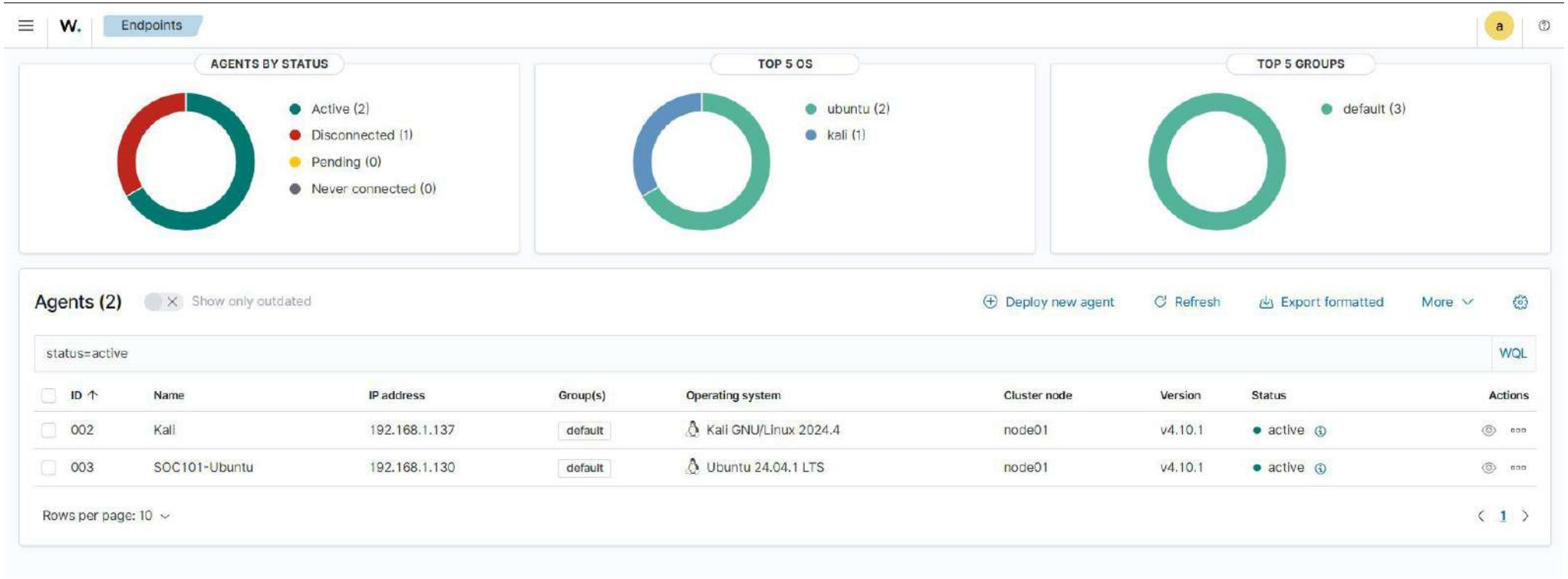
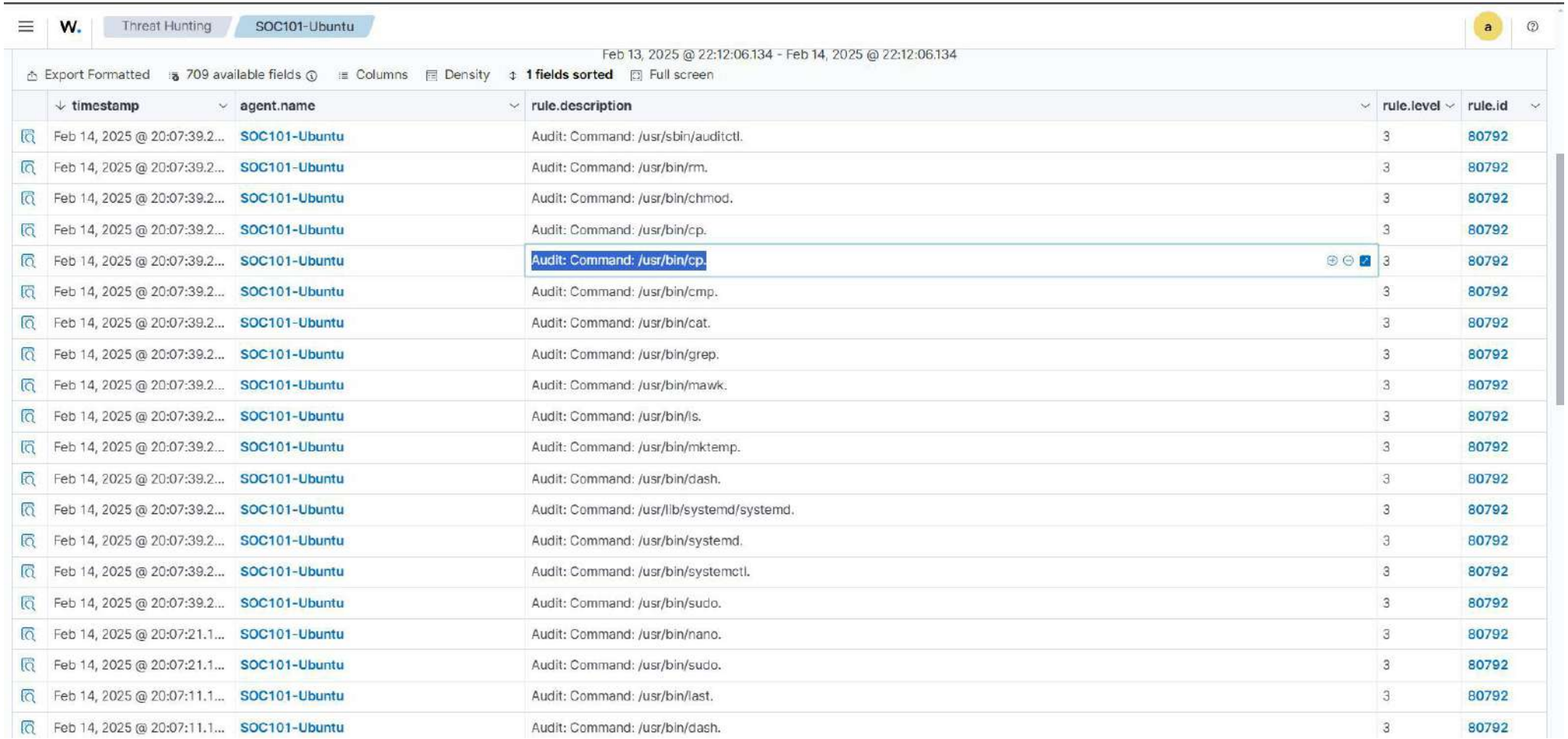
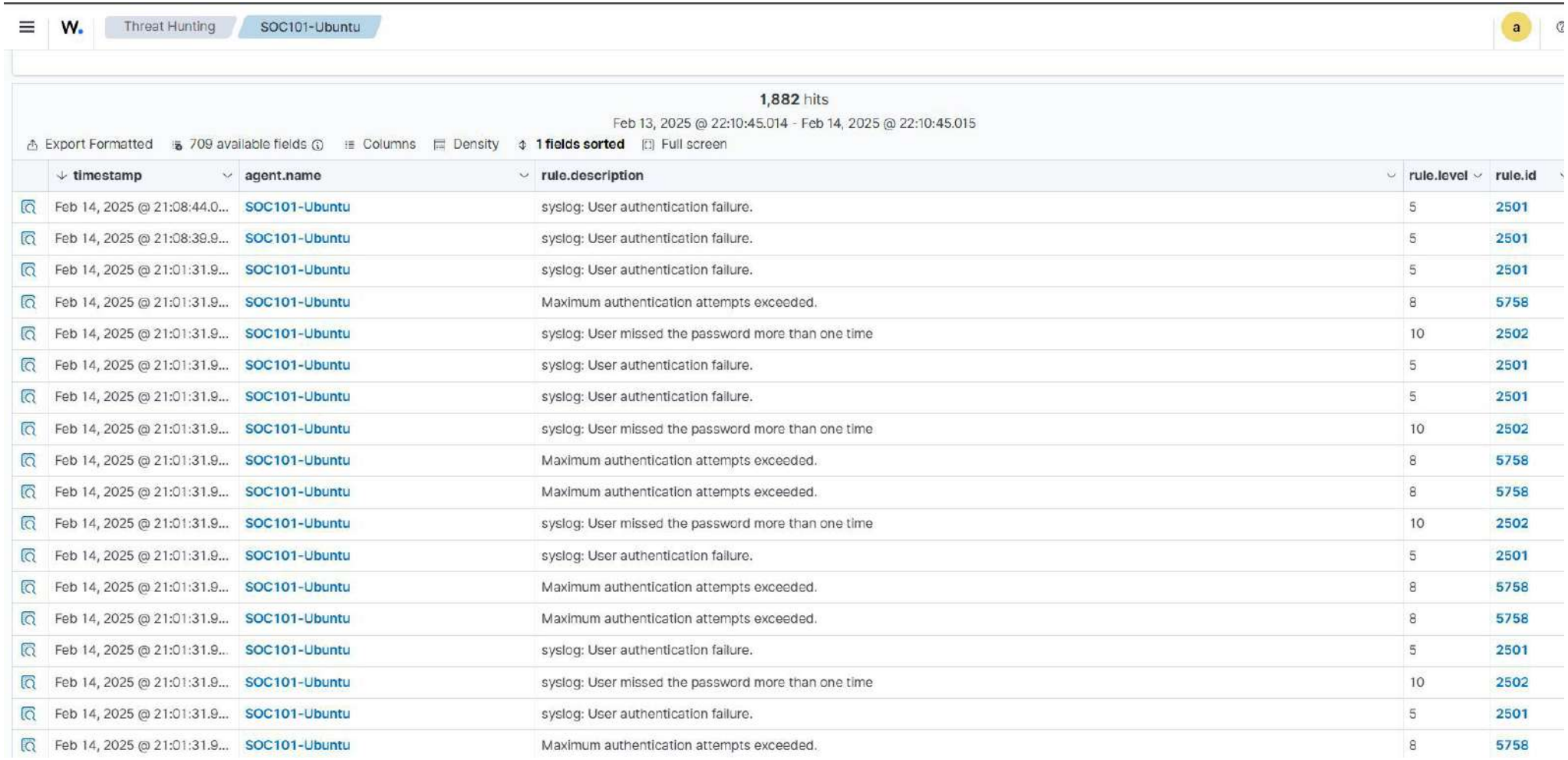
