A structured classification system was developed to map SOC alerts to MITRE ATT&CK techniques and assign priority based on associated risk. This was implemented conceptually using a Google Sheets model that included:

Alert ID	Alert Type	Priority	MITRE Tactic (ID)
001	Phishing Email	High	T1566

Purpose

The goal of this exercise was to:

Standardize alert interpretation

Associate events with real adversary behavior

Increase SOC efficiency by separating critical alerts from low-risk noise

Outcome & Learning

This classification process highlighted the value of using MITRE ATT&CK for:

attribution of techniques

behavioral mapping

understanding adversary methodology

For example:
T1566 maps to phishing activity, helping quickly identify the technique used.

This reinforced the importance of connecting logs to adversary tactics instead of treating alerts in isolation.
Incident Ticket Creation
Activity Performed

A mock incident ticket was drafted in TheHive with realistic SOC data.

Title: [Critical] Ransomware Detected on Server-X
Description: Indicators observed:
• File: crypto_locker.exe
• Source IP: 192.168.1.50

Alert Prioritization Exercise
Activity Performed

Alert scenarios were simulated and assigned priority levels using CVSS scoring.

Examples:

“Log4Shell Exploit Detected”

CVSS Score: 9.8

Classification: Critical

“Port Scan Detected”

CVSS Score: 3.7

Classification: Low

Dashboard Visualization
Activity Performed

An alert-priority visualization dashboard was built in Wazuh to display the distribution of alert types.

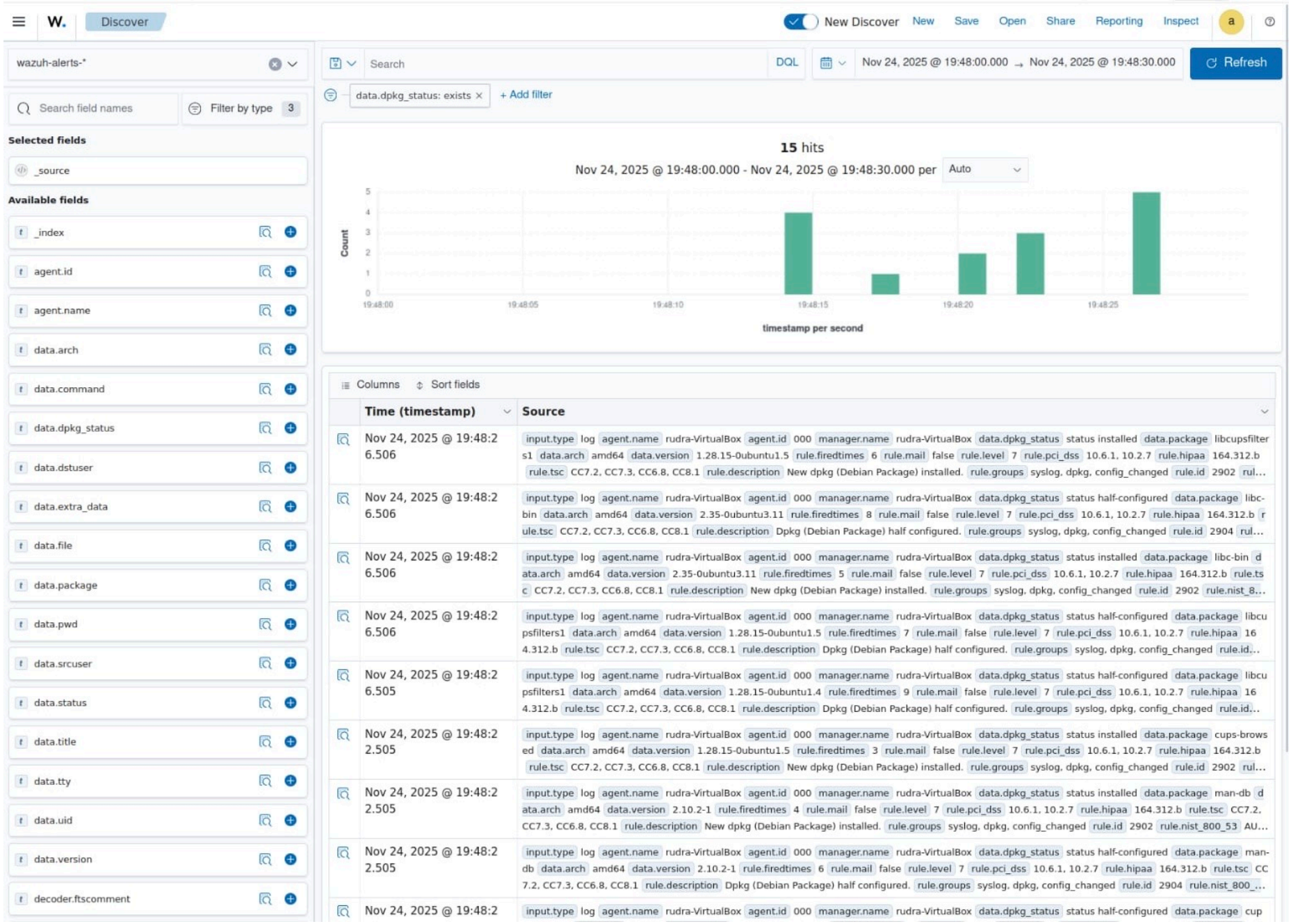
Example visual concept:

