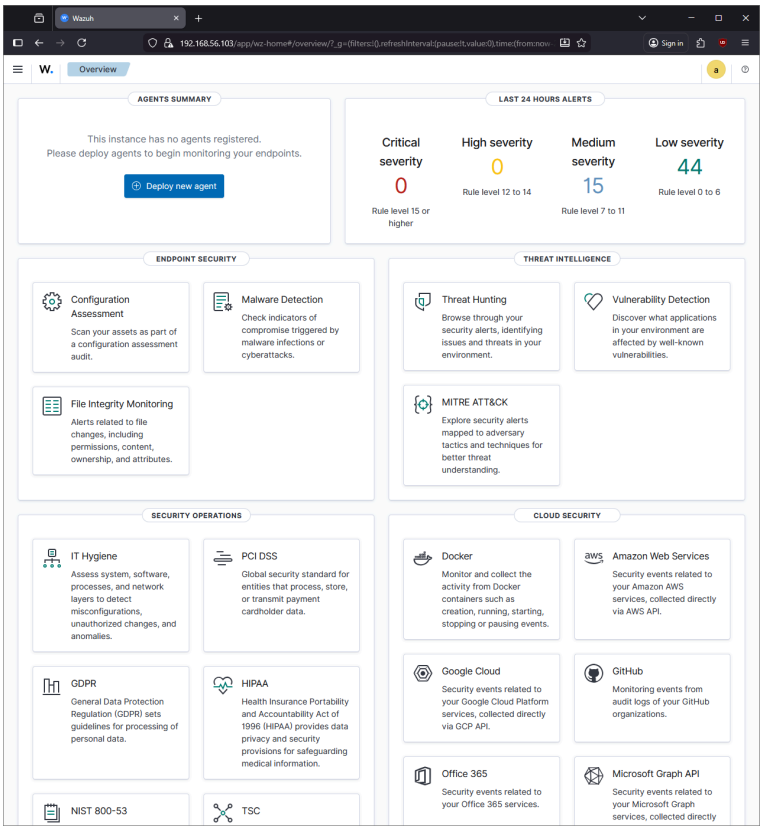
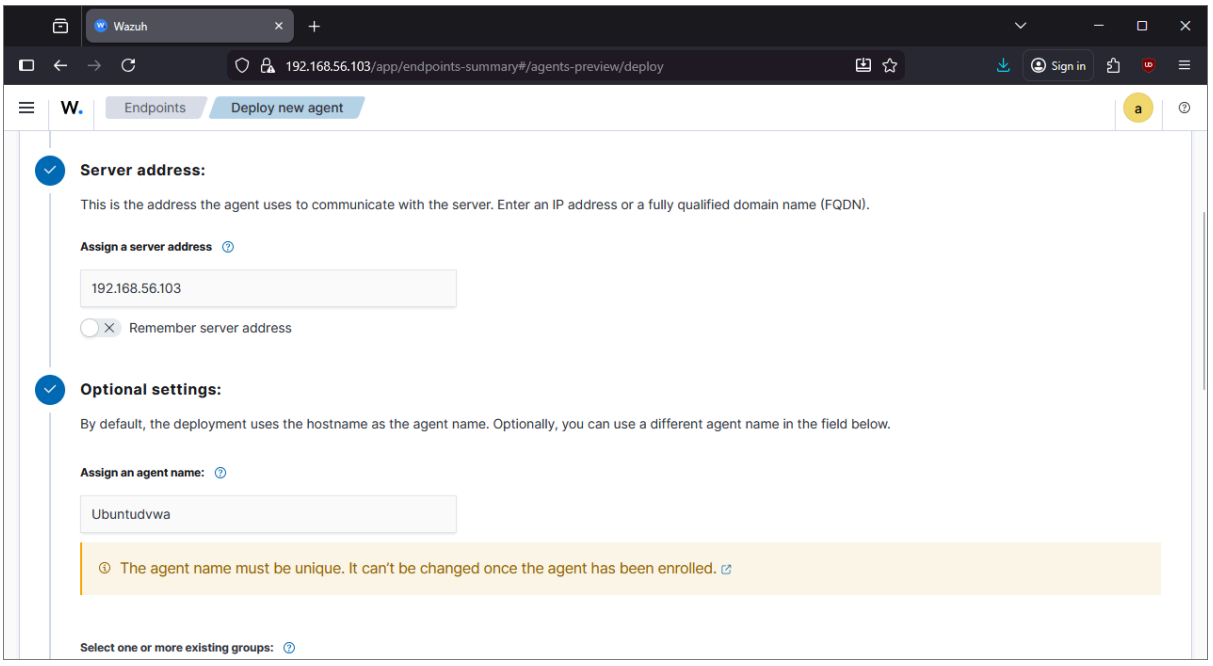
Wazuh SIEM (Centralized Logging, Detection, and Alerting)