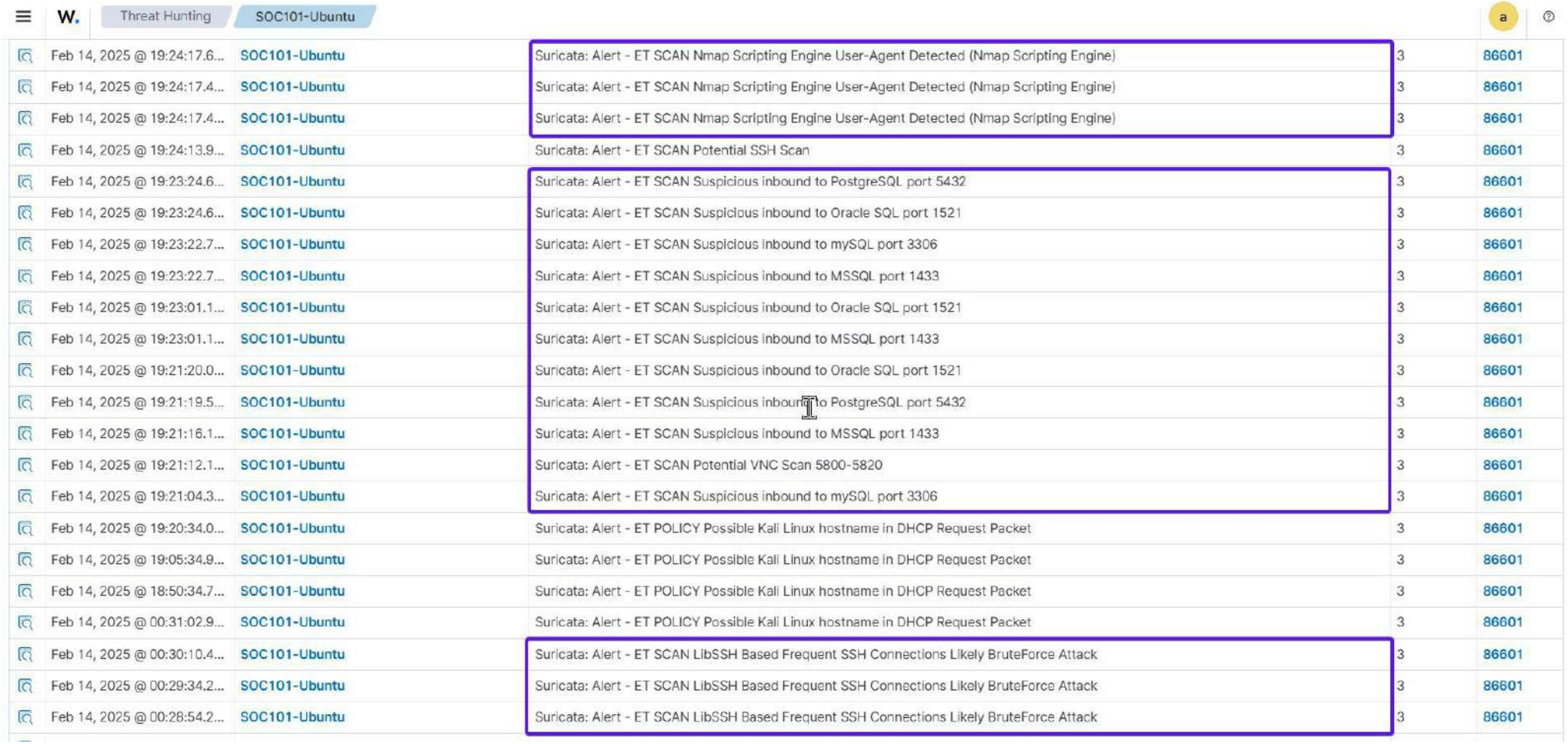
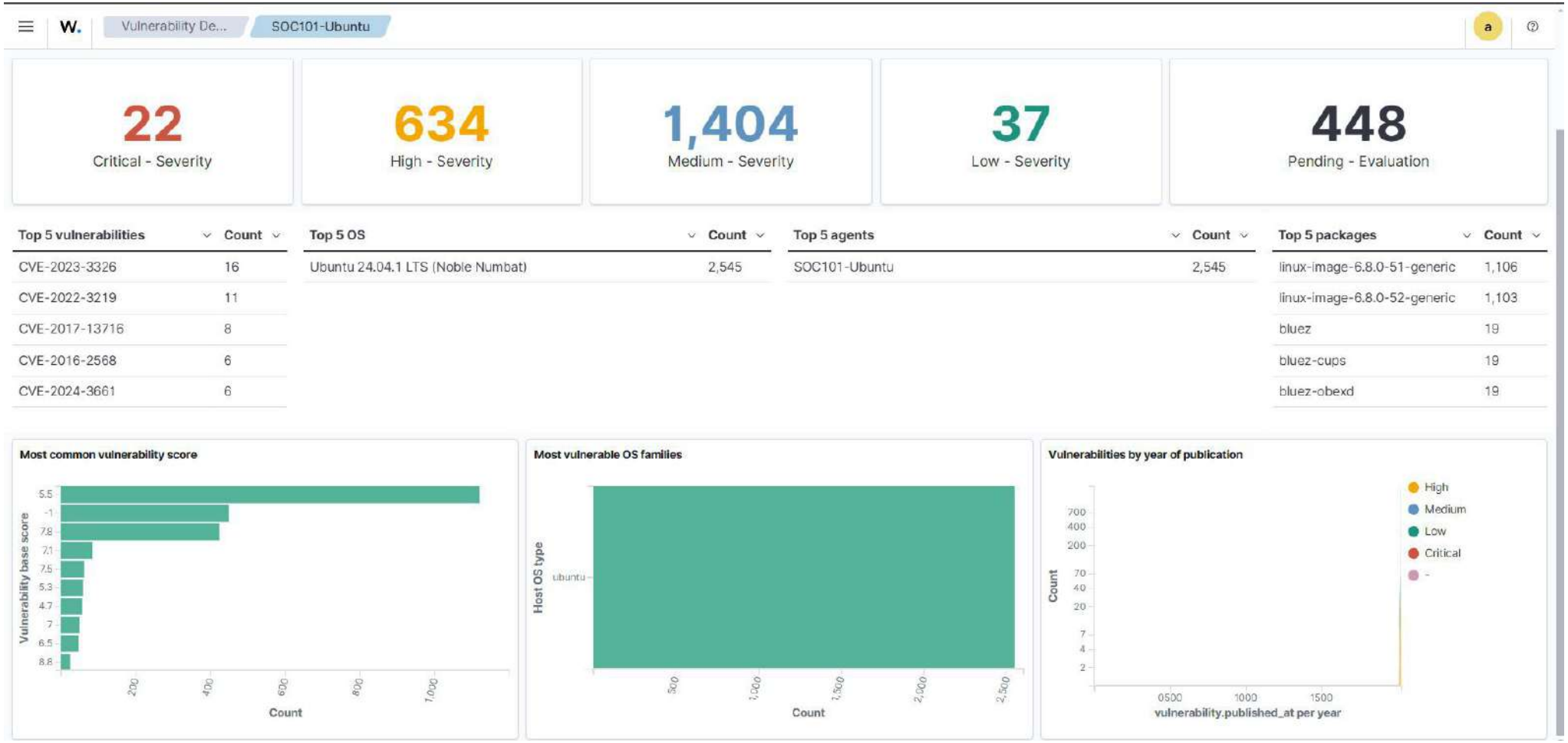
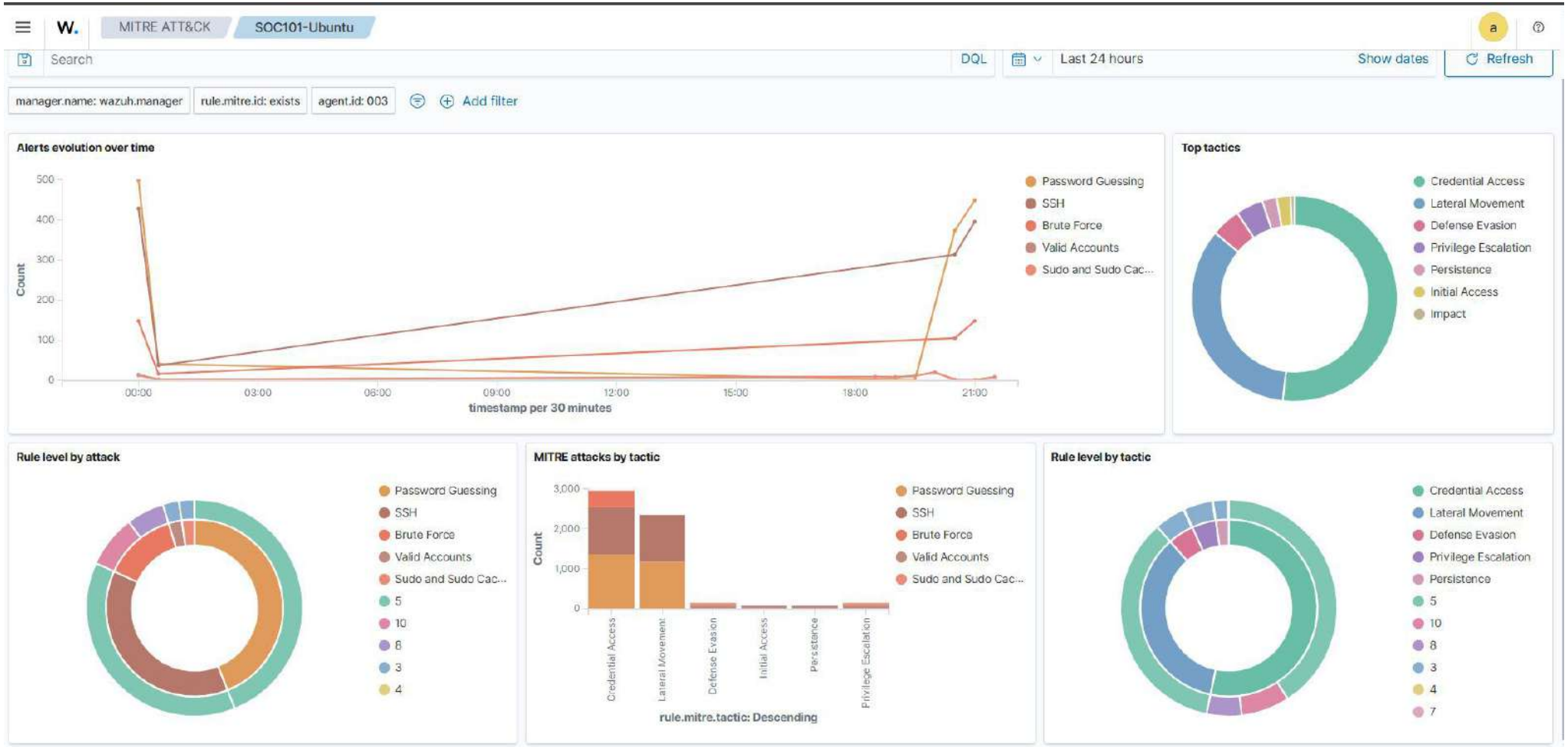