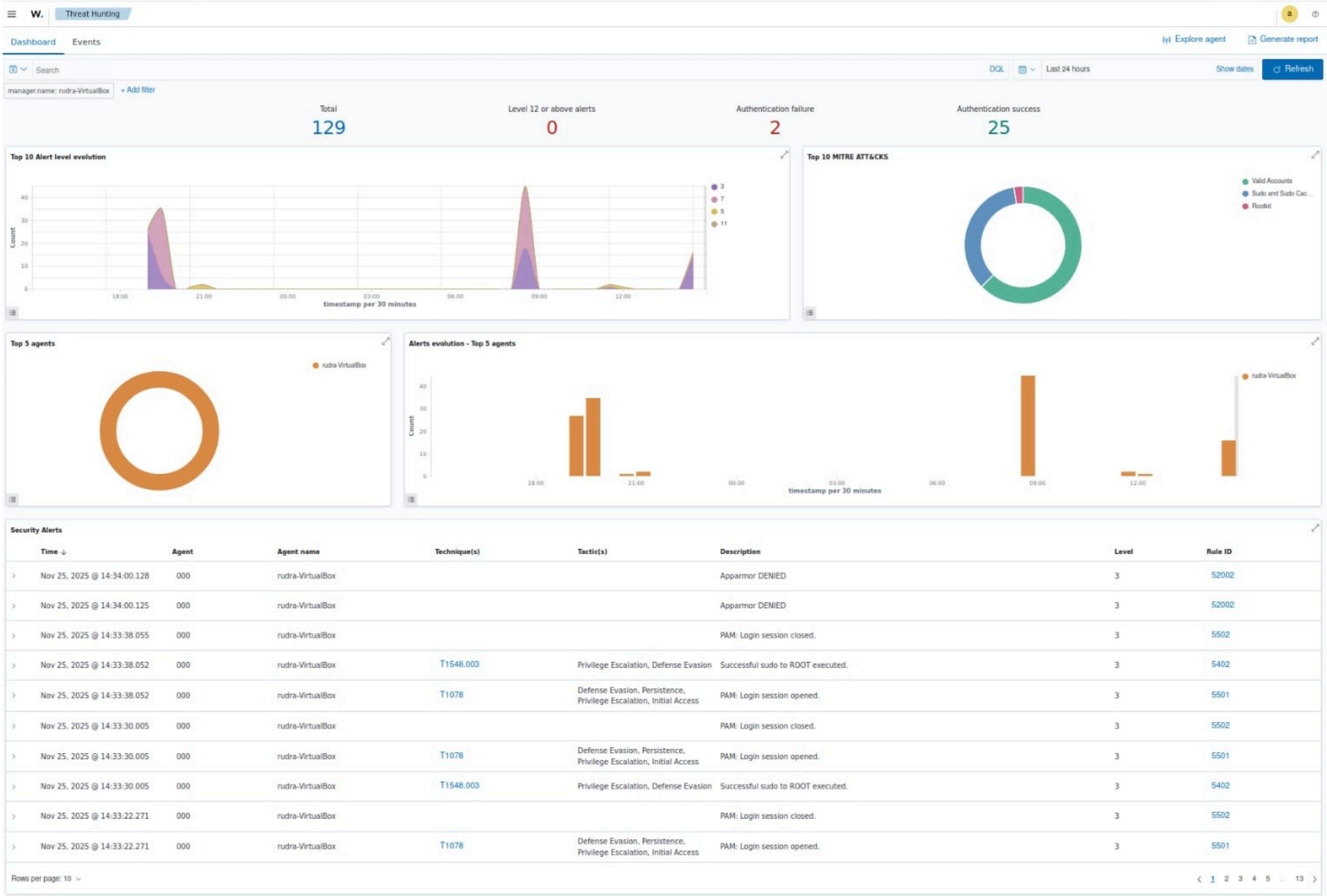
Critical = Red

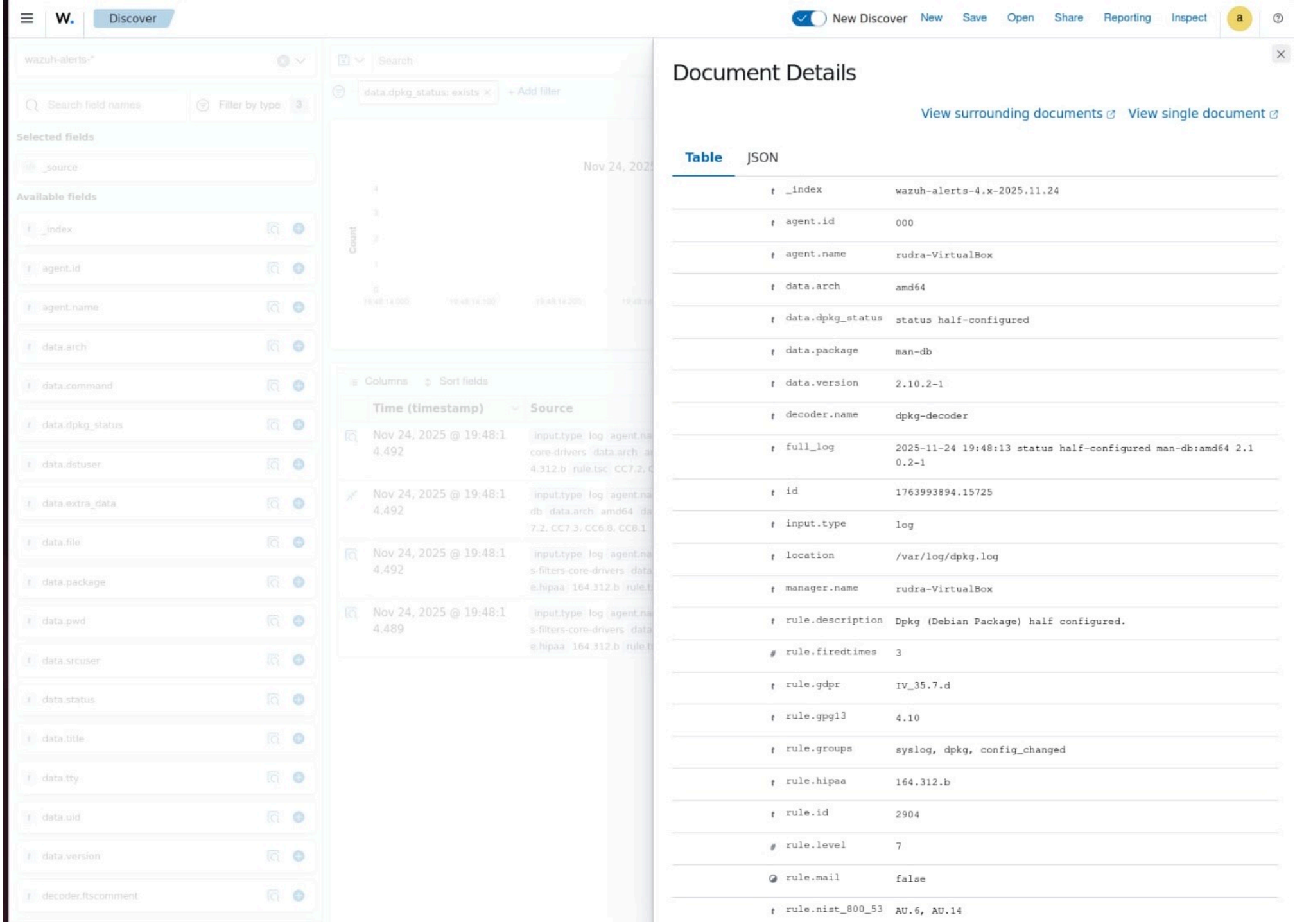
High = Orange

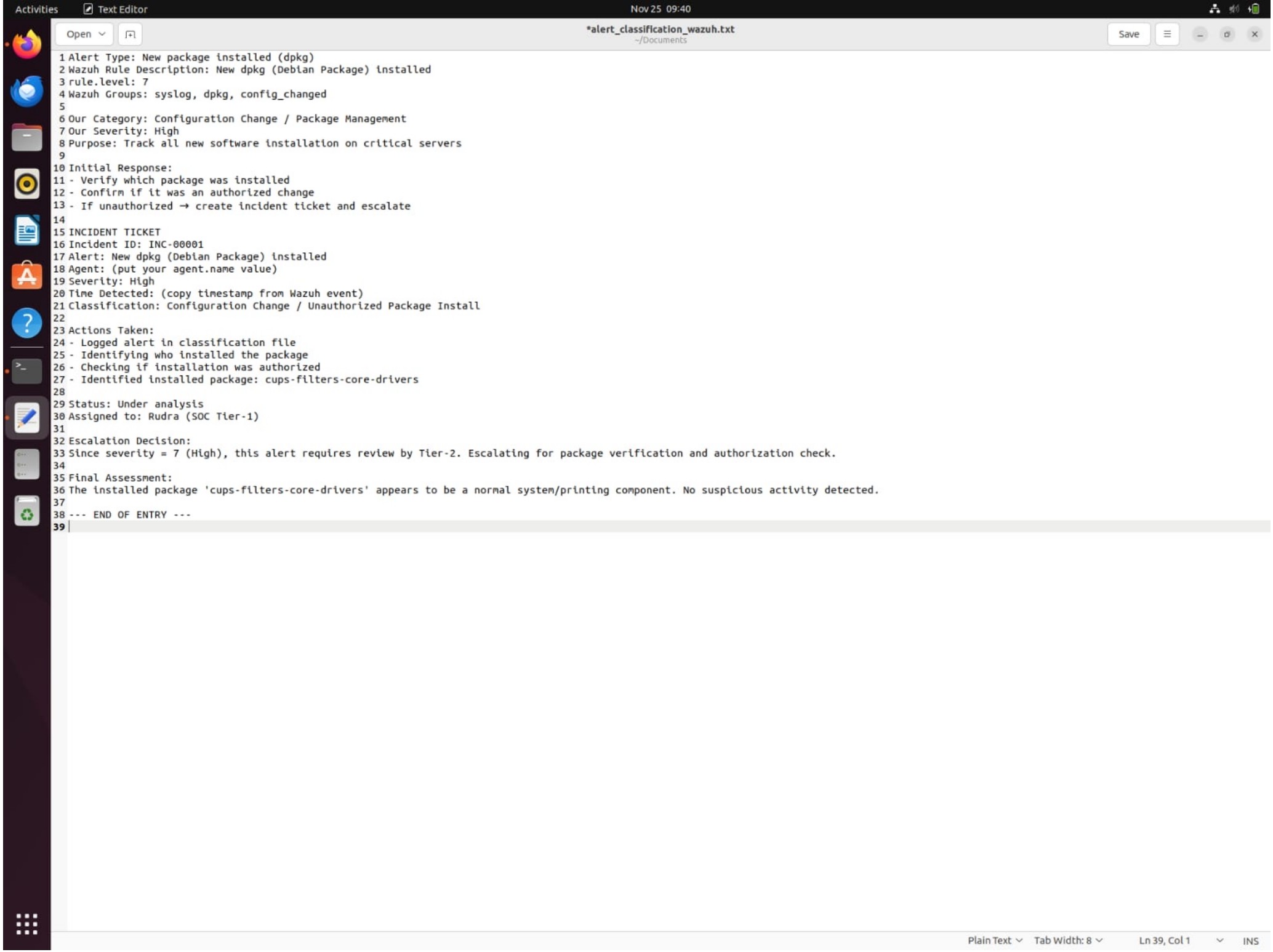
Medium = Yellow

Low = Blue


Discover
New Discover
New
Save
Open
Share
Reporting
Inspect
wazuh-alerts-*
Search
DQL
Nov 24, 2025 @ 19:48:00.000 → Nov 24, 2025 @ 19:48:30.000
Refresh
data.dpkg_status: exists
+ Add filter
Search field names
Filter by type 3
Selected fields
_source
Available fields
_index
agent.id
agent.name
data.arch
data.command
data.dpkg_status
data.dstuser
data.extra_data
data.file
data.package
data.pwd
data.srcuser
data.status
data.title
data.tty
data.uid
data.version
decoder.ftscomment
15 hits
Nov 24, 2025 @ 19:48:00.000 - Nov 24, 2025 @ 19:48:30.000 per Auto
Count
timestamp per second
Columns
Sort fields
Time (timestamp)
Source
Nov 24, 2025 @ 19:48:26.506
input.type log agent.name rudra-VirtualBox agent.id 000 manager.name rudra-VirtualBox data.dpkg_status status installed data.package libcupsfilters1 data.arch amd64 data.version 1.28.15-0ubuntu1.5 rule.firedtimes 6 rule.mail false rule.level 7 rule.pci_dss 10.6.1, 10.2.7 rule.hipaa 164.312.b rule.tsc CC7.2, CC7.3, CC6.8, CC8.1 rule.description New dpkg (Debian Package) installed. rule.groups syslog, dpkg, config_changed rule.id 2902 rul...
Nov 24, 2025 @ 19:48:26.506
input.type log agent.name rudra-VirtualBox agent.id 000 manager.name rudra-VirtualBox data.dpkg_status status half-configured data.package libc-bin data.arch amd64 data.version 2.35-0ubuntu3.11 rule.firedtimes 8 rule.mail false rule.level 7 rule.pci_dss 10.6.1, 10.2.7 rule.hipaa 164.312.b rule.tsc CC7.2, CC7.3, CC6.8, CC8.1 rule.description Dpkg (Debian Package) half configured. rule.groups syslog, dpkg, config_changed rule.id 2904 rul...
Nov 24, 2025 @ 19:48:26.506
input.type log agent.name rudra-VirtualBox agent.id 000 manager.name rudra-VirtualBox data.dpkg_status status installed data.package libc-bin data.arch amd64 data.version 2.35-0ubuntu3.11 rule.firedtimes 5 rule.mail false rule.level 7 rule.pci_dss 10.6.1, 10.2.7 rule.hipaa 164.312.b rule.tsc CC7.2, CC7.3, CC6.8, CC8.1 rule.description New dpkg (Debian Package) installed. rule.groups syslog, dpkg, config_changed rule.id 2902 rule.nist_8...