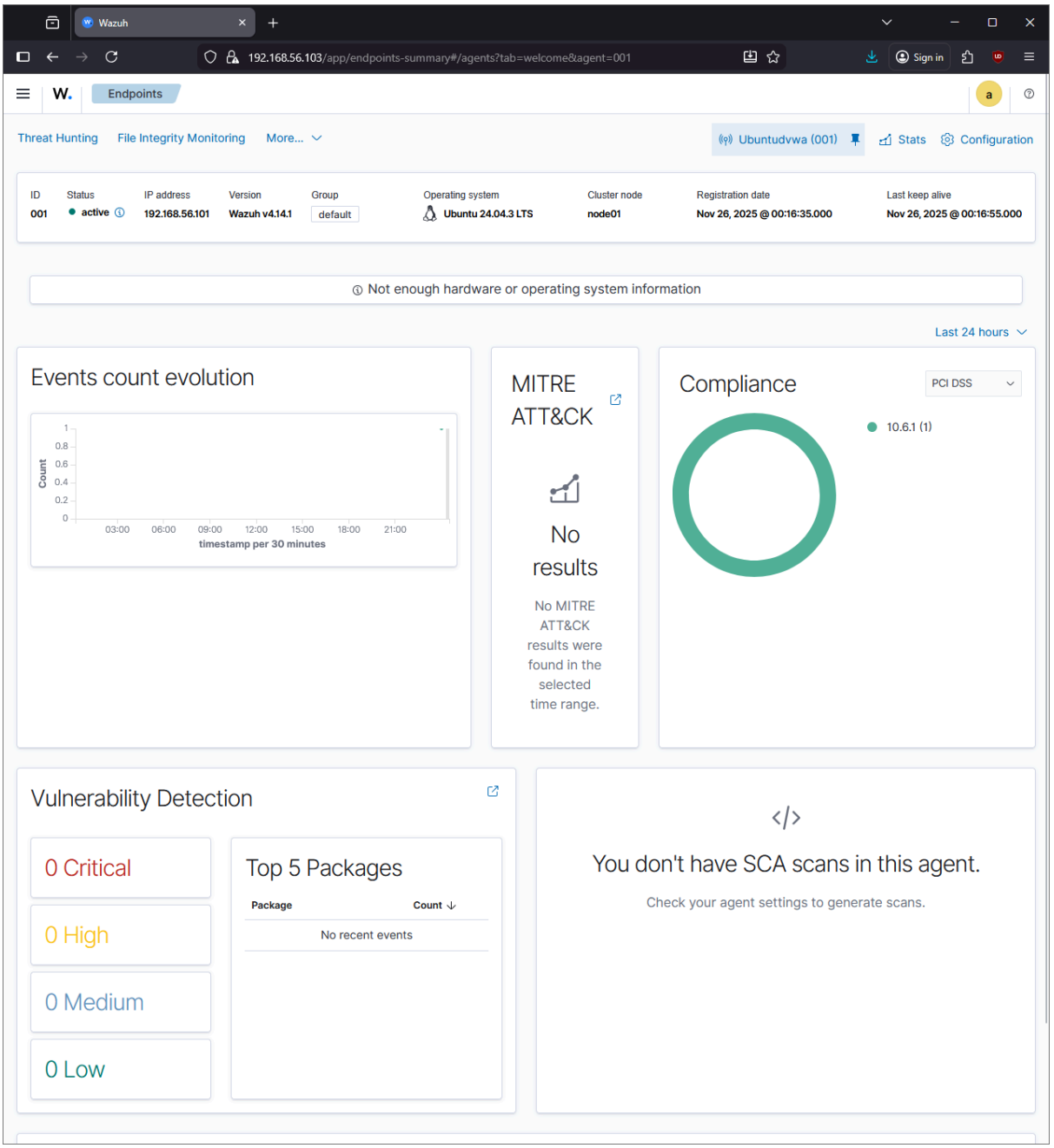
Wazuh dashboard



I added an agent which was an Ubuntu server that contains dvwa. I tried with metaspolitable2 and OWASP, Wazuh didn't support them. So, I configured the Ubuntu server installing dvwa to use for the lab5.



