

# 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](#)

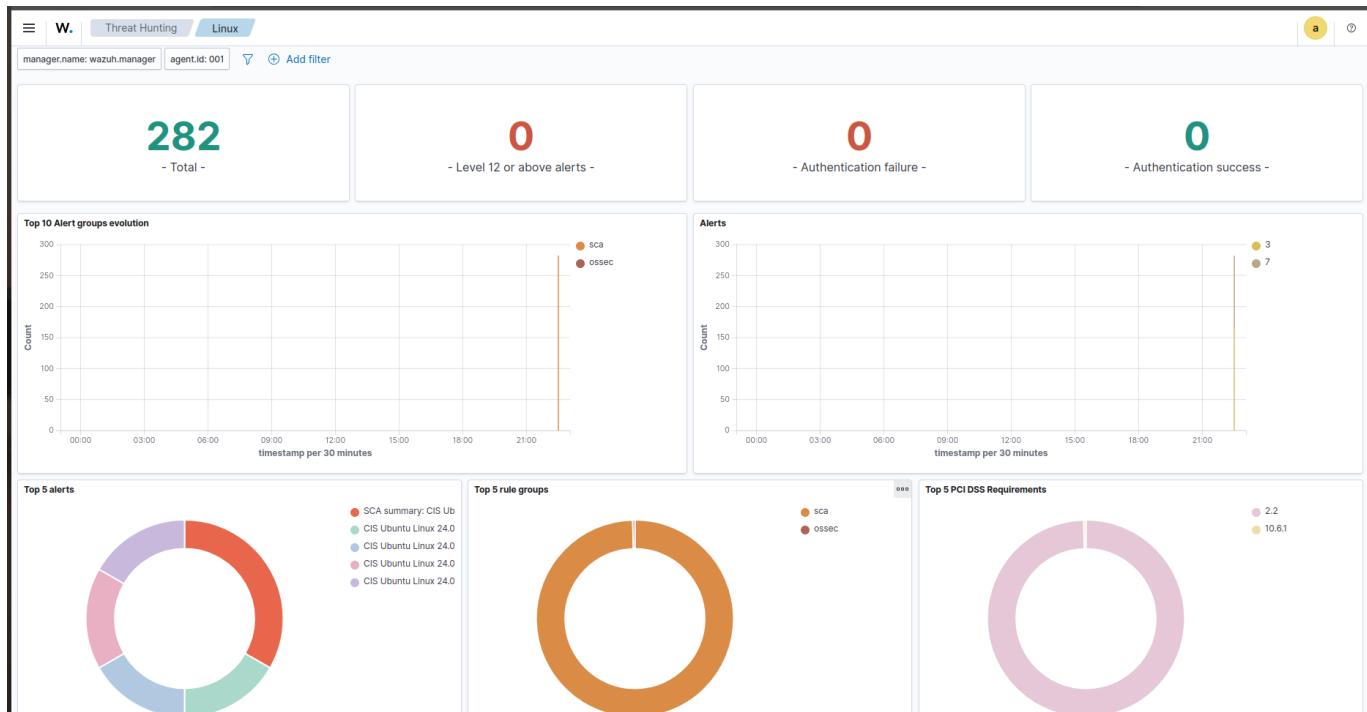
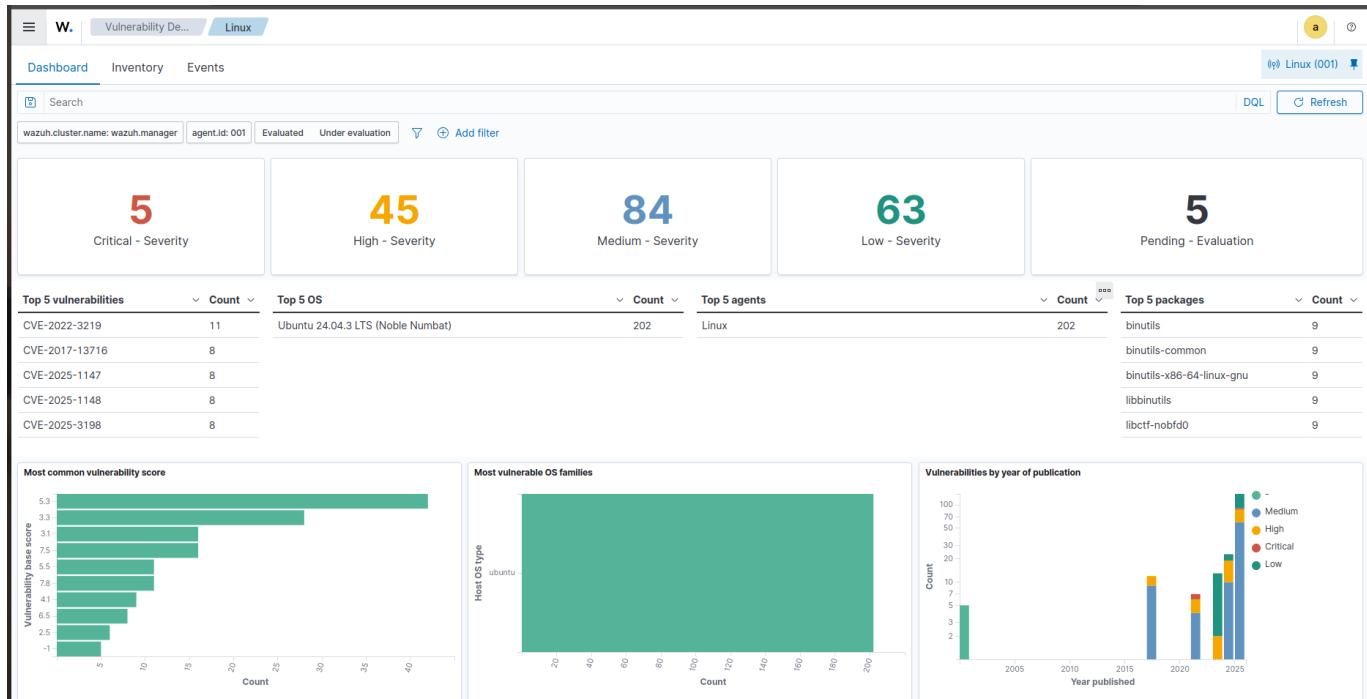
## Exercise 1: Vulnerability Detection and SCA

