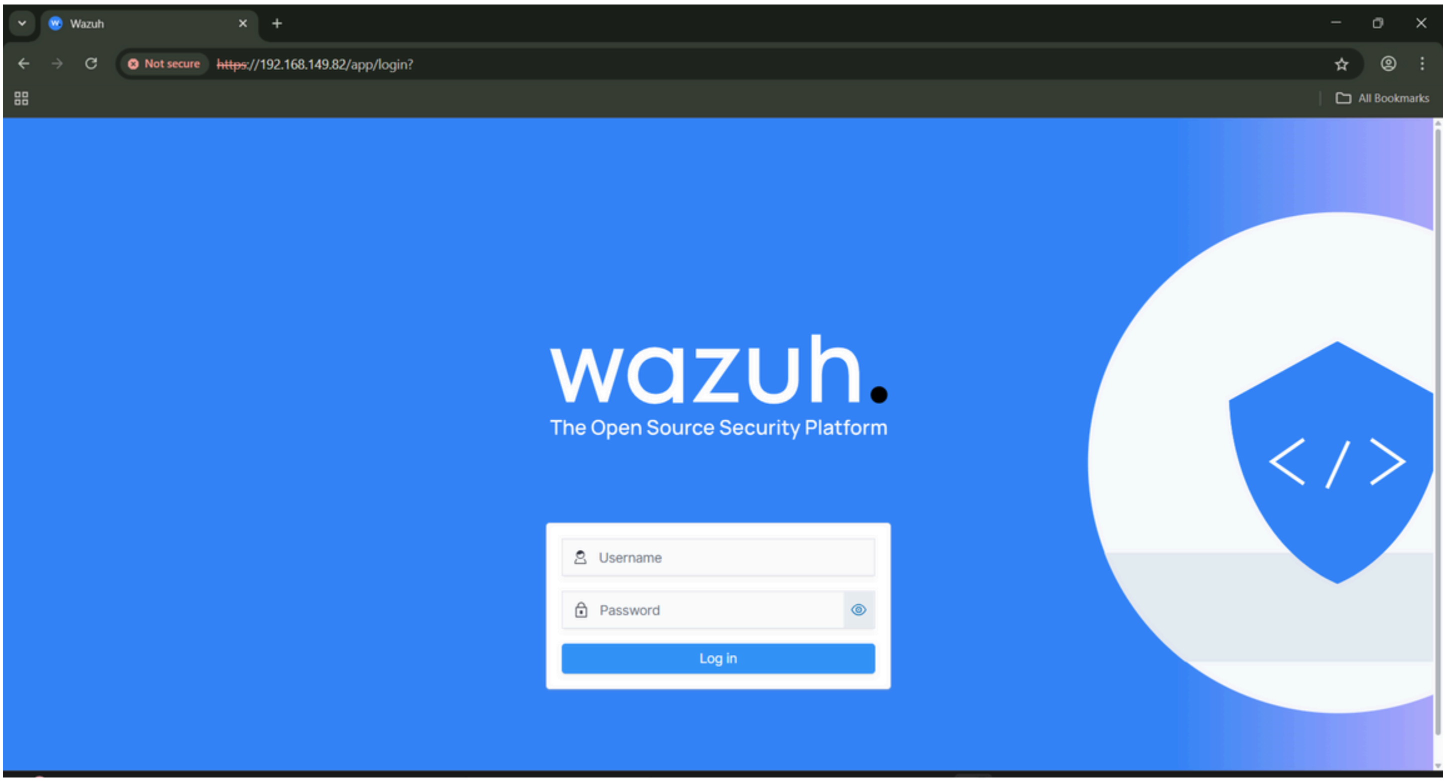
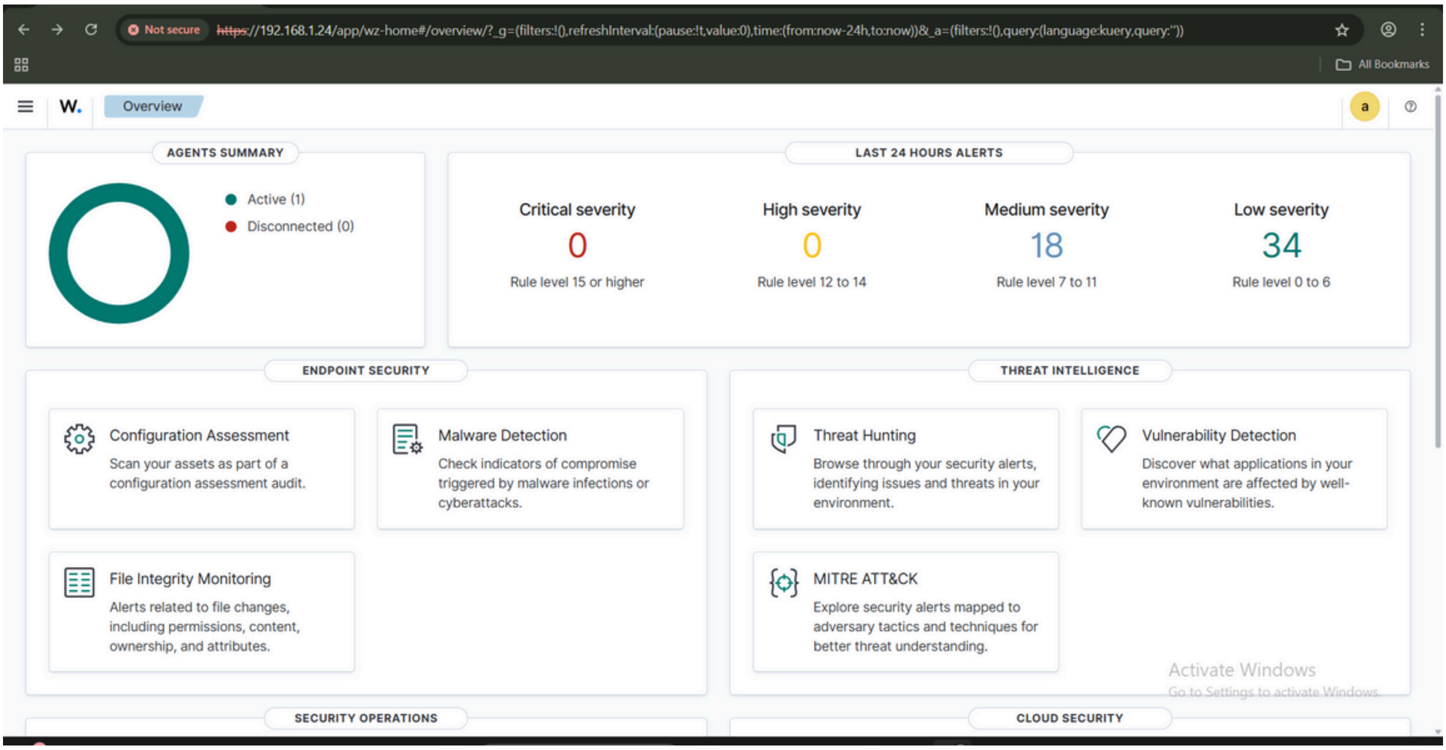
☐ Wazuh - Homelab🕵️

- **Wazuh-login page :**


Wazuh
Not secure
https://192.168.149.82/app/login?
All Bookmarks
wazuh.
The Open Source Security Platform
Username
Password
Log in

- **Wazuh-Home Overview :**


Not secure
https://192.168.1.24/app/wz-home#/overview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,to:now))&_a=(filters:!(),query:(language:kuery,query:''))
All Bookmarks
W.
Overview
a

AGENTS SUMMARY

● Active (1)
● Disconnected (0)

LAST 24 HOURS ALERTS

Critical severity	High severity	Medium severity	Low severity
0	0	18	34
Rule level 15 or higher	Rule level 12 to 14	Rule level 7 to 11	Rule level 0 to 6

ENDPOINT SECURITY

Configuration Assessment
Scan your assets as part of a configuration assessment audit.

Malware Detection
Check indicators of compromise triggered by malware infections or cyberattacks.

File Integrity Monitoring
Alerts related to file changes, including permissions, content, ownership, and attributes.

THREAT INTELLIGENCE

Threat Hunting
Browse through your security alerts, identifying issues and threats in your environment.

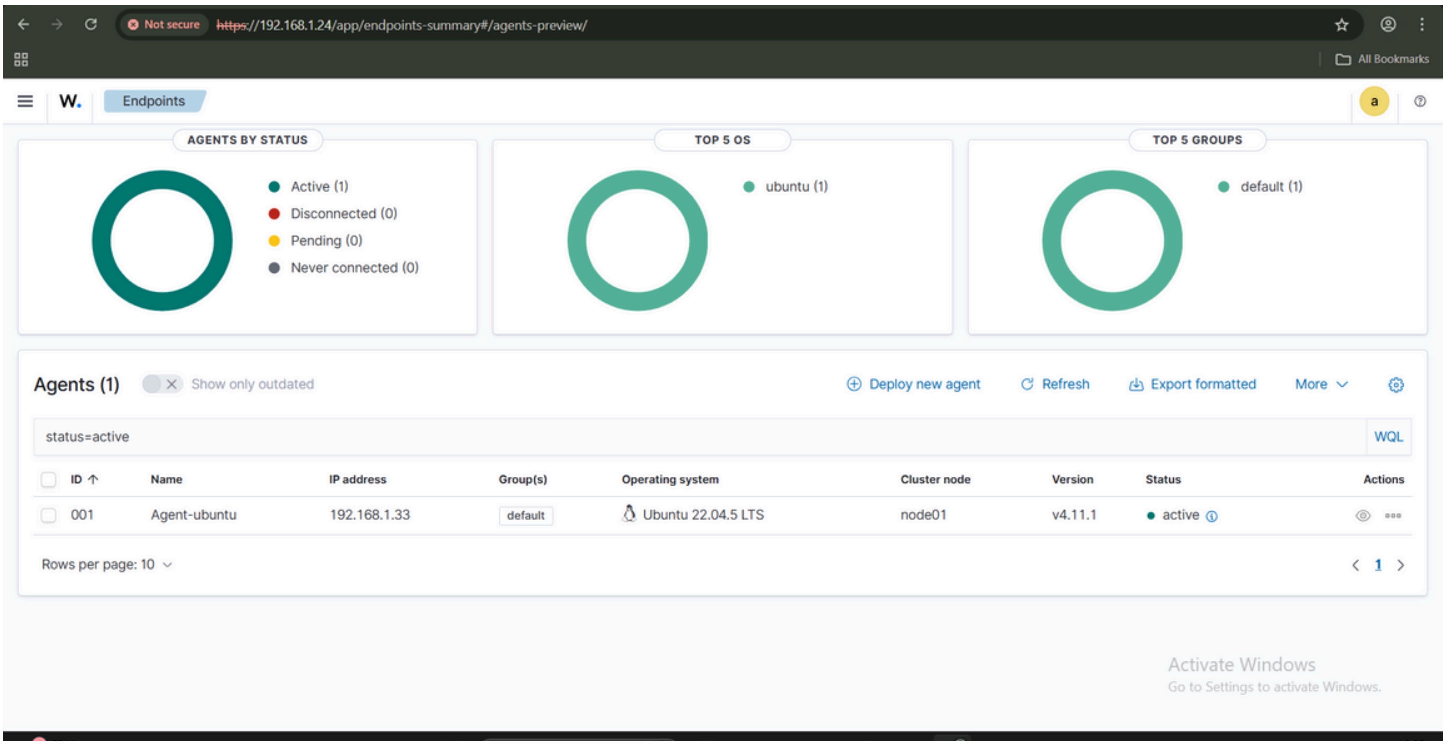
Vulnerability Detection
Discover what applications in your environment are affected by well-known vulnerabilities.