Successfully connected the agent.



I tried with using dvwa to make wazuh to alert by setting up monitoring apache logs, but there was an issue with the pipeline or something, I couldn’t move forward. So, I changed to ssh brute force and nmap.

I tested ssh bruteforce, nmap to see if it worked.

```
┌──(kali㉿kali)-[~]
└─$ ssh lab@192.168.56.101
The authenticity of host '192.168.56.101 (192.168.56.101)' can't be established.
ED25519 key fingerprint is SHA256:RUwrluFQ2WfabLFqGYNMsnPuWV+dmrUdz8YUIYU2zEw.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.56.101' (ED25519) to the list of known hosts.
lab@192.168.56.101's password:
Permission denied, please try again.
lab@192.168.56.101's password:
Permission denied, please try again.
lab@192.168.56.101's password:
Connection closed by 192.168.56.101 port 22
```

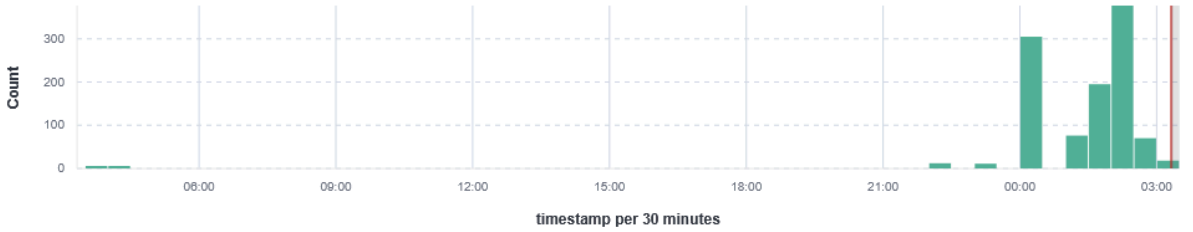
It detected the login failure.

nmap A

```
┌──(kali㉿kali)-[~]
└─$ nmap -A 192.168.56.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-26 03:18 EST
Nmap scan report for 192.168.56.101
Host is up (0.00016s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.58 ((Ubuntu))
| http-title: Login :: Damn Vulnerable Web Application (DVWA)
|_Requested resource was login.php
| http-robots.txt: 1 disallowed entry
|_/
| http-git:
|   192.168.56.101:80/.git/
|     Git repository found!
|     Repository description: Unnamed repository; edit this file 'description' to
 name the ...
|     Remotes:
|       https://github.com/digininja/DVWA.git
|_    Project type: PHP application (guessed from .gitignore)
|_http-server-header: Apache/2.4.58 (Ubuntu)
MAC Address: 08:00:27:90:91:4C (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:r
outeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS 7.2 -
 7.5 (Linux 5.6.3)
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.16 ms 192.168.56.101
```

Nov 25, 2025 @ 03:19:18.432 - Nov 26, 2025 @ 03:19:18.432 per Auto



Time	_source
Nov 26, 2025 @ 03:18:47.357	input.type: log agent.ip: 192.168.56.101 agent.name: Ubuntudvwa agent.id: 002 manager.name: wazuh-server data.protocol: GET data.srcip: 192.168.56.102 data.id: 404 data.url: /.git/COMMIT_EDITMSG rule.firedtimes: 18 rule.mail: false rule.level: 5 rule.pci_dss: 6.5, 11.4 rule.tsc: CC6.6, CC7.1, CC8.1, CC6.1, CC6.8, CC7.2, CC7.3 rule.description: Web server 400 error code. rule.groups: web, accesslog, attack rule.id: 31101 rule.nist_800_53: SA.11, SI.4 rule.gdpr: IV_

Expanded document View surrounding documents View single document

Table JSON

t	_index	wazuh-alerts-4.x-2025.11.26
t	agent.id	002
t	agent.ip	192.168.56.101
t	agent.name	Ubuntudvwa
t	data.id	404
t	data.protocol	GET
t	data.srcip	192.168.56.102
t	data.url	/.git/COMMIT_EDITMSG
t	decoder.name	web-accesslog
t	full_log	192.168.56.102 - - [26/Nov/2025:08:18:46 +0000] "GET /.git/COMMIT_EDITMSG HTTP/1.1" 404 0 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
t	id	1764145127.2662376
t	input.type	log
t	location	/var/log/apache2/access.log
t	manager.name	wazuh-server
t	rule.description	Web server 400 error code.
#	rule.firedtimes	18
t	rule.gdpr	IV_35.7.d

nmap sS

```
┌──(kali㉿kali)-[~]
└─$ nmap -sS 192.168.56.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-26 03:02 EST
Nmap scan report for 192.168.56.101
Host is up (0.00023s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 08:00:27:90:91:4C (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.38 seconds
```