---

- 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:

The screenshot shows the Wazuh Threat Hunting interface. At the top, there are tabs for Dashboard, Events, and Threat Hunting (which is selected). Below the tabs, a search bar contains the query "data.sca.check.file: /etc/ssh/sshd\_config". A histogram on the left shows event counts from 21:00 to 06:00, with a single bar at 00:00. The main area displays a table of audit findings:

Timestamp	agent.name	rule.description
Nov 27, 2025 @ 01:16:11.025	LinuxLL	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0
Nov 27, 2025 @ 01:16:11.015	LinuxLL	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0
Nov 27, 2025 @ 01:16:11.002	LinuxLL	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0
Nov 27, 2025 @ 01:16:10.975	LinuxLL	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0
Nov 27, 2025 @ 01:16:10.914	LinuxLL	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0
Nov 27, 2025 @ 01:16:10.906	LinuxLL	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0
Nov 27, 2025 @ 01:16:10.843	LinuxLL	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0

To the right, a detailed view of a specific audit finding is shown:

**Document Details**

**data.sca.check.compliance.mi TA0008**  
**tre\_tactics**  
**tre\_techniques**  
**st\_sp\_800-53**  
**data.sca.check.compliance.ni AC-5,AC-6**  
**1\_dss\_v3.2.1**  
**data.sca.check.compliance.pc 7.1,7.1.1,7.1.2,7.1.3**  
**1\_dss\_v4.0**  
**data.sca.check.compliance.so CC5.2,CC6.1**  
**c\_2**

**data.sca.check.description** There are several options available to limit which users and group can access the system via SSH. It is recommended that at least one of the following options be leveraged: - All owners: o The AllowUsers variable gives the system administrator the option of allowing specific users to ssh into the system. The list consists of space separated user names. Numeric user IDs are not recognized with this variable. If a system administrator wants to restrict user access further by only allowing the allowed users to log in from a particular host, the entry can be specified in the form of user@host - AllowGroups: o The AllowGroups variable gives the system administrator the option of allowing specific groups to ssh into the system. The list consists of space separated group names. Numeric group IDs are not recognized with this variable.