Endpoints
a
AGENTS BY STATUS
Active (2)
Disconnected (1)
Pending (0)
Never connected (0)
TOP 5 OS
ubuntu (2)
kali (1)
TOP 5 GROUPS
default (3)
Agents (2)
Show only outdated
Deploy new agent
Refresh
Export formatted
More
status=active
WQL
ID
Name
IP address
Group(s)
Operating system
Cluster node
Version
Status
Actions
002
Kali
192.168.1.137
default
Kali GNU/Linux 2024.4
node01
v4.10.1
active
003
SOC101-Ubuntu
192.168.1.130
default
Ubuntu 24.04.1 LTS
node01
v4.10.1
active
Rows per page: 10
1

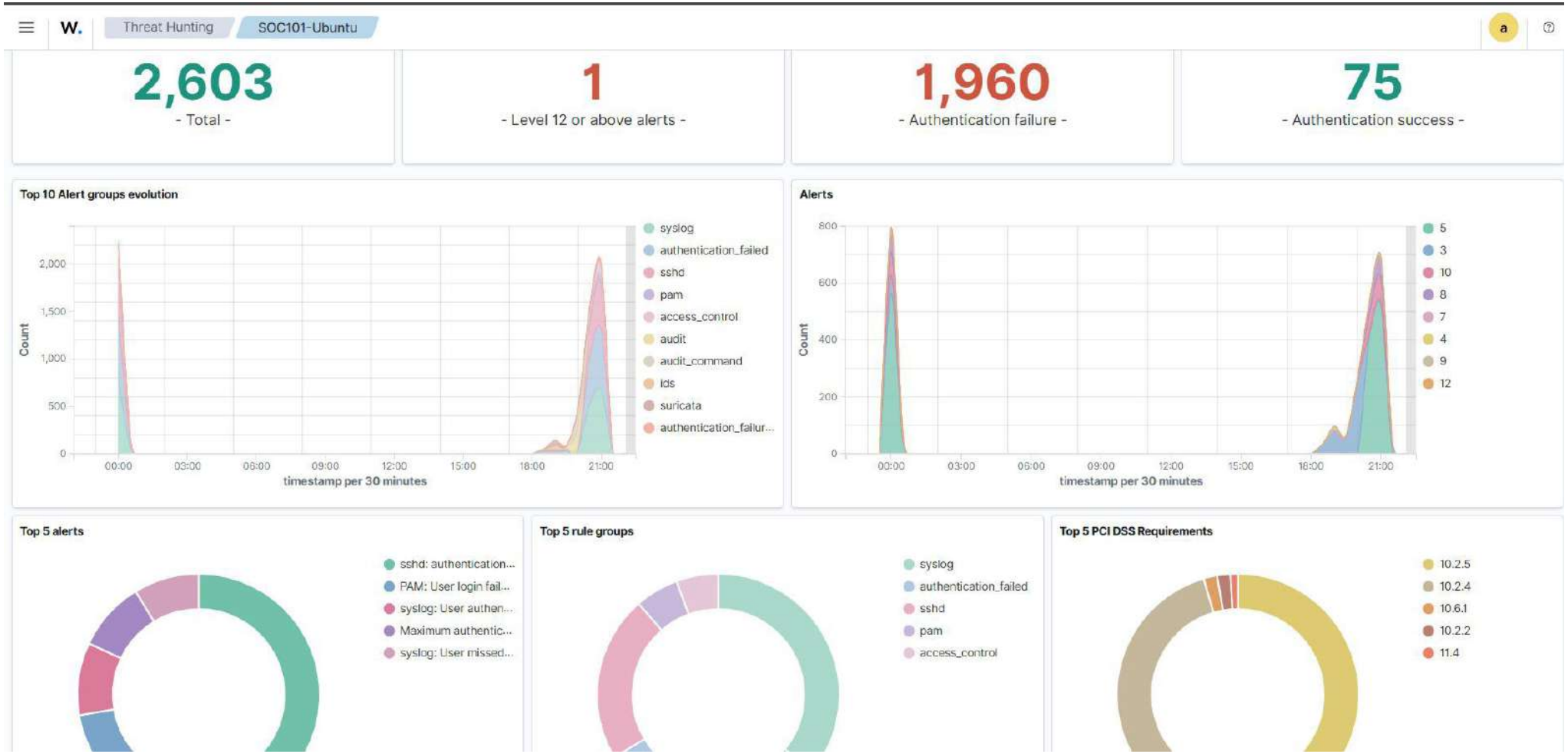

Threat Hunting
SOC101-Ubuntu
a
Feb 13, 2025 @ 22:12:06.134 - Feb 14, 2025 @ 22:12:06.134
Export Formatted
709 available fields
Columns
Density
1 fields sorted
Full screen
timestamp
agent.name
rule.description
rule.level
rule.id
Feb 14, 2025 @ 20:07:39.2... SOC101-Ubuntu Audit: Command: /usr/sbin/auditctl. 3 80792
Feb 14, 2025 @ 20:07:39.2... SOC101-Ubuntu Audit: Command: /usr/bin/rm. 3 80792
Feb 14, 2025 @ 20:07:39.2... SOC101-Ubuntu Audit: Command: /usr/bin/chmod. 3 80792
Feb 14, 2025 @ 20:07:39.2... SOC101-Ubuntu Audit: Command: /usr/bin/cp. 3 80792
Feb 14, 2025 @ 20:07:39.2... SOC101-Ubuntu Audit: Command: /usr/bin/cp. 3 80792
Feb 14, 2025 @ 20:07:39.2... SOC101-Ubuntu Audit: Command: /usr/bin/cmp. 3 80792
Feb 14, 2025 @ 20:07:39.2... SOC101-Ubuntu Audit: Command: /usr/bin/cat. 3 80792
Feb 14, 2025 @ 20:07:39.2... SOC101-Ubuntu Audit: Command: /usr/bin/grep. 3 80792
Feb 14, 2025 @ 20:07:39.2... SOC101-Ubuntu Audit: Command: /usr/bin/mawk. 3 80792
Feb 14, 2025 @ 20:07:39.2... SOC101-Ubuntu Audit: Command: /usr/bin/ls. 3 80792
Feb 14, 2025 @ 20:07:39.2... SOC101-Ubuntu Audit: Command: /usr/bin/mktemp. 3 80792
Feb 14, 2025 @ 20:07:39.2... SOC101-Ubuntu Audit: Command: /usr/bin/dash. 3 80792
Feb 14, 2025 @ 20:07:39.2... SOC101-Ubuntu Audit: Command: /usr/lib/systemd/systemd. 3 80792
Feb 14, 2025 @ 20:07:39.2... SOC101-Ubuntu Audit: Command: /usr/bin/systemd. 3 80792
Feb 14, 2025 @ 20:07:39.2... SOC101-Ubuntu Audit: Command: /usr/bin/systemctl. 3 80792
Feb 14, 2025 @ 20:07:39.2... SOC101-Ubuntu Audit: Command: /usr/bin/sudo. 3 80792
Feb 14, 2025 @ 20:07:21.1... SOC101-Ubuntu Audit: Command: /usr/bin/nano. 3 80792