Nov 24, 2025 @ 19:48:26.506
input.type log agent.name rudra-VirtualBox agent.id 000 manager.name rudra-VirtualBox data.dpkg_status status half-configured data.package libcupsfilters1 data.arch amd64 data.version 1.28.15-0ubuntu1.5 rule.firedtimes 7 rule.mail false rule.level 7 rule.pci_dss 10.6.1, 10.2.7 rule.hipaa 164.312.b rule.tsc CC7.2, CC7.3, CC6.8, CC8.1 rule.description Dpkg (Debian Package) half configured. rule.groups syslog, dpkg, config_changed rule.id...
Nov 24, 2025 @ 19:48:26.505
input.type log agent.name rudra-VirtualBox agent.id 000 manager.name rudra-VirtualBox data.dpkg_status status half-configured data.package libcupsfilters1 data.arch amd64 data.version 1.28.15-0ubuntu1.4 rule.firedtimes 9 rule.mail false rule.level 7 rule.pci_dss 10.6.1, 10.2.7 rule.hipaa 164.312.b rule.tsc CC7.2, CC7.3, CC6.8, CC8.1 rule.description Dpkg (Debian Package) half configured. rule.groups syslog, dpkg, config_changed rule.id...
Nov 24, 2025 @ 19:48:22.505
input.type log agent.name rudra-VirtualBox agent.id 000 manager.name rudra-VirtualBox data.dpkg_status status installed data.package cups-browsed data.arch amd64 data.version 1.28.15-0ubuntu1.5 rule.firedtimes 3 rule.mail false rule.level 7 rule.pci_dss 10.6.1, 10.2.7 rule.hipaa 164.312.b rule.tsc CC7.2, CC7.3, CC6.8, CC8.1 rule.description New dpkg (Debian Package) installed. rule.groups syslog, dpkg, config_changed rule.id 2902 rul...
Nov 24, 2025 @ 19:48:22.505
input.type log agent.name rudra-VirtualBox agent.id 000 manager.name rudra-VirtualBox data.dpkg_status status installed data.package man-db data.arch amd64 data.version 2.10.2-1 rule.firedtimes 4 rule.mail false rule.level 7 rule.pci_dss 10.6.1, 10.2.7 rule.hipaa 164.312.b rule.tsc CC7.2, CC7.3, CC6.8, CC8.1 rule.description New dpkg (Debian Package) installed. rule.groups syslog, dpkg, config_changed rule.id 2902 rule.nist_800_53 AU...
Nov 24, 2025 @ 19:48:22.505
