Project Title: A Simple Elastic SIEM Lab

Author: Aditya Sangle

Date: September 2, 2024

Introduction

This project demonstrates how to create a home lab for Elastic Stack Security Information and Event Management (SIEM) using the Elastic Cloud platform and a Kali Linux Virtual Machine (VM). The goal of this lab is to simulate security events, collect logs using an Elastic agent, and analyze the data in the SIEM. This project serves as a practical introduction to security monitoring and is a valuable addition to your skill set for security-related roles.

Project Tasks

1. **Create an Elastic Account.**
2. **Install and configure the Kali Linux VM.**
3. **Deploy the Elastic Agent to collect logs.**
4. **Generate security events on the Kali VM.**
5. **Analyze security events in Elastic SIEM.**
6. **Create a Dashboard to visualize data.**
7. **Set up alerts for security events.**

Task 1: Creating an Elastic Account

Sign Up for Free: Register for a free trial on the Elastic Cloud.

Deploy an Instance:

- Log in and click "Create Deployment".
- Choose "Elasticsearch" as the deployment type.
- Select a suitable region and deployment size, then click "Create Deployment".
- Wait for the configuration to complete and click "Continue".

Task 2: Setting Up the Kali Linux VM

Download the Kali VM: Get the VM file from Kali's official website.

Create and Start a New VM:

- Use VirtualBox or VMware to create a new VM.
- Start the VM and follow the on-screen instructions to install Kali.

Login: Use the default credentials "kali" for both username and password.

Task 3: Deploying the Elastic Agent

Navigate to Integrations:

- Log in to your Elastic SIEM instance and go to the "Integrations" page from the Kibana main menu.

Install Elastic Defend:

- Search for "Elastic Defend" and install it.
- Copy the command provided for Linux installation and run it in the Kali terminal.

Verify Installation:

- Execute sudo systemctl status elastic-agent.service to ensure the agent is running properly.

Task 4: Generating Security Events on Kali VM

Install Nmap (if not preinstalled): Run sudo apt-get install nmap.

Simulate Security Events:

- Use commands like sudo nmap <vm-ip> to scan and generate security logs.
- Experiment with different Nmap scans such as nmap -sS <ip> or nmap -p- <ip>.

Task 5: Analyzing Security Events in Elastic SIEM

View Logs:

- Navigate to the "Logs" tab under "Observability" in your Elastic Deployment.

Search Events:

- Use queries like event.action: "nmap_scan" to filter specific events.
- Review the displayed results to understand the security events.

Task 6: Creating a Dashboard to Visualize Events

Build a New Dashboard:

- Go to "Dashboards" under "Analytics" in Elastic Cloud.

Create Visualizations:

- Click "Create Visualization" and select a type like "Line" or "Area".
- Configure metrics using "Count" as the vertical axis and "Timestamp" as the horizontal axis.

Task 7: Setting Up Alerts for Security Events

Create a New Alert:

- Go to "Security" > "Alerts" and click "Manage rules".
- Click "Create new rule" and choose a custom query such as event.action: "nmap_scan".

Configure the Alert:

- Define the rule name, description, and severity.
- Set up actions such as sending email notifications or triggering webhooks.
- Save and activate the rule.

Conclusion

This lab provides a comprehensive introduction to using Elastic SIEM for security monitoring and incident response. You have learned how to:

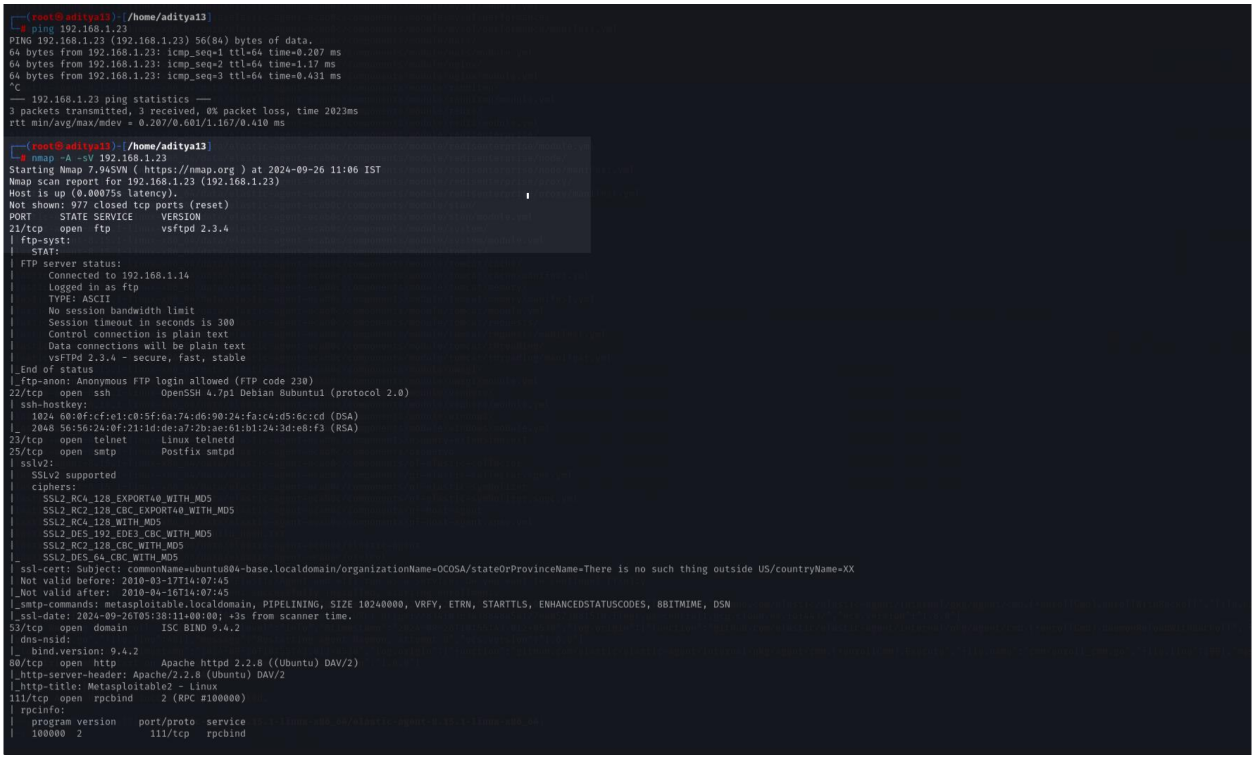
- Collect and analyze security logs.
- Visualize data using dashboards.
- Create alerts for critical security events.

Next Steps:

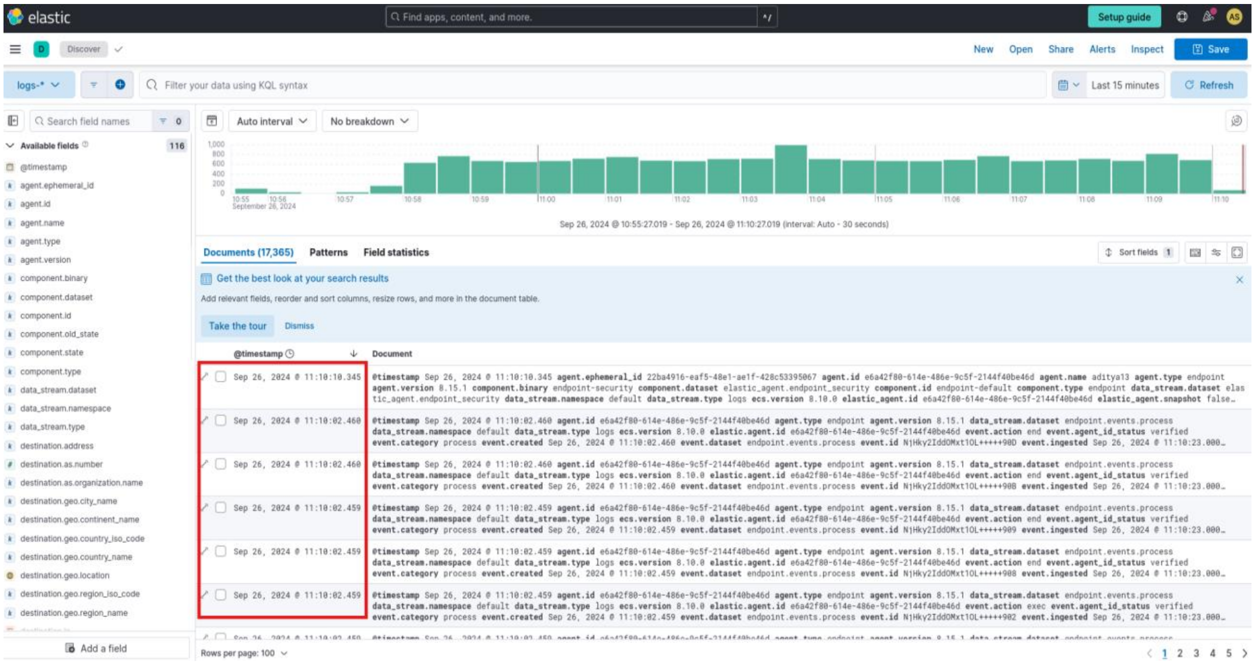
- Explore generating different types of security events.
- Test the alerts by running Nmap scans on the Kali VM.
- Learn more about Elastic's analysis and visualization tools to enhance your security skills.