**data.sca.check.directory** /etc/ssh/sshd\_config.d  
**data.sca.check.file** /etc/ssh/sshd\_config  
**data.sca.check.id** 35643  
**data.sca.check.rationale** Restricting which users can remotely access the system via SSH will help ensure that only authorized users access the system.  
**data.sca.check.remediation** Edit the /etc/ssh/sshd\_config file to set one or more of the parameters above any Include and Match set statements as follows: allowUsers <userlist> - AND/OR - AllowGroups <group list> Note: - First occurrence of a option takes precedence, Match set statements withstanding. If Include locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a .conf file in an Include directory. - Be advised that these options are "ANDed" together. If both AllowUsers and AllowGroups are set connections will be limited to the list of users that are also a member of an allowed group.  
**data.sca.check.result** failed  
**data.sca.check.title** Ensure sshd access is configured.  
**data.sca.policy** CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.  
**data.sca.scan\_id** 86127415  
**data.sca.type** check

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

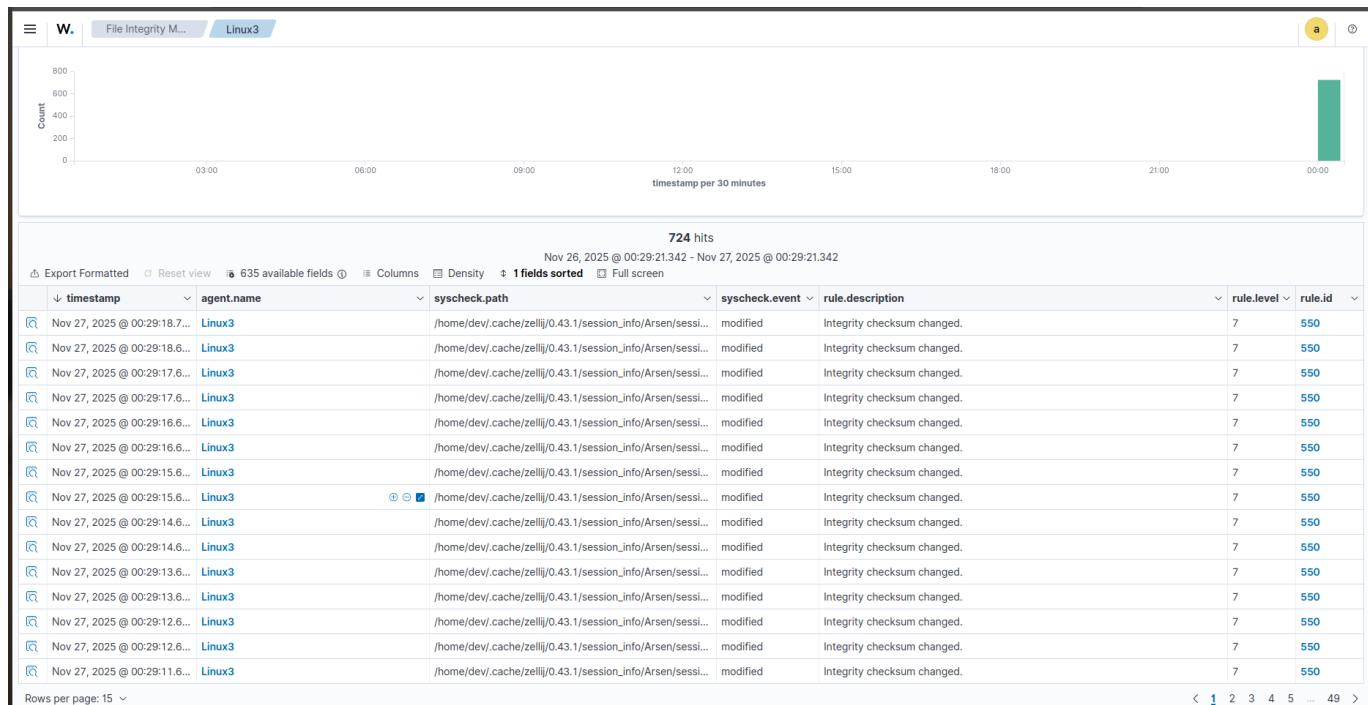
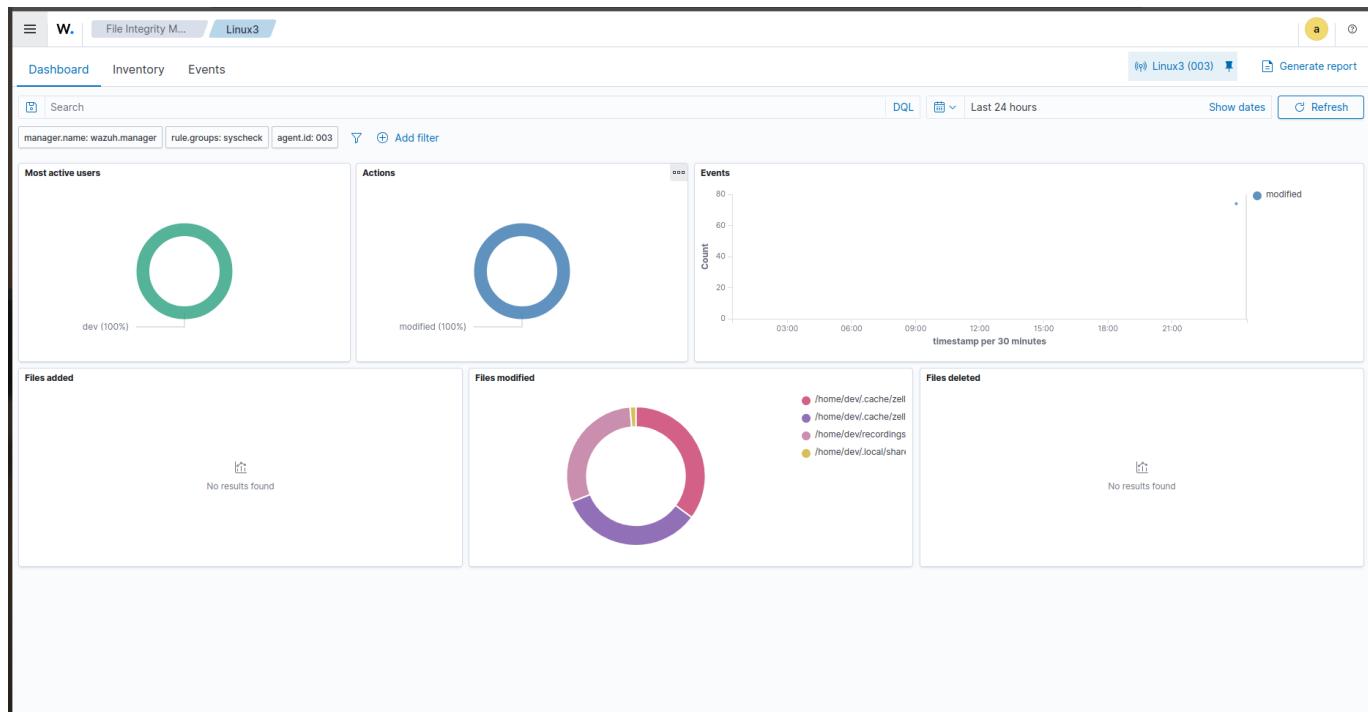
Configure Wazuh's File Integrity Monitoring (FIM) to audit a directory of your choice.

