

Wazuh - Endpoint Security

By:

- Galiev Arsen - a.galiev@innopolis.university
- Nguen Ilya-Linh - i.nguen@innopolis.university
- Zavadskii Peter - p.zavadskii@innopolis.university

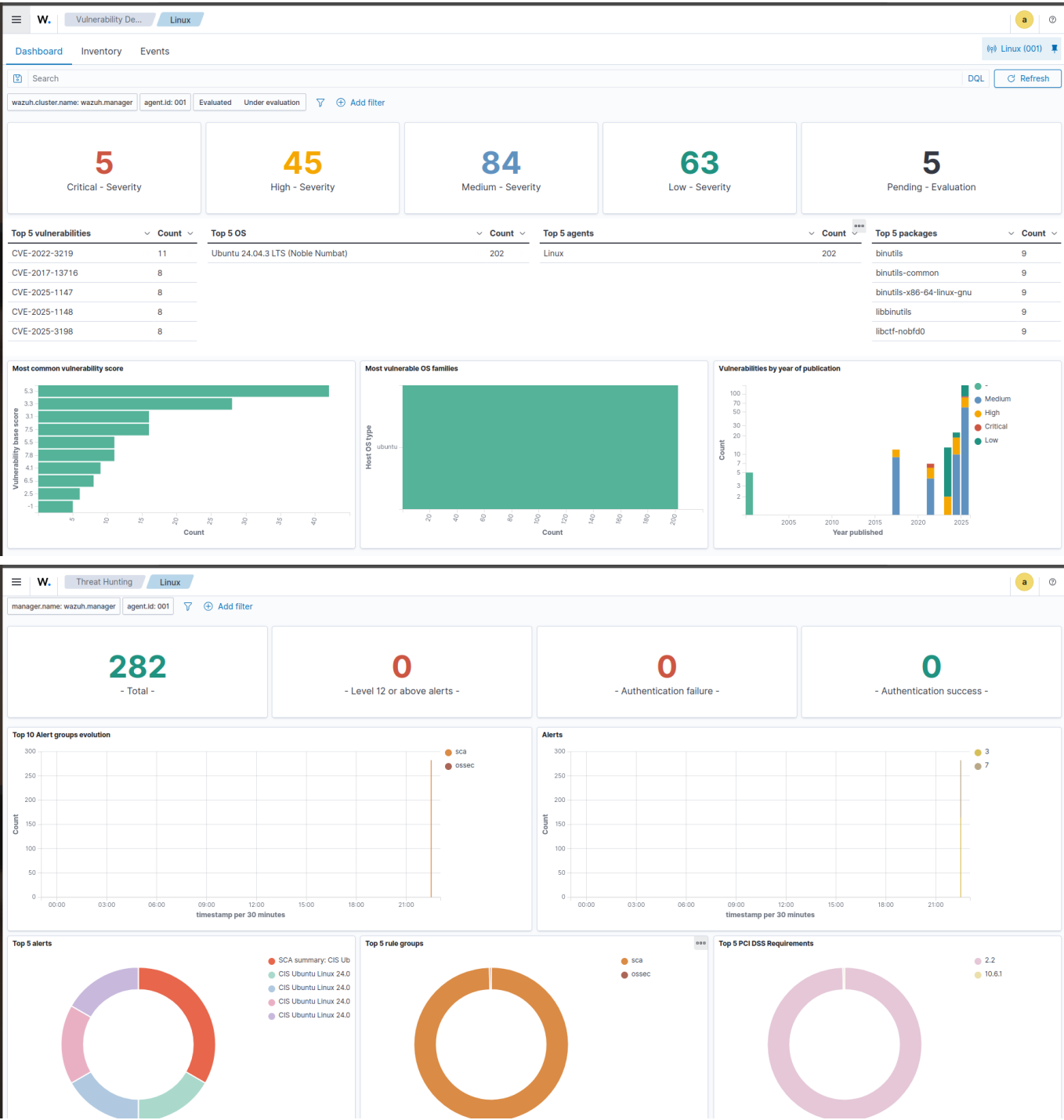
Reference to Innopolis University F25 Network and Cybersecurity course: [link](#)

Exercise 1: Vulnerability Detection and SCA

- What is the difference between authenticated and unauthenticated vulnerability scans? Why do both types need to be performed periodically?

