info@wazuh.com
https://wazuh.com

Threat hunting report

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

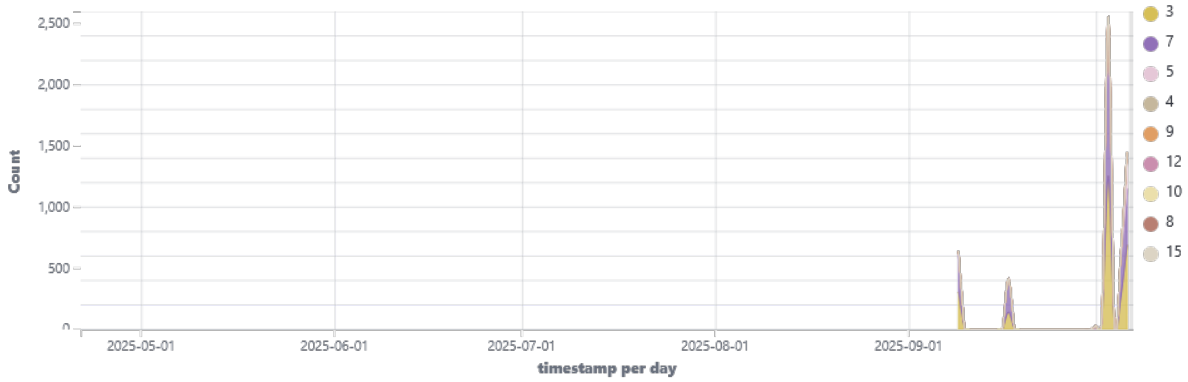
2025-04-21T07:34:42 to 2025-10-06T07:34:42

manager.name: siem-VMware-Virtual-Platform

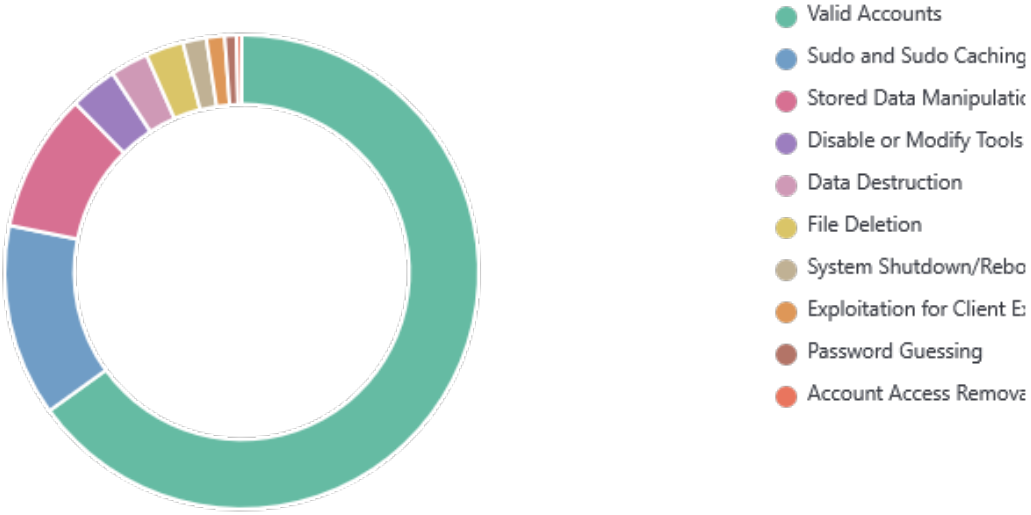
Top 3 agents with level 15 alerts

ID	Name	IP address	Version	Manager	Operating system	Registration date	Last keep alive
001	kali	192.168.84.135	Wazuh v4.12.0	siem-VMware-Virtual-Platform	Kali GNU/Linux 2025.3	Sep 9, 2025 @ 15:07:31.000	Oct 6, 2025 @ 07:34:43.000

