Threat hunting report

ID	Name	IP address	Version	Manager	Operating system	Registration date	Last keep alive
003	ahmedwindows	192.168.84.131	Wazuh v4.12.0	siem-VMware-Virtual-Platform	Microsoft Windows 10 Pro 10.0.19045.2965	Oct 3, 2025 @ 10:26:37.000	Oct 3, 2025 @ 14:24:14.000

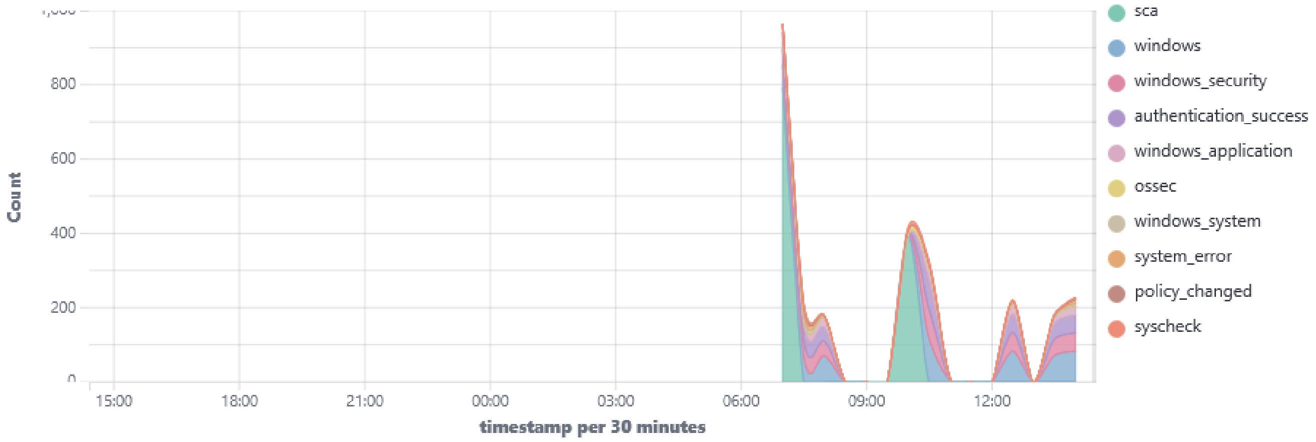
Group: Windows

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

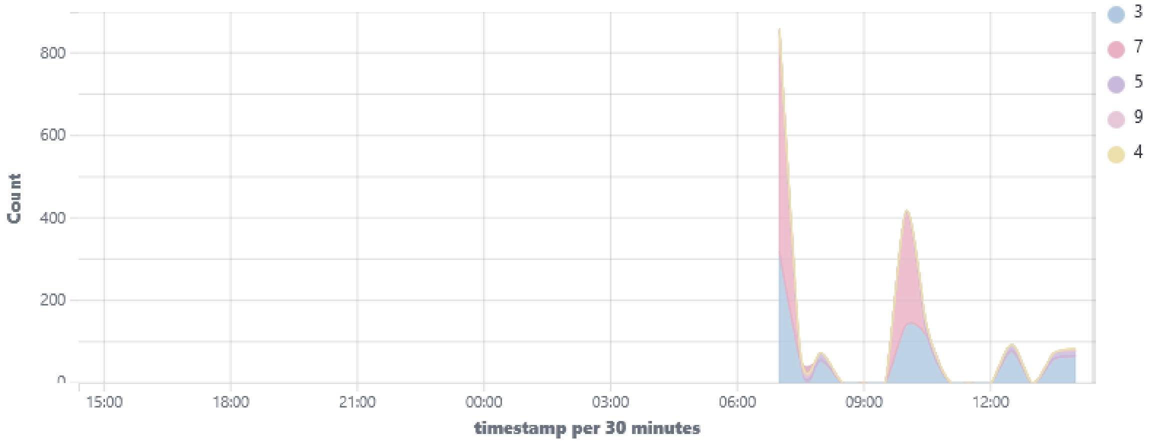
2025-10-02T14:23:58 to 2025-10-03T14:23:58