MITRE ATT&CK
Explore security alerts mapped to adversary tactics and techniques for better threat understanding.

SECURITY OPERATIONS

CLOUD SECURITY

- **Wazuh-Agent deployed on Ubuntu :**

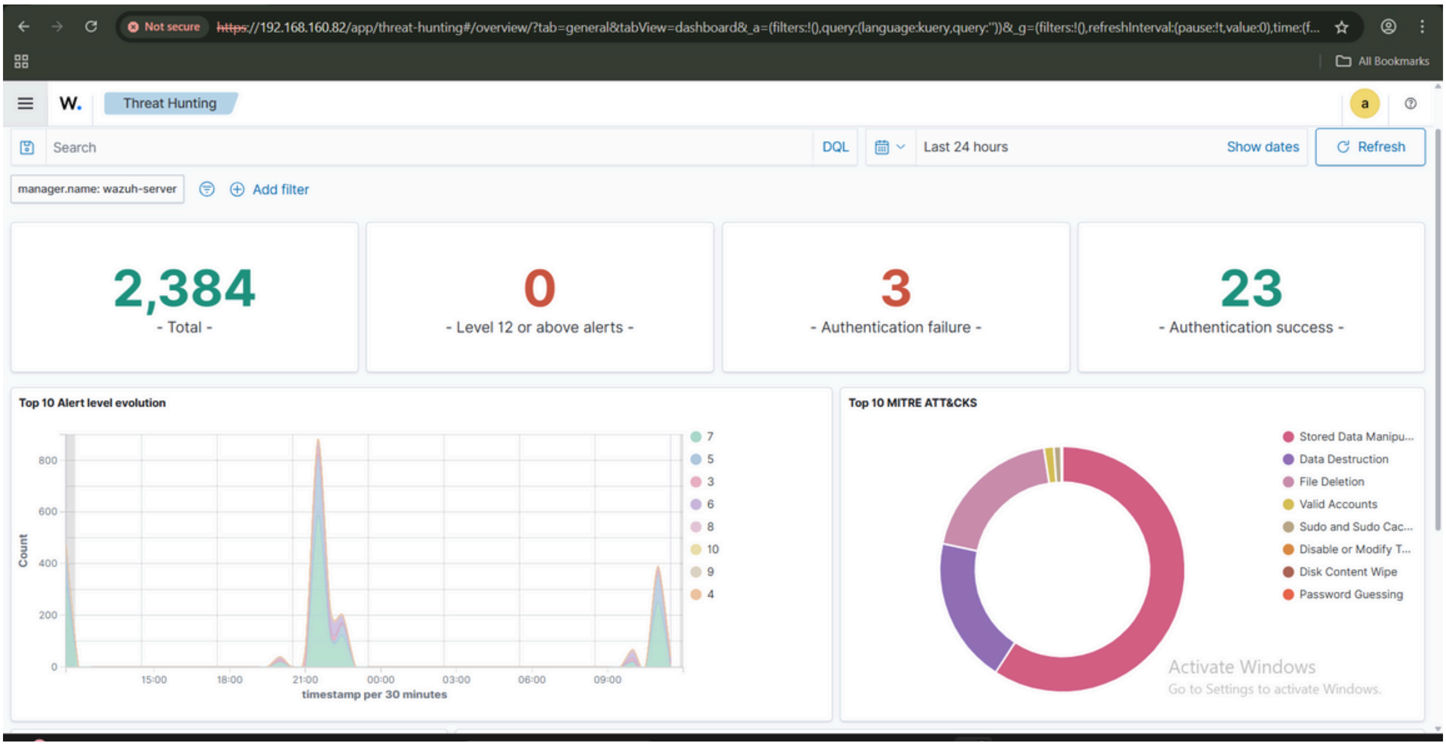


Agents (1)

status=active

ID ↑	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
001	Agent-ubuntu	192.168.1.33	default	Ubuntu 22.04.5 LTS	node01	v4.11.1	● active	

- **Threat Hunting Dashboard :**



2,384 - Total -

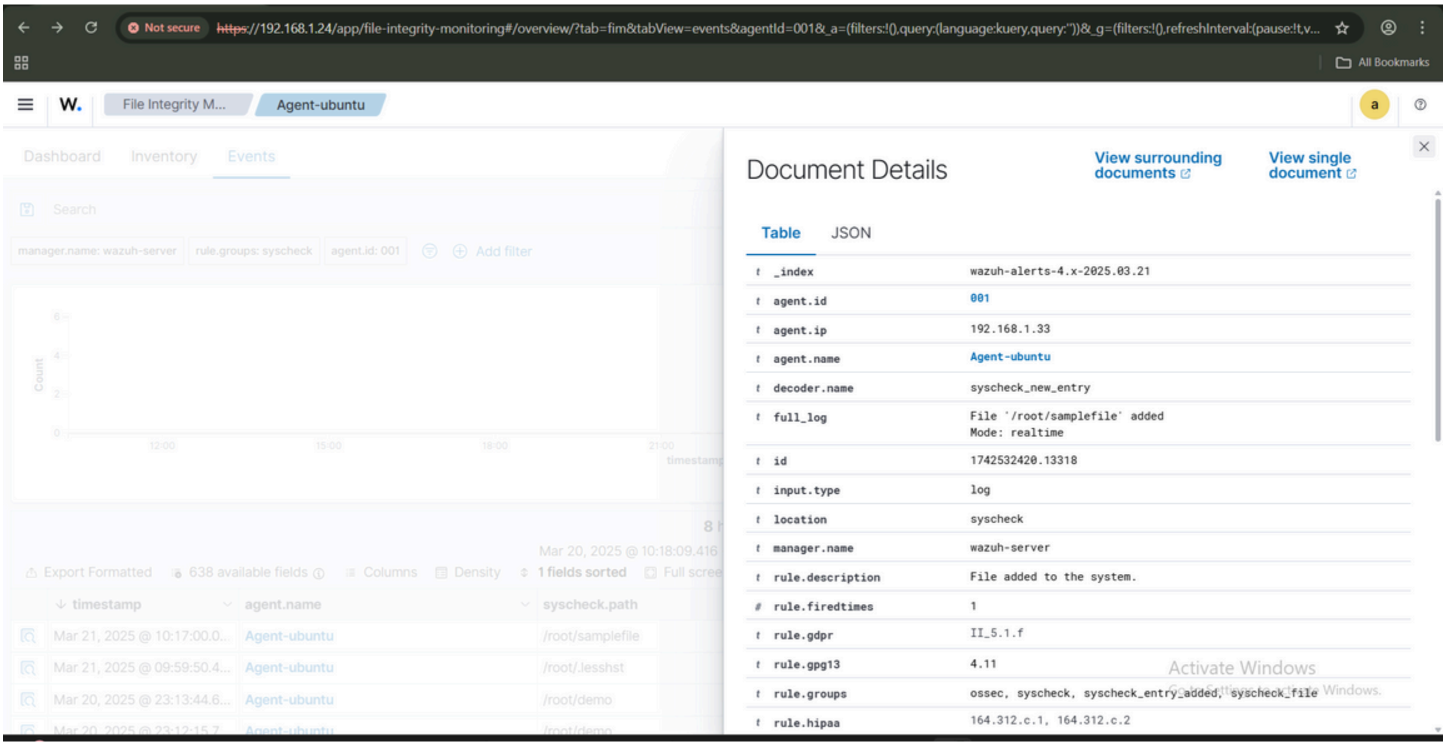
0 - Level 12 or above alerts -

3 - Authentication failure -

23 - Authentication success -

- **File Integrity Monitoring:**

i) Detected a file added :


Not secure
https://192.168.1.24/app/file-integrity-monitoring#/overview/?tab=fim&tabView=events&agentId=001&_a=(filters:!(),query:(language:kuery,query:''))&_g=(filters:!(),refreshInterval:(pause:!t,v...
All Bookmarks
File Integrity M...
Agent-ubuntu
Dashboard
Inventory
Events
Search
manager.name: wazuh-server
rule.groups: syscheck
agent.id: 001
Add filter
Export Formatted
638 available fields
Columns
Density
1 fields sorted
Full scree

timestamp	agent.name	syscheck.path
Mar 21, 2025 @ 10:17:00.0...	Agent-ubuntu	/root/samplefile
Mar 21, 2025 @ 09:59:50.4...	Agent-ubuntu	/root/.lesshst
Mar 20, 2025 @ 23:13:44.6...	Agent-ubuntu	/root/demo
Mar 20, 2025 @ 23:12:15.7	Agent-ubuntu	/root/demo