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

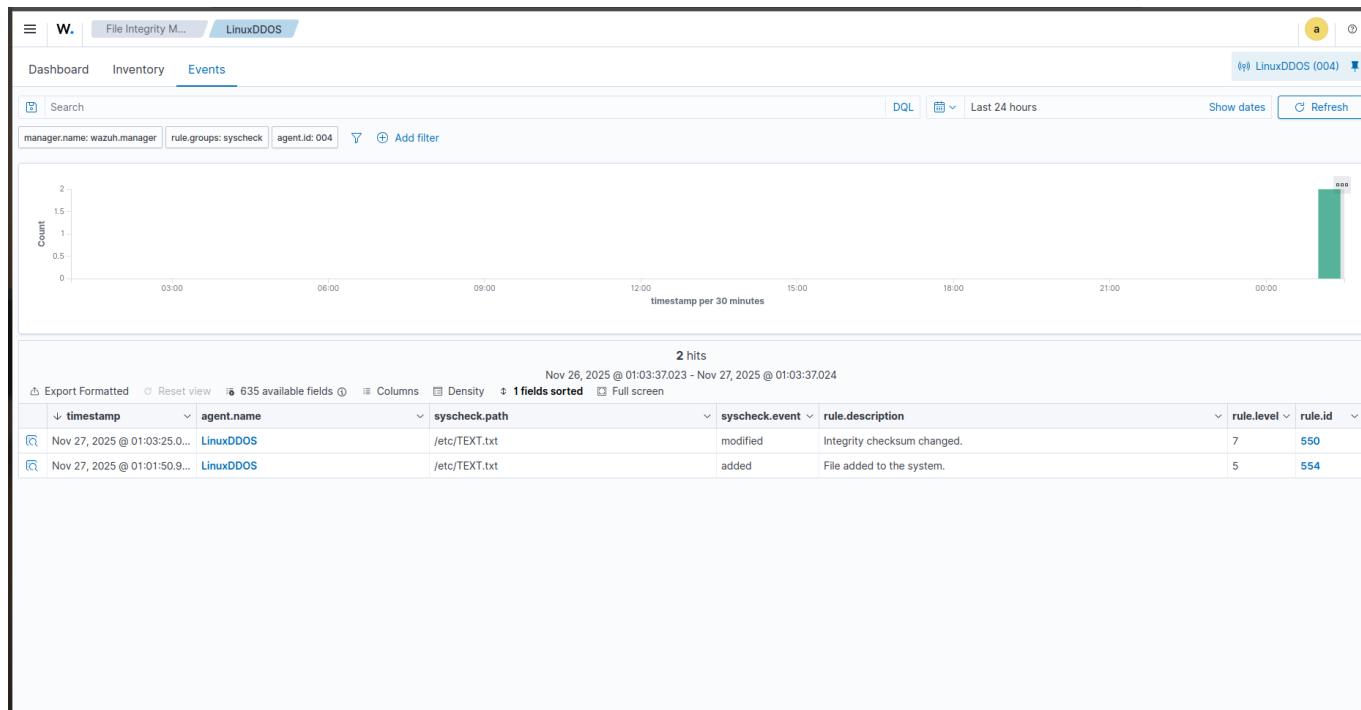
- <https://asciinema.org/a/2NqmTUFVYLzuL3YtXH9c4hD8x>
- <https://asciinema.org/a/X8QlU6s76aemuJrYL21jBvYOB>