This project offers practical experience in security monitoring, making you better prepared for roles such as a security analyst or engineer.

Implementation:



```
┌──(root㉿aditya13)-[/home/aditya13]
└─# ping 192.168.1.23
PING 192.168.1.23 (192.168.1.23) 56(84) bytes of data.
64 bytes from 192.168.1.23: icmp_seq=1 ttl=64 time=0.207 ms
64 bytes from 192.168.1.23: icmp_seq=2 ttl=64 time=1.17 ms
64 bytes from 192.168.1.23: icmp_seq=3 ttl=64 time=0.431 ms
^C
── 192.168.1.23 ping statistics ──
3 packets transmitted, 3 received, 0% packet loss, time 2023ms
rtt min/avg/max/mdev = 0.207/0.601/1.167/0.410 ms

┌──(root㉿aditya13)-[/home/aditya13]
└─# nmap -A -sV 192.168.1.23
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-26 11:06 IST
Nmap scan report for 192.168.1.23 (192.168.1.23)
Host is up (0.00075s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.1.14
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|_    SSL2_DES_64_CBC_WITH_MD5
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
|_ssl-date: 2024-09-26T05:38:11+00:00; +3s from scanner time.
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
```

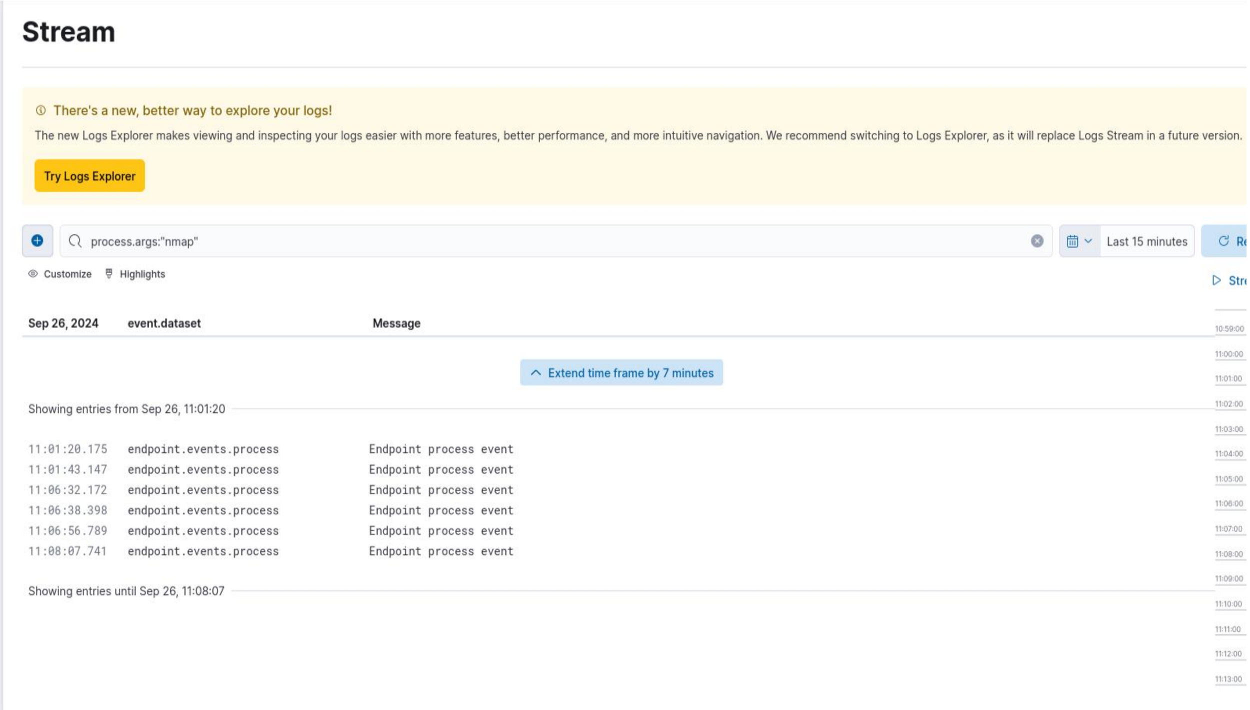


Sep 26, 2024 @ 10:55:27.019 - Sep 26, 2024 @ 11:10:27.019 (interval: Auto - 30 seconds)