Nov 25, 2025 @ 03:02:27.912 - Nov 26, 2025 @ 03:02:27.912 per Auto

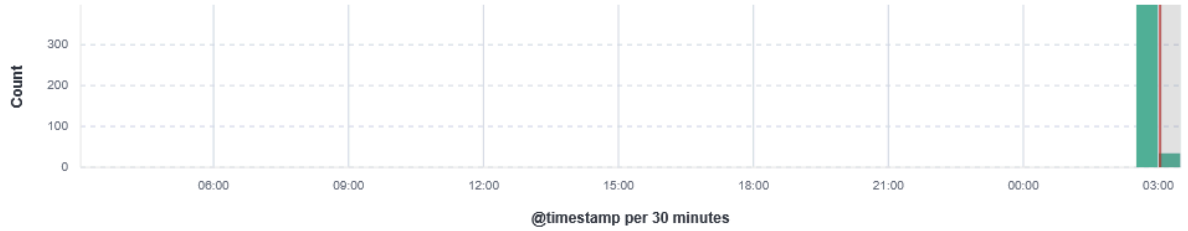


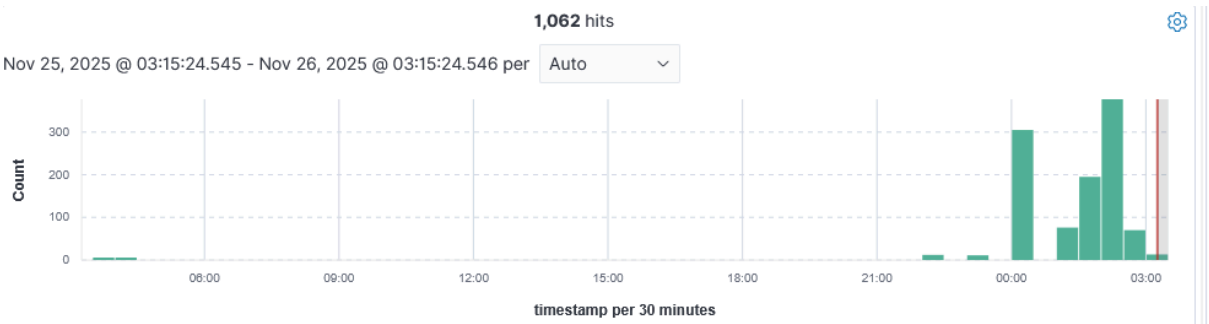
Table JSON


```
{
  "_index": "wazuh-archives-4.x-2025.11.26",
  "_id": "Ymctv5oB1_88ng91_4wF",
  "_version": 1,
  "_score": null,
  "_source": {
    "agent": {
      "name": "wazuh-server",
      "id": "000"
    },
    "manager": {
      "name": "wazuh-server"
    },
    "decoder": {
      "name": "ossec"
    },
    "full_log": "ossec: output: 'netstat listening ports':\ntcp 0.0.0.0:22 0.0.0.0:* /usr\ntcp6 :::22 :::* /usr\nudp 10.0.3.15
:68 0.0.0.0:* 2035/systemd-networ\nudp 192.168.56.103:68 0.0.0.0:* 2035/systemd-networ\nudp 127.0.0.1:323 0.0.0.0:* 1837/chron
yd\nudp6 ::1:323 :::* 1837/chronyd\ntcp 0.0.0.0:443 0.0.0.0:* 1747/node\ntcp 0.0.0.0:1514 0.0.0.0:* 8953/wazuh-remoted\ntcp 0.
0.0.0:1515 0.0.0.0:* 8814/wazuh-authd\ntcp6 127.0.0.1:9200 :::* 2098/java\ntcp6 127.0.0.1:9300 :::* 2098/java\ntcp 0.0.0.0:550
00 0.0.0.0:* 8764/python3\ntcp6 :::55000 :::* 8764/python3",
    "input": {
      "type": "log"
    },
    "@timestamp": "2025-11-26T08:00:52.043Z",
    "location": "netstat listening ports",
    "id": "1764144052.2653277",
    "timestamp": "2025-11-26T08:00:52.043+0000"
  },
  "fields": {
    "timestamp": [
      "2025-11-26T08:00:52.043Z"
    ],
    "@timestamp": [
      "2025-11-26T08:00:52.043Z"
    ]
  },
  "sort": [
    1764144052043
  ]
}
```

