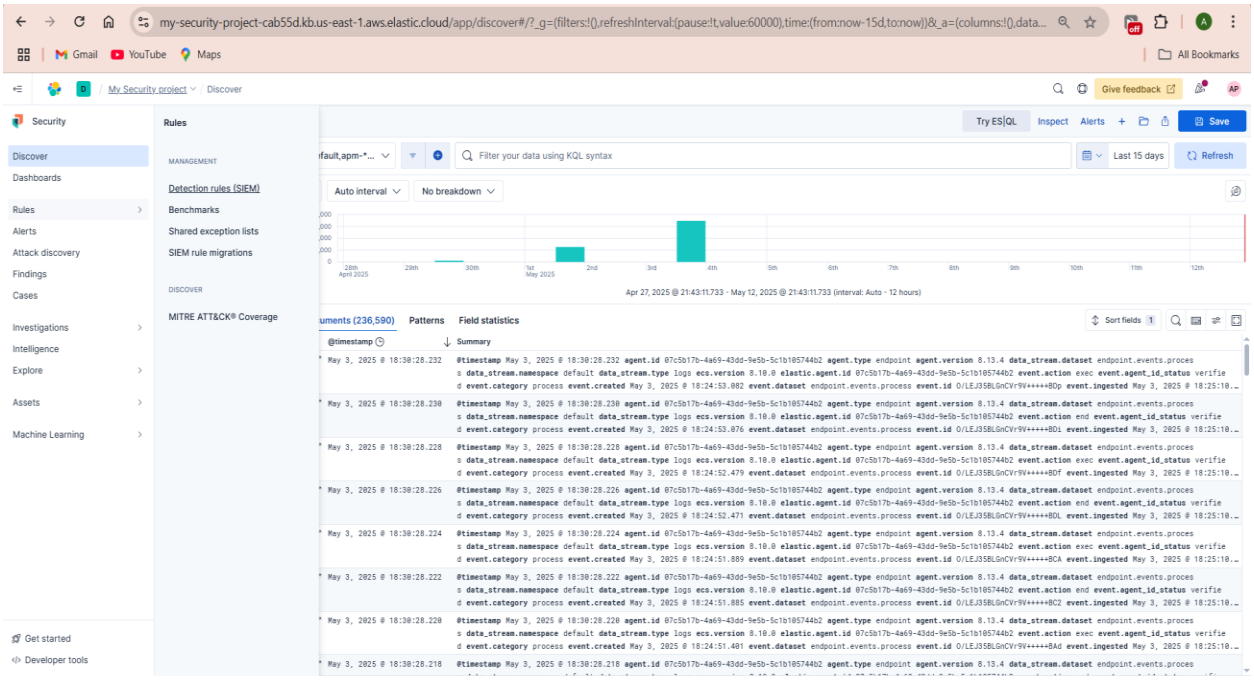
Nmap Scan Detected

This rule was designed to detect reconnaissance activity generated by Nmap scans from the Kali machine. The Elastic Defend agent successfully logged the network activity, and the custom detection rule triggered, classifying it under **MITRE ATT&CK Technique T1046 – Network Service Scanning**.



Next, Raw endpoint telemetry was successfully ingested into Elastic SIEM after deploying and enrolling the Elastic Agent. The Discover view allows analysts to query and validate that logs are flowing into the SIEM correctly before building detection rules.

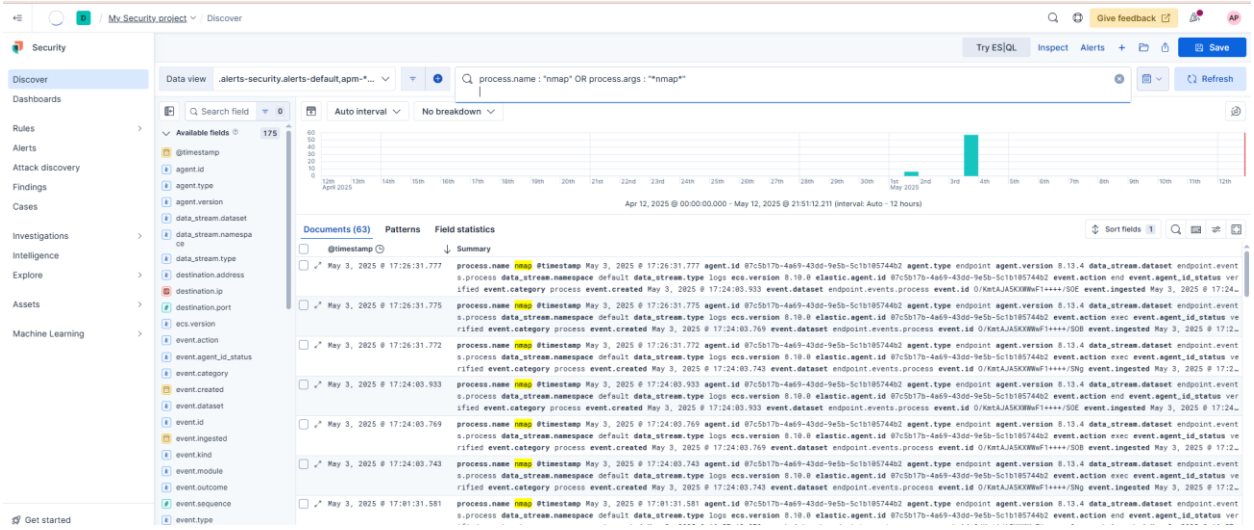
The ingested data includes process creation events, command-line arguments, and execution context. This confirms that the SIEM has full visibility into endpoint activity, providing the foundation for building custom detection rules against simulated attacker behaviors.



NMAP SQUERY ENTERED TO LOOK FOR ALERTS

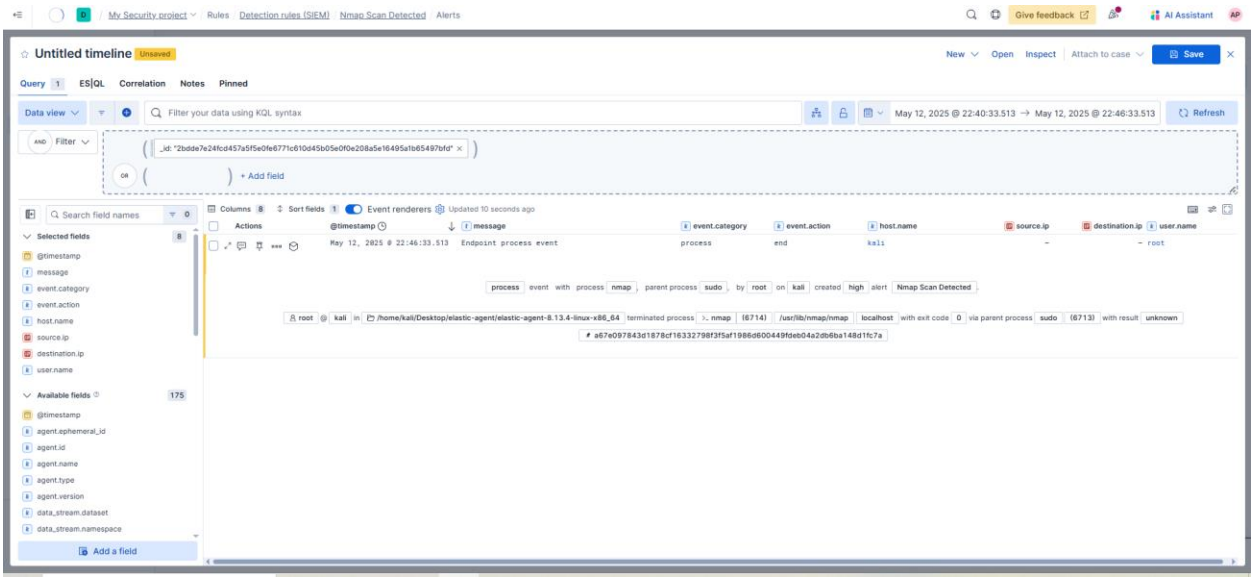
This screenshot demonstrates a filtered search in Elastic SIEM for nmap processes. The filter was applied to verify that reconnaissance activity simulated from the attacker's machine (via Nmap) was captured in the telemetry data.