Document Details

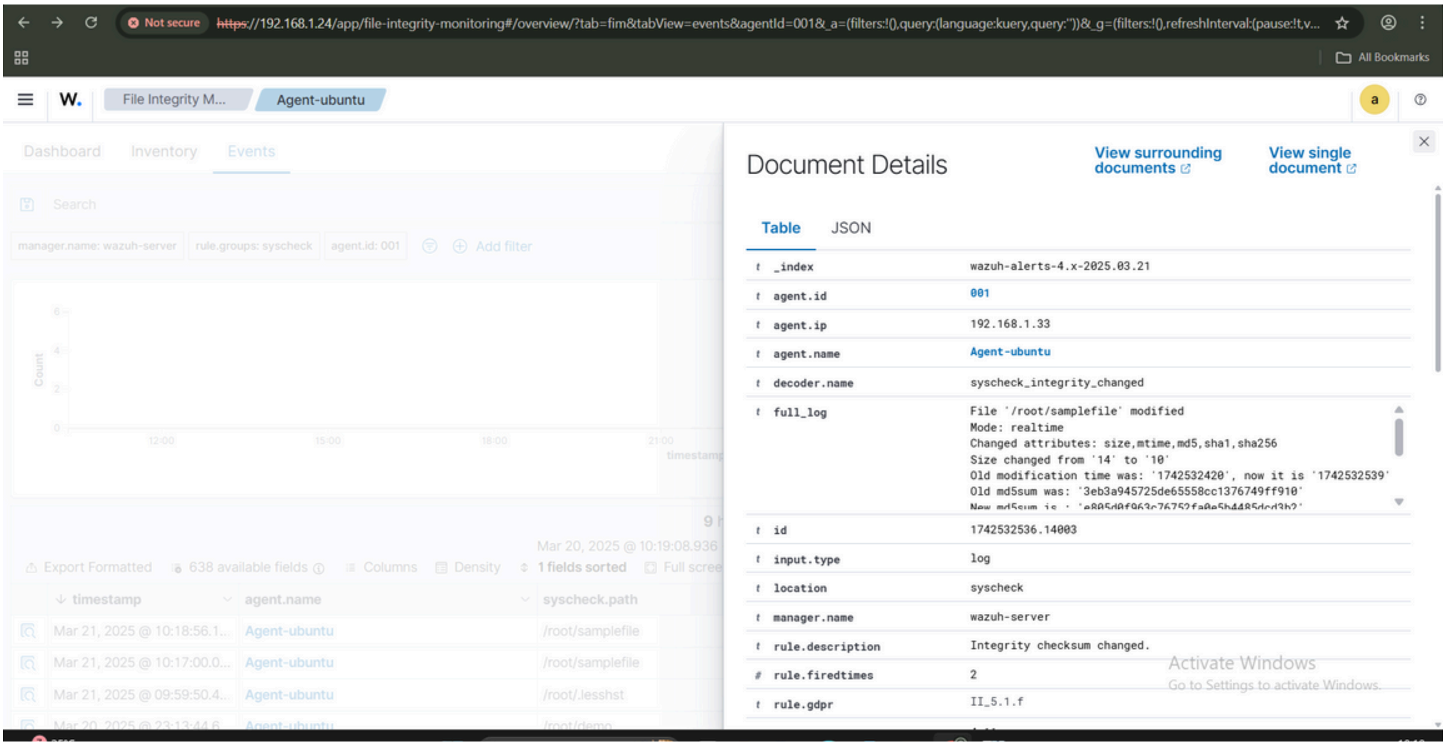
View surrounding documents

View single document

Table JSON

_index	wazuh-alerts-4.x-2025.03.21
agent.id	001
agent.ip	192.168.1.33
agent.name	Agent-ubuntu
decoder.name	syscheck_new_entry
full_log	File '/root/samplefile' added Mode: realtime
id	1742532420.13318
input.type	log
location	syscheck
manager.name	wazuh-server
rule.description	File added to the system.
rule.firedtimes	1
rule.gdpr	II_5.1.f
rule.gpg13	4.11
rule.groups	ossec, syscheck, syscheck_entry_added, syscheck_file
rule.hipaa	164.312.c.1, 164.312.c.2

ii) Detected modified file :


Not secure
https://192.168.1.24/app/file-integrity-monitoring#/overview/?tab=fim&tabView=events&agentId=001&_a=(filters:!(),query:(language:kuery,query:''))&_g=(filters:!(),refreshInterval:(pause:!t,v...
All Bookmarks
File Integrity M...
Agent-ubuntu
Dashboard
Inventory
Events
Search
manager.name: wazuh-server
rule.groups: syscheck
agent.id: 001
Add filter
Export Formatted
638 available fields
Columns
Density
1 fields sorted
Full scree

timestamp	agent.name	syscheck.path
Mar 21, 2025 @ 10:18:56.1...	Agent-ubuntu	/root/samplefile
Mar 21, 2025 @ 10:17:00.0...	Agent-ubuntu	/root/samplefile
Mar 21, 2025 @ 09:59:50.4...	Agent-ubuntu	/root/.lesshst
Mar 20, 2025 @ 23:13:44.6	Agent-ubuntu	/root/demo

Document Details

View surrounding documents

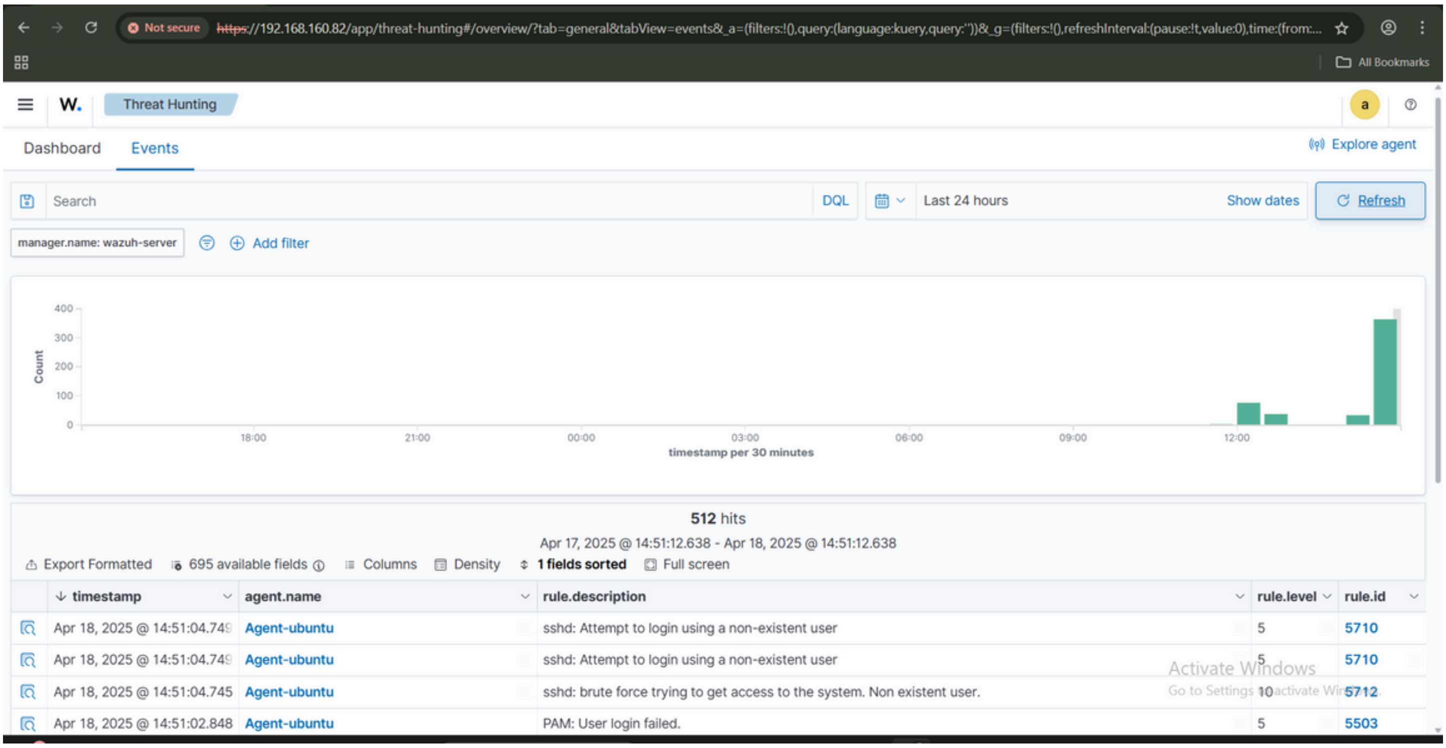
View single document

Table JSON

_index	wazuh-alerts-4.x-2025.03.21
agent.id	001
agent.ip	192.168.1.33
agent.name	Agent-ubuntu
decoder.name	syscheck_integrity_changed
full_log	File '/root/samplefile' modified Mode: realtime Changed attributes: size,mtime,md5,sha1,sha256 Size changed from '14' to '10' Old modification time was: '1742532420', now it is '1742532539' Old md5sum was: '3eb3a945725de65558cc1376749ff910' New md5sum is : 'e805d0f963c76752fa0e5b4485dcd3b2'
id	1742532536.14003
input.type	log
location	syscheck
manager.name	wazuh-server
rule.description	Integrity checksum changed.
rule.firedtimes	2
rule.gdpr	II_5.1.f

- ## Detected Bruteforce Attack :

i) Detected Failed Login attempt :

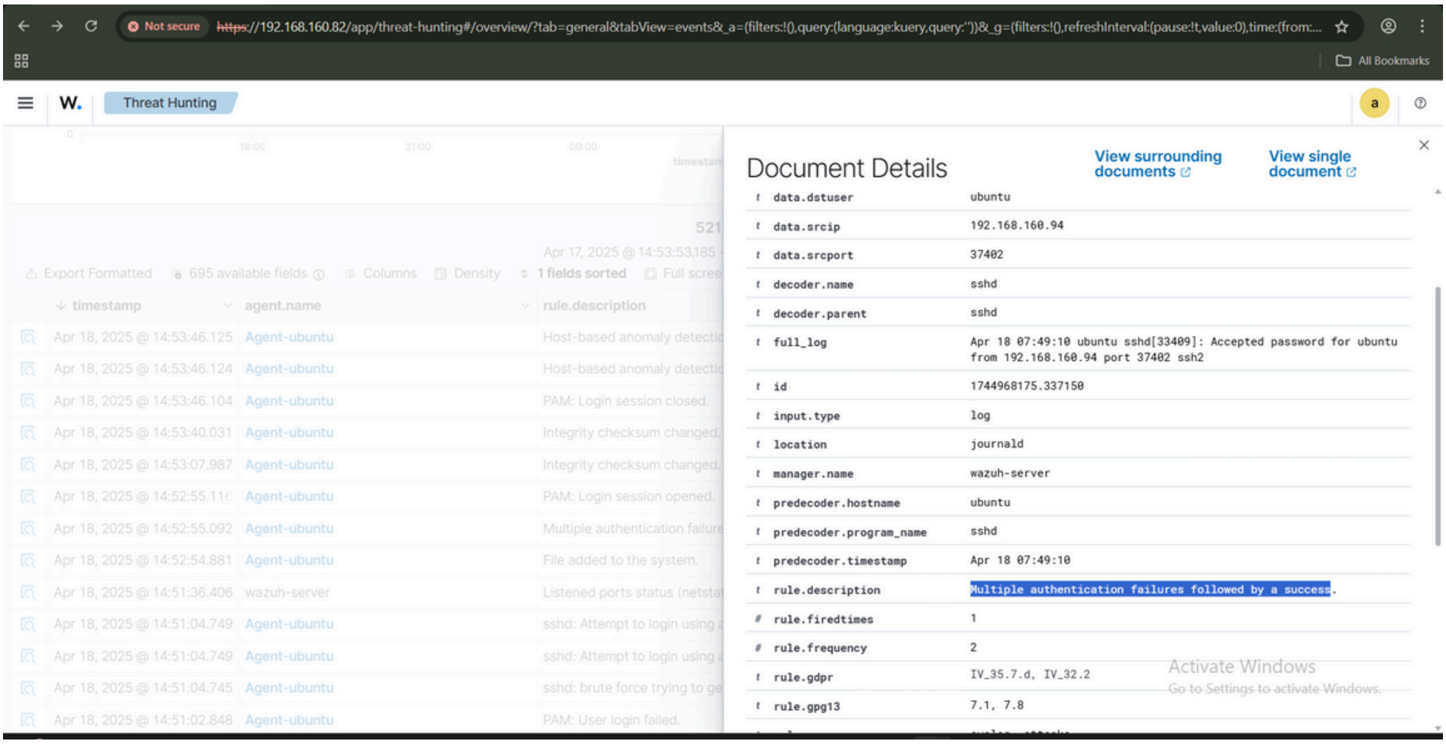


512 hits

Apr 17, 2025 @ 14:51:12.638 - Apr 18, 2025 @ 14:51:12.638

timestamp	agent.name	rule.description	rule.level	rule.id
Apr 18, 2025 @ 14:51:04.749	Agent-ubuntu	sshd: Attempt to login using a non-existent user	5	5710
Apr 18, 2025 @ 14:51:04.749	Agent-ubuntu	sshd: Attempt to login using a non-existent user	5	5710
Apr 18, 2025 @ 14:51:04.745	Agent-ubuntu	sshd: brute force trying to get access to the system. Non existent user.	10	5712
Apr 18, 2025 @ 14:51:02.848	Agent-ubuntu	PAM: User login failed.	5	5503

ii) Detected Successfull login attempt :



Not secure
https://192.168.160.82/app/threat-hunting#/overview/?tab=general&tabView=events&_a=(filters:!(),query:(language:kuery,query:''))&_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:...
All Bookmarks
W.
Threat Hunting
Export Formatted
695 available fields
Columns
Density
1 fields sorted
Full scree
View surrounding documents
View single document
Activate Windows
Go to Settings to activate Windows.