Get the best look at your search results

Add relevant fields, reorder and sort columns, resize rows, and more in the document table.

```
Sep 26, 2024 @ 11:10:10.345  @timestamp Sep 26, 2024 @ 11:10:10.345 agent.ephemeral_id 22ba4916-eaf5-48e1-ae1f-428c53395067 agent.id e6a42f80-614e-486e-9c5f-2144f40be46d agent.name aditya13 agent.type endpoint
                             agent.version 8.15.1 component.binary endpoint-security component.dataset elastic_agent.endpoint_security component.id endpoint-default component.type endpoint data_stream.dataset elas
                             tic_agent.endpoint_security data_stream.namespace default data_stream.type logs ecs.version 8.10.0 elastic_agent.id e6a42f80-614e-486e-9c5f-2144f40be46d elastic_agent.snapshot false…
Sep 26, 2024 @ 11:10:02.460  @timestamp Sep 26, 2024 @ 11:10:02.460 agent.id e6a42f80-614e-486e-9c5f-2144f40be46d agent.type endpoint agent.version 8.15.1 data_stream.dataset endpoint.events.process
                             data_stream.namespace default data_stream.type logs ecs.version 8.10.0 elastic.agent.id e6a42f80-614e-486e-9c5f-2144f40be46d event.action end event.agent_id_status verified
                             event.category process event.created Sep 26, 2024 @ 11:10:02.460 event.dataset endpoint.events.process event.id NjHky2IddOMxt1OL+++++90D event.ingested Sep 26, 2024 @ 11:10:23.000…
Sep 26, 2024 @ 11:10:02.460  @timestamp Sep 26, 2024 @ 11:10:02.460 agent.id e6a42f80-614e-486e-9c5f-2144f40be46d agent.type endpoint agent.version 8.15.1 data_stream.dataset endpoint.events.process
                             data_stream.namespace default data_stream.type logs ecs.version 8.10.0 elastic.agent.id e6a42f80-614e-486e-9c5f-2144f40be46d event.action end event.agent_id_status verified
                             event.category process event.created Sep 26, 2024 @ 11:10:02.460 event.dataset endpoint.events.process event.id NjHky2IddOMxt1OL+++++90B event.ingested Sep 26, 2024 @ 11:10:23.000…
Sep 26, 2024 @ 11:10:02.459  @timestamp Sep 26, 2024 @ 11:10:02.459 agent.id e6a42f80-614e-486e-9c5f-2144f40be46d agent.type endpoint agent.version 8.15.1 data_stream.dataset endpoint.events.process
                             data_stream.namespace default data_stream.type logs ecs.version 8.10.0 elastic.agent.id e6a42f80-614e-486e-9c5f-2144f40be46d event.action end event.agent_id_status verified
                             event.category process event.created Sep 26, 2024 @ 11:10:02.459 event.dataset endpoint.events.process event.id NjHky2IddOMxt1OL+++++909 event.ingested Sep 26, 2024 @ 11:10:23.000…
Sep 26, 2024 @ 11:10:02.459  @timestamp Sep 26, 2024 @ 11:10:02.459 agent.id e6a42f80-614e-486e-9c5f-2144f40be46d agent.type endpoint agent.version 8.15.1 data_stream.dataset endpoint.events.process
                             data_stream.namespace default data_stream.type logs ecs.version 8.10.0 elastic.agent.id e6a42f80-614e-486e-9c5f-2144f40be46d event.action end event.agent_id_status verified
                             event.category process event.created Sep 26, 2024 @ 11:10:02.459 event.dataset endpoint.events.process event.id NjHky2IddOMxt1OL+++++908 event.ingested Sep 26, 2024 @ 11:10:23.000…
Sep 26, 2024 @ 11:10:02.459  @timestamp Sep 26, 2024 @ 11:10:02.459 agent.id e6a42f80-614e-486e-9c5f-2144f40be46d agent.type endpoint agent.version 8.15.1 data_stream.dataset endpoint.events.process
                             data_stream.namespace default data_stream.type logs ecs.version 8.10.0 elastic.agent.id e6a42f80-614e-486e-9c5f-2144f40be46d event.action exec event.agent_id_status verified
                             event.category process event.created Sep 26, 2024 @ 11:10:02.459 event.dataset endpoint.events.process event.id NjHky2IddOMxt1OL+++++902 event.ingested Sep 26, 2024 @ 11:10:23.000…
```