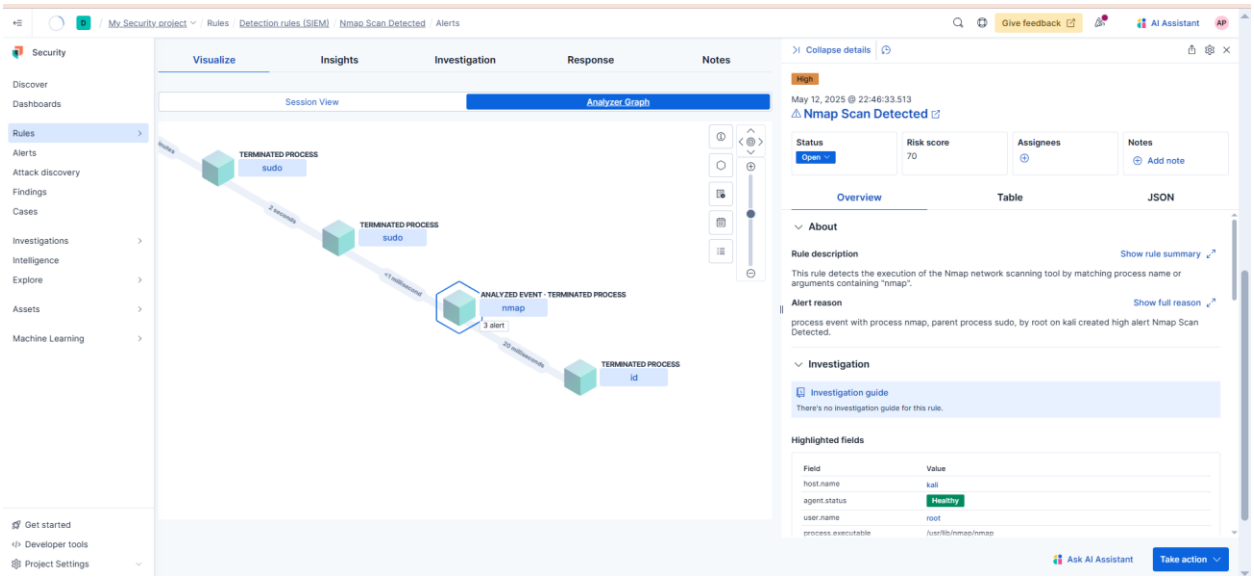
The query results confirm that Nmap executions were successfully logged, showing process names, arguments, and contextual details. This validated that the SIEM can detect MITRE ATT&CK Technique T1046 – Network Service Scanning at the raw log level, before rule-based detection.

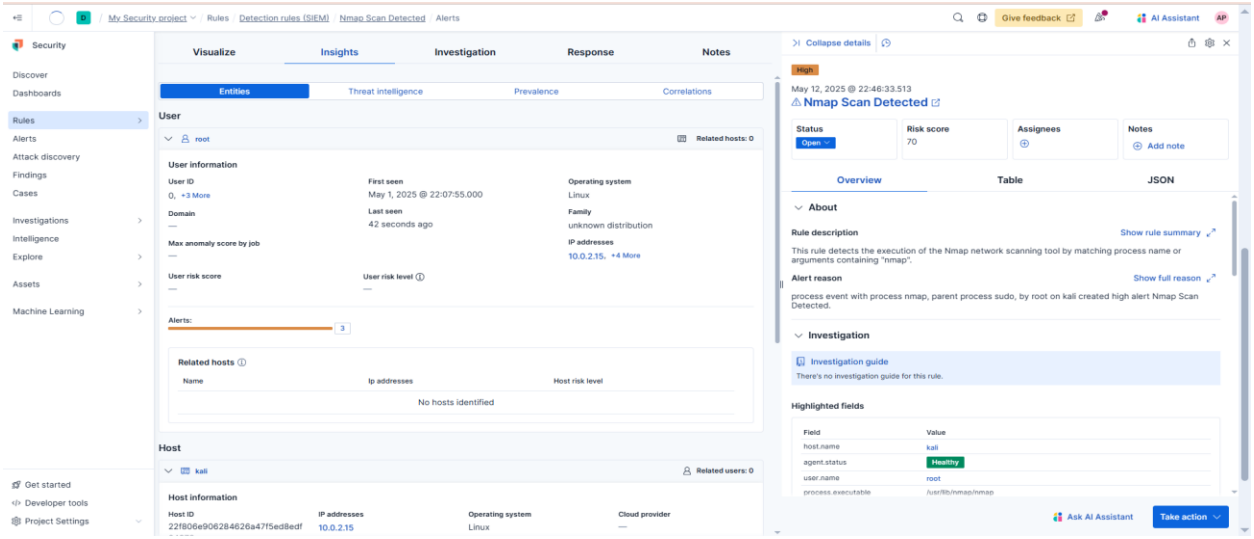

My Security project / Discover
Give feedback
Security
Try ES|QL
Inspect
Alerts
Save
Discover
Dashboards
Data view
.alerts-security.alerts-default,apm-*...
process.name : "nmap" OR process.args : "*nmap*"
Refresh
Rules
Alerts
Attack discovery
Findings
Cases
Investigations
Intelligence
Explore
Assets
Machine Learning
Search field
Available fields
Auto interval
No breakdown
Documents (63)
Patterns
Field statistics
Sort fields
@timestamp
Summary
Get started

