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

Threat hunting report

ID	Name	IP address	Version	Manager	Operating system	Registration date	Last keep alive
003	3omda_Win	192.168.84.130	Wazuh v4.12.0	siem-VMware-Virtual-Platform	Microsoft Windows 10 Pro 10.0.19045.2965	Oct 3, 2025 @ 07:06:46.000	Oct 3, 2025 @ 07:07:47.000

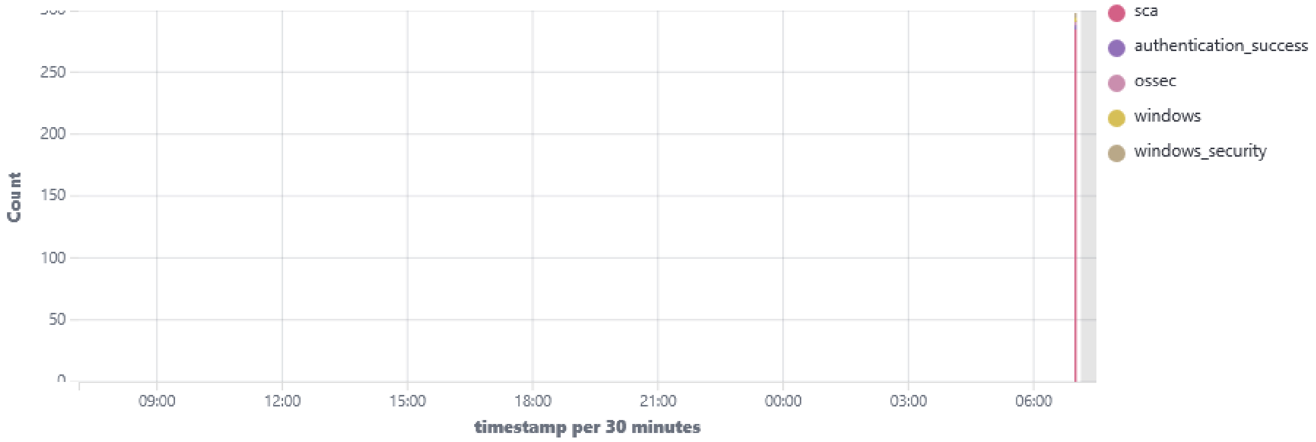
Group: default

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

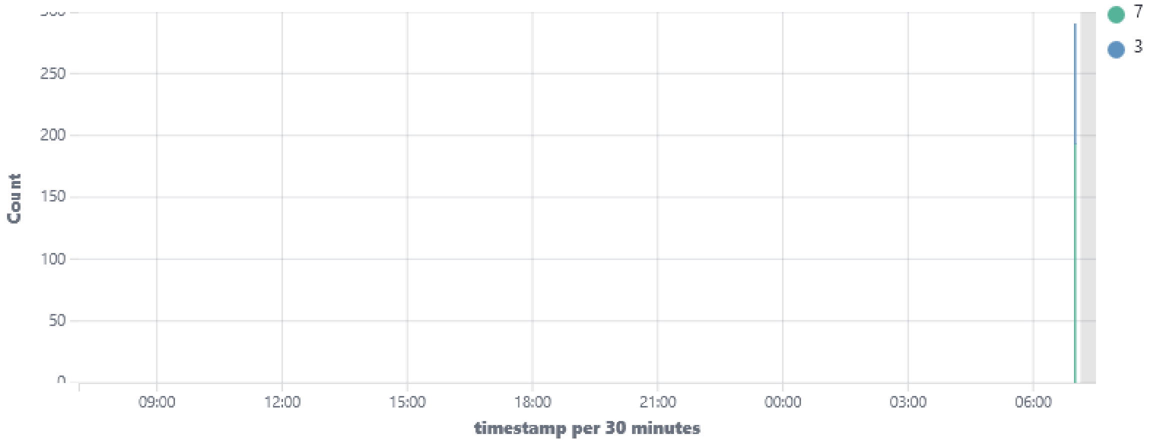
2025-10-02T07:07:32 to 2025-10-03T07:07:32