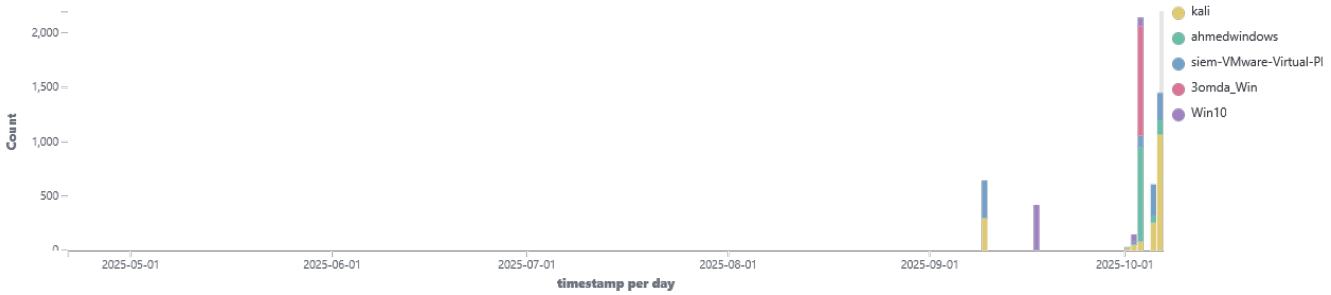
Top 10 Alert level evolution



Top 10 MITRE ATT&CKS



Alerts evolution - Top 5 agents



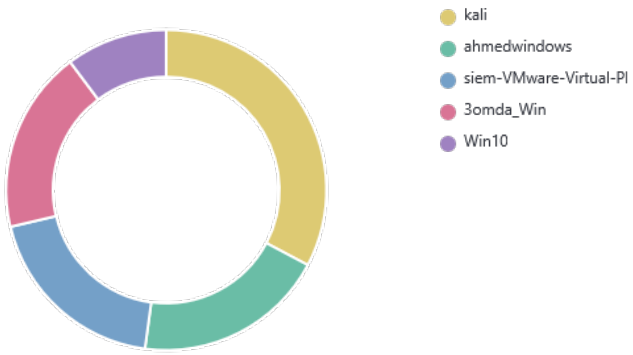
5,856
- Total -

19
- Level 12 or above alerts -

14
- Authentication failure -

730
- Authentication success -

Top 5 agents



Alerts summary

Rule ID	Description	Level	Count
60106	Windows Logon Success	3	533
510	Host-based anomaly detection event (rootcheck).	7	371
87101	VirusTotal: Error: Public API request rate limit reached	3	234
5501	PAM: Login session opened.	3	195
2904	Dpkg (Debian Package) half configured.	7	194
5502	PAM: Login session closed.	3	187
5402	Successful sudo to ROOT executed.	3	143
2902	New dpkg (Debian Package) installed.	7	141
554	File added to the system.	5	127
87103	VirusTotal: Alert - No records in VirusTotal database	3	113
550	Integrity checksum changed.	7	106
40704	Systemd: Service exited due to a failure.	5	103
100300	File modified in /home directory.	5	94
533	Listened ports status (netstat) changed (new port opened or closed).	7	74
60642	Software protection service scheduled successfully.	3	74
2901	New dpkg (Debian Package) requested to install.	3	51
503	Wazuh agent started.	3	51
60646	License activation (slui.exe) failed.	5	40
60608	Summary event of the report's signatures.	4	39
506	Wazuh agent stopped.	3	35
61104	Service startup type was changed	3	35
502	Wazuh server started.	3	34
553	File deleted.	7	29
60775	SessionEnv was unavailable to handle a notification event.	5	23
60775	WSearch was unavailable to handle a notification event.	5	18
19008	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow Basic authentication' is set to 'Disabled'.	3	10
19008	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow unencrypted traffic' is set to 'Disabled'.	3	9
87104	VirusTotal: Alert - c:\ahmed\new text document.txt - No positives found	3	6
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Configure 'Accounts: Rename guest account'.	7	5
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Configure 'Interactive logon: Message text for users attempting to log on'.	7	5
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Account lockout duration' is set to '15 or more minute(s)'.	7	5
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow Clipboard synchronization across devices' is set to 'Disabled'.	7	5
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow Cortana' is set to 'Disabled'.	7	5
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow Diagnostic Data' is set to 'Enabled: Diagnostic data off (not recommended)' or 'Enabled: Send required diagnostic data'.	7	5
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow Online Tips' is set to 'Disabled'.	7	5
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Audit Authorization Policy Change' is set to include 'Success'.	7	5