Feb 14, 2025 @ 20:07:21.1... SOC101-Ubuntu Audit: Command: /usr/bin/sudo. 3 80792
Feb 14, 2025 @ 20:07:11.1... SOC101-Ubuntu Audit: Command: /usr/bin/last. 3 80792
Feb 14, 2025 @ 20:07:11.1... SOC101-Ubuntu Audit: Command: /usr/bin/dash. 3 80792

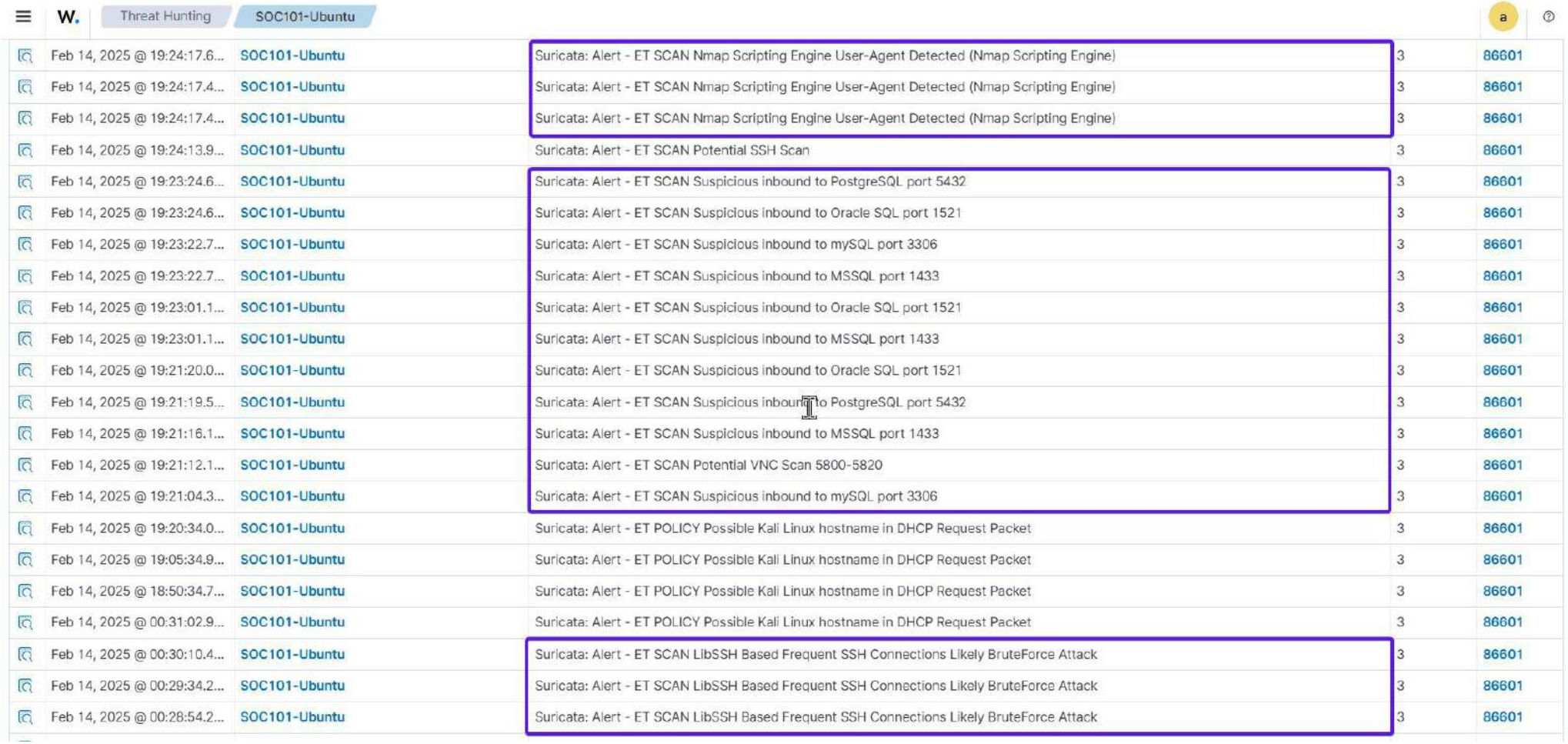

Threat Hunting
SOC101-Ubuntu
a
1,882 hits
Feb 13, 2025 @ 22:10:45.014 - Feb 14, 2025 @ 22:10:45.015
Export Formatted
709 available fields
Columns
Density
1 fields sorted
Full screen
timestamp
agent.name
rule.description
rule.level
rule.id
Feb 14, 2025 @ 21:08:44.0... SOC101-Ubuntu syslog: User authentication failure. 5 2501
Feb 14, 2025 @ 21:08:39.9... SOC101-Ubuntu syslog: User authentication failure. 5 2501
Feb 14, 2025 @ 21:01:31.9... SOC101-Ubuntu syslog: User authentication failure. 5 2501
Feb 14, 2025 @ 21:01:31.9... SOC101-Ubuntu Maximum authentication attempts exceeded. 8 5758
Feb 14, 2025 @ 21:01:31.9... SOC101-Ubuntu syslog: User missed the password more than one time 10 2502
Feb 14, 2025 @ 21:01:31.9... SOC101-Ubuntu syslog: User authentication failure. 5 2501
Feb 14, 2025 @ 21:01:31.9... SOC101-Ubuntu syslog: User authentication failure. 5 2501
Feb 14, 2025 @ 21:01:31.9... SOC101-Ubuntu syslog: User missed the password more than one time 10 2502
Feb 14, 2025 @ 21:01:31.9... SOC101-Ubuntu Maximum authentication attempts exceeded. 8 5758
Feb 14, 2025 @ 21:01:31.9... SOC101-Ubuntu Maximum authentication attempts exceeded. 8 5758
Feb 14, 2025 @ 21:01:31.9... SOC101-Ubuntu syslog: User missed the password more than one time 10 2502
Feb 14, 2025 @ 21:01:31.9... SOC101-Ubuntu syslog: User authentication failure. 5 2501
Feb 14, 2025 @ 21:01:31.9... SOC101-Ubuntu Maximum authentication attempts exceeded. 8 5758
Feb 14, 2025 @ 21:01:31.9... SOC101-Ubuntu Maximum authentication attempts exceeded. 8 5758
Feb 14, 2025 @ 21:01:31.9... SOC101-Ubuntu syslog: User authentication failure. 5 2501
Feb 14, 2025 @ 21:01:31.9... SOC101-Ubuntu syslog: User missed the password more than one time 10 2502
Feb 14, 2025 @ 21:01:31.9... SOC101-Ubuntu syslog: User authentication failure. 5 2501
Feb 14, 2025 @ 21:01:31.9... SOC101-Ubuntu Maximum authentication attempts exceeded. 8 5758