521

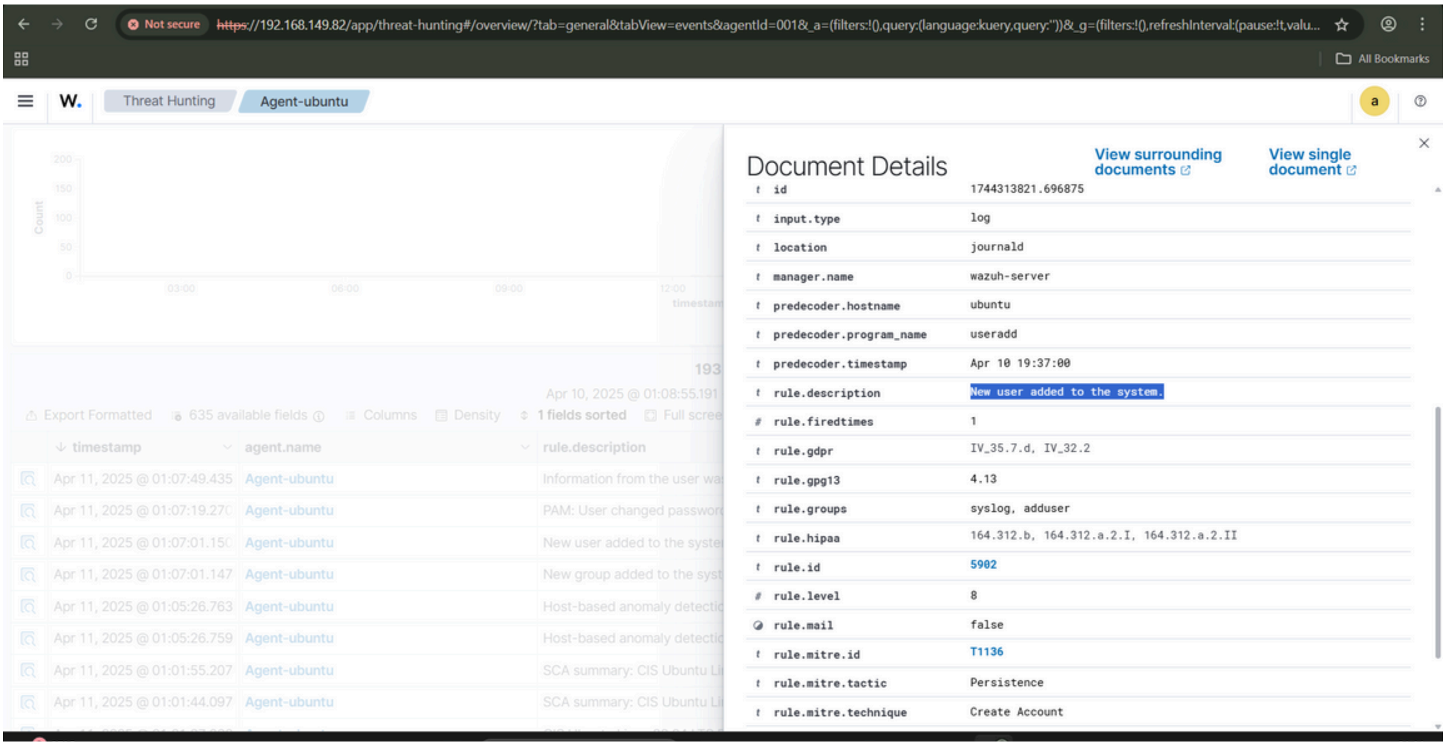
Apr 17, 2025 @ 14:53:53.185

timestamp	agent.name	rule.description
Apr 18, 2025 @ 14:53:46.125	Agent-ubuntu	Host-based anomaly detectio
Apr 18, 2025 @ 14:53:46.124	Agent-ubuntu	Host-based anomaly detectio
Apr 18, 2025 @ 14:53:46.104	Agent-ubuntu	PAM: Login session closed.
Apr 18, 2025 @ 14:53:40.031	Agent-ubuntu	Integrity checksum changed.
Apr 18, 2025 @ 14:53:07.987	Agent-ubuntu	Integrity checksum changed.
Apr 18, 2025 @ 14:52:55.110	Agent-ubuntu	PAM: Login session opened.
Apr 18, 2025 @ 14:52:55.092	Agent-ubuntu	Multiple authentication failure
Apr 18, 2025 @ 14:52:54.881	Agent-ubuntu	File added to the system.
Apr 18, 2025 @ 14:51:36.406	wazuh-server	Listened ports status (netstat
Apr 18, 2025 @ 14:51:04.749	Agent-ubuntu	sshd: Attempt to login using a
Apr 18, 2025 @ 14:51:04.749	Agent-ubuntu	sshd: Attempt to login using a
Apr 18, 2025 @ 14:51:04.745	Agent-ubuntu	sshd: brute force trying to ge
Apr 18, 2025 @ 14:51:02.848	Agent-ubuntu	PAM: User login failed.

Document Details

data.dstuser	ubuntu
data.srcip	192.168.160.94
data.srcport	37402
decoder.name	sshd
decoder.parent	sshd
full_log	Apr 18 07:49:10 ubuntu sshd[33409]: Accepted password for ubuntu from 192.168.160.94 port 37402 ssh2
id	1744968175.337150
input.type	log
location	journald
manager.name	wazuh-server
predecoder.hostname	ubuntu
predecoder.program_name	sshd
predecoder.timestamp	Apr 18 07:49:10
rule.description	Multiple authentication failures followed by a success.
rule.firedtimes	1
rule.frequency	2
rule.gdpr	IV_35.7.d, IV_32.2
rule.gpg13	7.1, 7.8

- **Detected Newly Added User Account :**


https://192.168.149.82/app/threat-hunting#/overview/?tab=general&tabView=events&agentId=001&_a=(filters:!(),query:(language:kuery,query:''))&_g=(filters:!(),refreshInterval:(pause:!t,valu...
Not secure
All Bookmarks
W.
Threat Hunting
Agent-ubuntu
Export Formatted
635 available fields
Columns
Density
1 fields sorted
Full scree

timestamp	agent.name	rule.description
Apr 11, 2025 @ 01:07:49.435	Agent-ubuntu	Information from the user wa
Apr 11, 2025 @ 01:07:19.270	Agent-ubuntu	PAM: User changed passwor
Apr 11, 2025 @ 01:07:01.150	Agent-ubuntu	New user added to the syste
Apr 11, 2025 @ 01:07:01.147	Agent-ubuntu	New group added to the syst
Apr 11, 2025 @ 01:05:26.763	Agent-ubuntu	Host-based anomaly detectio
Apr 11, 2025 @ 01:05:26.759	Agent-ubuntu	Host-based anomaly detectio
Apr 11, 2025 @ 01:01:55.207	Agent-ubuntu	SCA summary: CIS Ubuntu Li
Apr 11, 2025 @ 01:01:44.097	Agent-ubuntu	SCA summary: CIS Ubuntu Li

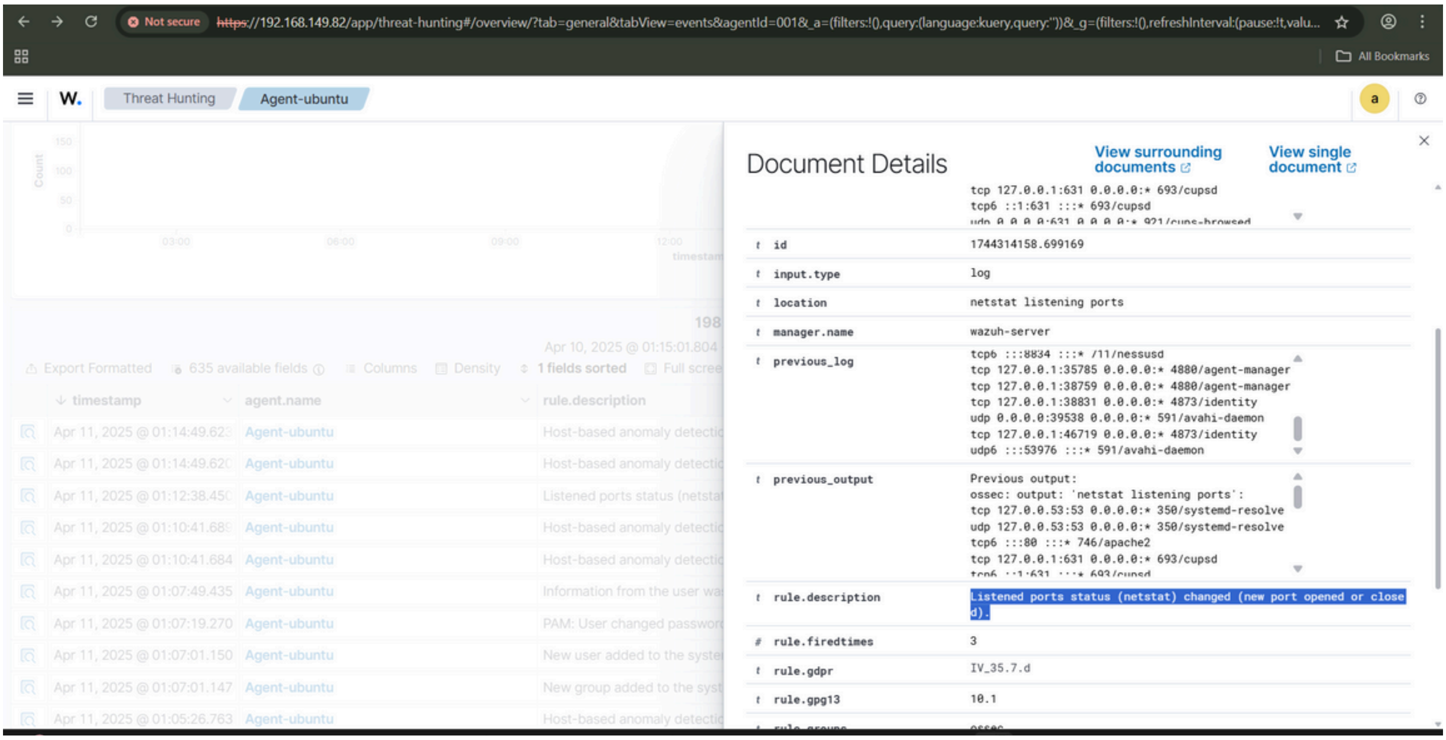
Document Details

View surrounding documents

View single document

id	1744313821.696875
input.type	log
location	journald
manager.name	wazuh-server
predecoder.hostname	ubuntu
predecoder.program_name	useradd
predecoder.timestamp	Apr 10 19:37:00
rule.description	New user added to the system.
rule.firedtimes	1
rule.gdpr	IV_35.7.d, IV_32.2
rule.gpg13	4.13
rule.groups	syslog, adduser
rule.hipaa	164.312.b, 164.312.a.2.I, 164.312.a.2.II
rule.id	5902
rule.level	8
rule.mail	false
rule.mitre.id	T1136
rule.mitre.tactic	Persistence
rule.mitre.technique	Create Account