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

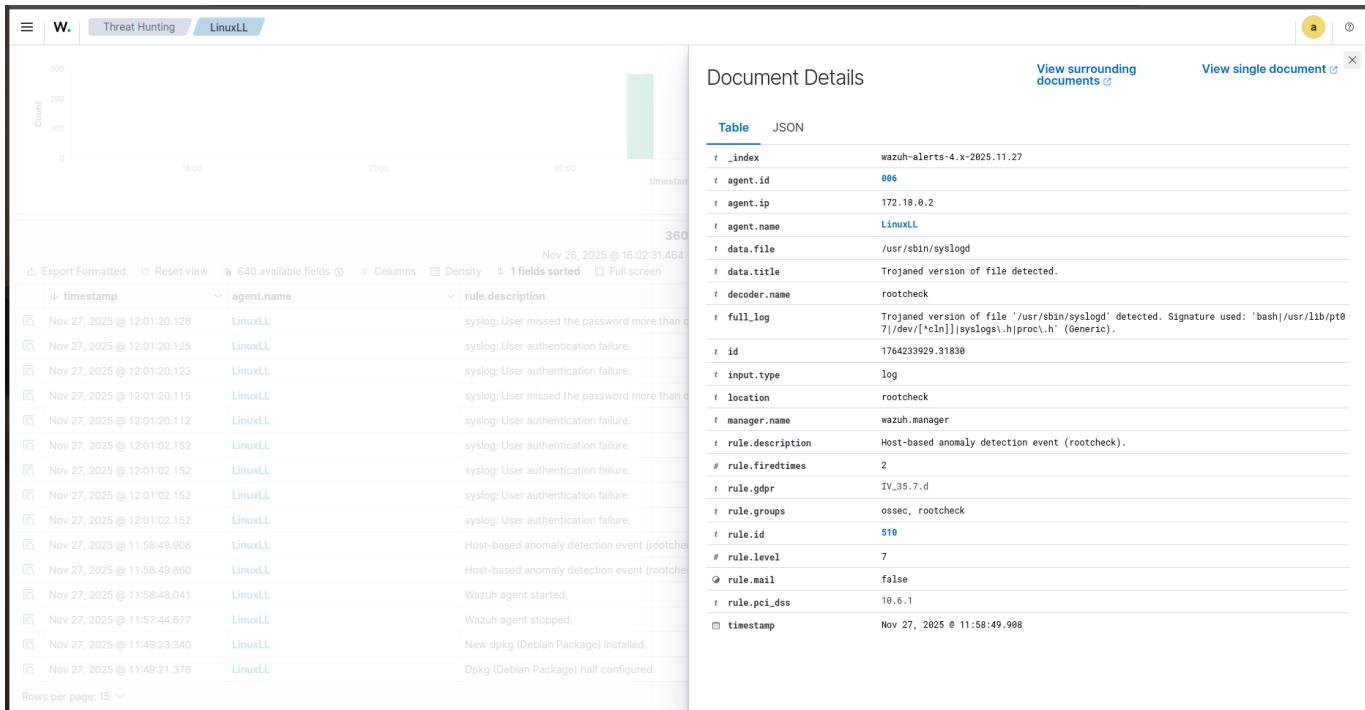
---

There are several obstacles here:

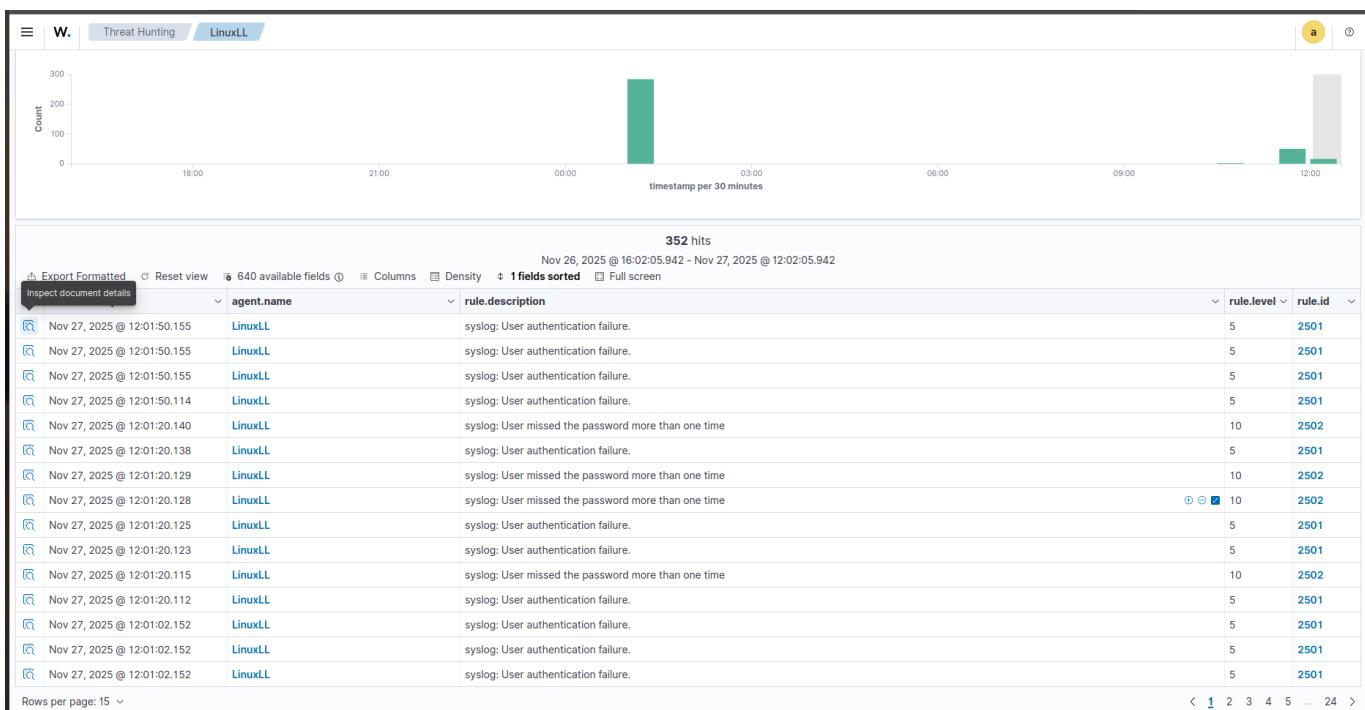
1. The agent by default does not have SSH server logging and logger.
2. The Wazuh manager container has a minimal security setup, with almost no way to change the config at the moment and restart.
3. The Wazuh manager lacks rulesets for DDoS, SSH, PAM, and syslog.