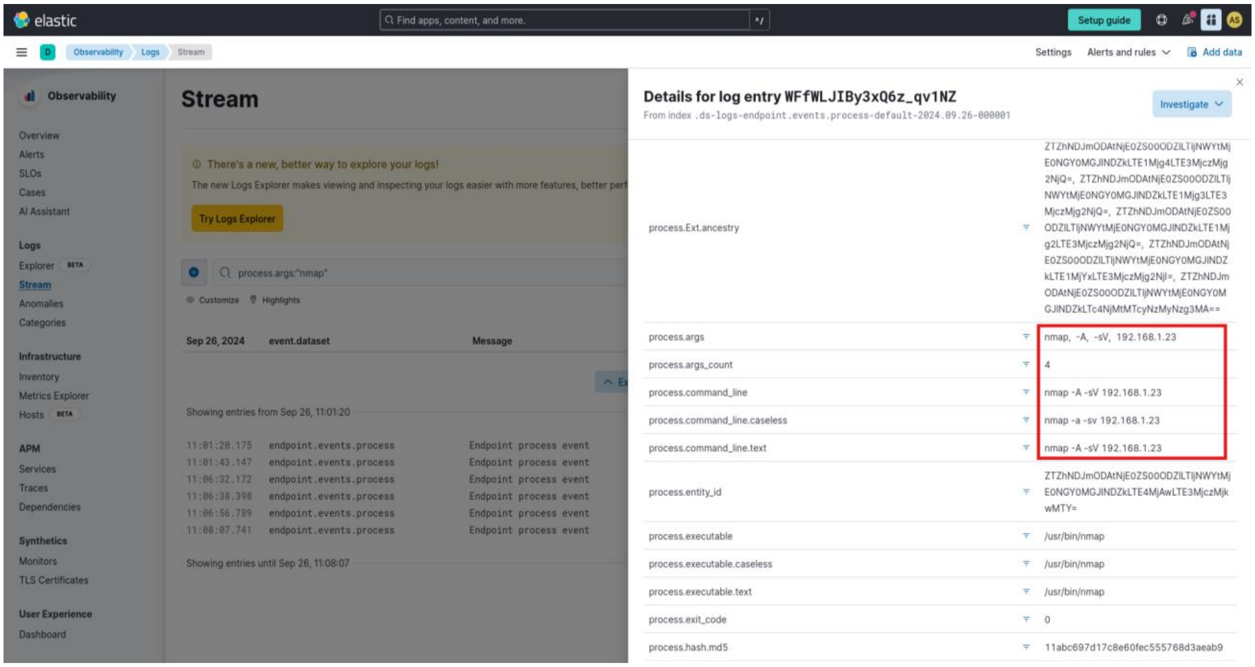
Stream

ⓘ There's a new, better way to explore your logs!

The new Logs Explorer makes viewing and inspecting your logs easier with more features, better performance, and more intuitive navigation. We recommend switching to Logs Explorer, as it will replace Logs Stream in a future version.

process.args:"nmap"

```
Sep 26, 2024   event.dataset                Message

Showing entries from Sep 26, 11:01:20

11:01:20.175   endpoint.events.process      Endpoint process event
11:01:43.147   endpoint.events.process      Endpoint process event
11:06:32.172   endpoint.events.process      Endpoint process event
11:06:38.398   endpoint.events.process      Endpoint process event
11:06:56.789   endpoint.events.process      Endpoint process event
11:08:07.741   endpoint.events.process      Endpoint process event

Showing entries until Sep 26, 11:08:07
```



Stream

ⓘ There's a new, better way to explore your logs!