An **unauthenticated** scan is performed as an *external attacker*, while an **authenticated** scan is an authorized process that analyzes internal resources (not available to external users).

- Show detected vulnerabilities on the monitored endpoint. Explain whether the results indicate that Wazuh performed an authenticated or an unauthenticated scan.



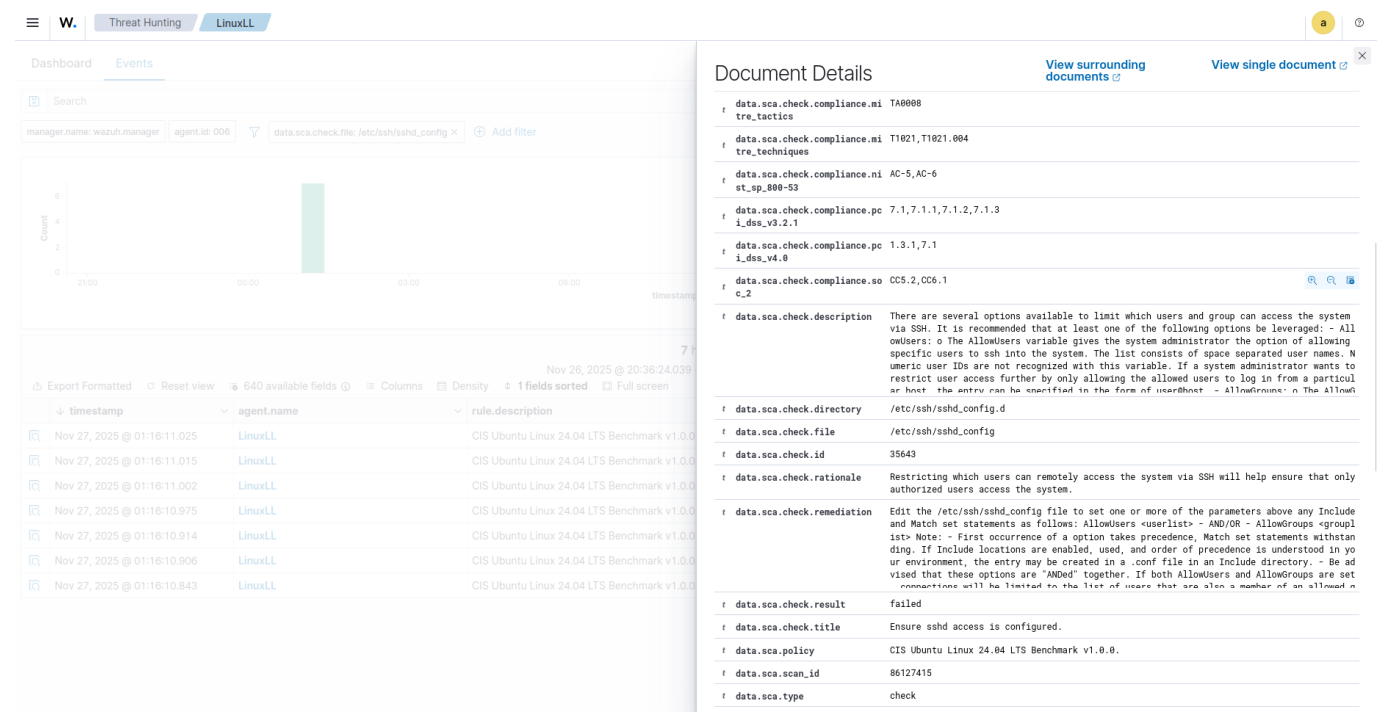
Wazuh obviously performed an authenticated scan. Two facts can be provided:

- 1. The scan was done by the agent *we installed* on the endpoint, so it has full access to the system.
 - 2. The scan contains results for system packages (e.g., Debian toolkit utilities).
- What is SCA? Show and explain the relevant scans carried out by Wazuh's SCA module against the monitored endpoint.

SCA (Software Composition Analysis) is an automated process where software is checked for Open Source Software (OSS), which is further checked for updates, vulnerabilities, license problems, and policy creation.

Reference: [Solar blog](#)

I chose an SCA scan for the openssh-server (sshd) that I had previously installed on the agent:



Yes, there are different agent names in the screenshots because I am still struggling with Active Response and added another screenshot.