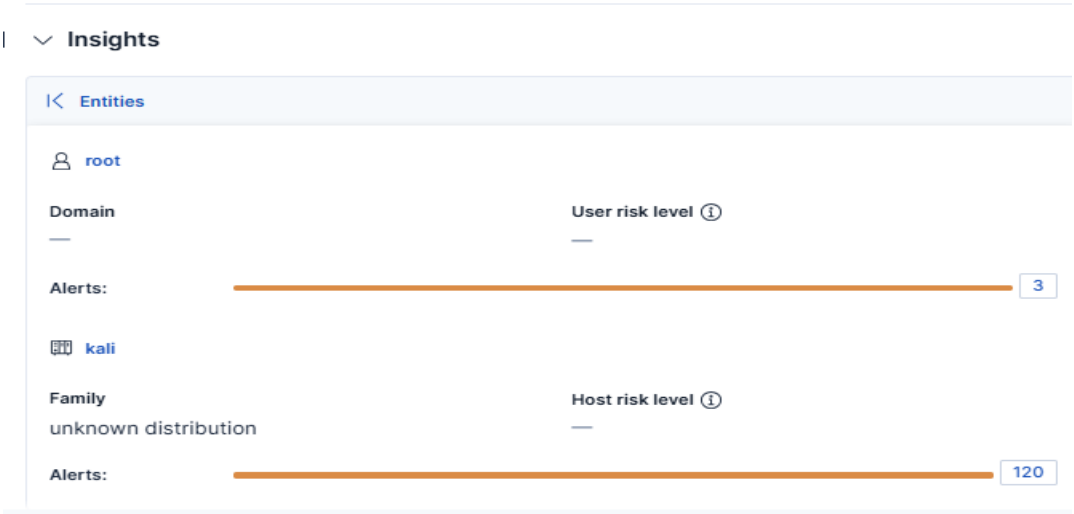

Trend
Showing: 3 alerts
Stack by
event.category
process
3

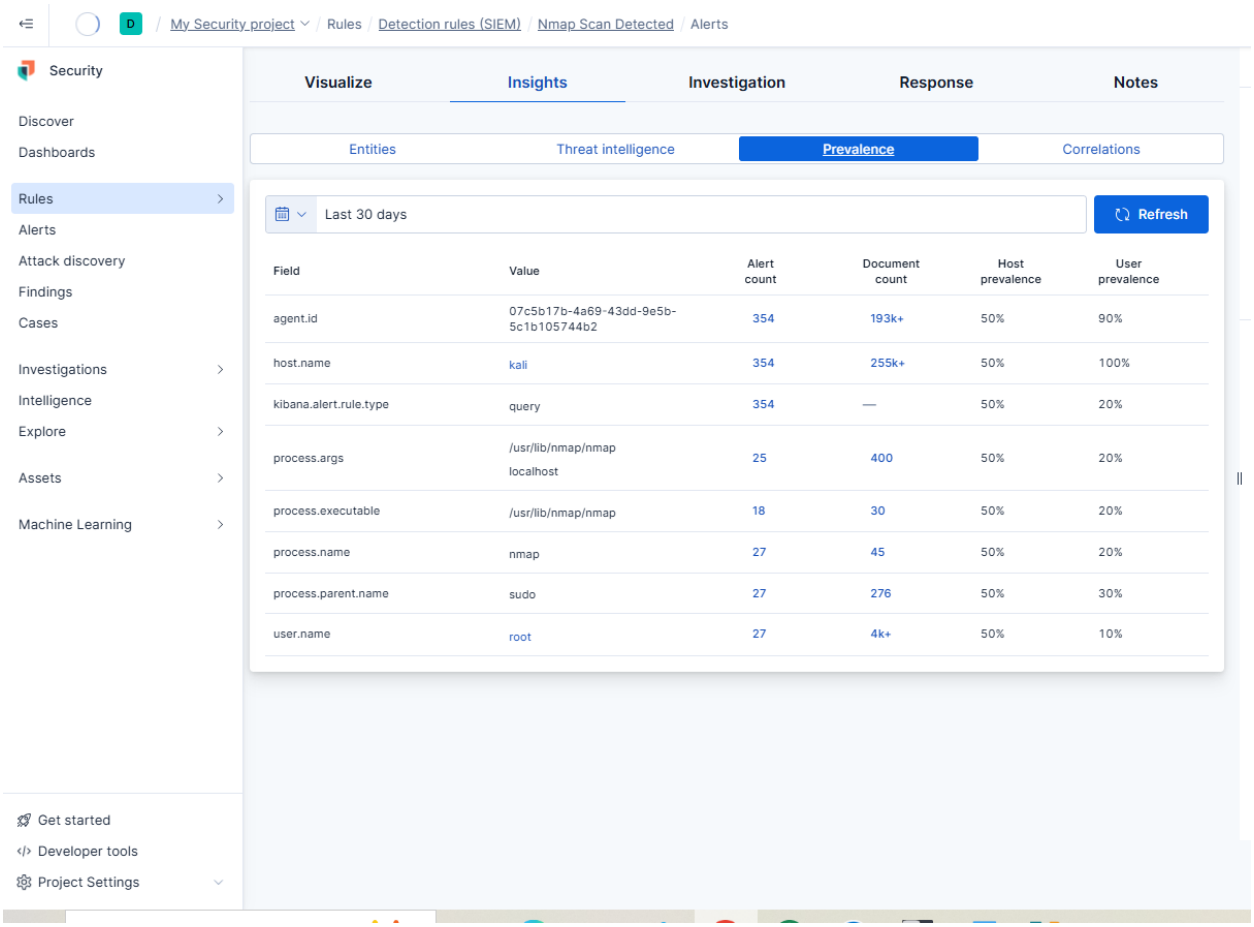

Columns 18
Sort fields 1
3 alerts
Fields
Updated 20 seconds ago
Grid view
Additional filters
Group alerts by: None
Actions
@timestamp
Rule
Assignees
Severity
Risk Score
Reason
host.name
user.name
May 12, 2025 @ 22:46:33.513
Nmap Scan Detected
high
70
process event with process nmap, parent process sudo, by root on kali cre...
kali
root
May 12, 2025 @ 22:46:33.511
May 12, 2025 @ 22:46:33.508

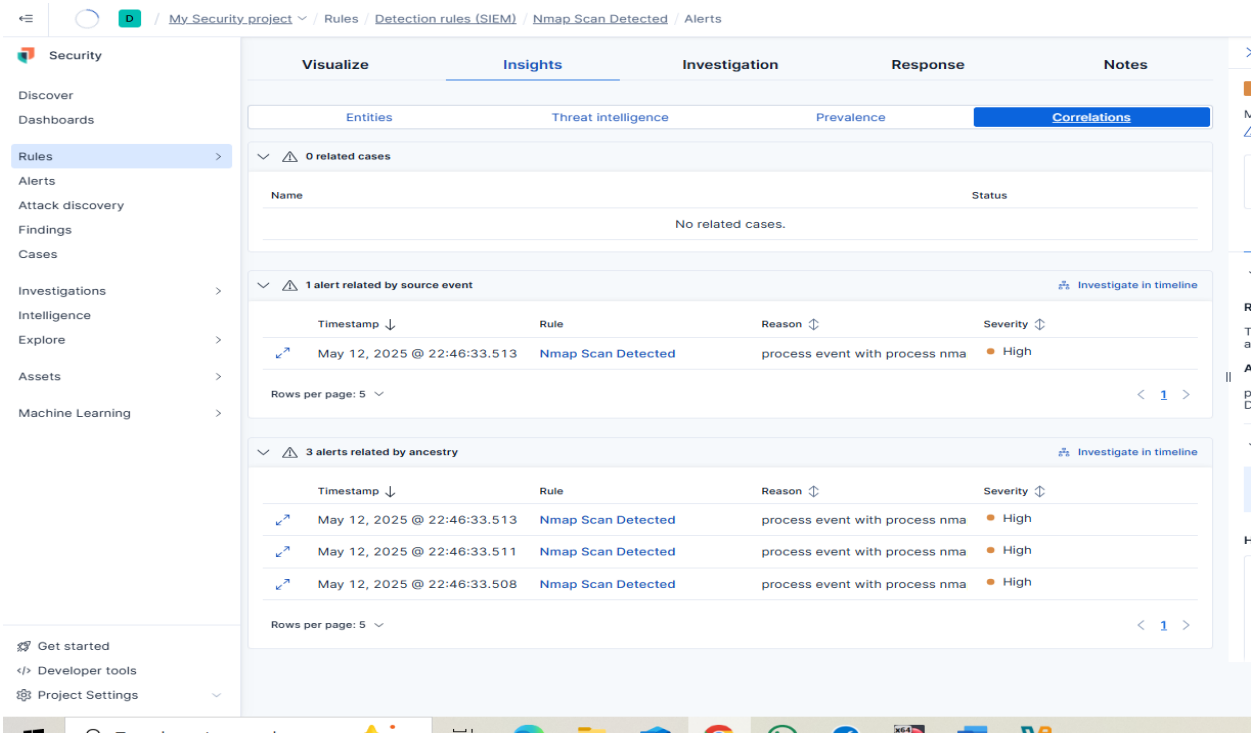

My Security project / Rules / Detection rules (SIEM) / Nmap Scan Detected / Alerts
Give feedback
AI Assistant
Untitled timeline
Unsaved
New
Open
Inspect
Attach to case
Save
Query 1
ES|QL
Correlation
Notes
Pinned
Data view
Filter your data using KQL syntax
May 12, 2025 @ 22:40:33.513 → May 12, 2025 @ 22:46:33.513
Refresh
Filter
+ Add field
Search field names
Columns 8
Sort fields 1
Event renderers
Updated 10 seconds ago
Actions
@timestamp
message
event.category
event.action
host.name
source.ip
destination.ip
user.name
Endpoint process event
process
end
kali
root
Selected fields
Available fields
Add a field