manager.name: siem-VMware-Virtual-Platform AND agent.id: 003

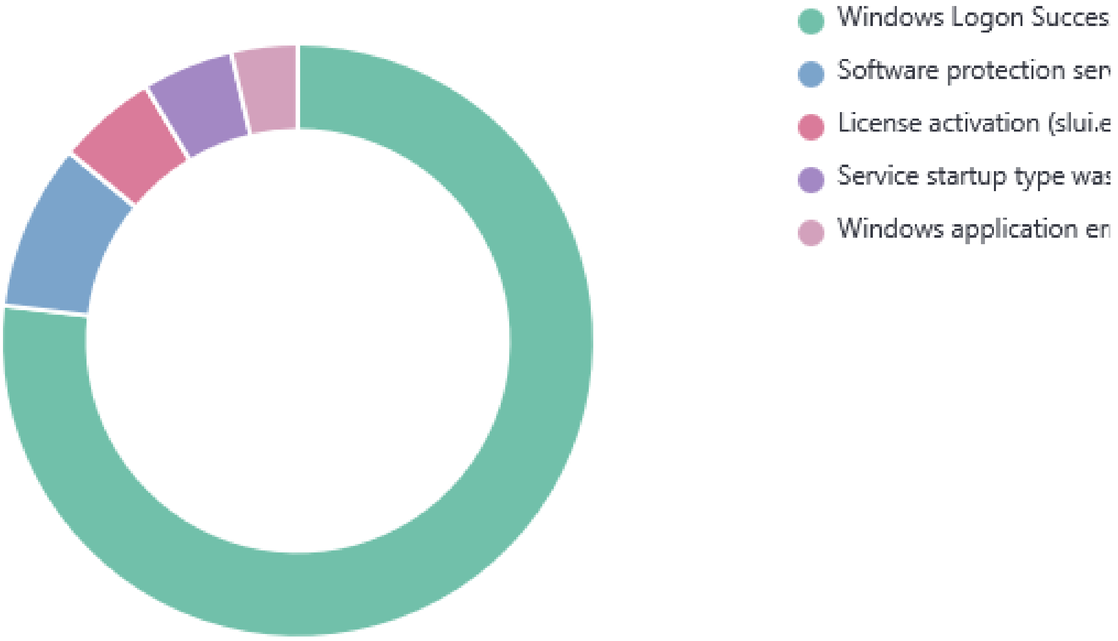
Top 10 Alert groups evolution



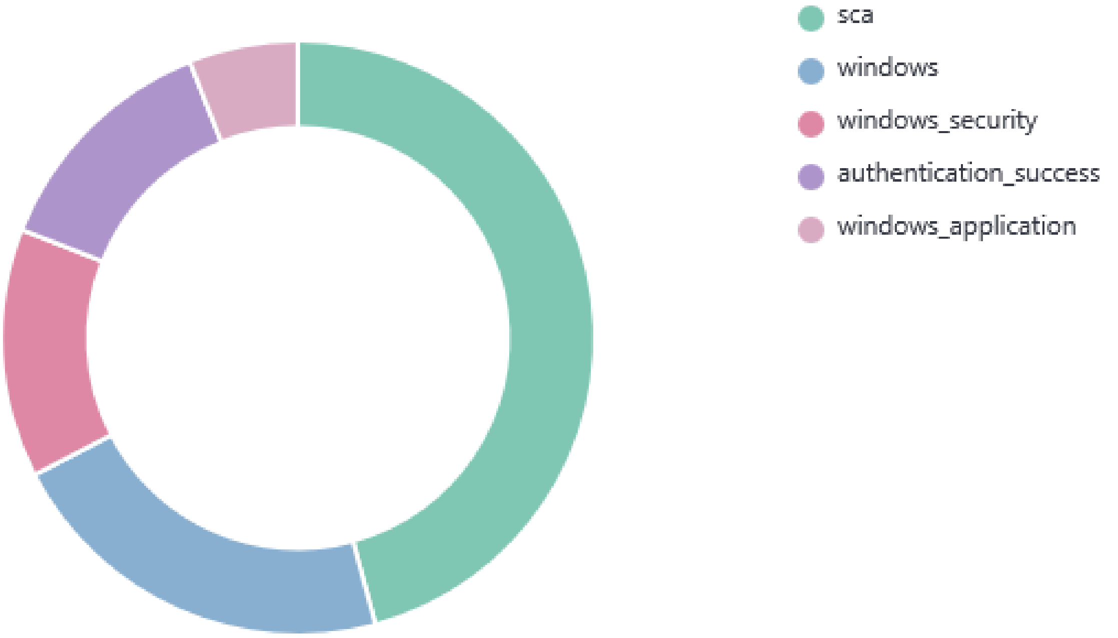
Alerts



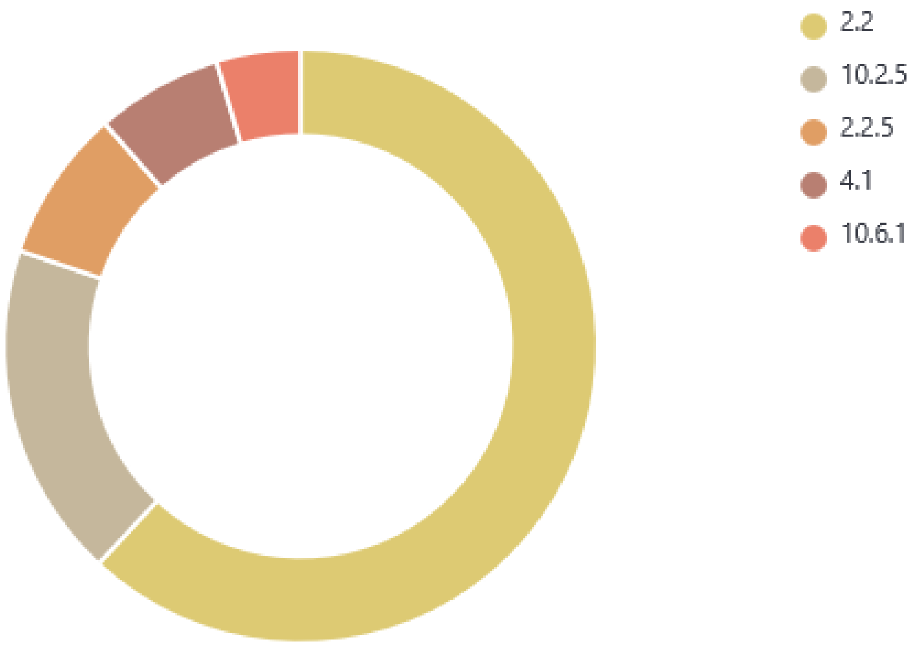
Top 5 alerts



Top 5 rule groups



Top 5 PCI DSS Requirements



1,806

- Total -

0

- Level 12 or above alerts -

0

- Authentication failure -

340

- Authentication success -

Alerts summary

Rule ID	Description	Level	Count
60106	Windows Logon Success	3	340
60642	Software protection service scheduled successfully.	3	40
60646	License activation (slui.exe) failed.	5	24
61104	Service startup type was changed	3	22
60602	Windows application error event.	9	16
60775	SessionEnv was unavailable to handle a notification event.	5	14
503	Wazuh agent started.	3	13
60702	The VSS service is shutting down due to idle timeout.	5	12
60775	WSearch was unavailable to handle a notification event.	5	11
60137	Windows User Logoff	3	11
67018	System shutdown initiated.	3	11
60668	The Windows search service started.	3	10
60798	The database engine attached a database.	3	10
60805	The database engine is starting a new instance.	3	10
61102	Windows System error event	5	10
554	File added to the system.	5	9
553	File deleted.	7	8
19008	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow Basic authentication' is set to 'Disabled'.	3	6
19008	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow unencrypted traffic' is set to 'Disabled'.	3	6
87104	VirusTotal: Alert - c:\ahmed\new text document.txt - No positives found	3	6
19004	SCA summary: CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Score less than 50% (32)	7	6
60608	Summary event of the report's signatures.	4	4
61109	Name resolution for the name t-s2-ring.msedge.net timed out	5	4
62154	Windows Defender: Antimalware platform feature configuration changed	5	4
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Configure 'Accounts: Rename guest account'.	7	3
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Disable IPv6 (Ensure TCPIP6 Parameter 'DisabledComponents' is set to '0xff (255)').	7	3
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	3
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow Remote Shell Access' is set to 'Disabled'.	7	3
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Audit Authorization Policy Change' is set to include 'Success'.	7	3
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Audit Removable Storage' is set to 'Success and Failure'.	7	3
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Boot-Start Driver Initialization Policy' is set to 'Enabled: Good, unknown and bad but critical'.	7	3
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Configure Windows Defender SmartScreen' is set to 'Enabled: Warn and prevent bypass'.	7	3
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Do not allow password expiration time longer than required by policy' is set to 'Enabled'.	7	3