- **Detected Anamolous Network traffic :**


https://192.168.149.82/app/threat-hunting#/overview/?tab=general&tabView=events&agentId=001&_a=(filters:!(),query:(language:kuery,query:''))&_g=(filters:!(),refreshInterval:(pause:!t,valu...
Not secure
All Bookmarks
W.
Threat Hunting
Agent-ubuntu
Export Formatted
635 available fields
Columns
Density
1 fields sorted
Full scree

timestamp	agent.name	rule.description
Apr 11, 2025 @ 01:14:49.623	Agent-ubuntu	Host-based anomaly detectio
Apr 11, 2025 @ 01:14:49.620	Agent-ubuntu	Host-based anomaly detectio
Apr 11, 2025 @ 01:12:38.450	Agent-ubuntu	Listened ports status (netsta
Apr 11, 2025 @ 01:10:41.680	Agent-ubuntu	Host-based anomaly detectio
Apr 11, 2025 @ 01:10:41.684	Agent-ubuntu	Host-based anomaly detectio
Apr 11, 2025 @ 01:07:49.435	Agent-ubuntu	Information from the user wa
Apr 11, 2025 @ 01:07:19.270	Agent-ubuntu	PAM: User changed passwor
Apr 11, 2025 @ 01:07:01.150	Agent-ubuntu	New user added to the syste
Apr 11, 2025 @ 01:07:01.147	Agent-ubuntu	New group added to the syst
Apr 11, 2025 @ 01:05:26.763	Agent-ubuntu	Host-based anomaly detectio

Document Details

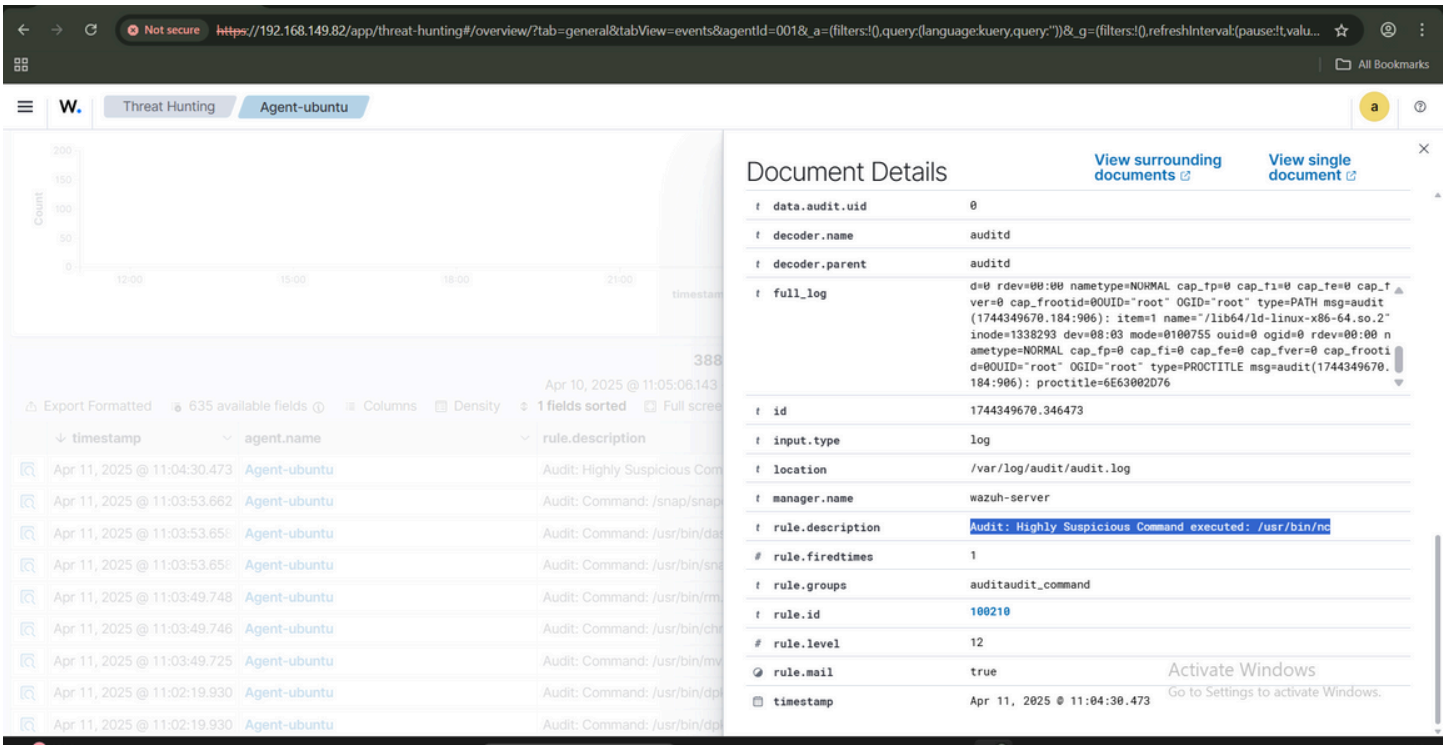
View surrounding documents

View single document

```
tcp 127.0.0.1:631 0.0.0.0:* 693/cupsd
tcp6 ::1:631 :::* 693/cupsd
```

id	1744314158.699169
input.type	log
location	netstat listening ports
manager.name	wazuh-server
previous_log	tcp6 :::8834 :::* 711/nessusd tcp 127.0.0.1:35785 0.0.0.0:* 4880/agent-manager tcp 127.0.0.1:38759 0.0.0.0:* 4880/agent-manager tcp 127.0.0.1:38831 0.0.0.0:* 4873/identity udp 0.0.0.0:39538 0.0.0.0:* 591/avahi-daemon tcp 127.0.0.1:46719 0.0.0.0:* 4873/identity udp6 :::53976 :::* 591/avahi-daemon
previous_output	Previous output: ossec: output: 'netstat listening ports': tcp 127.0.0.53:53 0.0.0.0:* 350/systemd-resolve udp 127.0.0.53:53 0.0.0.0:* 350/systemd-resolve tcp6 :::80 :::* 746/apache2 tcp 127.0.0.1:631 0.0.0.0:* 693/cupsd
rule.description	Listened ports status (netstat) changed (new port opened or closed).
rule.firedtimes	3
rule.gdpr	IV_35.7.d
rule.gpg13	10.1

- **Monitored the execution of malicious commands:**



Not secure
https://192.168.149.82/app/threat-hunting#/overview/?tab=general&tabView=events&agentId=001&_a=(filters:!(),query:(language:kuery,query:''))&_g=(filters:!(),refreshInterval:(pause:!t,valu...
All Bookmarks
W.
Threat Hunting
Agent-ubuntu
a
Count
timestamp
Export Formatted
635 available fields
Columns
Density
1 fields sorted
Full scree
View surrounding documents
View single document
Activate Windows
Go to Settings to activate Windows.

388

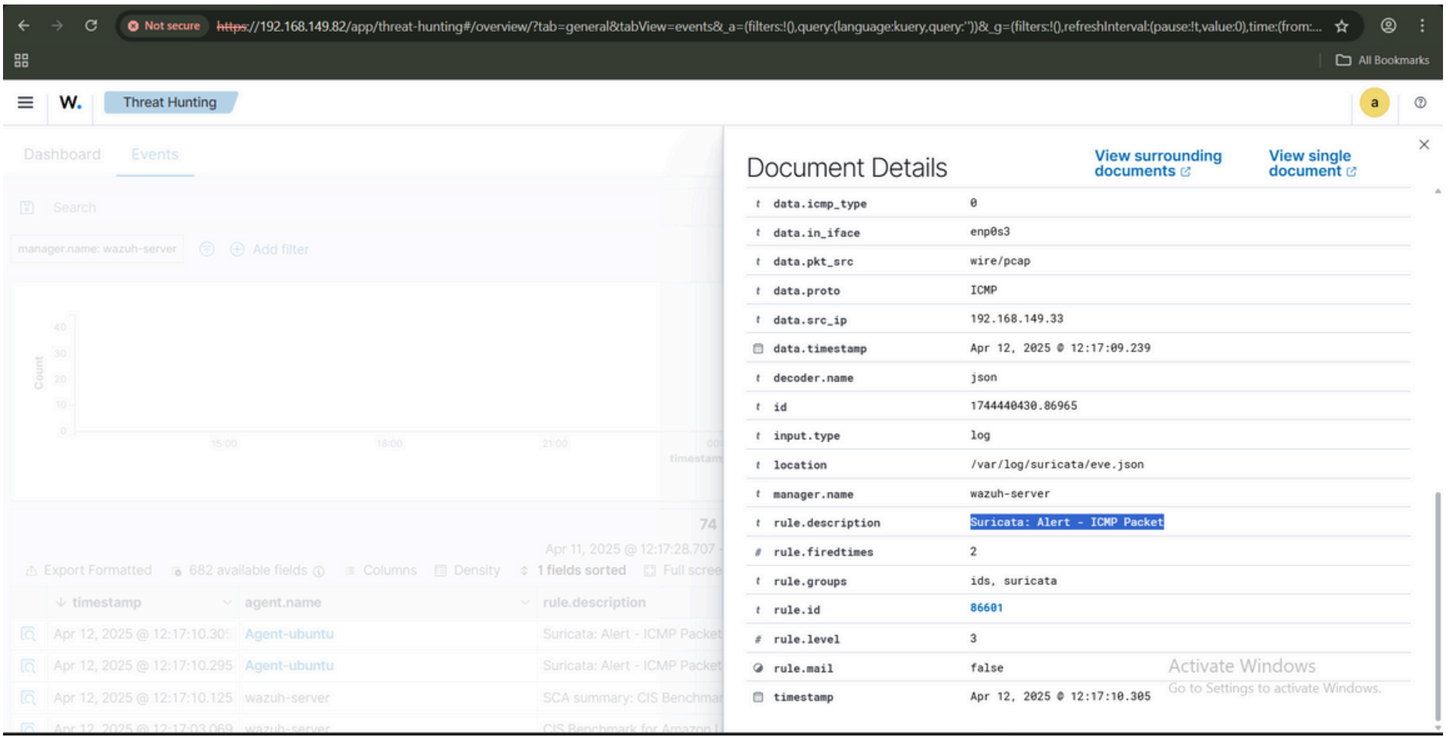
Apr 10, 2025 @ 11:05:06.143

timestamp	agent.name	rule.description
Apr 11, 2025 @ 11:04:30.473	Agent-ubuntu	Audit: Highly Suspicious Com
Apr 11, 2025 @ 11:03:53.662	Agent-ubuntu	Audit: Command: /snap/snap
Apr 11, 2025 @ 11:03:53.658	Agent-ubuntu	Audit: Command: /usr/bin/da
Apr 11, 2025 @ 11:03:53.658	Agent-ubuntu	Audit: Command: /usr/bin/sna
Apr 11, 2025 @ 11:03:49.748	Agent-ubuntu	Audit: Command: /usr/bin/rm
Apr 11, 2025 @ 11:03:49.746	Agent-ubuntu	Audit: Command: /usr/bin/ch
Apr 11, 2025 @ 11:03:49.725	Agent-ubuntu	Audit: Command: /usr/bin/mv
Apr 11, 2025 @ 11:02:19.930	Agent-ubuntu	Audit: Command: /usr/bin/dp
Apr 11, 2025 @ 11:02:19.930	Agent-ubuntu	Audit: Command: /usr/bin/dp