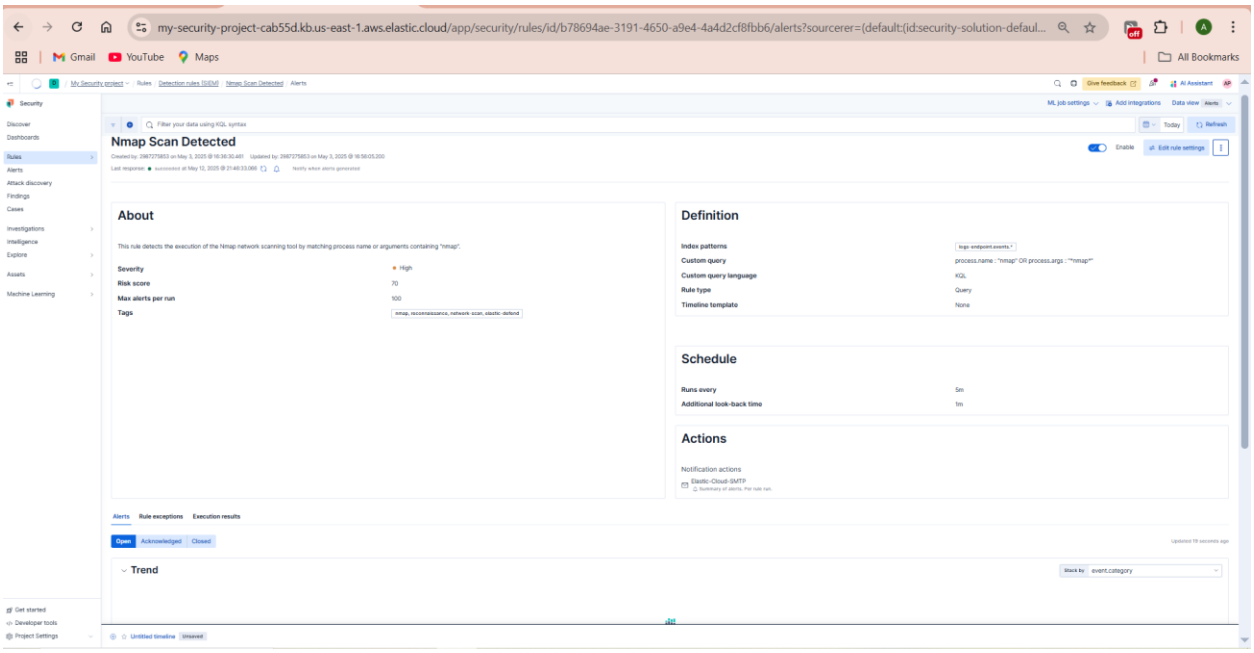

My Security project / Rules / Detection rules (SIEM) / Nmap Scan Detected / Alerts
Give feedback
AI Assistant
Security
Discover
Dashboards
Rules
Alerts
Attack discovery
Findings
Cases
Investigations
Intelligence
Explore
Assets
Machine Learning
Get started
Developer tools
Project Settings
Visualize
Insights
Investigation
Response
Notes
Session View
Analyzer Graph
TERMINATED PROCESS
sudo
2 seconds
TERMINATED PROCESS
sudo
<1 millisecond
ANALYZED EVENT - TERMINATED PROCESS
nmap
3 alert
20 milliseconds
TERMINATED PROCESS
id
Collapse details
High
May 12, 2025 @ 22:46:33.513
Nmap Scan Detected
Status
Open
Risk score
70
Assignees
Notes
Add note
Overview
Table
JSON
About
Rule description
Show rule summary
This rule detects the execution of the Nmap network scanning tool by matching process name or arguments containing "nmap".
Alert reason
Show full reason
process event with process nmap, parent process sudo, by root on kali created high alert Nmap Scan Detected.
Investigation
Investigation guide
There's no investigation guide for this rule.
Highlighted fields
Field
Value
host.name
kali
agent.status
Healthy
user.name
root
process.executable
/usr/lib/nmap/nmap
Ask AI Assistant
Take action

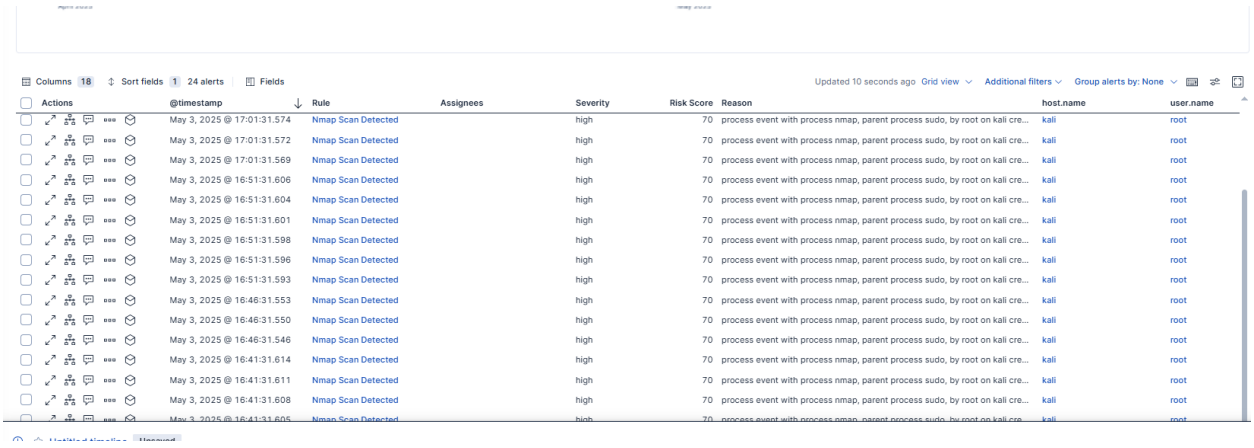

My Security project / Rules / Detection rules (SIEM) / Nmap Scan Detected / Alerts
Give feedback
AI Assistant
Security
Discover
Dashboards
Rules
Alerts
Attack discovery
Findings
Cases
Investigations
Intelligence
Explore
Assets
Machine Learning
Get started
Developer tools
Project Settings
Visualize
Insights
Investigation
Response
Notes
Entities
Threat intelligence
Prevalence
Correlations
User
root
Related hosts: 0
User information
User ID
0, +3 More
First seen
May 1, 2025 @ 22:07:55.000
Operating system
Linux
Domain
Last seen
42 seconds ago
Family
unknown distribution
Max anomaly score by job
IP addresses
10.0.2.15, +4 More
User risk score
User risk level
Alerts:
3
Related hosts
Name
Ip addresses
Host risk level
No hosts identified
Host
kali
Related users: 0
Host information
Host ID
22f806e906284626a47f5ed8edf
IP addresses
10.0.2.15
Operating system
Linux
Cloud provider
Collapse details
High
May 12, 2025 @ 22:46:33.513
Nmap Scan Detected
Status
Open
Risk score
70
Assignees
Notes
Add note
Overview
Table
JSON
About
Rule description
Show rule summary
This rule detects the execution of the Nmap network scanning tool by matching process name or arguments containing "nmap".
Alert reason
Show full reason
process event with process nmap, parent process sudo, by root on kali created high alert Nmap Scan Detected.
Investigation
Investigation guide
There's no investigation guide for this rule.
Highlighted fields
Field
Value
host.name
kali
agent.status
Healthy
user.name
root
process.executable
/usr/lib/nmap/nmap
Ask AI Assistant
Take action


Insights
Entities
root
Domain
—
User risk level
—
Alerts:
3
kali
Family
unknown distribution
Host risk level
—
Alerts:
120


D
My Security project
Rules
Detection rules (SIEM)
Nmap Scan Detected
Alerts
Security
Discover
Dashboards
Rules
Alerts
Attack discovery
Findings
Cases
Investigations
Intelligence
Explore
Assets
Machine Learning
Get started
Developer tools
Project Settings
Visualize
Insights
Investigation
Response
Notes
Entities
Threat intelligence
Prevalence
Correlations
Last 30 days
Refresh
Field
Value
Alert count
Document count
Host prevalence
User prevalence
agent.id
07c5b17b-4a69-43dd-9e5b-5c1b105744b2
354
193k+
50%
90%
host.name
kali
354
255k+
50%
100%
kibana.alert.rule.type
query
354
—
50%
20%
process.args
/usr/lib/nmap/nmap
localhost
25
400
50%
20%
process.executable
/usr/lib/nmap/nmap
18
30
50%
20%
process.name
nmap
27
45
50%
20%
process.parent.name
sudo
27
276
50%
30%
user.name
root
27
4k+
50%
10%


D
My Security project
Rules
Detection rules (SIEM)
Nmap Scan Detected
Alerts
Security
Discover
Dashboards
Rules
Alerts
Attack discovery
Findings
Cases
Investigations
Intelligence
Explore
Assets
Machine Learning
Get started
Developer tools
Project Settings
Visualize
Insights
Investigation
Response
Notes
Entities
Threat intelligence
Prevalence
Correlations
0 related cases
Name
Status
No related cases.
1 alert related by source event
Investigate in timeline
Timestamp
Rule
Reason
Severity
May 12, 2025 @ 22:46:33.513
Nmap Scan Detected
process event with process nma
High
Rows per page: 5
1
3 alerts related by ancestry
Investigate in timeline
Timestamp
Rule
Reason
Severity
May 12, 2025 @ 22:46:33.513
Nmap Scan Detected
process event with process nma
High
May 12, 2025 @ 22:46:33.511
Nmap Scan Detected
process event with process nma
High
May 12, 2025 @ 22:46:33.508
Nmap Scan Detected
process event with process nma
High
Rows per page: 5
1