input.type log agent.name rudra-VirtualBox agent.id 000 manager.name rudra-VirtualBox data.dpkg_status status half-configured data.package man-db data.arch amd64 data.version 2.10.2-1 rule.firedtimes 6 rule.mail false rule.level 7 rule.pci_dss 10.6.1, 10.2.7 rule.hipaa 164.312.b rule.tsc CC7.2, CC7.3, CC6.8, CC8.1 rule.description Dpkg (Debian Package) half configured. rule.groups syslog, dpkg, config_changed rule.id 2904 rule.nist_800_...
Nov 24, 2025 @ 19:48:2
input.type log agent.name rudra-VirtualBox agent.id 000 manager.name rudra-VirtualBox data.dpkg_status status half-configured data.package cup


Threat Hunting
Dashboard
Events
Explore agent
Generate report
Search
DQL
Last 24 hours
Show dates
Refresh
manager.name: rudra-VirtualBox
+ Add filter
Total
129
Level 12 or above alerts
0
Authentication failure
2
Authentication success
25
Top 10 Alert level evolution
Count
timestamp per 30 minutes
3
7
5
11
Top 10 MITRE ATT&CKS
Valid Accounts
Sudo and Sudo Cac...
Rootkit
Top 5 agents
rudra-VirtualBox
Alerts evolution - Top 5 agents
Count
timestamp per 30 minutes
rudra-VirtualBox
Security Alerts
Time
Agent
Agent name
Technique(s)
Tactic(s)
Description
Level
Rule ID
Nov 25, 2025 @ 14:34:00.128 000 rudra-VirtualBox Apparmor DENIED 3 52002
Nov 25, 2025 @ 14:34:00.125 000 rudra-VirtualBox Apparmor DENIED 3 52002
Nov 25, 2025 @ 14:33:38.055 000 rudra-VirtualBox PAM: Login session closed. 3 5502
Nov 25, 2025 @ 14:33:38.052 000 rudra-VirtualBox T1548.003 Privilege Escalation, Defense Evasion Successful sudo to ROOT executed. 3 5402
Nov 25, 2025 @ 14:33:38.052 000 rudra-VirtualBox T1078 Defense Evasion, Persistence, Privilege Escalation, Initial Access PAM: Login session opened. 3 5501
Nov 25, 2025 @ 14:33:30.005 000 rudra-VirtualBox PAM: Login session closed. 3 5502
Nov 25, 2025 @ 14:33:30.005 000 rudra-VirtualBox T1078 Defense Evasion, Persistence, Privilege Escalation, Initial Access PAM: Login session opened. 3 5501
Nov 25, 2025 @ 14:33:30.005 000 rudra-VirtualBox T1548.003 Privilege Escalation, Defense Evasion Successful sudo to ROOT executed. 3 5402
Nov 25, 2025 @ 14:33:22.271 000 rudra-VirtualBox PAM: Login session closed. 3 5502
Nov 25, 2025 @ 14:33:22.271 000 rudra-VirtualBox T1078 Defense Evasion, Persistence, Privilege Escalation, Initial Access PAM: Login session opened. 3 5501
Rows per page: 10
1 2 3 4 5 ... 13