Exercise 2: File Integrity Monitoring

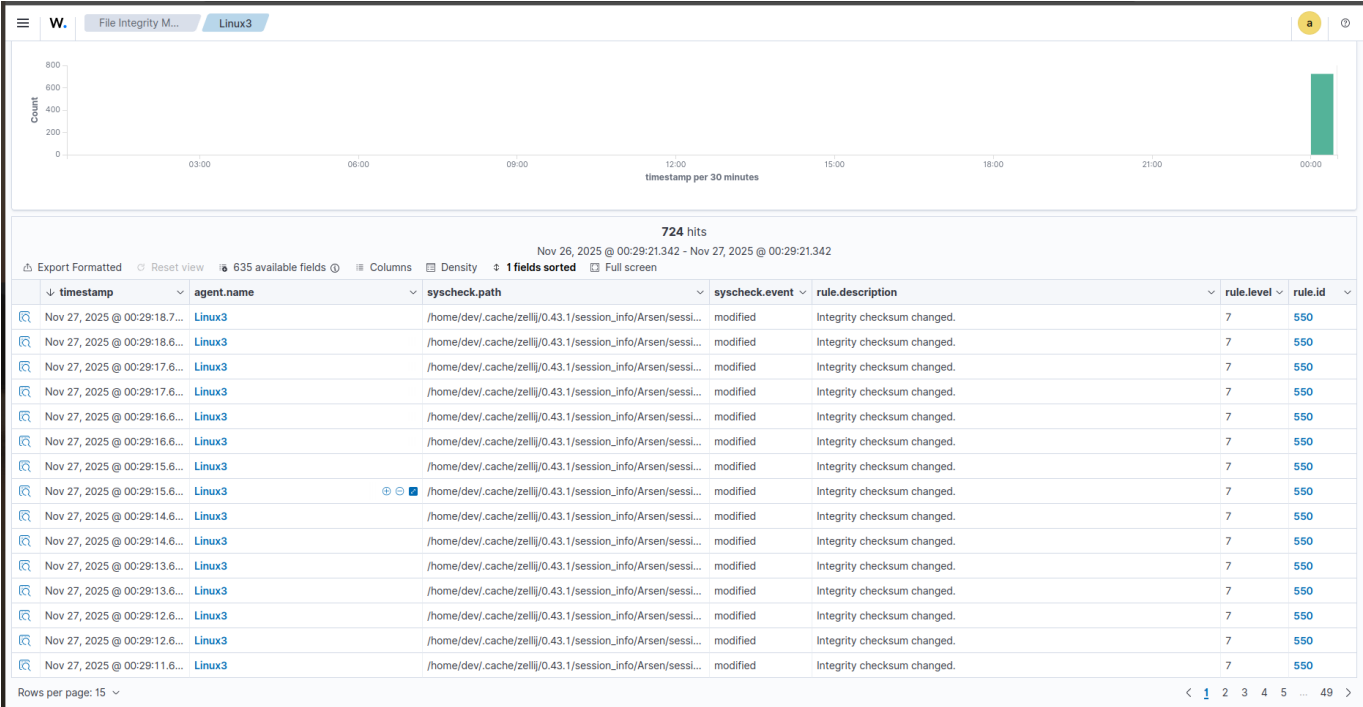
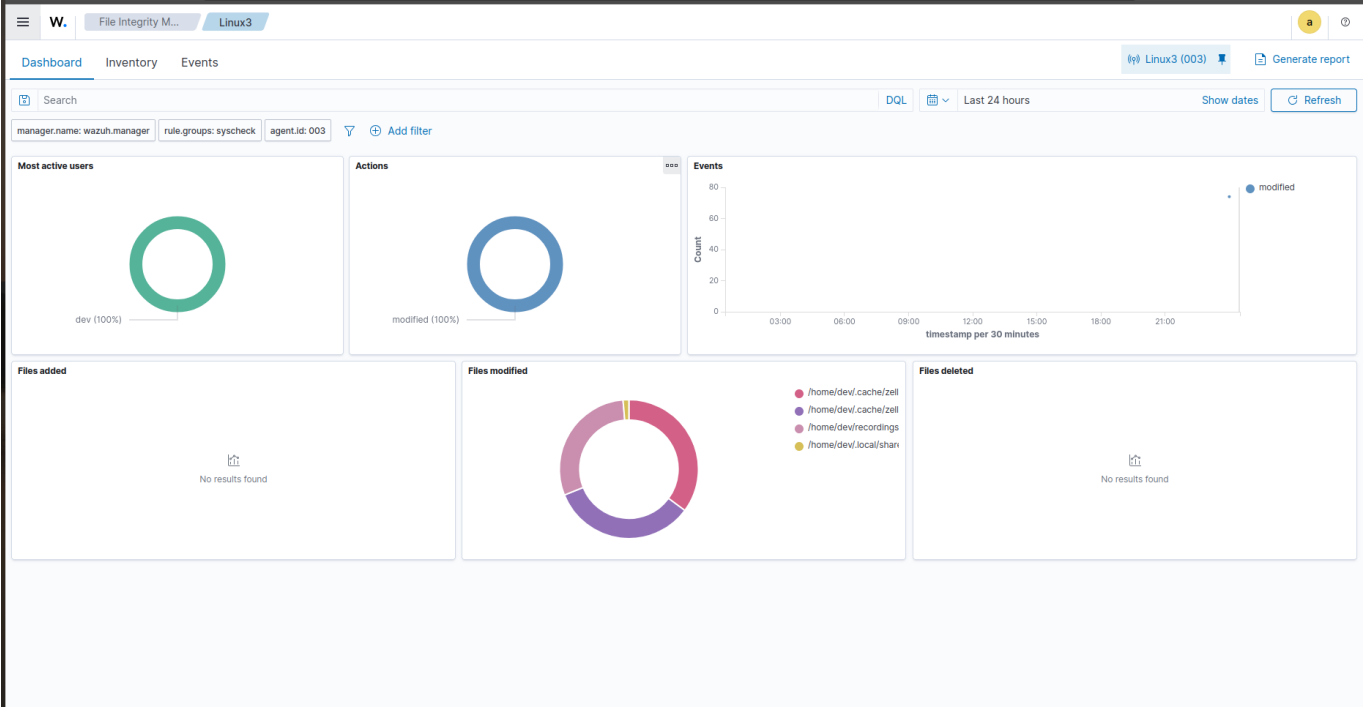
Configure Wazuh's File Integrity Monitoring (FIM) to audit a directory of your choice.