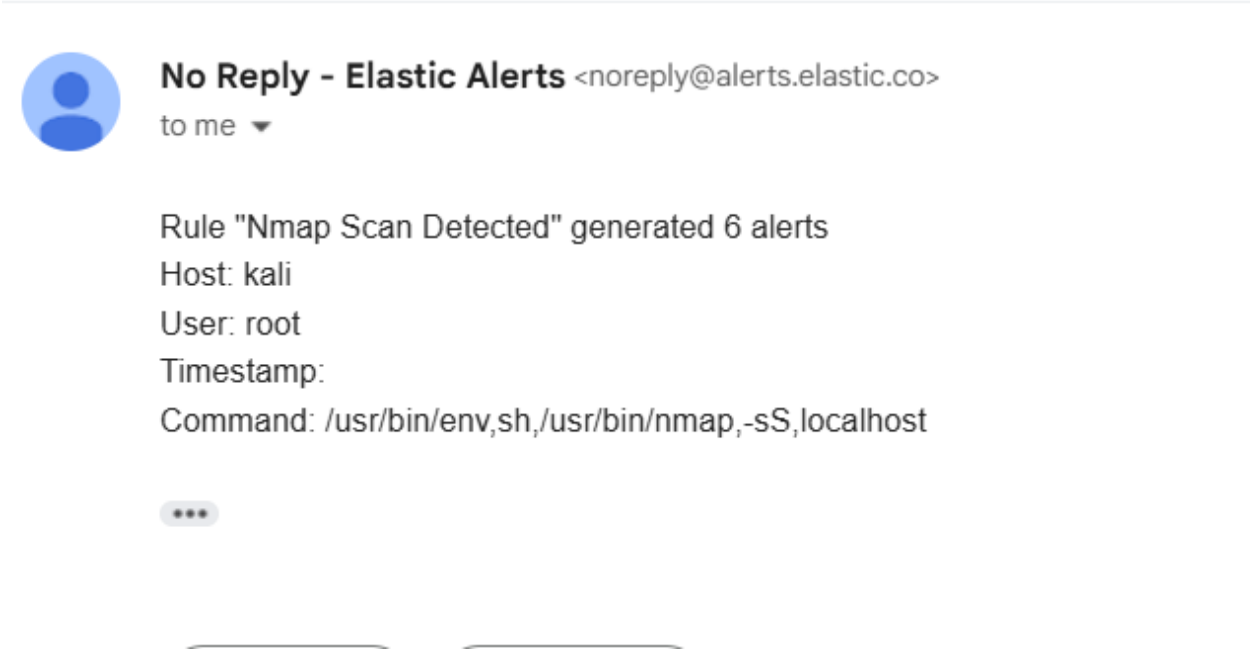


Actions	@timestamp	Rule	Assignees	Severity	Risk Score	Reason	host.name	user.name
	May 3, 2025 @ 17:01:31.574	Nmap Scan Detected		high	70	process event with process nmap, parent process sudo, by root on kali cre...	kali	root
	May 3, 2025 @ 17:01:31.572	Nmap Scan Detected		high	70	process event with process nmap, parent process sudo, by root on kali cre...	kali	root
	May 3, 2025 @ 17:01:31.569	Nmap Scan Detected		high	70	process event with process nmap, parent process sudo, by root on kali cre...	kali	root
	May 3, 2025 @ 16:51:31.606	Nmap Scan Detected		high	70	process event with process nmap, parent process sudo, by root on kali cre...	kali	root
	May 3, 2025 @ 16:51:31.604	Nmap Scan Detected		high	70	process event with process nmap, parent process sudo, by root on kali cre...	kali	root
	May 3, 2025 @ 16:51:31.601	Nmap Scan Detected		high	70	process event with process nmap, parent process sudo, by root on kali cre...	kali	root
	May 3, 2025 @ 16:51:31.598	Nmap Scan Detected		high	70	process event with process nmap, parent process sudo, by root on kali cre...	kali	root
	May 3, 2025 @ 16:51:31.596	Nmap Scan Detected		high	70	process event with process nmap, parent process sudo, by root on kali cre...	kali	root
	May 3, 2025 @ 16:51:31.593	Nmap Scan Detected		high	70	process event with process nmap, parent process sudo, by root on kali cre...	kali	root
	May 3, 2025 @ 16:46:31.553	Nmap Scan Detected		high	70	process event with process nmap, parent process sudo, by root on kali cre...	kali	root
	May 3, 2025 @ 16:46:31.550	Nmap Scan Detected		high	70	process event with process nmap, parent process sudo, by root on kali cre...	kali	root
	May 3, 2025 @ 16:46:31.546	Nmap Scan Detected		high	70	process event with process nmap, parent process sudo, by root on kali cre...	kali	root
	May 3, 2025 @ 16:41:31.614	Nmap Scan Detected		high	70	process event with process nmap, parent process sudo, by root on kali cre...	kali	root
	May 3, 2025 @ 16:41:31.611	Nmap Scan Detected		high	70	process event with process nmap, parent process sudo, by root on kali cre...	kali	root
	May 3, 2025 @ 16:41:31.608	Nmap Scan Detected		high	70	process event with process nmap, parent process sudo, by root on kali cre...	kali	root

Email Alert Notifications

Email connectors were configured in Kibana so that triggered rules automatically generated analyst notifications.

This step confirmed that the detection pipeline extended beyond dashboards to real SOC-style workflows, ensuring analysts are alerted in near real-time.