Document Details

data.audit.uid	0
decoder.name	auditd
decoder.parent	auditd
full_log	d=0 rdev=00:00 nametype=NORMAL cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0OUID="root" OGID="root" type=PATH msg=audit(1744349670.184:906): item=1 name="/lib64/ld-linux-x86-64.so.2" inode=1338293 dev=08:03 mode=0100755 ouid=0 ogid=0 rdev=00:00 nametype=NORMAL cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0OUID="root" OGID="root" type=PROCTITLE msg=audit(1744349670.184:906): proctitle=6E63002D76
id	1744349670.346473
input.type	log
location	/var/log/audit/audit.log
manager.name	wazuh-server
rule.description	Audit: Highly Suspicious Command executed: /usr/bin/nc
rule.firedtimes	1
rule.groups	auditaudit_command
rule.id	100210
rule.level	12
rule.mail	true
timestamp	Apr 11, 2025 @ 11:04:30.473

- **<u>Integrated Suricata IDS & Detected An Anamoly:</u>**



Not secure
https://192.168.149.82/app/threat-hunting#/overview/?tab=general&tabView=events&_a=(filters:!(),query:(language:kuery,query:''))&_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:...
All Bookmarks
W.
Threat Hunting
a
Dashboard
Events
Search
manager.name: wazuh-server
Add filter
Count
timestamp
Export Formatted
682 available fields
Columns
Density
1 fields sorted
Full scree
View surrounding documents
View single document
Activate Windows
Go to Settings to activate Windows.

74

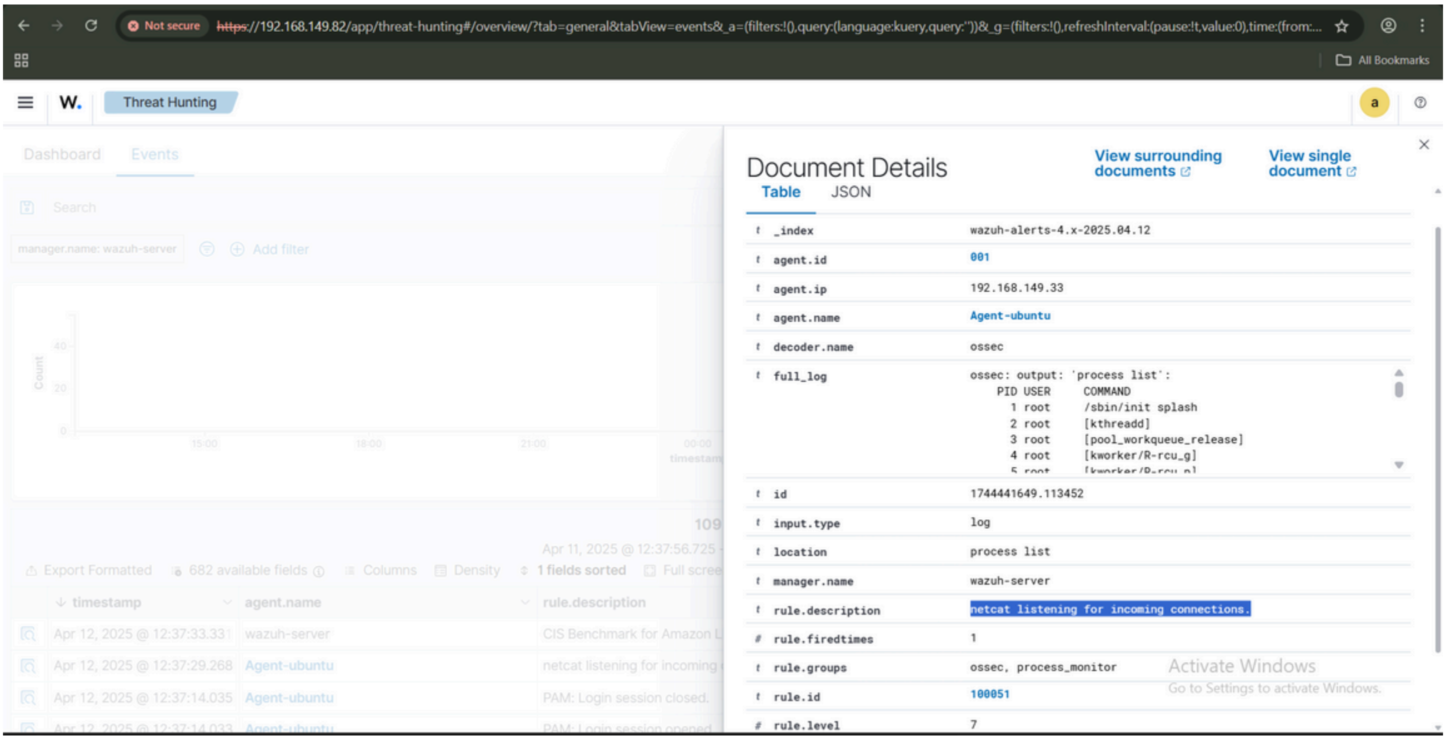
Apr 11, 2025 @ 12:17:28.707

timestamp	agent.name	rule.description
Apr 12, 2025 @ 12:17:10.305	Agent-ubuntu	Suricata: Alert - ICMP Packet
Apr 12, 2025 @ 12:17:10.295	Agent-ubuntu	Suricata: Alert - ICMP Packet
Apr 12, 2025 @ 12:17:10.125	wazuh-server	SCA summary: CIS Benchmar
Apr 12, 2025 @ 12:17:03.069	wazuh-server	CIS Benchmark for Amazon L

Document Details

data.icmp_type	0
data.in_iface	enp0s3
data.pkt_src	wire/pcap
data.proto	ICMP
data.src_ip	192.168.149.33
data.timestamp	Apr 12, 2025 @ 12:17:09.239
decoder.name	json
id	1744440430.86965
input.type	log
location	/var/log/suricata/eve.json
manager.name	wazuh-server
rule.description	Suricata: Alert - ICMP Packet
rule.firedtimes	2
rule.groups	ids, suricata
rule.id	86601
rule.level	3
rule.mail	false
timestamp	Apr 12, 2025 @ 12:17:10.305

- **<u>Detected Unauthorised Process:</u>**

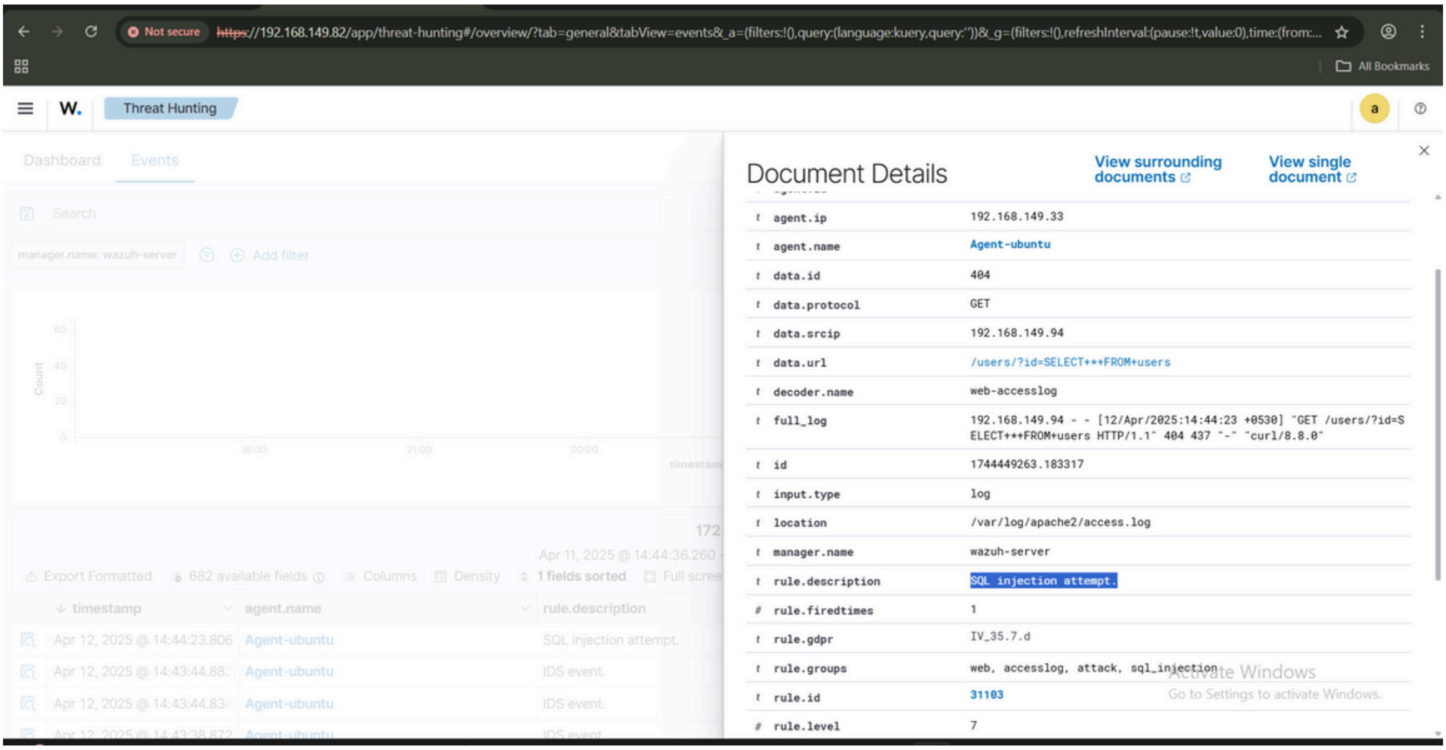


https://192.168.149.82/app/threat-hunting#/overview/?tab=general&tabView=events&_a=(filters:!(),query:(language:kuery,query:''))&_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:...