How I did it... (two attempts with two different folders)

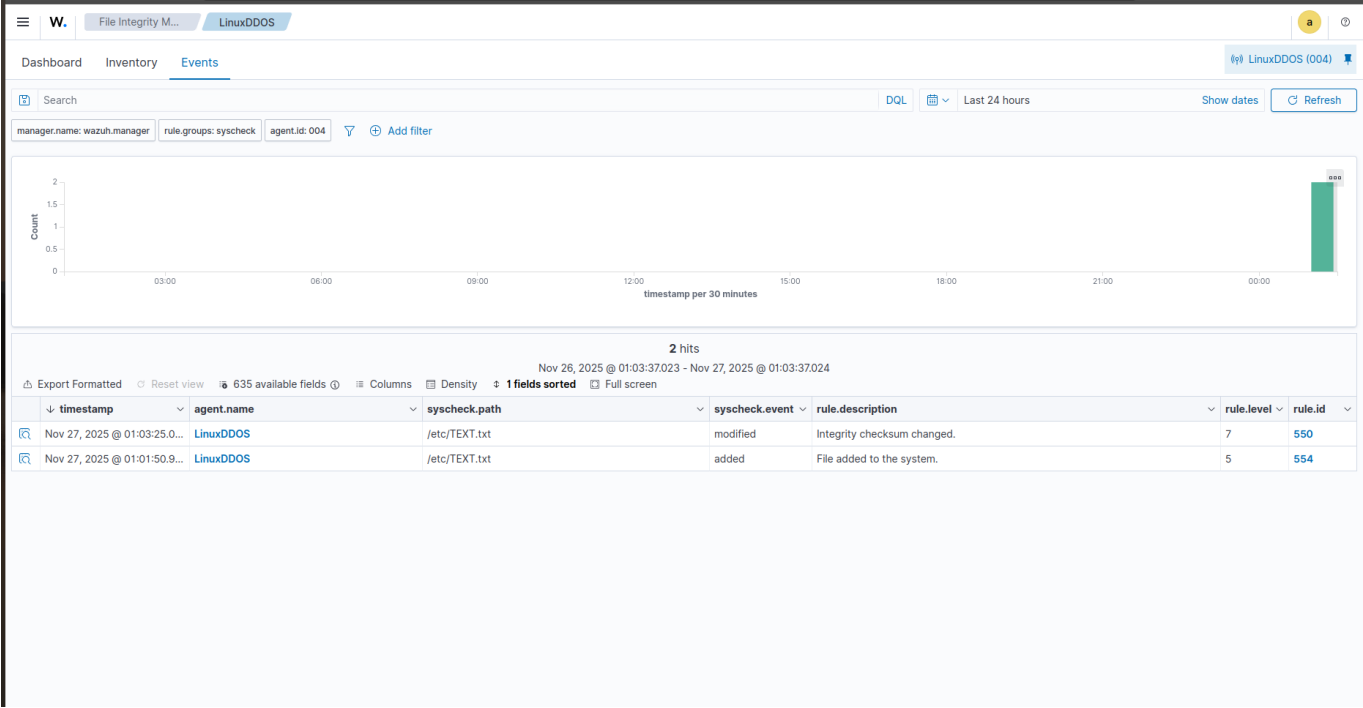
- <https://asciinema.org/a/2NqmTUFVYLzuL3YtXH9c4hD8x>
- <https://asciinema.org/a/X8QlU6s76aemuJrYL21jBvYOB>