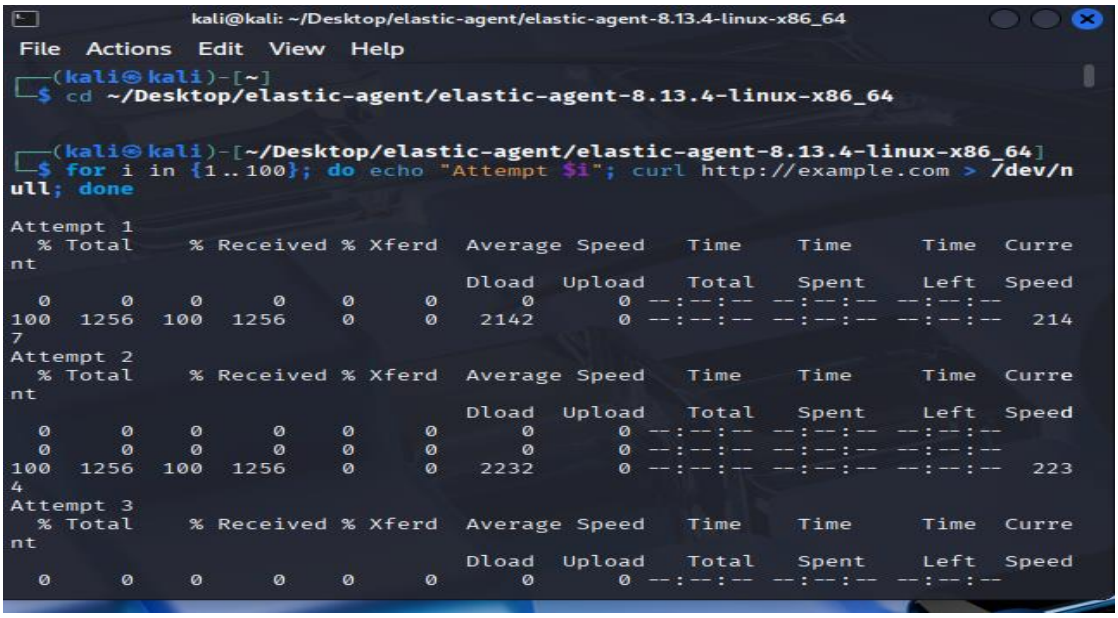


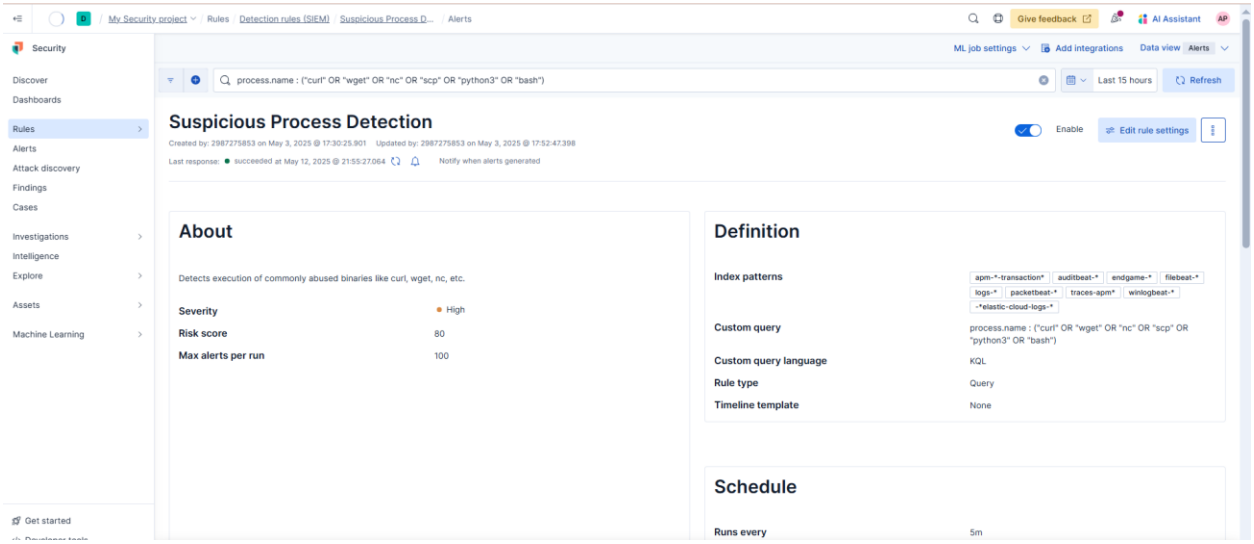
SUSPICIOUS PROCESS DETECTED

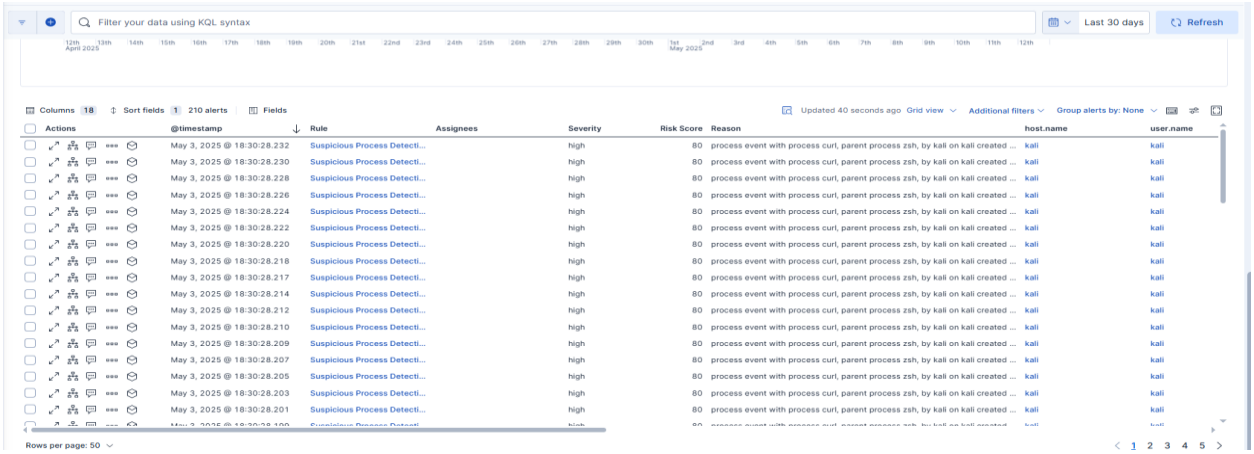
Suspicious Process Detected

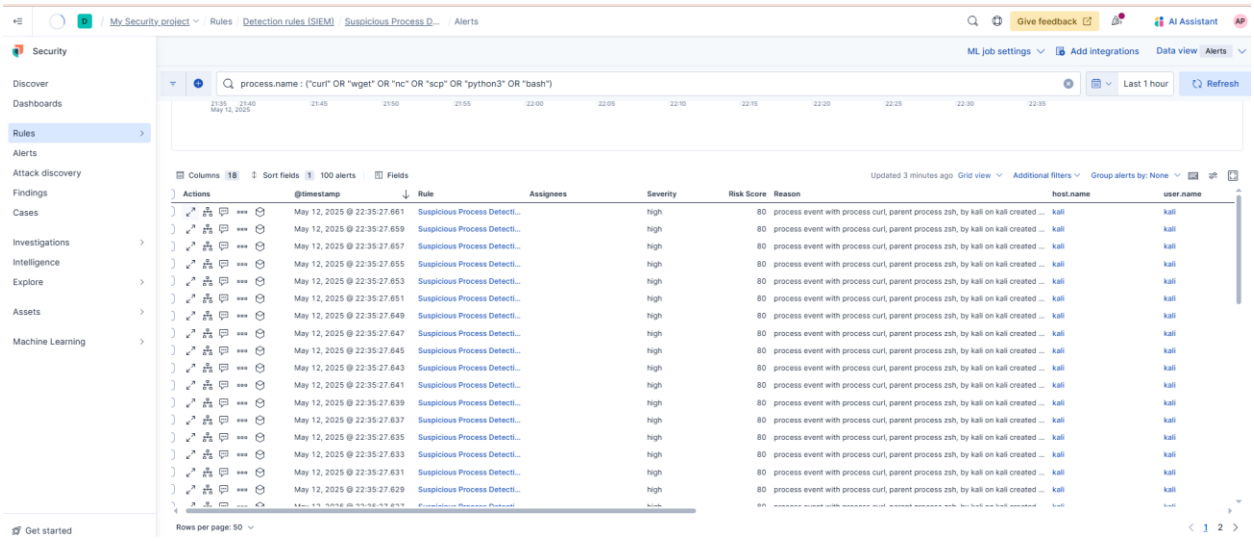
This detection rule monitored for execution of suspicious processes such as netcat and curl launched from unexpected contexts. These are often used in exploitation and lateral movement scenarios.

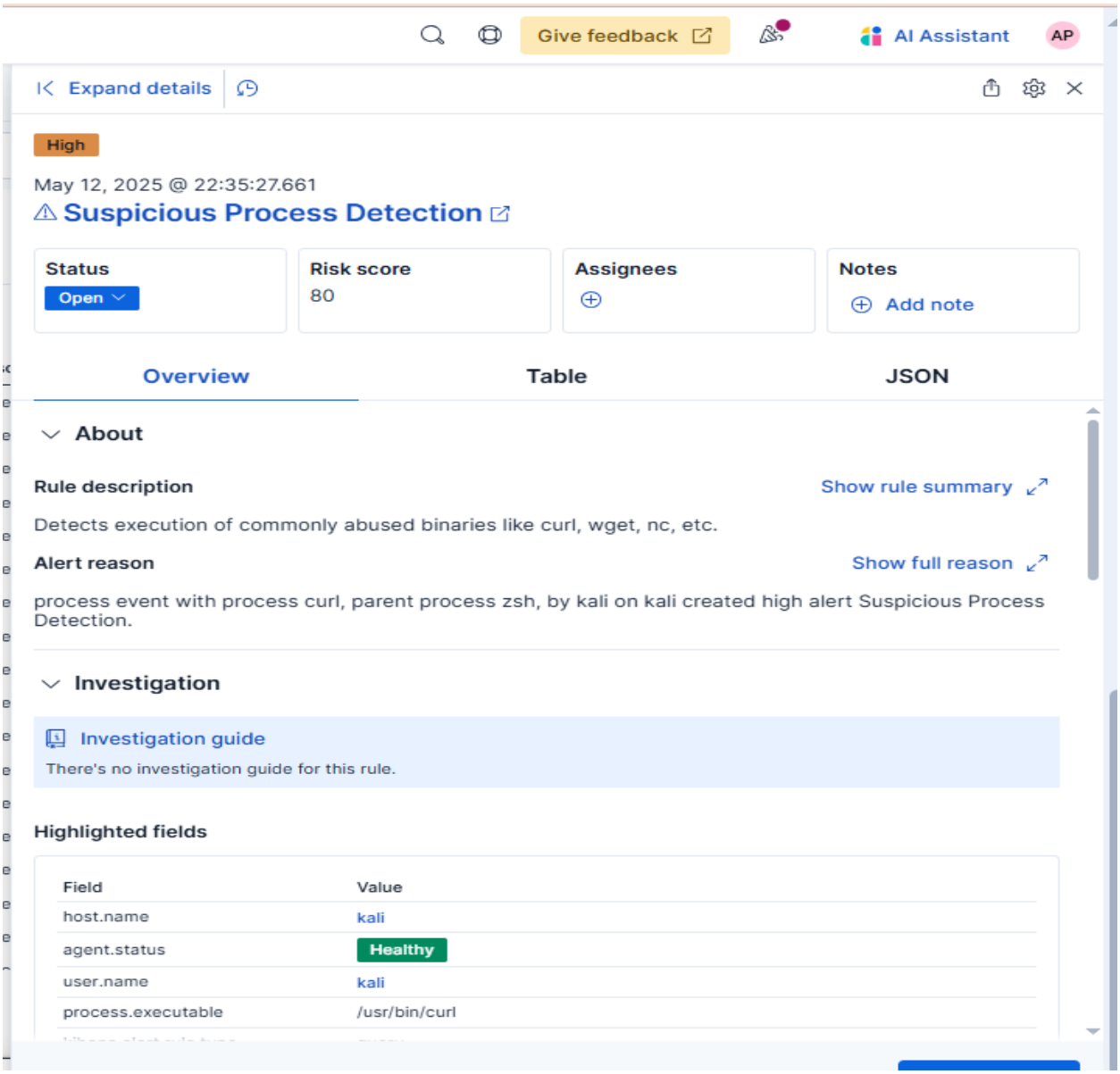
The rule triggered when the attacker machine attempted command execution, demonstrating the lab's ability to detect **MITRE ATT&CK Technique T1059 – Command and Scripting Interpret**