namp sV

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.56.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-26 03:12 EST
Nmap scan report for 192.168.56.101
Host is up (0.00012s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.58 ((Ubuntu))
MAC Address: 08:00:27:90:91:4C (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.
org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.87 seconds
```



Time	_source
Nov 26, 2025 @ 03:12:37.275	input.type: log agent.ip: 192.168.56.101 agent.name: Ubuntudvwa agent.id: 002 manager.name: wazuh-server data.protocol: GET data.srcip: 192.168.56.102 data.id: 404 data.url: /nmaplowercheck1764144753 rule.firedtimes: 13 rule.mail: false rule.level: 5 rule.pci_dss: 6.5, 11.4 rule.tsc: CC6.6, CC7.1, CC8.1, CC6.1, CC6.8, CC7.2, CC7.3 rule.description: Web server 400 error code. rule.groups: web, accesslog, attack rule.id: 31101 rule.nist_800_53: SA.11, SI.4

Expanded document View surrounding documents View single document

Table JSON

t	_index	wazuh-alerts-4.x-2025.11.26
t	agent.id	002
t	agent.ip	192.168.56.101
t	agent.name	Ubuntudvwa
t	data.id	404
t	data.protocol	GET
t	data.srcip	192.168.56.102
t	data.url	/nmaplowercheck1764144753
t	decoder.name	web-accesslog
t	full_log	192.168.56.102 - - [26/Nov/2025:08:12:36 +0000] "GET /nmaplowercheck1764144753 HTTP/1.1" 404 456 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
t	id	1764144757.2659799
t	input.type	log
t	location	/var/log/apache2/access.log
t	manager.name	wazuh-server
t	rule.description	Web server 400 error code.
#	rule.firedtimes	13
t	rule.gdpr	IV_35.7.d

I checked that the system was working properly, then I tested the custom rules. The first custom rule was it detected a login failure which was id 5760. This would wrap rule id 5760 which was the login failure already in the system rule. The second one counted how many logins failed, if it was more than 3 times, it alerted with id 100991, SSH: Brute-force suspected.

```
┌──(kali㉿kali)-[~]
└─$ hydra -l lab -P smalllist.txt ssh://192.168.56.101
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in mil
itary or secret service organizations, or for illegal purposes (this is non-bindi
ng, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-11-26 06:16:2
7
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recom
mended to reduce the tasks: use -t 4
[DATA] max 13 tasks per 1 server, overall 13 tasks, 13 login tries (l:1/p:13), ~1
 try per task
[DATA] attacking ssh://192.168.56.101:22/
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-11-26 06:16:3
1
```

	Time	rule.id
>	Nov 26, 2025 @ 06:16:38.924	100990
>	Nov 26, 2025 @ 06:16:38.922	100990
v	Nov 26, 2025 @ 06:16:38.920	100991

Expanded document View surrounding documents View single document

Table JSON

t	_index	wazuh-alerts-4.x-2025.11.26
t	agent.id	002
t	agent.ip	192.168.56.101
t	agent.name	Ubuntudvwa
t	data.dstuser	lab
t	data.srcip	192.168.56.102
t	data.srcport	48452
t	decoder.name	sshd
t	decoder.parent	sshd
t	full_log	Nov 26 11:16:38 labserver sshd[22415]: Failed password for lab from 192.168.56.102 port 48452 ssh2
t	id	1764155798.2982787
t	input.type	log
t	location	journald
t	manager.name	wazuh-server
t	predecoder.hostname	labserver
t	predecoder.program_name	sshd
t	predecoder.timestamp	Nov 26 11:16:38

It successfully worked.

This was the custom rule.

local_rules.xml

Ruleset Test | Save

```
<group name="custom-ssh-bruteforce,">

  <rule id="100990" level="8">
    <if_sid>5760</if_sid>

    <description>SSH: Failed login (wrapped SID 5760).</description>
    <group>ssh,authentication_failed,</group>
    <mitre>
      <id>T1110</id>
    </mitre>
  </rule>

  <rule id="100991" level="12" frequency="3" timeframe="60">
    <if_matched_sid>100990</if_matched_sid>
    <same_srcip/>

    <description>SSH: Brute-force suspected (>=3 wrapped 5760 events from same IP in 60s).</description>
    <group>ssh,authentication_failures,bruteforce,</group>
    <mitre>
      <id>T1110</id>
    </mitre>
  </rule>

</group>
```