The new Logs Explorer makes viewing and inspecting your logs easier with more features, better perf

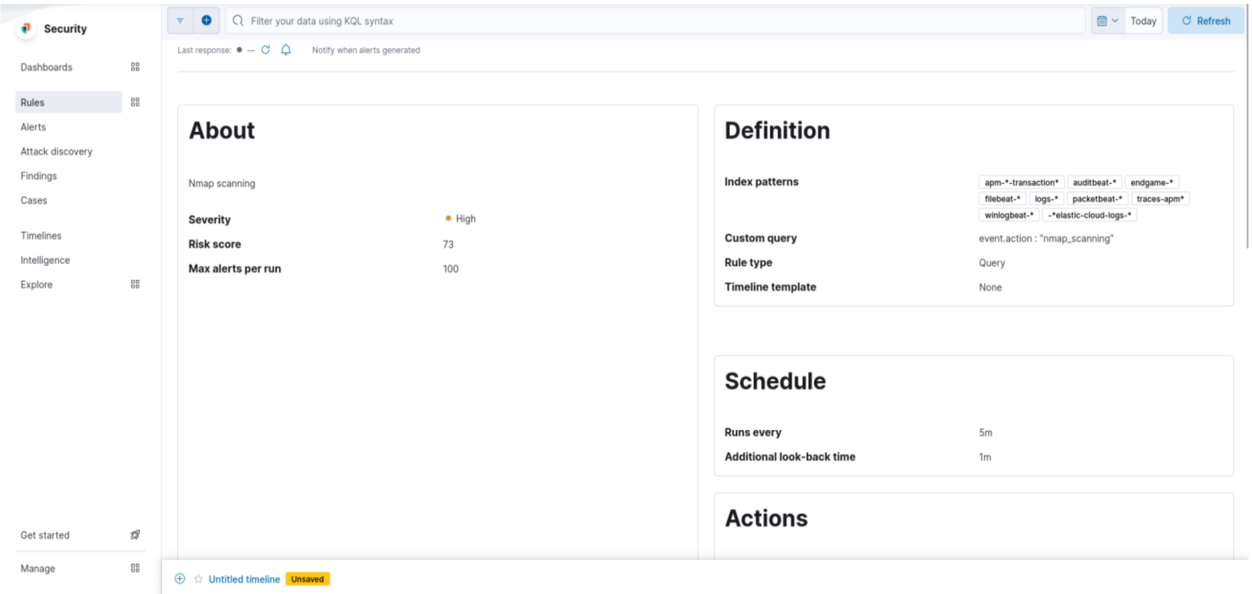
process.args:"nmap"

```
Sep 26, 2024   event.dataset                Message

Showing entries from Sep 26, 11:01:20

11:01:20.175   endpoint.events.process      Endpoint process event
11:01:43.147   endpoint.events.process      Endpoint process event
11:06:32.172   endpoint.events.process      Endpoint process event
11:06:38.398   endpoint.events.process      Endpoint process event
11:06:56.789   endpoint.events.process      Endpoint process event
11:08:07.741   endpoint.events.process      Endpoint process event

Showing entries until Sep 26, 11:08:07
```

Details for log entry WFfWLJIBy3xQ6z_qv1NZ

From index .ds-logs-endpoint.events.process-default-2024.09.26-000001

process.Ext.ancestry	ZTZhNDJmODAtNjE0ZS00ODZlLTljNWYtMjE0NGY0MGJlNDZkLTE1Mjg4LTE3MjczMjg2NjQ=, ZTZhNDJmODAtNjE0ZS00ODZlLTljNWYtMjE0NGY0MGJlNDZkLTE1Mjg3LTE3MjczMjg2NjQ=, ZTZhNDJmODAtNjE0ZS00ODZlLTljNWYtMjE0NGY0MGJlNDZkLTE1Mjg2LTE3MjczMjg2NjQ=, ZTZhNDJmODAtNjE0ZS00ODZlLTljNWYtMjE0NGY0MGJlNDZkLTE1MjYxLTE3MjczMjg2NjI=, ZTZhNDJmODAtNjE0ZS00ODZlLTljNWYtMjE0NGY0MGJlNDZkLTc4NjMtMTcyNzMyNzg3MA==
process.args	nmap, -A, -sV, 192.168.1.23
process.args_count	4
process.command_line	nmap -A -sV 192.168.1.23
process.command_line.caseless	nmap -a -sv 192.168.1.23
process.command_line.text	nmap -A -sV 192.168.1.23
process.entity_id	ZTZhNDJmODAtNjE0ZS00ODZlLTljNWYtMjE0NGY0MGJlNDZkLTE4MjAwLTE3MjczMjkwMTY=
process.executable	/usr/bin/nmap
process.executable.caseless	/usr/bin/nmap
process.executable.text	/usr/bin/nmap
process.exit_code	0
process.hash.md5	11abc697d17c8e60fec555768d3aeab9