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-syslog` and installing `rsyslog`. Now Wazuh correlates logs correctly.

Let's check the rule for the threat:

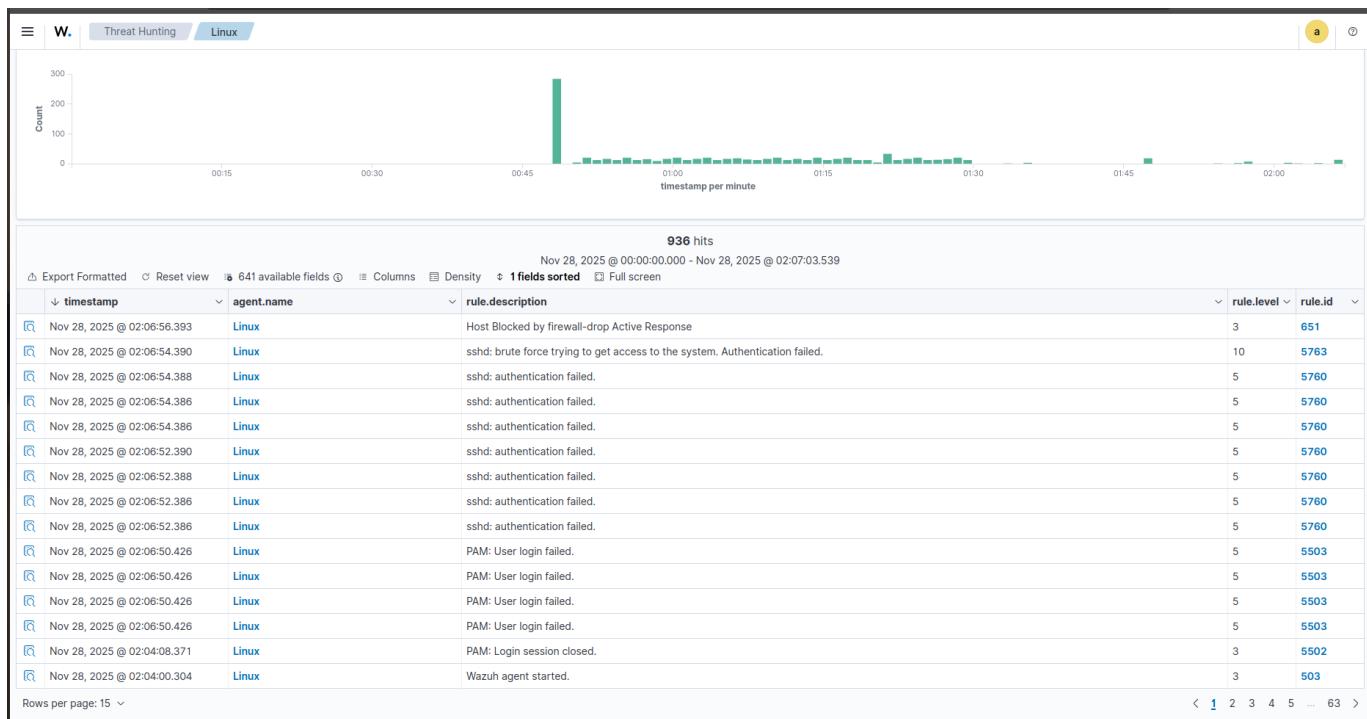
### 1. Hydra attacking.

```
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 00:50:48
[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
```