Create a text file in the monitored directory then wait for 5 seconds. Add content to the text file and save it. Wait for 5 seconds. Delete the text file from the monitored directory. Show relevant events (triggered rules) in the dashboard.

Since in one of the solutions I specified the `/home` folder, the changes made during the `asciinema` recording affected the events:



Here is another attempt, as required by the task:



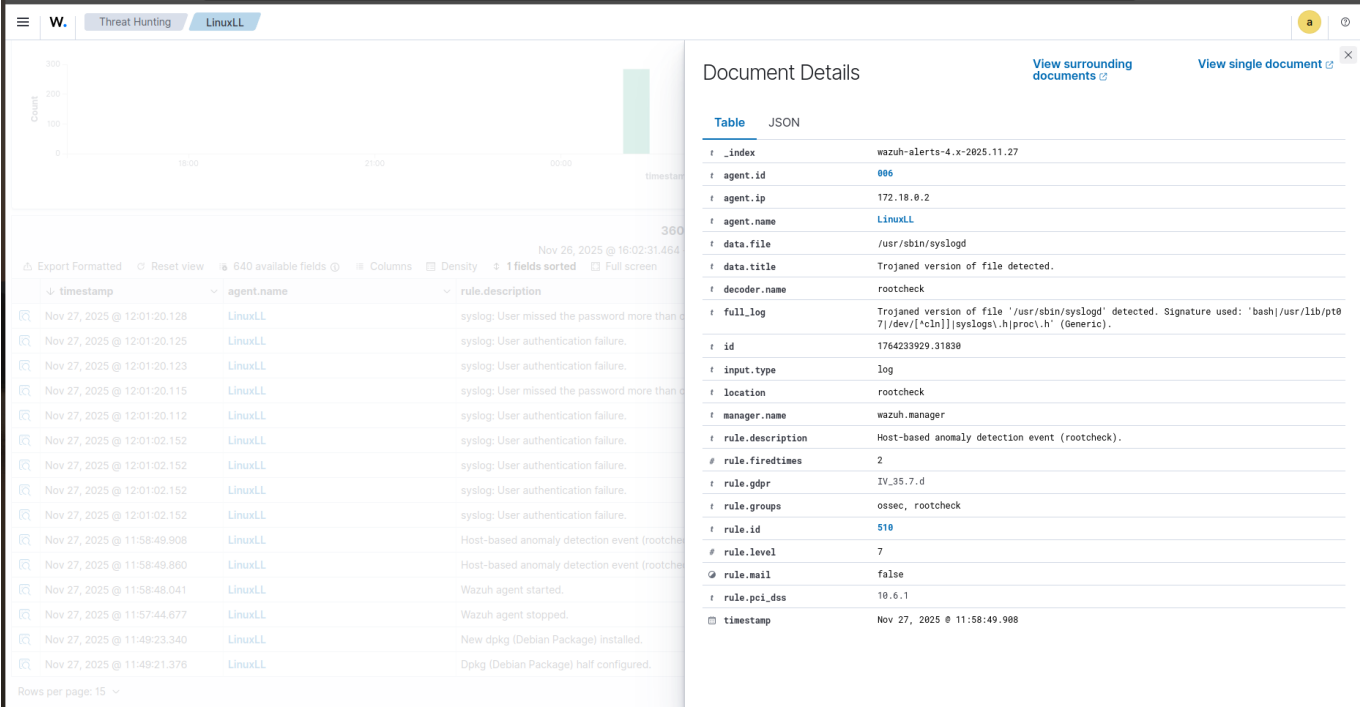
Exercise 3: Active Response

There are several obstacles here:

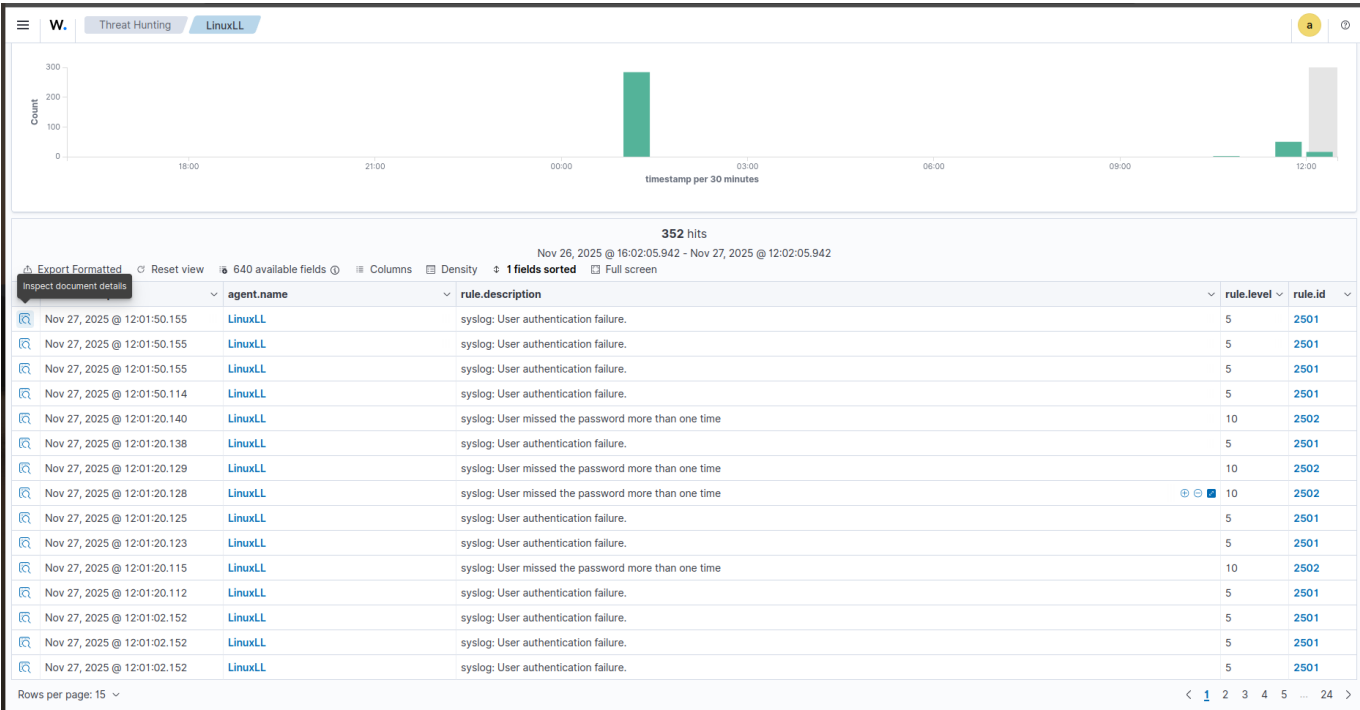
- 1. The agent by default does not have SSH server logging and logger.
- 2. The Wazuh manager container has a minimal security setup, with almost no way to change the config at the moment and restart.
- 3. The Wazuh manager lacks rulesets for DDoS, SSH, PAM, and syslog.

Below are some screenshots of my attempts before I found the manager config in the lab folders. Now I will redeploy everything.

Here, Wazuh alerts that busybox-syslog is a trojan.



Here I got SSH logs.



A brief overview of my attempts: <https://asciinema.org/a/iy68DxlqF74J8yMZkt5IoHdjn>

The issue was that I used `busybox-syslogd` instead of `rsyslogd`...