Discover
New Discover
New
Save
Open
Share
Reporting
Inspect
wazuh-alerts-*
Search
data.dpkg_status: exists
+ Add filter
Search field names
Filter by type
Selected fields
_source
Available fields
Columns
Sort fields
Time (timestamp)
Source
Document Details
View surrounding documents
View single document
Table
JSON
_index wazuh-alerts-4.x-2025.11.24
agent.id 000
agent.name rudra-VirtualBox
data.arch amd64
data.dpkg_status status half-configured
data.package man-db
data.version 2.10.2-1
decoder.name dpkg-decoder
full_log 2025-11-24 19:48:13 status half-configured man-db:amd64 2.10.2-1
id 1763993894.15725
input.type log
location /var/log/dpkg.log
manager.name rudra-VirtualBox
rule.description Dpkg (Debian Package) half configured.
rule.firedtimes 3
rule.gdpr IV_35.7.d
rule.gpg13 4.10
rule.groups syslog, dpkg, config_changed
rule.hipaa 164.312.b
rule.id 2904
rule.level 7
rule.mail false
rule.nist_800_53 AU.6, AU.14


Activities
Text Editor
Nov 25 09:40
Open
*alert_classification_wazuh.txt
~/Documents
Save
1 Alert Type: New package installed (dpkg)
2 Wazuh Rule Description: New dpkg (Debian Package) installed
3 rule.level: 7
4 Wazuh Groups: syslog, dpkg, config_changed
5
6 Our Category: Configuration Change / Package Management
7 Our Severity: High
8 Purpose: Track all new software installation on critical servers
9
10 Initial Response:
11 - Verify which package was installed
12 - Confirm if it was an authorized change
13 - If unauthorized → create incident ticket and escalate
14
15 INCIDENT TICKET
16 Incident ID: INC-00001
17 Alert: New dpkg (Debian Package) installed
18 Agent: (put your agent.name value)
19 Severity: High
20 Time Detected: (copy timestamp from Wazuh event)
21 Classification: Configuration Change / Unauthorized Package Install
22
23 Actions Taken:
24 - Logged alert in classification file
25 - Identifying who installed the package
26 - Checking if installation was authorized
27 - Identified installed package: cups-filters-core-drivers
28
29 Status: Under analysis
30 Assigned to: Rudra (SOC Tier-1)
31
32 Escalation Decision:
33 Since severity = 7 (High), this alert requires review by Tier-2. Escalating for package verification and authorization check.
34
35 Final Assessment:
36 The installed package 'cups-filters-core-drivers' appears to be a normal system/printing component. No suspicious activity detected.
37
38 --- END OF ENTRY ---
39
Plain Text
Tab Width: 8
Ln 39, Col 1
INS

L44

Alert ID	Type	Priority	MITRE Technique ID	MITRE Tactic	CVSS Scor	Final Priority Score
1	Phishing Email: Suspicious Link	High	T1566	Initial Access	7.4	High
2	Suspicious Attachment (Email)	High	T1566.001	Initial Access	8	High
3	Multiple Failed Logins	Medium	T1110	Credential Access	5.3	Medium
4	Successful Login from New Geo	High	T1078	Credential Access	7.1	High
5	Ransomware Activity Detected	Critical	T1486	Impact	9.1	Critical
6	PowerShell Download Command	High	T1059.001	Execution	7	High
7	Port Scan Detected	Low	T1046	Discovery	3.7	Low
8	Possible Data Exfiltration	Critical	T1041	Exfiltration	9	Critical
9	New Admin User Created	High	T1136.001	Persistence	6.8	Medium
10	Suspicious Outbound C2 Traffic	High	T1071	Command and Contro	8.2	High

Sheet1

1. Executive Summary
A phishing email campaign targeted internal users, resulting in several suspicious authentication attempts. No confirmed compromise occurred due to early detection and containment.

2. Timeline
- 14:00 — Phishing email received by mailbox
- 14:05 — User reports suspicious link
- 14:10 — IT alerted
- 14:15 — Affected accounts checked
- 14:30 — Endpoint isolated
- 15:00 — Memory dump collected
- 15:30 — Forensic review completed

3. Impact Analysis
- Users targeted: 3
- Accounts compromised: 0
- System downtime: None
- Data loss: None
- Risk level: Medium

4. Remediation Steps
- Blocked phishing sender domain
- Reset passwords of exposed accounts
- Enabled stricter email filtering
- Improved user awareness training

5. Lessons Learned
- Earlier user reporting significantly improved response time.
- Additional email filtering rules should be implemented.
- Users need further training to detect malicious links.