kali@kali: ~/Desktop/elastic-agent/elastic-agent-8.13.4-linux-x86_64
File Actions Edit View Help
(kali㉿kali)-[~]
$ cd ~/Desktop/elastic-agent/elastic-agent-8.13.4-linux-x86_64
(kali㉿kali)-[~/Desktop/elastic-agent/elastic-agent-8.13.4-linux-x86_64]
$ for i in {1..100}; do echo "Attempt $i"; curl http://example.com > /dev/null; done
Attempt 1
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
0 0 0 0 0 0 0 0 --:--:-- --:--:-- --:--:-- 0
100 1256 100 1256 0 0 2142 0 --:--:-- --:--:-- --:--:-- 2147
Attempt 2
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
0 0 0 0 0 0 0 0 --:--:-- --:--:-- --:--:-- 0
0 0 0 0 0 0 0 0 --:--:-- --:--:-- --:--:-- 0
100 1256 100 1256 0 0 2232 0 --:--:-- --:--:-- --:--:-- 2234
Attempt 3
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
0 0 0 0 0 0 0 0 --:--:-- --:--:-- --:--:-- 0

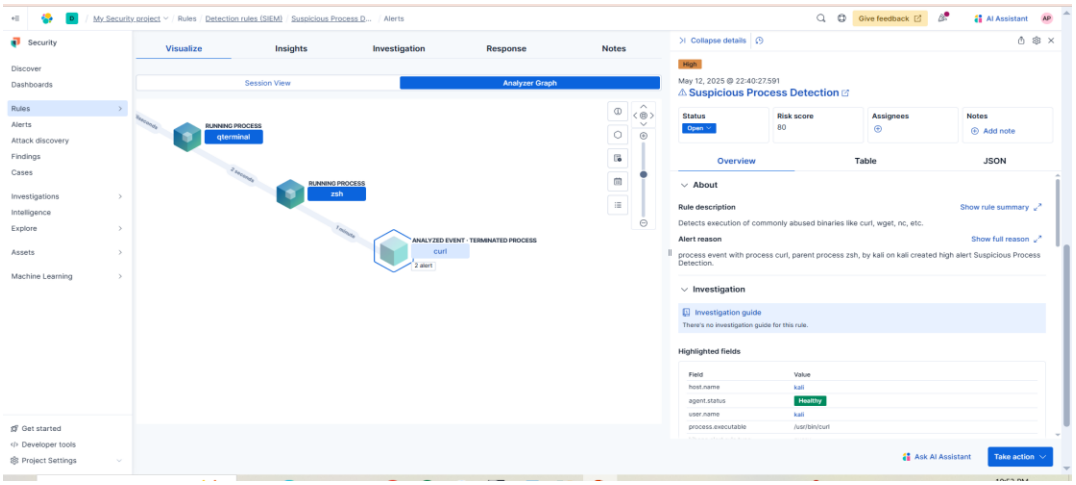

Security
Discover
Dashboards
Rules
Alerts
Attack discovery
Findings
Cases
Investigations
Intelligence
Explore
Assets
Machine Learning
Get started
Suspicious Process Detection
Enable
Edit rule settings
About
Detects execution of commonly abused binaries like curl, wget, nc, etc.
Severity
High
Risk score
80
Max alerts per run
100
Definition
Index patterns
Custom query
process.name : ("curl" OR "wget" OR "nc" OR "scp" OR "python3" OR "bash")
Custom query language
KQL
Rule type
Query
Timeline template
None
Schedule
Runs every
5m

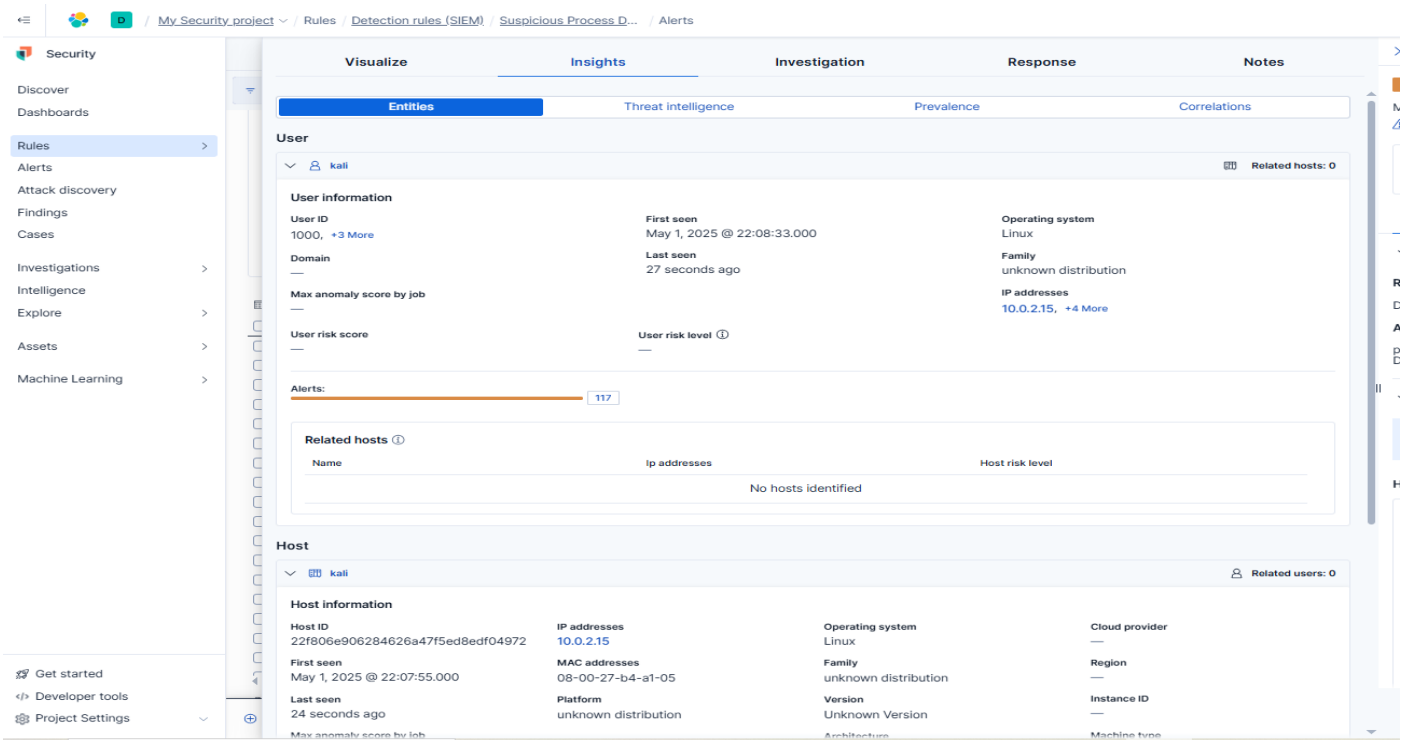

Filter your data using KQL syntax
Last 30 days
Refresh
Columns 18
Sort fields 1 210 alerts
Fields
Updated 40 seconds ago
Grid view
Additional filters
Group alerts by: None
Actions
@timestamp
Rule
Assignees
Severity
Risk Score
Reason
host.name
user.name
May 3, 2025 @ 18:30:28.232
Suspicious Process Detecti...
high
80
process event with process curl, parent process zsh, by kali on kali created ...
kali
Rows per page: 50
1 2 3 4 5