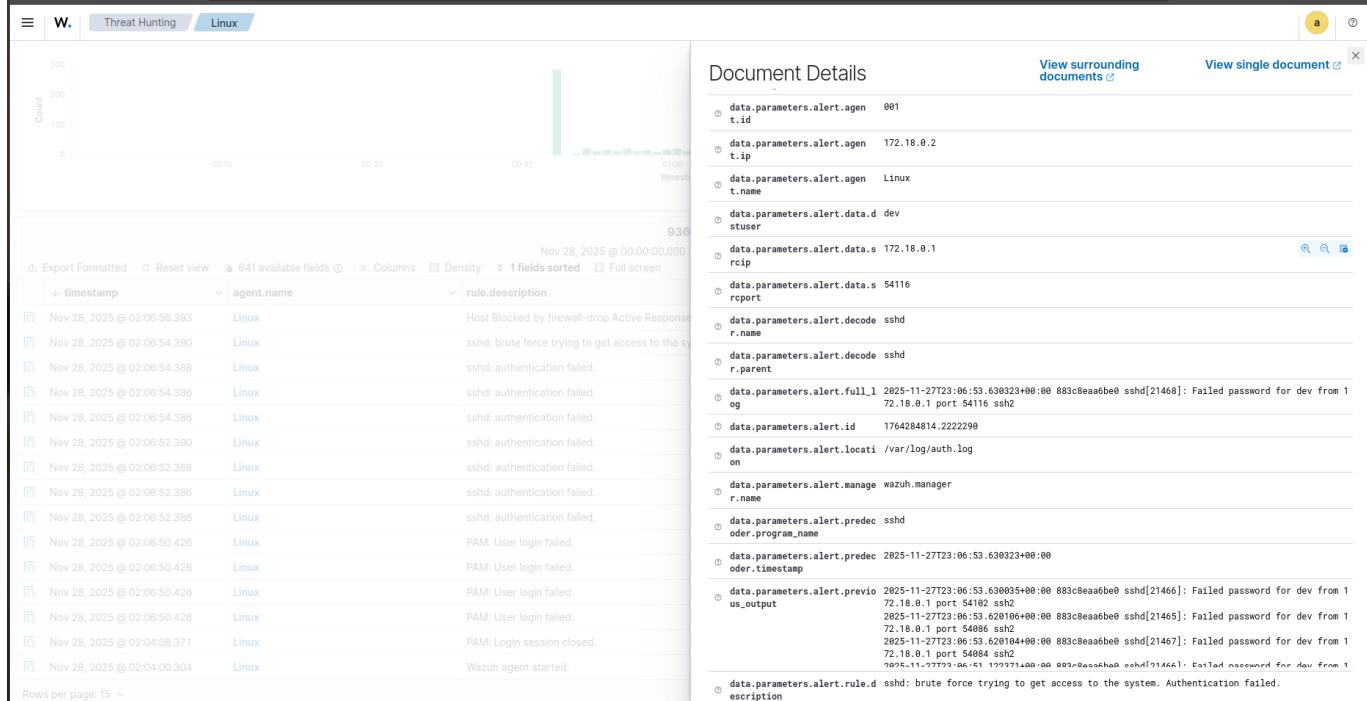
## 2. Wazuh logs



Rows per page: 15

&lt; 1 2 3 4 5 ... 63 &gt;

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



### Document Details

[View surrounding documents](#)[View single document](#)

- ④ data.parameters.alert.agen 001
- ④ data.parameters.alert.agen 172.18.0.2
- ④ data.parameters.alert.agen Linux
- ④ data.parameters.alert.agen.t.name
- ④ data.parameters.alert.data.d dev
- ④ data.parameters.alert.data.s 172.18.0.1
- ④ data.parameters.alert.data.s report
- ④ data.parameters.alert.decode sshd
- ④ data.parameters.alert.decode sshd.r.name
- ④ data.parameters.alert.decode sshd.r.parent
- ④ data.parameters.alert.full.l 2025-11-27T23:06:53.630323+00:00 883c8ea6be0 sshd[21468]: Failed password for dev from 1 0g
- ④ data.parameters.alert.id 1764284014.222298
- ④ data.parameters.alert.locati /var/log/auth.log
- ④ data.parameters.alert.manage wazuh.manager.r.name
- ④ data.parameters.alert.predec sshd
- ④ data.parameters.alert.predec sshd.order.program\_name
- ④ data.parameters.alert.predec 2025-11-27T23:06:53.630323+00:00
- ④ data.parameters.alert.previo 2025-11-27T23:06:53.630323+00:00 883c8ea6be0 sshd[21466]: Failed password for dev from 1 us\_output
- ④ data.parameters.alert.previo 2025-11-27T23:06:53.620106+00:00 883c8ea6be0 sshd[21465]: Failed password for dev from 1 72.18.0.1 port 54086 ssh2
- ④ data.parameters.alert.previo 2025-11-27T23:06:53.620104+00:00 883c8ea6be0 sshd[21467]: Failed password for dev from 1 72.18.0.1 port 54084 ssh2
- ④ data.parameters.alert.rule.d sshd: brute force trying to get access to the system. Authentication failed.

## 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.