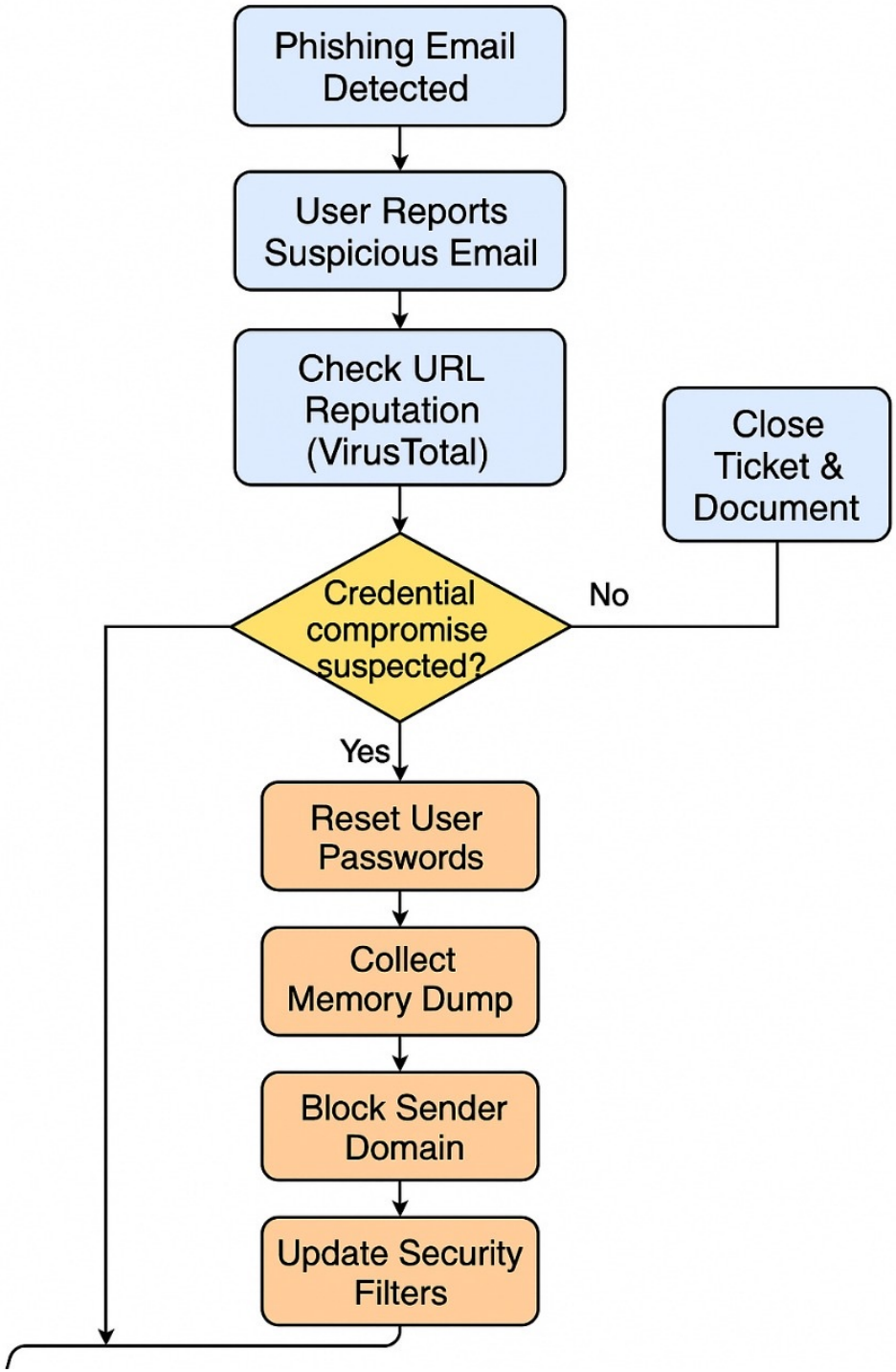
Investigation Log

Action	Timestamp
Isolated endpoint	2025-08-18 14:00:00
Collected memory dump	2025-08-18 14:30:00
Checked email headers	2025-08-18 14:35:00
Analyzed reputation of URL	2025-08-18

Phishing Response Checklist

- [ ] Confirm email headers
- [ ] Check link reputation (VirusTotal)
- [ ] Inspect sender domain
- [ ] Review other inbox recipients
- [ ] Identify affected users
- [ ] Reset credentials if necessary
- [ ] Block sender at email gateway
- [ ] Update SOC incident log

This phishing simulation showed that rapid user reporting and SOC monitoring prevented escalation. Key improvements include tighter email filters, faster endpoint isolation, and user training reinforcement. Strengthened password policies and MFA adoption will further reduce risk exposure and improve incident handling maturity.


Phishing Email Detected
User Reports Suspicious Email
Check URL Reputation (VirusTotal)
Credential compromise suspected?
No
Close Ticket & Document
Yes
Reset User Passwords
Collect Memory Dump
Block Sender Domain
Update Security Filters

Activity Performed

A simulated alert triage workflow was executed using Wazuh, handling a mock alert involving suspected brute-force SSH login activity. Tools including VirusTotal and AlienVault OTX were used to validate related indicators of compromise (IP / hash).