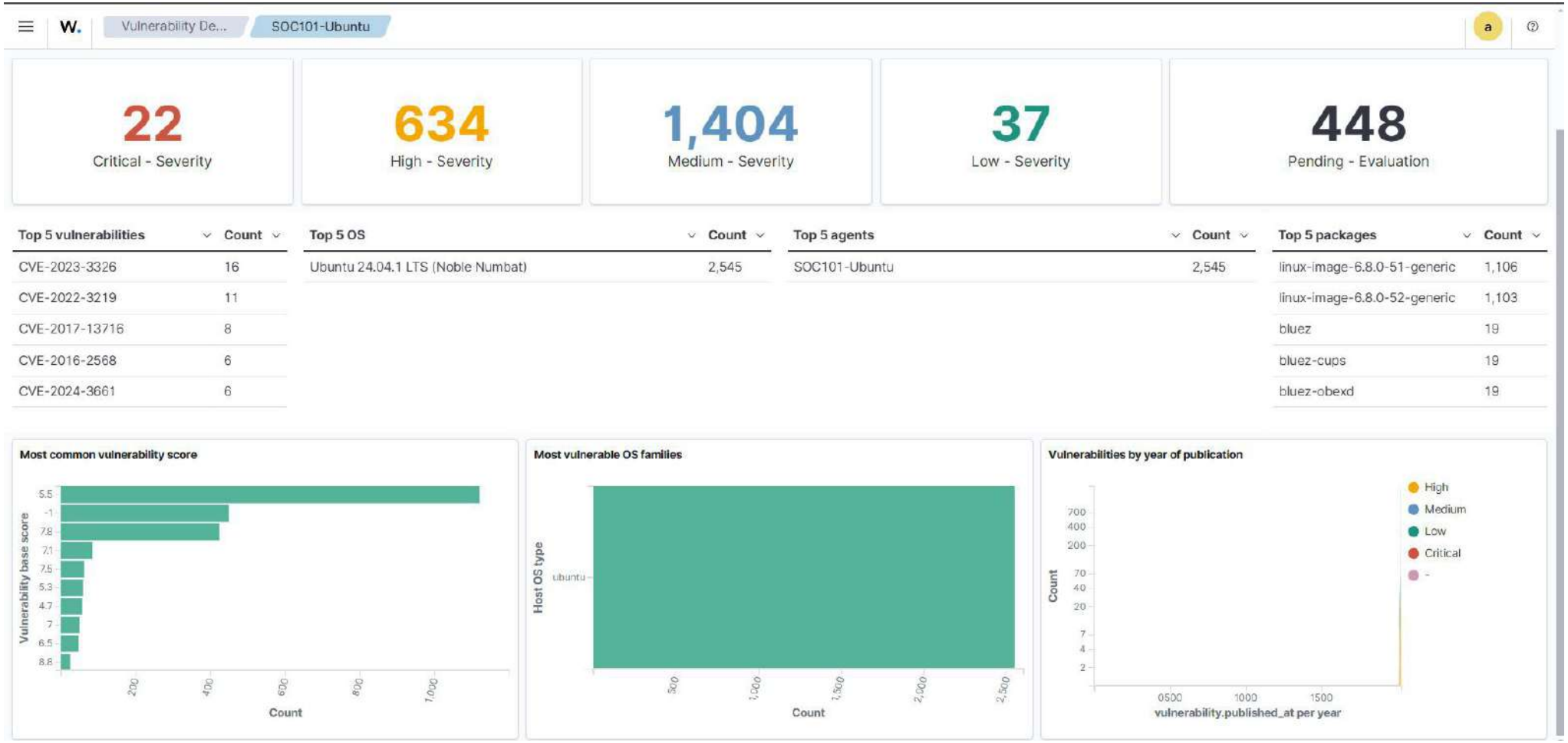

Threat Hunting
SOC101-Ubuntu
a
Feb 14, 2025 @ 19:24:17.6... SOC101-Ubuntu Suricata: Alert - ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine) 3 86601
Feb 14, 2025 @ 19:24:17.4... SOC101-Ubuntu Suricata: Alert - ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine) 3 86601
Feb 14, 2025 @ 19:24:17.4... SOC101-Ubuntu Suricata: Alert - ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine) 3 86601
Feb 14, 2025 @ 19:24:13.9... SOC101-Ubuntu Suricata: Alert - ET SCAN Potential SSH Scan 3 86601
Feb 14, 2025 @ 19:23:24.6... SOC101-Ubuntu Suricata: Alert - ET SCAN Suspicious inbound to PostgreSQL port 5432 3 86601
Feb 14, 2025 @ 19:23:24.6... SOC101-Ubuntu Suricata: Alert - ET SCAN Suspicious inbound to Oracle SQL port 1521 3 86601
Feb 14, 2025 @ 19:23:22.7... SOC101-Ubuntu Suricata: Alert - ET SCAN Suspicious inbound to mySQL port 3306 3 86601
Feb 14, 2025 @ 19:23:22.7... SOC101-Ubuntu Suricata: Alert - ET SCAN Suspicious inbound to MSSQL port 1433 3 86601
Feb 14, 2025 @ 19:23:01.1... SOC101-Ubuntu Suricata: Alert - ET SCAN Suspicious inbound to Oracle SQL port 1521 3 86601
Feb 14, 2025 @ 19:23:01.1... SOC101-Ubuntu Suricata: Alert - ET SCAN Suspicious inbound to MSSQL port 1433 3 86601
Feb 14, 2025 @ 19:21:20.0... SOC101-Ubuntu Suricata: Alert - ET SCAN Suspicious inbound to Oracle SQL port 1521 3 86601
Feb 14, 2025 @ 19:21:19.5... SOC101-Ubuntu Suricata: Alert - ET SCAN Suspicious inbound to PostgreSQL port 5432 3 86601
Feb 14, 2025 @ 19:21:16.1... SOC101-Ubuntu Suricata: Alert - ET SCAN Suspicious inbound to MSSQL port 1433 3 86601
Feb 14, 2025 @ 19:21:12.1... SOC101-Ubuntu Suricata: Alert - ET SCAN Potential VNC Scan 5800-5820 3 86601
Feb 14, 2025 @ 19:21:04.3... SOC101-Ubuntu Suricata: Alert - ET SCAN Suspicious inbound to mySQL port 3306 3 86601
Feb 14, 2025 @ 19:20:34.0... SOC101-Ubuntu Suricata: Alert - ET POLICY Possible Kali Linux hostname in DHCP Request Packet 3 86601
Feb 14, 2025 @ 19:05:34.9... SOC101-Ubuntu Suricata: Alert - ET POLICY Possible Kali Linux hostname in DHCP Request Packet 3 86601
Feb 14, 2025 @ 18:50:34.7... SOC101-Ubuntu Suricata: Alert - ET POLICY Possible Kali Linux hostname in DHCP Request Packet 3 86601
Feb 14, 2025 @ 00:31:02.9... SOC101-Ubuntu Suricata: Alert - ET POLICY Possible Kali Linux hostname in DHCP Request Packet 3 86601
Feb 14, 2025 @ 00:30:10.4... SOC101-Ubuntu Suricata: Alert - ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack 3 86601
Feb 14, 2025 @ 00:29:34.2... SOC101-Ubuntu Suricata: Alert - ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack 3 86601
Feb 14, 2025 @ 00:28:54.2... SOC101-Ubuntu Suricata: Alert - ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack 3 86601