Rule ID	Description	Level	Count
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Enable Font Providers' is set to 'Disabled'.	7	3
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'MSS: (KeepAliveTime) How often keep-alive packets are sent in milliseconds' is set to 'Enabled: 300,000 or 5 minutes (recommended)'.	7	3
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Network security: Allow Local System to use computer identity for NTLM' is set to 'Enabled'.	7	3
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Remote Desktop Services UserMode Port Redirector (UmRdpService)' is set to 'Disabled'.	7	3
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Server (LanmanServer)' is set to 'Disabled'.	7	3
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'System cryptography: Force strong key protection for user keys stored on the computer' is set to 'User is prompted when the key is first used' or higher.	7	3
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Turn On Virtualization Based Security: Credential Guard Configuration' is set to 'Enabled with UEFI lock'.	7	3
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Turn off the Windows Messenger Customer Experience Improvement Program' is set to 'Enabled'.	7	3
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Turn off the offer to update to the latest version of Windows' is set to 'Enabled'.	7	3
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Turn on e-mail scanning' is set to 'Enabled'.	7	3
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Windows Firewall: Domain: Logging: Log dropped packets' is set to 'Yes'.	7	3
19008	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Accounts: Administrator account status' is set to 'Disabled'.	3	3
19008	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Accounts: Guest account status' is set to 'Disabled'.	3	3
19008	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Accounts: Limit local account use of blank passwords to console logon only' is set to 'Enabled'.	3	3
19008	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow a Windows app to share application data between users' is set to 'Disabled'.	3	3
19008	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow indexing of encrypted files' is set to 'Disabled'.	3	3
19008	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow remote server management through WinRM' is set to 'Disabled'.	3	3
19008	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow user control over installs' is set to 'Disabled'.	3	3
19008	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow users to connect remotely by using Remote Desktop Services' is set to 'Disabled'.	3	3
19008	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Application: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'.	3	3
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	3
19008	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Audit Audit Policy Change' is set to include 'Success'.	3	3
19008	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Audit Authentication Policy Change' is set to include 'Success'.	3	3
19008	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Audit Logoff' is set to include 'Success'.	3	3
19008	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Audit Logon' is set to 'Success and Failure'.	3	3
19008	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Audit Other System Events' is set to 'Success and Failure'.	3	3
19008	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Audit Security Group Management' is set to include 'Success'.	3	3
19008	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Audit Special Logon' is set to include 'Success'.	3	3

Rule ID	Description	Level	Count
19008	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Audit System Integrity' is set to 'Success and Failure'.	3	3
87104	VirusTotal: Alert - c:\ahmed\3omda.txt - No positives found	3	3
19009	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Configure Automatic Updates: Scheduled install day' is set to '0 - Every day'.	3	3
19009	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Download Mode' is NOT set to 'Enabled: Internet'.	3	3
19009	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Select when Quality Updates are received' is set to 'Enabled: 0 days'.	3	3
19009	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Support device authentication using certificate' is set to 'Enabled: Automatic'.	3	3
501	New wazuh agent connected.	3	3
506	Wazuh agent stopped.	3	3
550	Integrity checksum changed.	7	3
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
60776	SessionEnv was unavailable to handle a critical notification event.	7	2
61138	New Windows Service Created	5	2
87104	VirusTotal: Alert - c:\ahmed\3omda.txt.txt - No positives found	3	1
87104	VirusTotal: Alert - c:\users\koji\desktop\ahmedemad.txt - No positives found	3	1
87104	VirusTotal: Alert - c:\users\koji\desktop\soidasoifhdoifhsdofg.txt - No positives found	3	1
87104	VirusTotal: Alert - c:\users\koji\desktop\wannacry.txt - No positives found	3	1
60132	System time changed	5	1
60747	WMI service started successfully.	3	1
62153	Windows Defender: Antivirus real-time protection feature configuration has changed	3	1

Groups summary

Groups	Count
sca	1188
windows	560
windows_security	352
authentication_success	340
windows_application	154
ossec	39
windows_system	38
system_error	26
policy_changed	22
syscheck	20
syscheck_file	20
virustotal	19
WEF	11
syscheck_entry_added	9
syscheck_entry_deleted	8
windows_defender	5
syscheck_entry_modified	3
time_changed	1