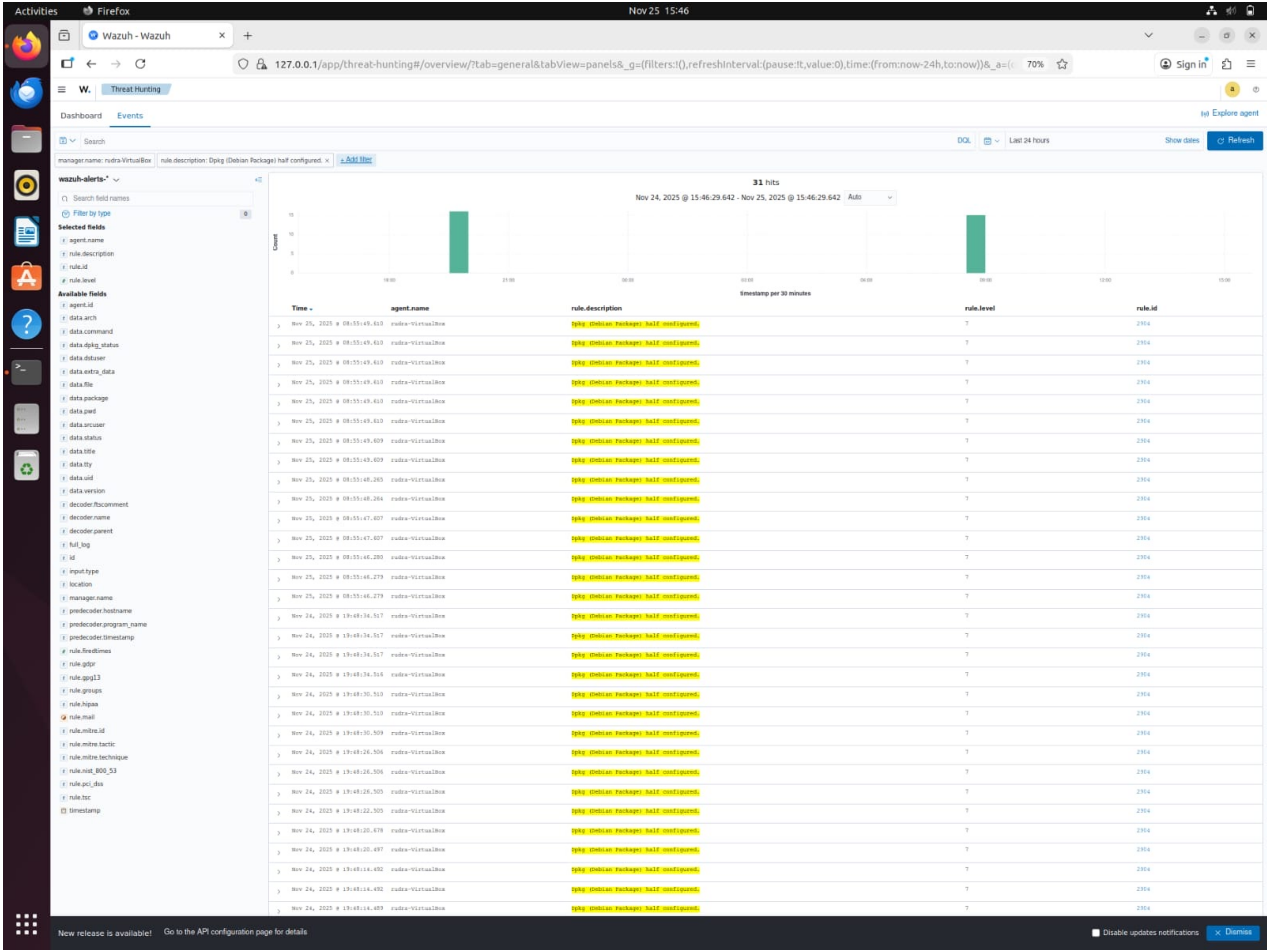
Observation & Initial Analysis

Alert indicates multiple failed SSH attempts from 192.168.1.100

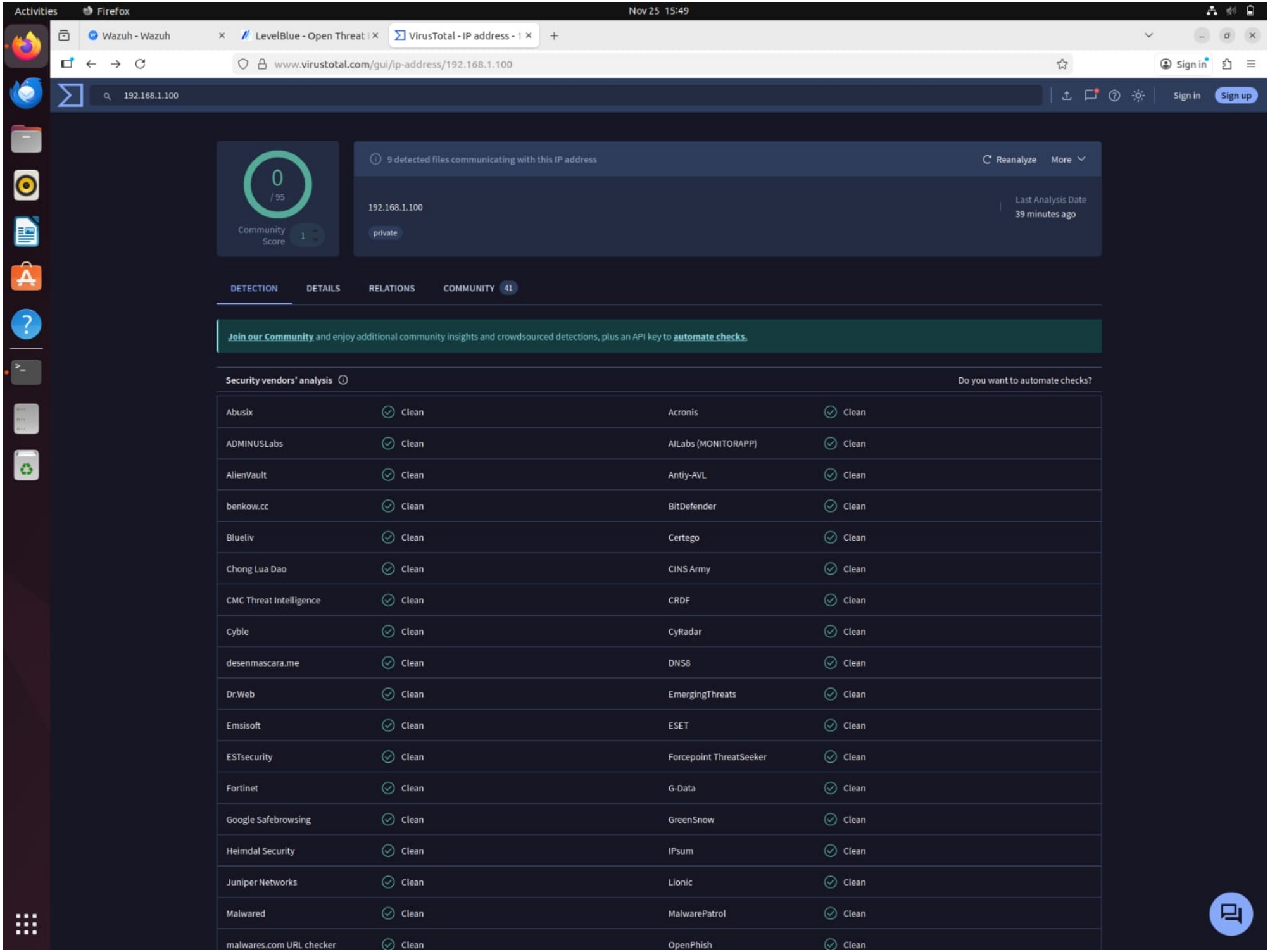
The frequency of failures suggests either mistyped credentials or automated attempt

Alert priority set to Medium, indicating risk but not immediate critical threat

Key question during triage:
“Is this a legitimate user error or malicious activity?”