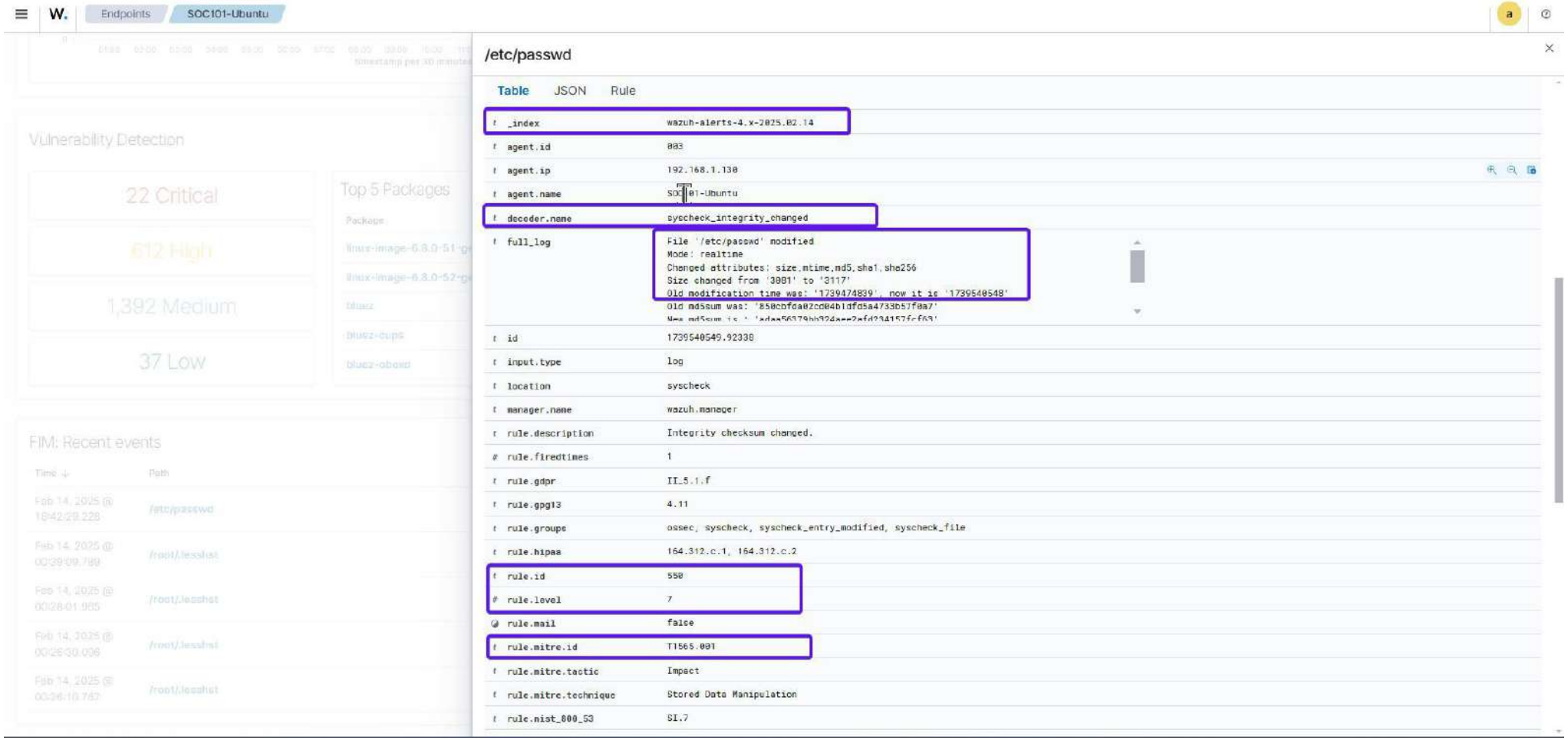

W.
Vulnerability De...
SOC101-Ubuntu
a
22
Critical - Severity
634
High - Severity
1,404
Medium - Severity
37
Low - Severity
448
Pending - Evaluation
Top 5 vulnerabilities
Count
CVE-2023-3326 16
CVE-2022-3219 11
CVE-2017-13716 8
CVE-2016-2568 6
CVE-2024-3661 6
Top 5 OS
Count
Ubuntu 24.04.1 LTS (Noble Numbat) 2,545
Top 5 agents
Count
SOC101-Ubuntu 2,545
Top 5 packages
Count
linux-image-6.8.0-51-generic 1,106
linux-image-6.8.0-52-generic 1,103
bluez 19
bluez-cups 19
bluez-obexd 19
Most common vulnerability score
Vulnerability base score
5.5
-1
7.8
7.1
7.5
5.3
4.7
7
6.5
8.8
200
400
600
800
1,000
Count
Most vulnerable OS families
Host OS type
ubuntu
500
1,000
1,500
2,000
2,500
Count
Vulnerabilities by year of publication
Count
700
400
200
70
40
20
7
4
2
0500
1000
1500
vulnerability.published_at per year
High
Medium
Low
Critical
-

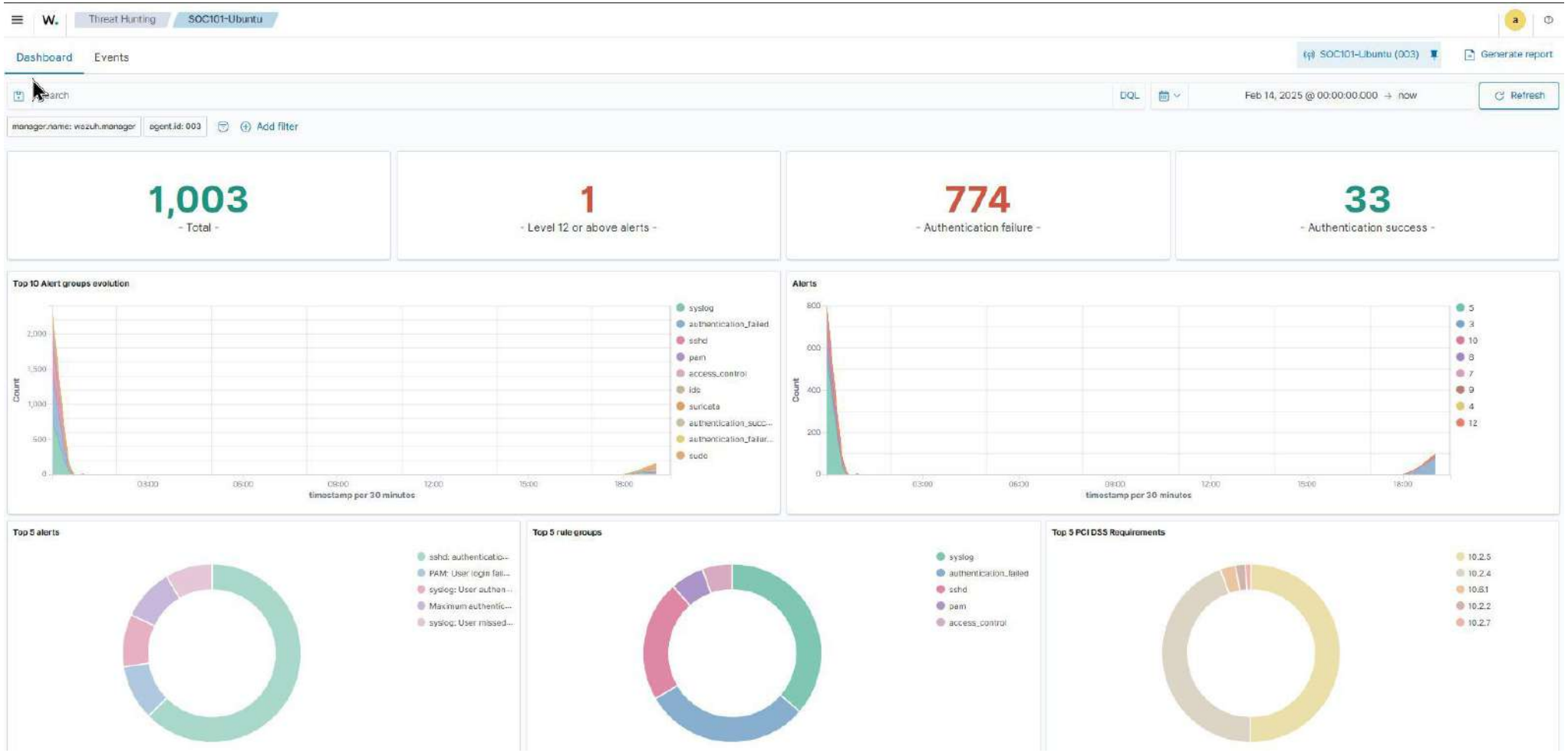

MITRE ATT&CK
SOC101-Ubuntu
Search
DQL
Last 24 hours
Show dates
Refresh
manager.name: wazuh.manager
rule.mitre.id: exists
agent.id: 003
Add filter
Alerts evolution over time
Count
timestamp per 30 minutes
Password Guessing
SSH
Brute Force
Valid Accounts
Sudo and Sudo Cac...
Top tactics
Credential Access
Lateral Movement
Defense Evasion
Privilege Escalation
Persistence
Initial Access
Impact
Rule level by attack
5
10
8
3
4
MITRE attacks by tactic
rule.mitre.tactic: Descending
Rule level by tactic
7