About

Nmap scanning

Severity	● High
Risk score	73
Max alerts per run	100

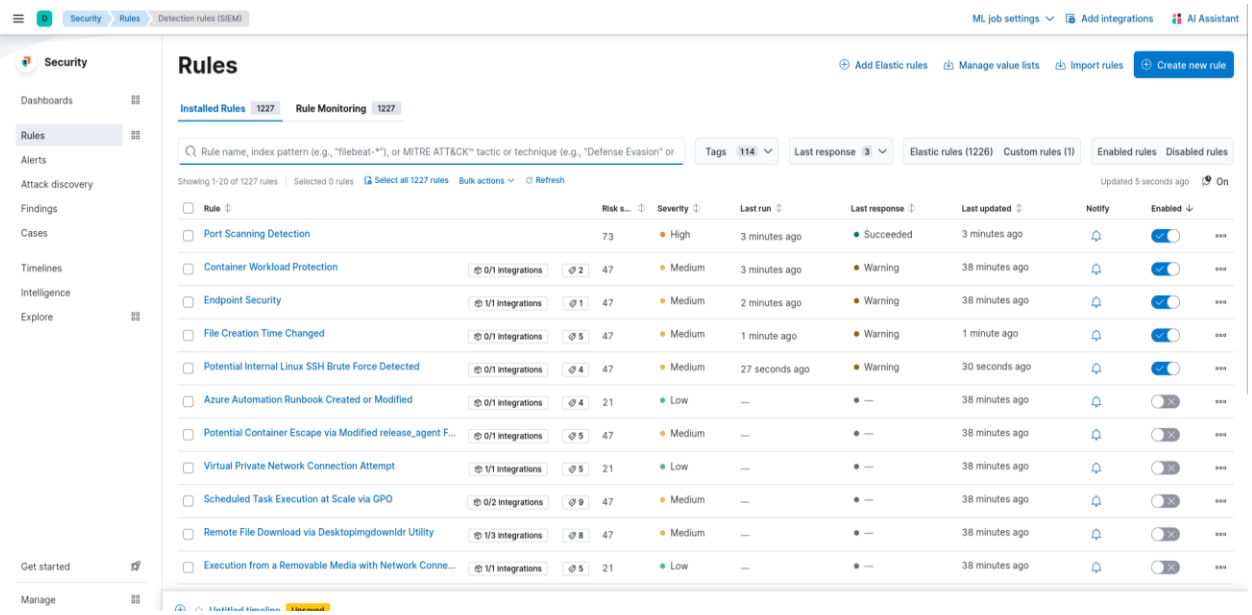
Definition

Index patterns	apm-*-transaction* auditbeat-* endgame-* filebeat-* logs-* packetbeat-* traces-apm* winlogbeat-* -*elastic-cloud-logs-*
Custom query	event.action : "nmap_scanning"
Rule type	Query
Timeline template	None