So what I have done to make it work:

- 1. (useless step) Changed `wazuh_manager.conf` from the repository:

```
<active-response>
<disabled>no</disabled>
<command>firewall-drop</command>
<location>local</location>
```

```
<rules_id>5763</rules_id>
<timeout>600</timeout>
</active-response>
```

A rule for IP blocking.

Then I restarted the container from the network. It didn't work since I had not configured `ossec.conf` correctly on the endpoint agent, and the logging system was not suitable for Wazuh analyzer.

2. Configuring `ossec.conf` on the endpoint:

```
<localfile>
  <log_format>syslog</log_format>
  <location>/var/log/auth.log</location>
</localfile>
```

This part is responsible for scanning the logs for authentication. The `sshd` writes logs about logins/logouts here.

```
<active-response>
  <disabled>no</disabled>
  <command>firewall-drop</command>
  <location>local</location>
  <rules_id>5763</rules_id>
  <timeout>600</timeout>
</active-response>
```

Duplicating the blocking rule.

```
<command>
  <name>firewall-drop</name>
  <executable>firewall-drop</executable>
  <timeout_allowed>yes</timeout_allowed>
</command>
```

Creating the command for IP block by endpoint firewall.

3. Removing `busybox-syslogd` and installing `rsyslog`. Now Wazuh correlates logs correctly.

Let's check the rule for the threat:

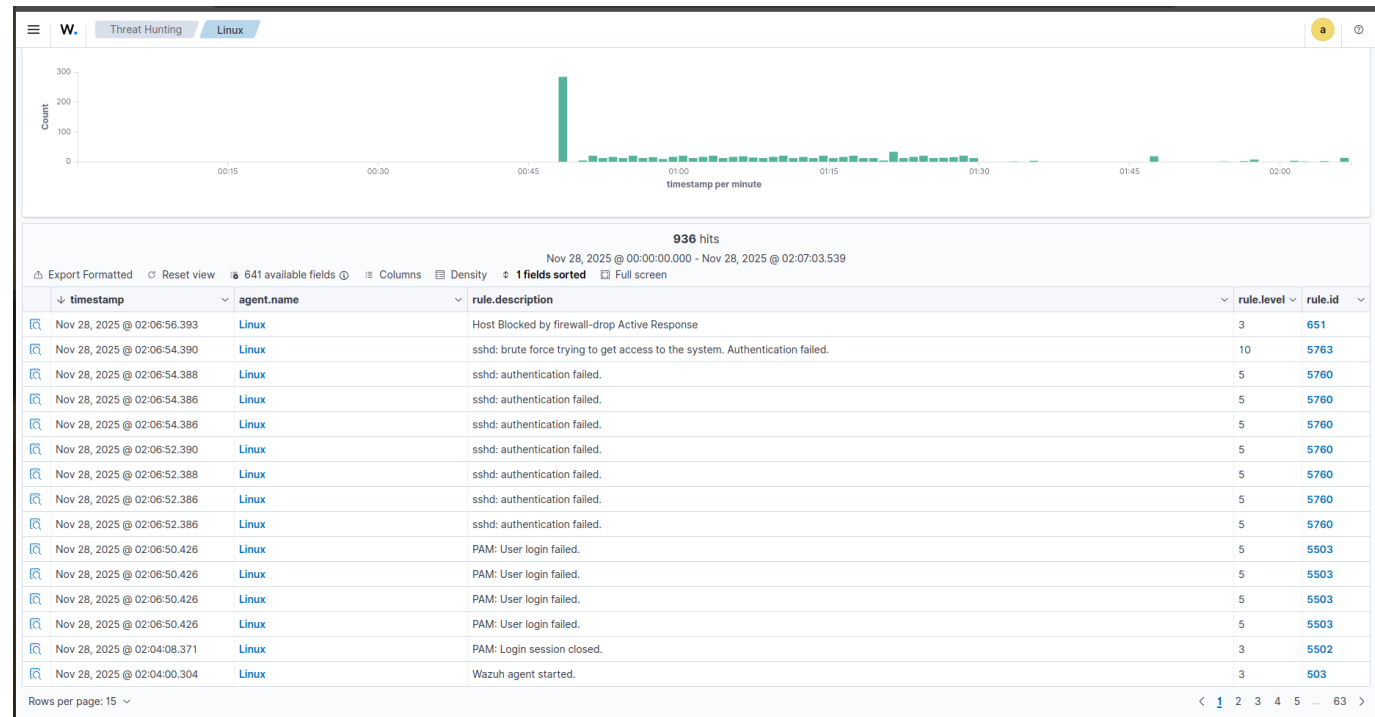
1. Hydra attacking.

```
sudo hydra -t 4 -l dev -P ~/Downloads/rockyou.txt 172.18.0.2 ssh
```