Activities
Firefox
Nov 25 15:46
Wazuh - Wazuh
127.0.0.1/app/threat-hunting#/overview/?tab=general&tabView=panels&_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,to:now))&_a=(
70%
Sign in
Threat Hunting
Dashboard
Events
Explore agent
Search
DQL
Last 24 hours
Show dates
Refresh
manager.name: rudra-VirtualBox
rule.description: Dpkg (Debian Package) half configured.
+ Add filter
wazuh-alerts-*
Search field names
Filter by type
0
Selected fields
agent.name
rule.description
rule.id
rule.level
Available fields
agent.id
data.arch
data.command
data.dpkg_status
data.dstuser
data.extra_data
data.file
data.package
data.pwd
data.srcuser
data.status
data.title
data.tty
data.uid
data.version
decoder.ftscomment
decoder.name
decoder.parent
full_log
id
input.type
location
manager.name
predecoder.hostname
predecoder.program_name
predecoder.timestamp
rule.firedtimes
rule.gdpr
rule.gpg13
rule.groups
rule.hipaa
rule.mail
rule.mitre.id
rule.mitre.tactic
rule.mitre.technique
rule.nist_800_53
rule.pci_dss
rule.tsc
timestamp
31 hits
Nov 24, 2025 @ 15:46:29.642 - Nov 25, 2025 @ 15:46:29.642
Auto
Count
timestamp per 30 minutes
Time
agent.name
rule.description
rule.level
rule.id
Nov 25, 2025 @ 08:55:49.610 rudra-VirtualBox Dpkg (Debian Package) half configured. 7 2904
Nov 25, 2025 @ 08:55:49.610 rudra-VirtualBox Dpkg (Debian Package) half configured. 7 2904
Nov 25, 2025 @ 08:55:49.610 rudra-VirtualBox Dpkg (Debian Package) half configured. 7 2904
Nov 25, 2025 @ 08:55:49.610 rudra-VirtualBox Dpkg (Debian Package) half configured. 7 2904
Nov 25, 2025 @ 08:55:49.610 rudra-VirtualBox Dpkg (Debian Package) half configured. 7 2904
Nov 25, 2025 @ 08:55:49.610 rudra-VirtualBox Dpkg (Debian Package) half configured. 7 2904
Nov 25, 2025 @ 08:55:49.609 rudra-VirtualBox Dpkg (Debian Package) half configured. 7 2904
Nov 25, 2025 @ 08:55:49.609 rudra-VirtualBox Dpkg (Debian Package) half configured. 7 2904
Nov 25, 2025 @ 08:55:48.265 rudra-VirtualBox Dpkg (Debian Package) half configured. 7 2904
Nov 25, 2025 @ 08:55:48.264 rudra-VirtualBox Dpkg (Debian Package) half configured. 7 2904
Nov 25, 2025 @ 08:55:47.607 rudra-VirtualBox Dpkg (Debian Package) half configured. 7 2904
Nov 25, 2025 @ 08:55:47.607 rudra-VirtualBox Dpkg (Debian Package) half configured. 7 2904
Nov 25, 2025 @ 08:55:46.280 rudra-VirtualBox Dpkg (Debian Package) half configured. 7 2904
Nov 25, 2025 @ 08:55:46.279 rudra-VirtualBox Dpkg (Debian Package) half configured. 7 2904
Nov 25, 2025 @ 08:55:46.279 rudra-VirtualBox Dpkg (Debian Package) half configured. 7 2904
Nov 24, 2025 @ 19:48:34.517 rudra-VirtualBox Dpkg (Debian Package) half configured. 7 2904
Nov 24, 2025 @ 19:48:34.517 rudra-VirtualBox Dpkg (Debian Package) half configured. 7 2904
Nov 24, 2025 @ 19:48:34.517 rudra-VirtualBox Dpkg (Debian Package) half configured. 7 2904
Nov 24, 2025 @ 19:48:34.516 rudra-VirtualBox Dpkg (Debian Package) half configured. 7 2904
Nov 24, 2025 @ 19:48:30.510 rudra-VirtualBox Dpkg (Debian Package) half configured. 7 2904
Nov 24, 2025 @ 19:48:30.510 rudra-VirtualBox Dpkg (Debian Package) half configured. 7 2904
Nov 24, 2025 @ 19:48:30.509 rudra-VirtualBox Dpkg (Debian Package) half configured. 7 2904
Nov 24, 2025 @ 19:48:26.506 rudra-VirtualBox Dpkg (Debian Package) half configured. 7 2904
Nov 24, 2025 @ 19:48:26.506 rudra-VirtualBox Dpkg (Debian Package) half configured. 7 2904
Nov 24, 2025 @ 19:48:26.505 rudra-VirtualBox Dpkg (Debian Package) half configured. 7 2904
Nov 24, 2025 @ 19:48:22.505 rudra-VirtualBox Dpkg (Debian Package) half configured. 7 2904
Nov 24, 2025 @ 19:48:20.678 rudra-VirtualBox Dpkg (Debian Package) half configured. 7 2904
Nov 24, 2025 @ 19:48:20.497 rudra-VirtualBox Dpkg (Debian Package) half configured. 7 2904
Nov 24, 2025 @ 19:48:14.492 rudra-VirtualBox Dpkg (Debian Package) half configured. 7 2904
Nov 24, 2025 @ 19:48:14.492 rudra-VirtualBox Dpkg (Debian Package) half configured. 7 2904
Nov 24, 2025 @ 19:48:14.489 rudra-VirtualBox Dpkg (Debian Package) half configured. 7 2904
New release is available!
Go to the API configuration page for details
Disable updates notifications
Dismiss


Activities
Firefox
Nov 25 15:49
Wazuh - Wazuh
LevelBlue - Open Threat
VirusTotal - IP address - 1
www.virustotal.com/gui/ip-address/192.168.1.100
Sign in
192.168.1.100
Sign in
Sign up
0
/ 95
Community Score
1
9 detected files communicating with this IP address
Reanalyze
More
192.168.1.100
private
Last Analysis Date
39 minutes ago
DETECTION
DETAILS
RELATIONS
COMMUNITY 41
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Security vendors' analysis
Do you want to automate checks?
Abusix Clean
Acronis Clean
ADMINUSLabs Clean
AILabs (MONITORAPP) Clean
AlienVault Clean
Antiy-AVL Clean
benkow.cc Clean
BitDefender Clean
Blueliv Clean
Certego Clean
Chong Lua Dao Clean
CINS Army Clean
CMC Threat Intelligence Clean
CRDF Clean
Cyble Clean
CyRadar Clean
desenmascara.me Clean
DNS8 Clean
Dr.Web Clean
EmergingThreats Clean
Emsisoft Clean
ESET Clean
ESTsecurity Clean
Forcepoint ThreatSeeker Clean
Fortinet Clean
G-Data Clean
Google Safebrowsing Clean
GreenSnow Clean
Heimdal Security Clean
IPsum Clean
Juniper Networks Clean
Lionic Clean
Malwared Clean
MalwarePatrol Clean
malwares.com URL checker Clean
OpenPhish Clean