Rule ID	Description	Level	Count
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Audit Removable Storage' is set to 'Success and Failure'.	7	5
19008	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow indexing of encrypted files' is set to 'Disabled'.	3	5
19008	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Apply UAC restrictions to local accounts on network logons' is set to 'Enabled'.	3	5
19008	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Audit Audit Policy Change' is set to include 'Success'.	3	5
19008	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Audit Authentication Policy Change' is set to include 'Success'.	3	5
19008	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Audit Logon' is set to 'Success and Failure'.	3	5
19008	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Audit Special Logon' is set to include 'Success'.	3	5
19008	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Audit System Integrity' is set to 'Success and Failure'.	3	5
19008	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Configure Offer Remote Assistance' is set to 'Disabled'.	3	5
19008	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Configure SMB v1 server' is set to 'Disabled'.	3	5
19008	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Configure Windows Defender SmartScreen' is set to 'Enabled'.	3	5
19008	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Do not delete temp folders upon exit' is set to 'Disabled'.	3	5
19008	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Enumerate administrator accounts on elevation' is set to 'Disabled'.	3	5
19008	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Interactive logon: Prompt user to change password before expiration' is set to 'between 5 and 14 days'.	3	5
19008	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Join Microsoft MAPS' is set to 'Disabled'.	3	5
19008	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)' is set to 'Enabled'.	3	5
19008	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Microsoft network client: Send unencrypted password to third-party SMB servers' is set to 'Disabled'.	3	5
19008	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts' is set to 'Enabled'.	3	5
19008	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Network access: Sharing and security model for local accounts' is set to 'Classic - local users authenticate as themselves'.	3	5
19009	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Configure Automatic Updates: Scheduled install day' is set to '0 - Every day'.	3	5
19009	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Download Mode' is NOT set to 'Enabled: Internet'.	3	5
19009	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Select when Quality Updates are received' is set to 'Enabled: 0 days'.	3	5
19009	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Support device authentication using certificate' is set to 'Enabled: Automatic'.	3	5
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Disable IPv6 (Ensure TCPIP6 Parameter 'DisabledComponents' is set to '0xff (255)').	7	4
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Accounts: Block Microsoft accounts' is set to 'Users can't add or log on with Microsoft accounts'.	7	4
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow Print Spooler to accept client connections' is set to 'Disabled'.	7	4
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow Remote Shell Access' is set to 'Disabled'.	7	4

Rule ID	Description	Level	Count
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow search and Cortana to use location' is set to 'Disabled'.	7	4
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow suggested apps in Windows Ink Workspace' is set to 'Disabled'.	7	4
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow upload of User Activities' is set to 'Disabled'.	7	4
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Always prompt for password upon connection' is set to 'Enabled'.	7	4
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Audit Application Group Management' is set to 'Success and Failure'.	7	4
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Audit Credential Validation' is set to 'Success and Failure'.	7	4
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Audit Detailed File Share' is set to include 'Failure'.	7	4
87104	VirusTotal: Alert - c:\ahmed\3omda.txt - No positives found	3	3
87104	VirusTotal: Alert - /home/kali/malware/3omda2.txt - No positives found	3	2
87104	VirusTotal: Alert - c:\ahmed\ahmedemad.txt - No positives found	3	2
87104	VirusTotal: Alert - c:\users\koji\desktop\3omda wannacry.sh - No positives found	3	2
87104	VirusTotal: Alert - c:\users\koji\desktop\new text document.txt - No positives found	3	2
19009	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure AppArmor is not disabled in bootloader configuration.	3	1
19009	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure SELinux policy is configured.	3	1
19009	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure password creation requirements are configured.	3	1
19009	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure password hashing algorithm is SHA-512.	3	1
19009	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure password reuse is limited.	3	1
19009	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure the SELinux state is enforcing.	3	1
19009	CIS Distribution Independent Linux Benchmark v2.0.0.: Ensure the audit configuration is immutable.	3	1
19009	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure GDM automatic mounting of removable media is disabled.	3	1
19009	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure GDM autorun-never is enabled.	3	1
19009	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure GDM autorun-never is not overridden.	3	1
19009	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure GDM disable-user-list option is enabled.	3	1
19009	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure GDM disabling automatic mounting of removable media is not overridden.	3	1
19009	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure GDM screen locks cannot be overridden.	3	1
19009	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure actions as another user are always logged.	3	1
19009	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure audit log files group owner is configured.	3	1
19009	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure audit log storage size is configured.	3	1
87104	VirusTotal: Alert - /home/kali/.cache/tracker3/files/ http%3A%2F%2Ftracker.api.gnome.org%2Fontology%2Fv3%2Ftracker%23Pictures.db-shm - No positives found	3	1
87104	VirusTotal: Alert - /home/kali/.cache/tracker3/files/ http%3A%2F%2Ftracker.api.gnome.org%2Fontology%2Fv3%2Ftracker%23Pictures.db-wal - No positives found	3	1
87104	VirusTotal: Alert - /home/kali/.cache/tracker3/files/ http%3A%2F%2Ftracker.api.gnome.org%2Fontology%2Fv3%2Ftracker%23Software.db-shm - No positives found	3	1
87104	VirusTotal: Alert - /home/kali/.cache/tracker3/files/ http%3A%2F%2Ftracker.api.gnome.org%2Fontology%2Fv3%2Ftracker%23Software.db-wal - No positives found	3	1
87104	VirusTotal: Alert - /home/kali/.local/share/nautilus/tags/meta.db-shm - No positives found	3	1
87104	VirusTotal: Alert - /home/kali/.local/share/nautilus/tags/meta.db-wal - No positives found	3	1

Rule ID	Description	Level	Count
87104	VirusTotal: Alert - /root/.cache/dconf/user - No positives found	3	1
87104	VirusTotal: Alert - c:\ahmed\3omda.txt.txt - No positives found	3	1