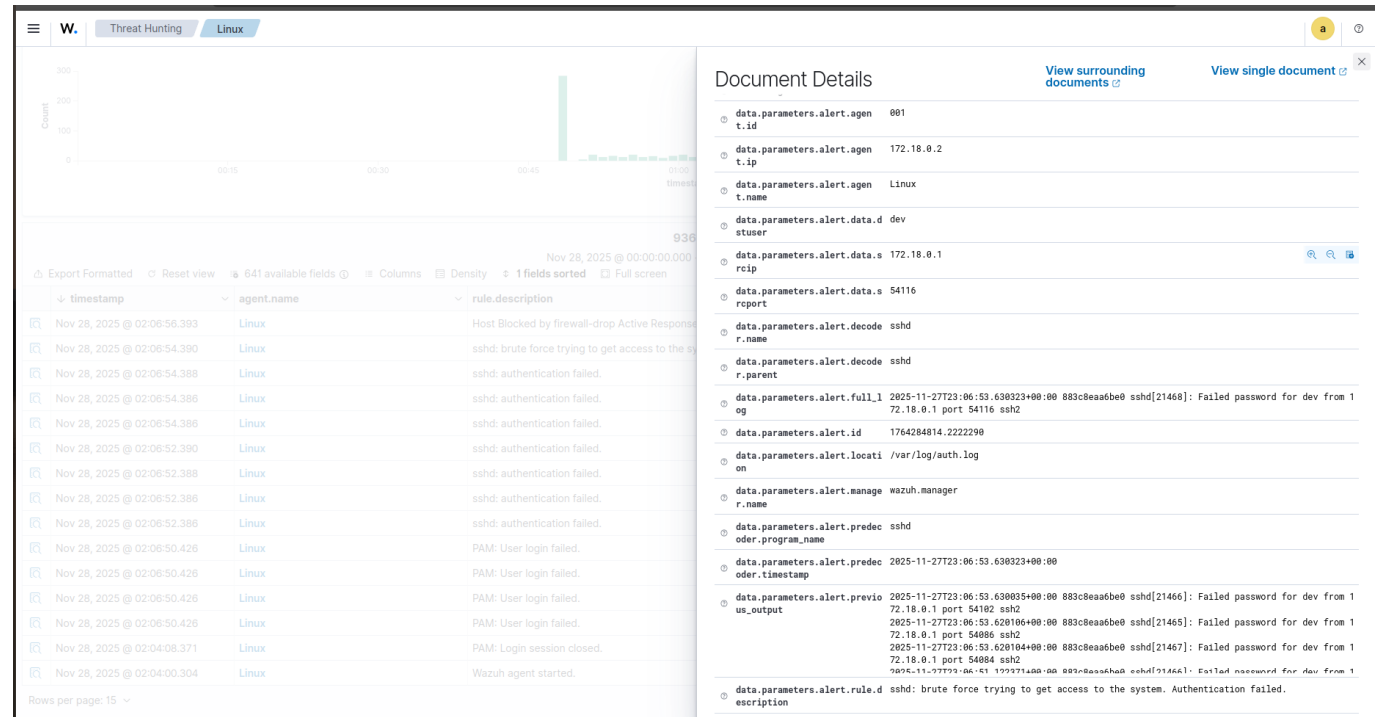
```
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-11-28 00:58:48
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries per task
[DATA] attacking ssh://172.18.0.2:22/
[STATUS] 44.00 tries/min, 44 tries in 00:01h, 14344355 to do in 5433:29h, 4 active
```

2. Wazuh logs



We can see that the manager detected brute-forcing and blocked our IP.



3. Checking the block

```
projacktor@projacktor-BOM-WXX9 ~/P/F/N/N/l/wazuh (main)> ping 172.18.0.2
PING 172.18.0.2 (172.18.0.2) 56(84) bytes of data.
^C
--- 172.18.0.2 ping statistics ---
6 packets transmitted, 0 received, 100% packet loss, time 5110ms
```

The protected agent is now unreachable.