Schedule

Runs every	5m
Additional look-back time	1m

Actions

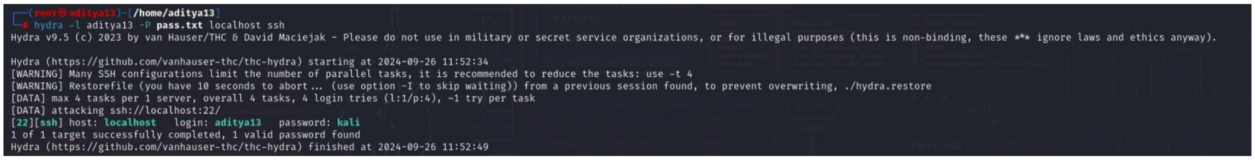


Rules

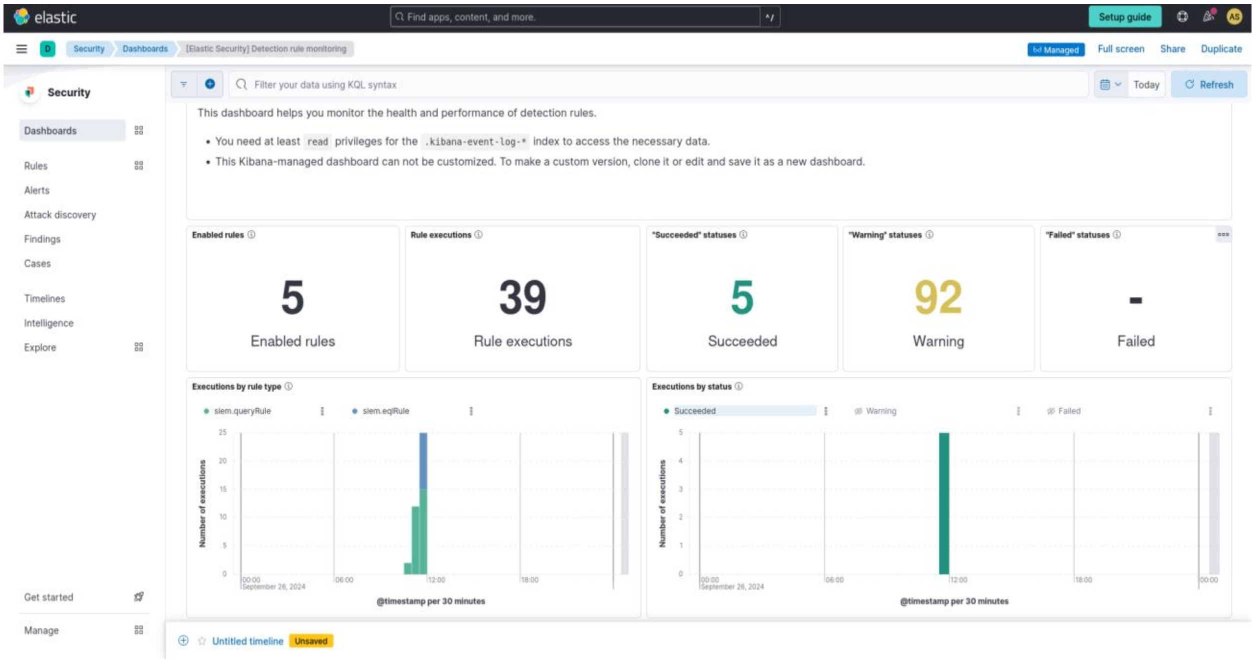
Showing 1-20 of 1227 rules | Selected 0 rules

Updated 5 seconds ago

Rule			Risk s...	Severity	Last run	Last response	Last updated	Notify	Enabled
Port Scanning Detection			73	● High	3 minutes ago	● Succeeded	3 minutes ago		✓
Container Workload Protection	0/1 integrations	2	47	● Medium	3 minutes ago	● Warning	38 minutes ago		✓
Endpoint Security	1/1 integrations	1	47	● Medium	2 minutes ago	● Warning	38 minutes ago		✓
File Creation Time Changed	0/1 integrations	5	47	● Medium	1 minute ago	● Warning	1 minute ago		✓
Potential Internal Linux SSH Brute Force Detected	0/1 integrations	4	47	● Medium	27 seconds ago	● Warning	30 seconds ago		✓
Azure Automation Runbook Created or Modified	0/1 integrations	4	21	● Low	—	● —	38 minutes ago		✕
Potential Container Escape via Modified release_agent F...	0/1 integrations	5	47	● Medium	—	● —	38 minutes ago		✕
Virtual Private Network Connection Attempt	1/1 integrations	5	21	● Low	—	● —	38 minutes ago		✕
Scheduled Task Execution at Scale via GPO	0/2 integrations	9	47	● Medium	—	● —	38 minutes ago		✕
Remote File Download via Desktopimgdownldr Utility	1/3 integrations	8	47	● Medium	—	● —	38 minutes ago		✕
Execution from a Removable Media with Network Conne...	1/1 integrations	5	21	● Low	—	● —	38 minutes ago		✕



```
┌──(root㉿aditya13)-[/home/aditya13]
└─# hydra -l aditya13 -P pass.txt localhost ssh
Hydra v9.5 (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 2024-09-26 11:52:34
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 4 login tries (l:1/p:4), ~1 try per task
[DATA] attacking ssh://localhost:22/
[22][ssh] host: localhost   login: aditya13   password: kali
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-09-26 11:52:49
```



This dashboard helps you monitor the health and performance of detection rules.

- You need at least `read` privileges for the `.kibana-event-log-*` index to access the necessary data.
- This Kibana-managed dashboard can not be customized. To make a custom version, clone it or edit and save it as a new dashboard.

Enabled rules	Rule executions	"Succeeded" statuses	"Warning" statuses	"Failed" statuses
5 Enabled rules	39 Rule executions	5 Succeeded	92 Warning	- Failed