Document Details

_index	wazuh-alerts-4.x-2025.04.12
agent.id	001
agent.ip	192.168.149.33
agent.name	Agent-ubuntu
decoder.name	ossec
full_log	ossec: output: 'process list': PID USER COMMAND 1 root /sbin/init splash 2 root [kthreadd] 3 root [pool_workqueue_release] 4 root [kworker/R-rcu_g] 5 root [kworker/R-rcu_p]
id	1744441649.113452
input.type	log
location	process list
manager.name	wazuh-server
rule.description	netcat listening for incoming connections.
rule.firedtimes	1
rule.groups	ossec, process_monitor
rule.id	100051
rule.level	7

- **Detected SQL injection :**

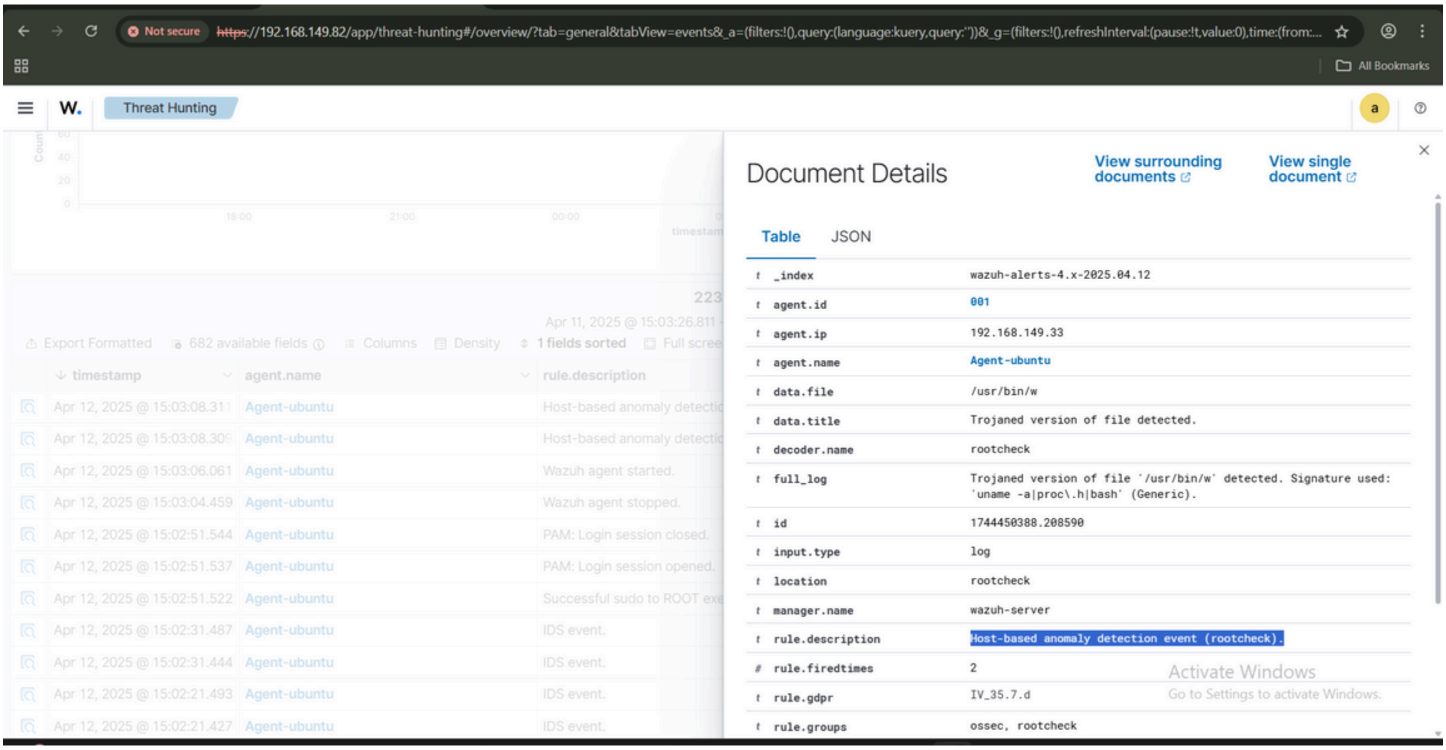


https://192.168.149.82/app/threat-hunting#/overview/?tab=general&tabView=events&_a=(filters:!(),query:(language:kuery,query:''))&_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:...

Document Details

agent.ip	192.168.149.33
agent.name	Agent-ubuntu
data.id	404
data.protocol	GET
data.srcip	192.168.149.94
data.url	/users/?id=SELECT+*+FROM+users
decoder.name	web-accesslog
full_log	192.168.149.94 - - [12/Apr/2025:14:44:23 +0530] "GET /users/?id=SELECT+*+FROM+users HTTP/1.1" 404 437 "-" "curl/8.8.0"
id	1744449263.183317
input.type	log
location	/var/log/apache2/access.log
manager.name	wazuh-server
rule.description	SQL injection attempt.
rule.firedtimes	1
rule.gdpr	IV_35.7.d
rule.groups	web, accesslog, attack, sql_injection
rule.id	31103
rule.level	7

- **Detected Suspicious Binaries :**



~~https~~://192.168.149.82/app/threat-hunting#/overview/?tab=general&tabView=events&_a=(filters:!(),query:(language:kuery,query:''))&_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:...

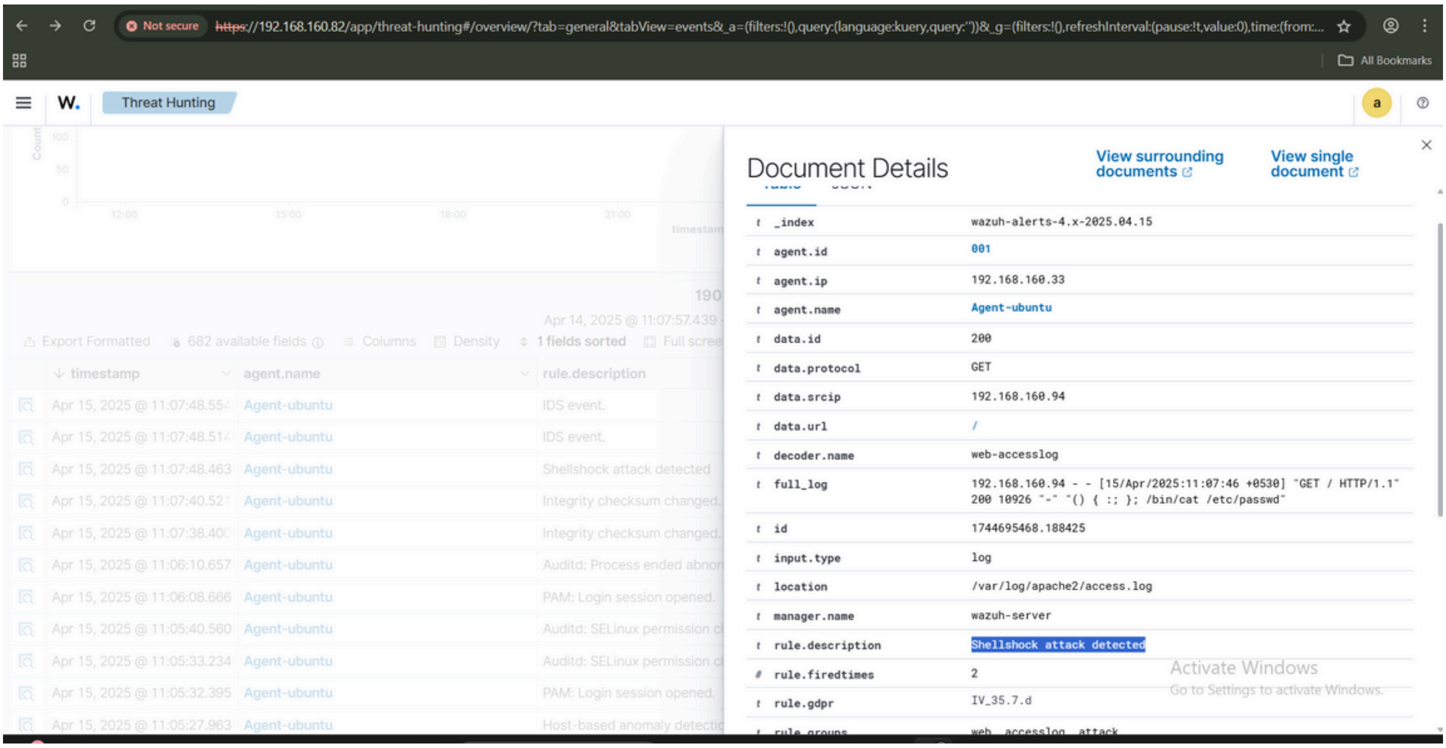
timestamp	agent.name	rule.description
Apr 12, 2025 @ 15:03:08.31	Agent-ubuntu	Host-based anomaly detectio
Apr 12, 2025 @ 15:03:08.309	Agent-ubuntu	Host-based anomaly detectio
Apr 12, 2025 @ 15:03:06.061	Agent-ubuntu	Wazuh agent started.
Apr 12, 2025 @ 15:03:04.459	Agent-ubuntu	Wazuh agent stopped.
Apr 12, 2025 @ 15:02:51.544	Agent-ubuntu	PAM: Login session closed.
Apr 12, 2025 @ 15:02:51.537	Agent-ubuntu	PAM: Login session opened.
Apr 12, 2025 @ 15:02:51.522	Agent-ubuntu	Successful sudo to ROOT exe
Apr 12, 2025 @ 15:02:31.487	Agent-ubuntu	IDS event.
Apr 12, 2025 @ 15:02:31.444	Agent-ubuntu	IDS event.
Apr 12, 2025 @ 15:02:21.493	Agent-ubuntu	IDS event.
Apr 12, 2025 @ 15:02:21.427	Agent-ubuntu	IDS event.

Document Details

View surrounding documents
View single document
Table
JSON
Activate Windows
Go to Settings to activate Windows.

t	_index	wazuh-alerts-4.x-2025.04.12
t	agent.id	001
t	agent.ip	192.168.149.33
t	agent.name	Agent-ubuntu
t	data.file	/usr/bin/w
t	data.title	Trojaned version of file detected.
t	decoder.name	rootcheck
t	full_log	Trojaned version of file '/usr/bin/w' detected. Signature used: 'uname -a|proc\.h|bash' (Generic).
t	id	1744450388.208590
t	input.type	log
t	location	rootcheck
t	manager.name	wazuh-server
t	rule.description	Host-based anomaly detection event (rootcheck).
#	rule.firedtimes	2
t	rule.gdpr	IV_35.7.d
t	rule.groups	ossec, rootcheck

- **Detected A Shellshock Attack :**



~~https~~://192.168.160.82/app/threat-hunting#/overview/?tab=general&tabView=events&_a=(filters:!(),query:(language:kuery,query:''))&_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:...