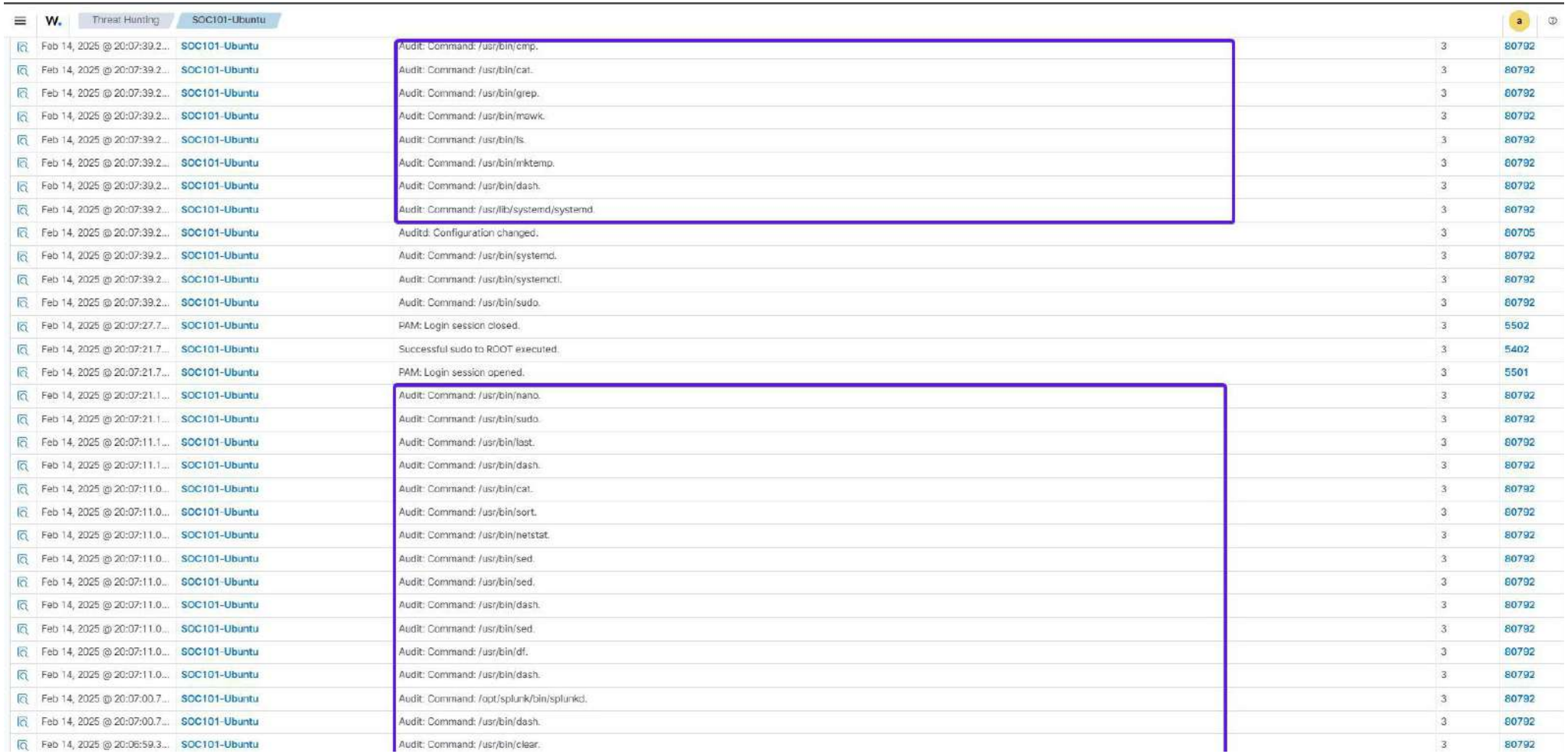

W.
Threat Hunting
SOC101-Ubuntu
a
2,603
- Total -
1
- Level 12 or above alerts -
1,960
- Authentication failure -
75
- Authentication success -
Top 10 Alert groups evolution
Count
2,000
1,500
1,000
500
0
00:00
03:00
06:00
09:00
12:00
15:00
18:00
21:00
timestamp per 30 minutes
syslog
authentication_failed
sshd
pam
access_control
audit
audit_command
ids
suricata
authentication_failur...
Alerts
Count
800
600
400
200
0
00:00
03:00
06:00
09:00
12:00
15:00
18:00
21:00
timestamp per 30 minutes
5
3
10
8
7
4
9
12
Top 5 alerts
sshd: authentication...
PAM: User login fail...
syslog: User authen...
Maximum authentic...
syslog: User missed...
Top 5 rule groups
syslog
authentication_failed
sshd
pam
access_control
Top 5 PCI DSS Requirements
10.2.5
10.2.4
10.6.1
10.2.2
11.4


Threat Hunting
SOC101-Ubuntu
a
Feb 14, 2025 @ 19:24:17.6... SOC101-Ubuntu Suricata: Alert - ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine) 3 86601
Feb 14, 2025 @ 19:24:17.4... SOC101-Ubuntu Suricata: Alert - ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine) 3 86601
Feb 14, 2025 @ 19:24:17.4... SOC101-Ubuntu Suricata: Alert - ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine) 3 86601
Feb 14, 2025 @ 19:24:13.9... SOC101-Ubuntu Suricata: Alert - ET SCAN Potential SSH Scan 3 86601
Feb 14, 2025 @ 19:23:24.6... SOC101-Ubuntu Suricata: Alert - ET SCAN Suspicious inbound to PostgreSQL port 5432 3 86601
Feb 14, 2025 @ 19:23:24.6... SOC101-Ubuntu Suricata: Alert - ET SCAN Suspicious inbound to Oracle SQL port 1521 3 86601
Feb 14, 2025 @ 19:23:22.7... SOC101-Ubuntu Suricata: Alert - ET SCAN Suspicious inbound to mySQL port 3306 3 86601
Feb 14, 2025 @ 19:23:22.7... SOC101-Ubuntu Suricata: Alert - ET SCAN Suspicious inbound to MSSQL port 1433 3 86601
Feb 14, 2025 @ 19:23:01.1... SOC101-Ubuntu Suricata: Alert - ET SCAN Suspicious inbound to Oracle SQL port 1521 3 86601
Feb 14, 2025 @ 19:23:01.1... SOC101-Ubuntu Suricata: Alert - ET SCAN Suspicious inbound to MSSQL port 1433 3 86601
Feb 14, 2025 @ 19:21:20.0... SOC101-Ubuntu Suricata: Alert - ET SCAN Suspicious inbound to Oracle SQL port 1521 3 86601
Feb 14, 2025 @ 19:21:19.5... SOC101-Ubuntu Suricata: Alert - ET SCAN Suspicious inbound to PostgreSQL port 5432 3 86601
Feb 14, 2025 @ 19:21:16.1... SOC101-Ubuntu Suricata: Alert - ET SCAN Suspicious inbound to MSSQL port 1433 3 86601
Feb 14, 2025 @ 19:21:12.1... SOC101-Ubuntu Suricata: Alert - ET SCAN Potential VNC Scan 5800-5820 3 86601
Feb 14, 2025 @ 19:21:04.3... SOC101-Ubuntu Suricata: Alert - ET SCAN Suspicious inbound to mySQL port 3306 3 86601
Feb 14, 2025 @ 19:20:34.0... SOC101-Ubuntu Suricata: Alert - ET POLICY Possible Kali Linux hostname in DHCP Request Packet 3 86601
Feb 14, 2025 @ 19:05:34.9... SOC101-Ubuntu Suricata: Alert - ET POLICY Possible Kali Linux hostname in DHCP Request Packet 3 86601
Feb 14, 2025 @ 18:50:34.7... SOC101-Ubuntu Suricata: Alert - ET POLICY Possible Kali Linux hostname in DHCP Request Packet 3 86601
Feb 14, 2025 @ 00:31:02.9... SOC101-Ubuntu Suricata: Alert - ET POLICY Possible Kali Linux hostname in DHCP Request Packet 3 86601
Feb 14, 2025 @ 00:30:10.4... SOC101-Ubuntu Suricata: Alert - ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack 3 86601
Feb 14, 2025 @ 00:29:34.2... SOC101-Ubuntu Suricata: Alert - ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack 3 86601
Feb 14, 2025 @ 00:28:54.2... SOC101-Ubuntu Suricata: Alert - ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack 3 86601


W.
Vulnerability De...
SOC101-Ubuntu
a
22
Critical - Severity
634
High - Severity
1,404
Medium - Severity
37
Low - Severity
448
Pending - Evaluation
Top 5 vulnerabilities
Count
CVE-2023-3326 16
CVE-2022-3219 11
CVE-2017-13716 8
CVE-2016-2568 6
CVE-2024-3661 6
Top 5 OS
Count
Ubuntu 24.04.1 LTS (Noble Numbat) 2,545
Top 5 agents
Count
SOC101-Ubuntu 2,545
Top 5 packages
Count
linux-image-6.8.0-51-generic 1,106
linux-image-6.8.0-52-generic 1,103
bluez 19
bluez-cups 19
bluez-obexd 19
Most common vulnerability score
Vulnerability base score
5.5
-1
7.8
7.1
7.5
5.3
4.7
7
6.5
8.8
200
400
600
800
1,000
Count
Most vulnerable OS families
Host OS type
ubuntu
500
1,000
1,500
2,000
2,500
Count
Vulnerabilities by year of publication
Count
700
400
200
70
40
20
7
4
2
0500
1000
1500
vulnerability.published_at per year
High
Medium
Low
Critical
-