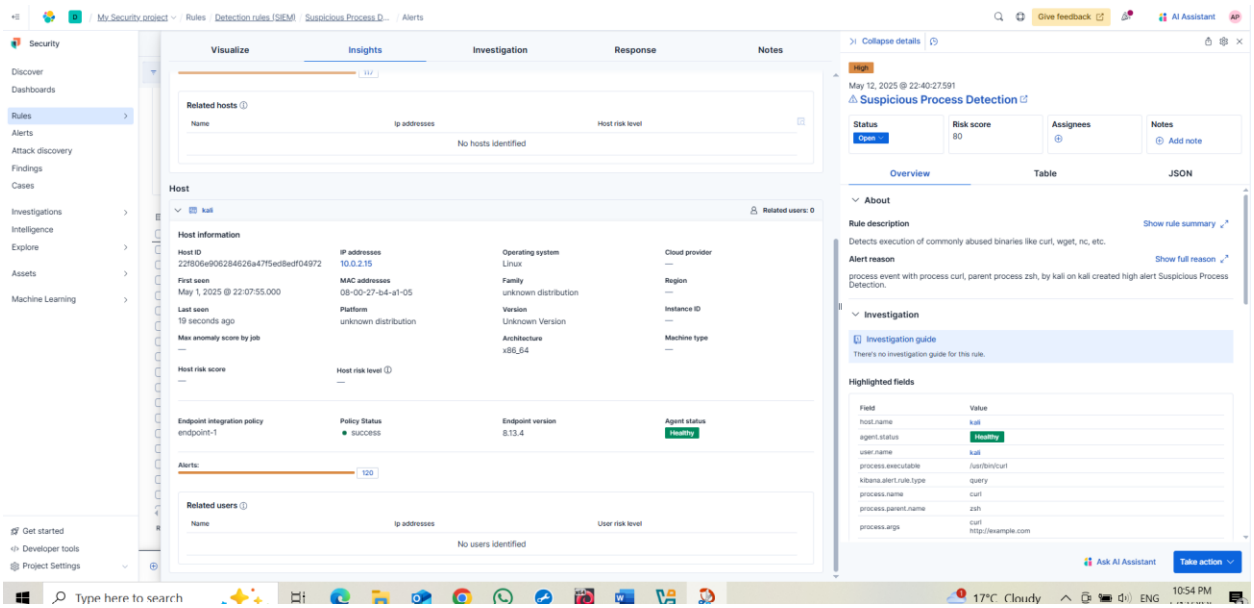

My Security project
Rules
Detection rules (SIEM)
Suspicious Process D...
Alerts
Give feedback
AI Assistant
Security
ML job settings
Add integrations
Data view
Alerts
Discover
Dashboards
Rules
Alerts
Attack discovery
Findings
Cases
Investigations
Intelligence
Explore
Assets
Machine Learning
Get started
process.name : ("curl" OR "wget" OR "nc" OR "scp" OR "python3" OR "bash")
Last 1 hour
Refresh
Columns 18
Sort fields 1 100 alerts
Fields
Updated 3 minutes ago
Grid view
Additional filters
Group alerts by: None
Actions
@timestamp
Rule
Assignees
Severity
Risk Score
Reason
host.name
user.name
May 12, 2025 @ 22:35:27.661
Suspicious Process Detecti...
high
80
process event with process curl, parent process zsh, by kali on kali created ...
kali
Rows per page: 50
1 2


Give feedback
AI Assistant
AP
Expand details
High
May 12, 2025 @ 22:35:27.661
Suspicious Process Detection
Status
Open
Risk score
80
Assignees
Notes
Add note
Overview
Table
JSON
About
Rule description
Show rule summary
Detects execution of commonly abused binaries like curl, wget, nc, etc.
Alert reason
Show full reason
process event with process curl, parent process zsh, by kali on kali created high alert Suspicious Process Detection.
Investigation
Investigation guide
There's no investigation guide for this rule.
Highlighted fields
Field
Value
host.name
kali
agent.status
Healthy
user.name
kali
process.executable
/usr/bin/curl


Entities
kali
Alerts:
100
kali
Alerts:
100
Threat intelligence
Threat matches detected
0
Fields enriched with threat intelligence
0


Security
Visualize
Insights
Investigation
Response
Notes
Session View
Analyzer Graph
RUNNING PROCESS
qterminal
RUNNING PROCESS
zsh
ANALYZED EVENT - TERMINATED PROCESS
curl
Collapse details
Suspicious Process Detection
Status
Open
Risk score
80
Assignees
Notes
Add note
Overview
Table
JSON
About
Rule description
Detects execution of commonly abused binaries like curl, wget, nc, etc.
Alert reason
Investigation
Investigation guide
Highlighted fields
Field
Value
host.name
kali
agent.status
Healthy
user.name
kali
process.executable
/usr/bin/curl
Ask AI Assistant
Take action


My Security project / Rules / Detection rules (SIEM) / Suspicious Process D... / Alerts
Security
Discover
Dashboards
Rules
Alerts
Attack discovery
Findings
Cases
Investigations
Intelligence
Explore
Assets
Machine Learning
Get started
Developer tools
Project Settings
Visualize
Insights
Investigation
Response
Notes
Entities
Threat intelligence
Prevalence
Correlations
User
kali
Related hosts: 0
User information
User ID
1000, +3 More
Domain
—
Max anomaly score by job
—
User risk score
—
First seen
May 1, 2025 @ 22:08:33.000
Last seen
27 seconds ago
User risk level
—
Operating system
Linux
Family
unknown distribution
IP addresses
10.0.2.15, +4 More
Alerts:
117
Related hosts
Name
Ip addresses
Host risk level
No hosts identified
Host
kali
Related users: 0
Host information
Host ID
22f806e906284626a47f5ed8edf04972
First seen
May 1, 2025 @ 22:07:55.000
Last seen
24 seconds ago
IP addresses
10.0.2.15
MAC addresses
08-00-27-b4-a1-05
Platform
unknown distribution
Operating system
Linux
Family
unknown distribution
Version
Unknown Version
Cloud provider
—
Region
—
Instance ID
—


Give feedback
AI Assistant
Collapse details
High
May 12, 2025 @ 22:40:27.591
Suspicious Process Detection
Status
Open
Risk score
80
Assignees
Notes
Add note
Overview
Table
JSON
About
Rule description
Show rule summary
Detects execution of commonly abused binaries like curl, wget, nc, etc.
Alert reason
Show full reason
process event with process curl, parent process zsh, by kali on kali created high alert Suspicious Process Detection.
Investigation
Investigation guide
There's no investigation guide for this rule.
Highlighted fields
Field
Value
host.name
kali
agent.status
Healthy
user.name
kali
process.executable
/usr/bin/curl
kibana.alert.rule.type
query
process.name
curl
process.parent.name
zsh
process.args
curl
http://example.com
Ask AI Assistant
Take action
Endpoint integration policy
endpoint-1
Policy Status
success
Endpoint version
8.13.4
Agent status
Healthy
Related users
No users identified
Type here to search
17°C Cloudy
ENG
10:54 PM

[ALERT] Suspicious Process Detected External Inbox ×

No Reply - Elastic Alerts <noreply@alerts.elastic.co>
to me

Rule "Suspicious Process Detection" triggered 3 alert(s) Host:
User:
Timestamp:
Process:
Command Line:
Executable Path:

This message was sent by Elastic. View rule in Kibana.

[ALERT] Suspicious Process Detected External Inbox ×

No Reply - Elastic Alerts <noreply@alerts.elastic.co>
to me

Rule "Suspicious Process Detection" triggered 100 alert(s)

Host: kali User: kali Timestamp: Process: curl Command Line: curl http://example.com Executable Path: /usr/bin/curl

---

This message was sent by Elastic. View rule in Kibana.