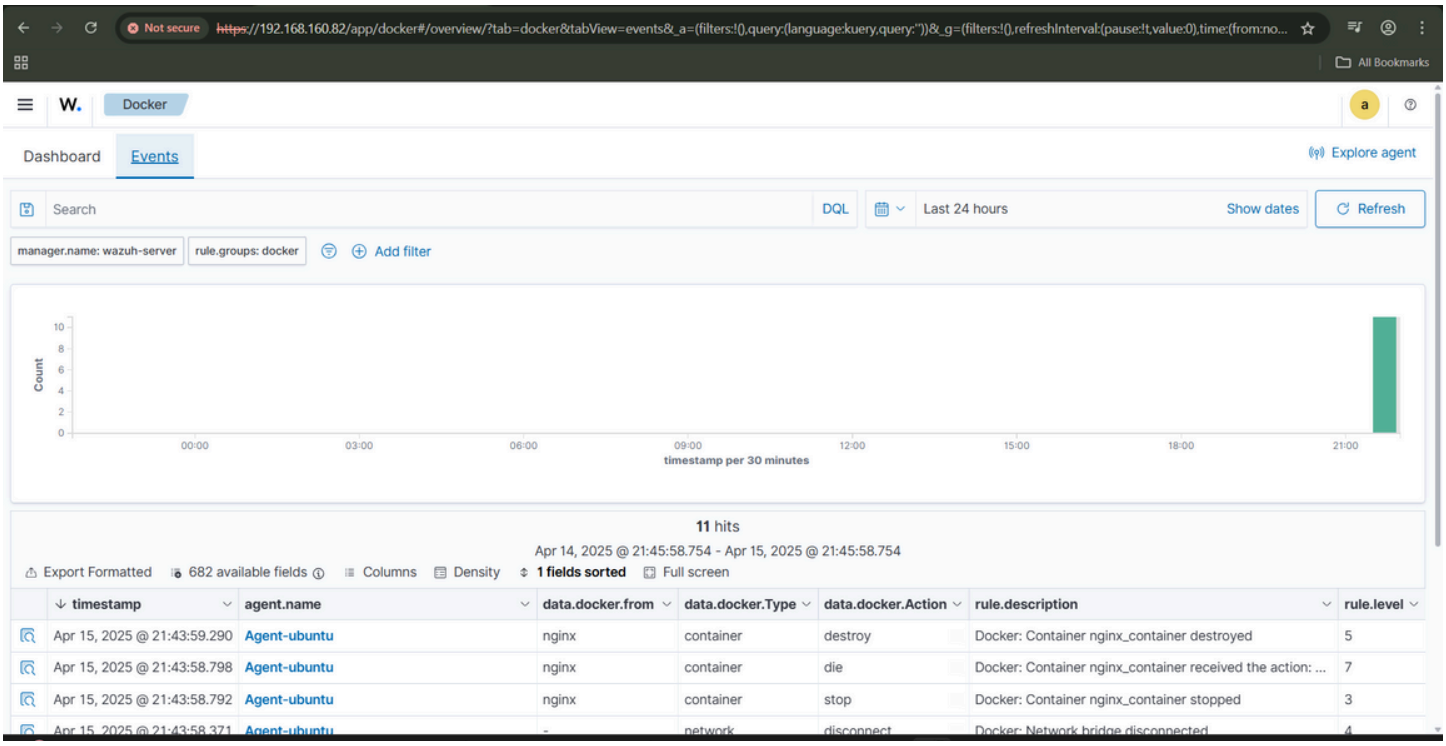
timestamp	agent.name	rule.description
Apr 15, 2025 @ 11:07:48.55	Agent-ubuntu	IDS event.
Apr 15, 2025 @ 11:07:48.51	Agent-ubuntu	IDS event.
Apr 15, 2025 @ 11:07:48.463	Agent-ubuntu	Shellshock attack detected
Apr 15, 2025 @ 11:07:40.52	Agent-ubuntu	Integrity checksum changed.
Apr 15, 2025 @ 11:07:38.40	Agent-ubuntu	Integrity checksum changed.
Apr 15, 2025 @ 11:06:10.657	Agent-ubuntu	Auditd: Process ended abnor
Apr 15, 2025 @ 11:06:08.666	Agent-ubuntu	PAM: Login session opened.
Apr 15, 2025 @ 11:05:40.560	Agent-ubuntu	Auditd: SELinux permission c
Apr 15, 2025 @ 11:05:33.234	Agent-ubuntu	Auditd: SELinux permission c
Apr 15, 2025 @ 11:05:32.395	Agent-ubuntu	PAM: Login session opened.
Apr 15, 2025 @ 11:05:27.963	Agent-ubuntu	Host-based anomaly detectio

Document Details

View surrounding documents
View single document
Activate Windows
Go to Settings to activate Windows.

t	_index	wazuh-alerts-4.x-2025.04.15
t	agent.id	001
t	agent.ip	192.168.160.33
t	agent.name	Agent-ubuntu
t	data.id	200
t	data.protocol	GET
t	data.srcip	192.168.160.94
t	data.url	/
t	decoder.name	web-accesslog
t	full_log	192.168.160.94 - - [15/Apr/2025:11:07:46 +0530] "GET / HTTP/1.1" 200 10926 "-" "() { :; }; /bin/cat /etc/passwd"
t	id	1744695468.188425
t	input.type	log
t	location	/var/log/apache2/access.log
t	manager.name	wazuh-server
t	rule.description	Shellshock attack detected
#	rule.firedtimes	2
t	rule.gdpr	IV_35.7.d
t	rule.groups	web, accesslog, attack

- **Monitored Docker Events :**

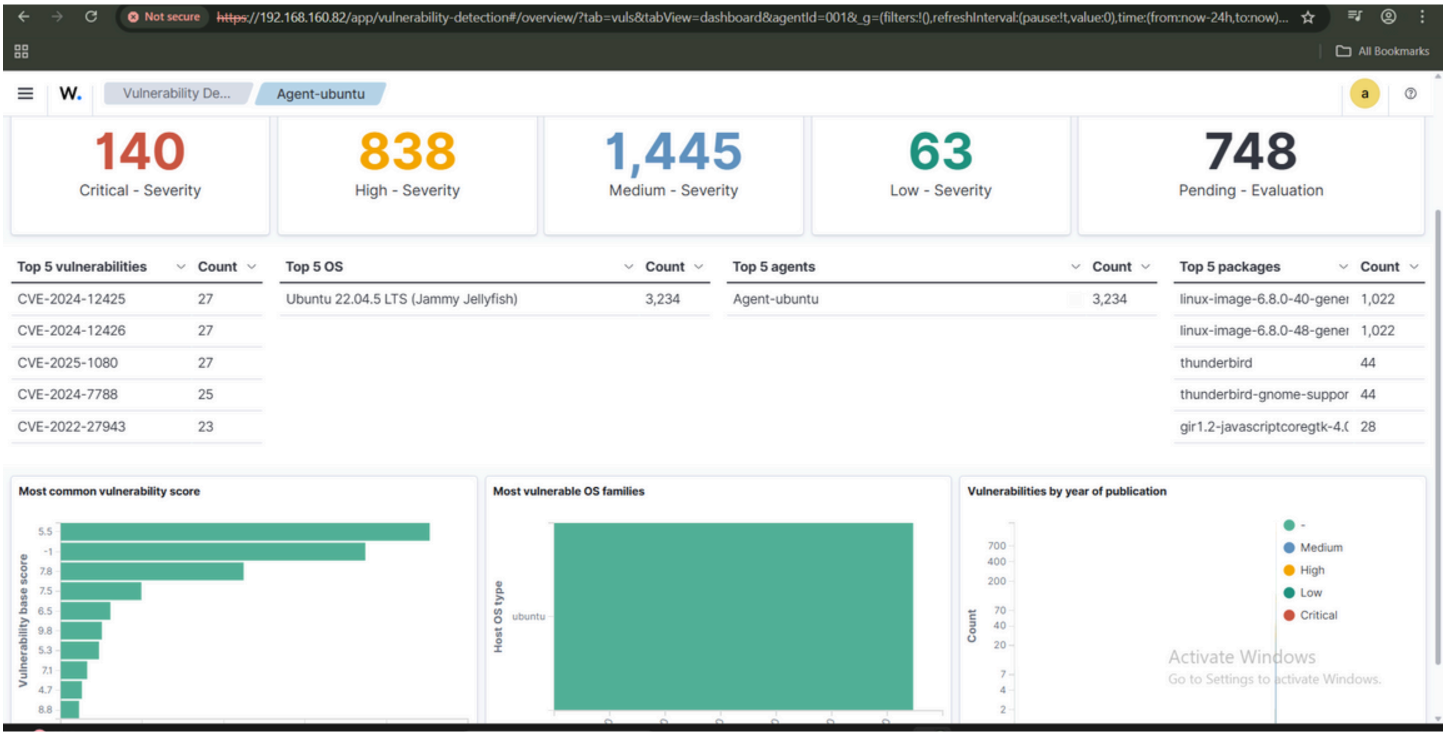


11 hits

Apr 14, 2025 @ 21:45:58.754 - Apr 15, 2025 @ 21:45:58.754

timestamp	agent.name	data.docker.from	data.docker.Type	data.docker.Action	rule.description	rule.level
Apr 15, 2025 @ 21:43:59.290	Agent-ubuntu	nginx	container	destroy	Docker: Container nginx_container destroyed	5
Apr 15, 2025 @ 21:43:58.798	Agent-ubuntu	nginx	container	die	Docker: Container nginx_container received the action: ...	7
Apr 15, 2025 @ 21:43:58.792	Agent-ubuntu	nginx	container	stop	Docker: Container nginx_container stopped	3
Apr 15, 2025 @ 21:43:58.371	Agent-ubuntu	-	network	disconnect	Docker: Network bridge disconnected	4

- **Vulnerability Detection :**


Not secure
~~https~~://192.168.160.82/app/vulnerability-detection#/overview/?tab=vuls&tabView=dashboard&agentId=001&_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,to:now))...
All Bookmarks
W.
Vulnerability De...
Agent-ubuntu
a
Most common vulnerability score
Vulnerability base score
5.5
-1
7.8
7.5
6.5
9.8
5.3
7.1
4.7
8.8
Most vulnerable OS families
Host OS type
ubuntu
Vulnerabilities by year of publication
Count
700
400
200
70
40
20
7
4
2
-
Medium
High
Low
Critical
Activate Windows
Go to Settings to activate Windows.

140	838	1,445	63	748
Critical - Severity	High - Severity	Medium - Severity	Low - Severity	Pending - Evaluation

Top 5 vulnerabilities	Count
CVE-2024-12425	27
CVE-2024-12426	27
CVE-2025-1080	27
CVE-2024-7788	25
CVE-2022-27943	23

Top 5 OS	Count
Ubuntu 22.04.5 LTS (Jammy Jellyfish)	3,234

Top 5 agents	Count
Agent-ubuntu	3,234

Top 5 packages	Count
linux-image-6.8.0-40-gener	1,022
linux-image-6.8.0-48-gener	1,022
thunderbird	44
thunderbird-gnome-suppor	44
gir1.2-javascriptcoregtk-4.(	28