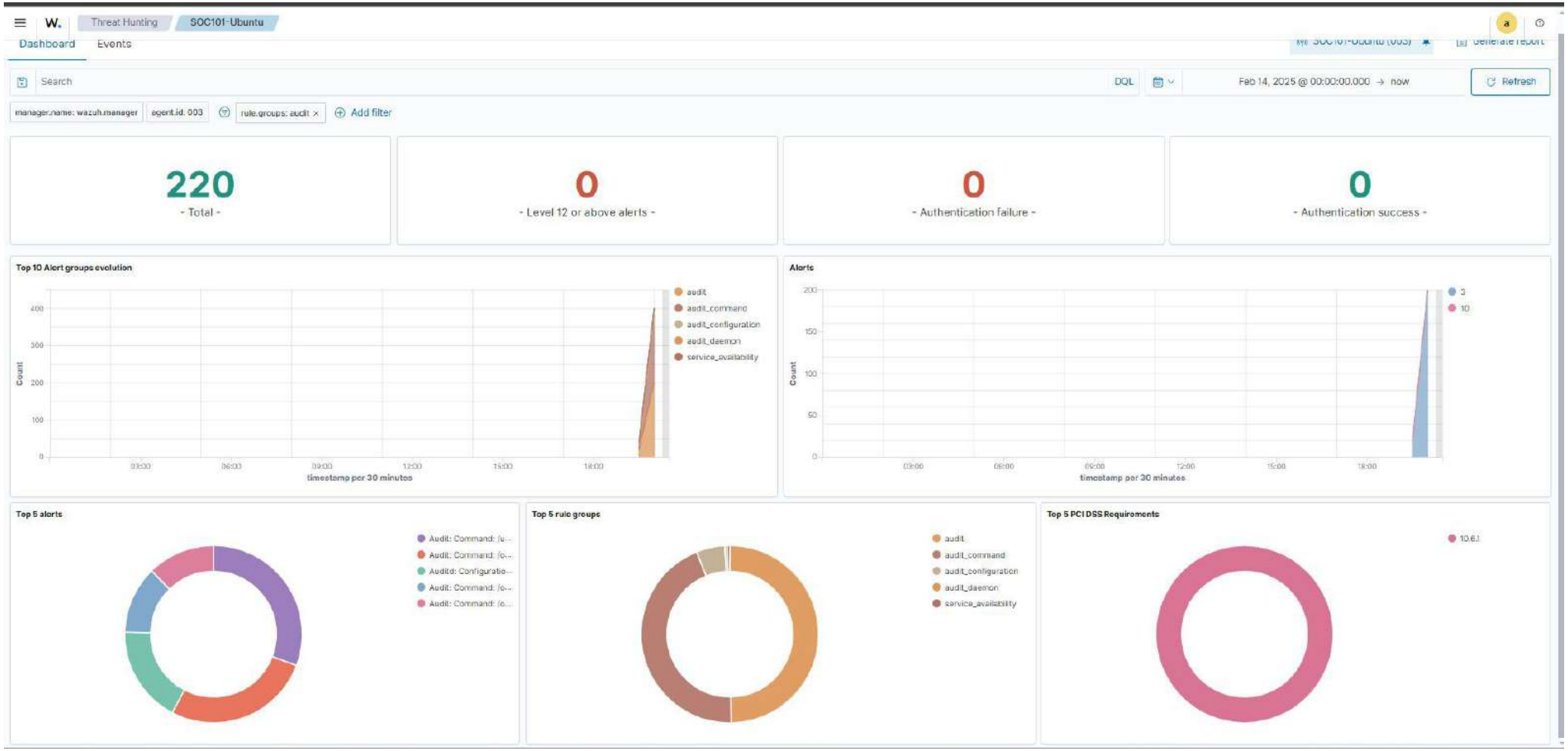

Endpoints
SOC101-Ubuntu
Vulnerability Detection
22 Critical
612 High
1,392 Medium
37 Low
Top 5 Packages
FIM: Recent events
/etc/passwd
Table
JSON
Rule
_index
wazuh-alerts-4.x-2025.02.14
agent.id
003
agent.ip
192.168.1.130
agent.name
SOC101-Ubuntu
decoder.name
syscheck_integrity_changed
full_log
File '/etc/passwd' modified
Mode: realtime
Changed attributes: size,mtime,md5,sha1,sha256
Size changed from '3001' to '3117'
Old modification time was: '1739474839', now it is '1739540548'
Old md5sum was: '850cbfda02cc04b1dfd5a4733b57fda7'
id
1739540549.92338
input.type
log
location
syscheck
manager.name
wazuh.manager
rule.description
Integrity checksum changed.
rule.firedtimes
1
rule.gdpr
II_5.1.f
rule.gpg13
4.11
rule.groups
ossec, syscheck, syscheck_entry_modified, syscheck_file
rule.hipaa
164.312.c.1, 164.312.c.2
rule.id
550
rule.level
7
rule.mail
false
rule.mitre.id
T1565.001
rule.mitre.tactic
Impact
rule.mitre.technique
Stored Data Manipulation
rule.nist_800_53
SI.7


Threat Hunting
SOC101-Ubuntu
Dashboard
Events
SOC101-Ubuntu (003)
Generate report
Search
DQL
Feb 14, 2025 @ 00:00:00.000 → now
Refresh
manager.name: wazuh.manager
agent.id: 003
Add filter
1,003
- Total -
1
- Level 12 or above alerts -
774
- Authentication failure -
33
- Authentication success -
Top 10 Alert groups evolution
Count
timestamp per 30 minutes
syslog
authentication_failed
sshd
pam
access_control
idc
suricata
authentication_succ...
authentication_failur...
sudo
Alerts
Count
timestamp per 30 minutes
5
3
10
8
7
9
4
12
Top 5 alerts
sshd: authentication...
PAM: User login fail...
syslog: User authen...
Maximum authentic...
syslog: User missed...
Top 5 rule groups
syslog
authentication_failed
sshd
pam
access_control
Top 5 PCI DSS Requirements
10.2.5
10.2.4
10.6.1
10.2.2
10.2.7



Threat Hunting | SOC101-Ubuntu

Feb 14, 2025 @ 20:07:39.2...	SOC101-Ubuntu	Audit: Command: /usr/bin/cmp.	3	80792
Feb 14, 2025 @ 20:07:39.2...	SOC101-Ubuntu	Audit: Command: /usr/bin/cat.	3	80792
Feb 14, 2025 @ 20:07:39.2...	SOC101-Ubuntu	Audit: Command: /usr/bin/grep.	3	80792
Feb 14, 2025 @ 20:07:39.2...	SOC101-Ubuntu	Audit: Command: /usr/bin/mawk.	3	80792
Feb 14, 2025 @ 20:07:39.2...	SOC101-Ubuntu	Audit: Command: /usr/bin/ls.	3	80792
Feb 14, 2025 @ 20:07:39.2...	SOC101-Ubuntu	Audit: Command: /usr/bin/mktemp.	3	80792
Feb 14, 2025 @ 20:07:39.2...	SOC101-Ubuntu	Audit: Command: /usr/bin/dash.	3	80792
Feb 14, 2025 @ 20:07:39.2...	SOC101-Ubuntu	Audit: Command: /usr/lib/systemd/systemd.	3	80792
Feb 14, 2025 @ 20:07:39.2...	SOC101-Ubuntu	Auditd: Configuration changed.	3	80705
Feb 14, 2025 @ 20:07:39.2...	SOC101-Ubuntu	Audit: Command: /usr/bin/systemd.	3	80792
Feb 14, 2025 @ 20:07:39.2...	SOC101-Ubuntu	Audit: Command: /usr/bin/systemctl.	3	80792
Feb 14, 2025 @ 20:07:39.2...	SOC101-Ubuntu	Audit: Command: /usr/bin/sudo.	3	80792
Feb 14, 2025 @ 20:07:27.7...	SOC101-Ubuntu	PAM: Login session closed.	3	5502
Feb 14, 2025 @ 20:07:21.7...	SOC101-Ubuntu	Successful sudo to ROOT executed.	3	5402
Feb 14, 2025 @ 20:07:21.7...	SOC101-Ubuntu	PAM: Login session opened.	3	5501
Feb 14, 2025 @ 20:07:21.1...	SOC101-Ubuntu	Audit: Command: /usr/bin/nano.	3	80792
Feb 14, 2025 @ 20:07:21.1...	SOC101-Ubuntu	Audit: Command: /usr/bin/sudo.	3	80792
Feb 14, 2025 @ 20:07:11.1...	SOC101-Ubuntu	Audit: Command: /usr/bin/last.	3	80792
Feb 14, 2025 @ 20:07:11.1...	SOC101-Ubuntu	Audit: Command: /usr/bin/dash.	3	80792
Feb 14, 2025 @ 20:07:11.0...	SOC101-Ubuntu	Audit: Command: /usr/bin/cat.	3	80792
Feb 14, 2025 @ 20:07:11.0...	SOC101-Ubuntu	Audit: Command: /usr/bin/sort.	3	80792
Feb 14, 2025 @ 20:07:11.0...	SOC101-Ubuntu	Audit: Command: /usr/bin/netstat.	3	80792
Feb 14, 2025 @ 20:07:11.0...	SOC101-Ubuntu	Audit: Command: /usr/bin/sed.	3	80792
Feb 14, 2025 @ 20:07:11.0...	SOC101-Ubuntu	Audit: Command: /usr/bin/sed.	3	80792
Feb 14, 2025 @ 20:07:11.0...	SOC101-Ubuntu	Audit: Command: /usr/bin/dash.	3	80792
Feb 14, 2025 @ 20:07:11.0...	SOC101-Ubuntu	Audit: Command: /usr/bin/sed.	3	80792
Feb 14, 2025 @ 20:07:11.0...	SOC101-Ubuntu	Audit: Command: /usr/bin/df.	3	80792
Feb 14, 2025 @ 20:07:11.0...	SOC101-Ubuntu	Audit: Command: /usr/bin/dash.	3	80792
Feb 14, 2025 @ 20:07:00.7...	SOC101-Ubuntu	Audit: Command: /opt/splunk/bin/splunkd.	3	80792
Feb 14, 2025 @ 20:07:00.7...	SOC101-Ubuntu	Audit: Command: /usr/bin/dash.	3	80792
Feb 14, 2025 @ 20:06:59.3...	SOC101-Ubuntu	Audit: Command: /usr/bin/clear.	3	80792


Threat Hunting
SOC101-Ubuntu
Dashboard
Events
Search
DQL
Feb 14, 2025 @ 00:00:00.000 → now
Refresh
manager.name: wazuh.manager
agent.id: 003
rule.groups: audit
Add filter
220
- Total -
0
- Level 12 or above alerts -
0
- Authentication failure -
0
- Authentication success -
Top 10 Alert groups evolution
Count
timestamp per 30 minutes
audit
audit_command
audit_configuration
audit_daemon
service_availability
Alerts
Count
timestamp per 30 minutes
3
10
Top 5 alerts
Top 5 rule groups
audit
audit_command
audit_configuration
audit_daemon
service_availability
Top 5 PCI DSS Requirements
10.6.1