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

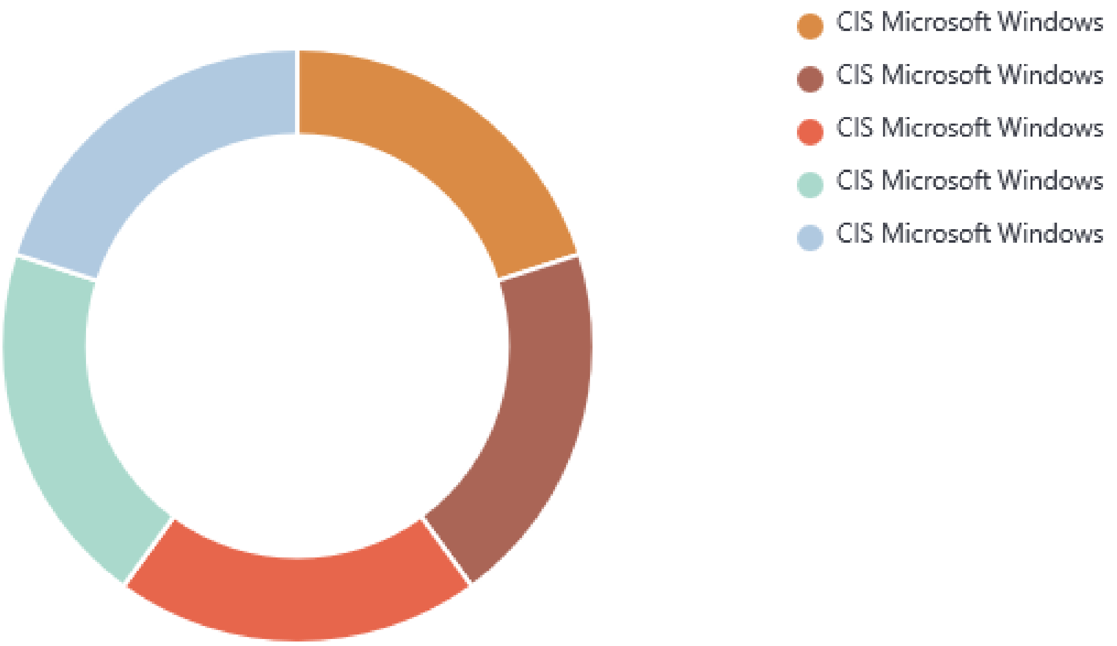
Top 10 Alert groups evolution



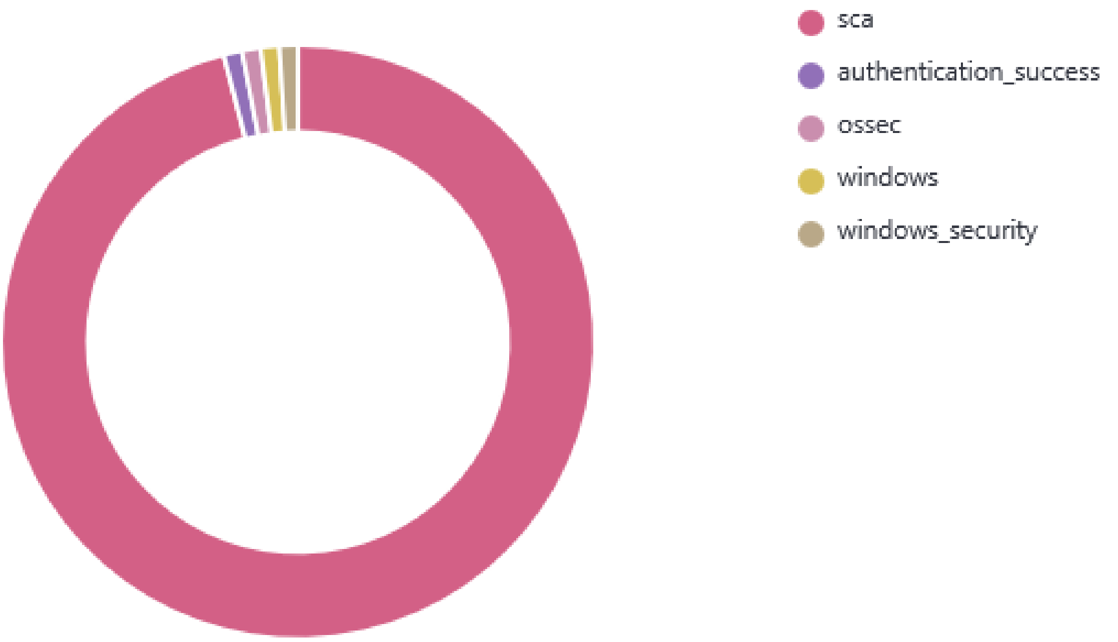
Alerts



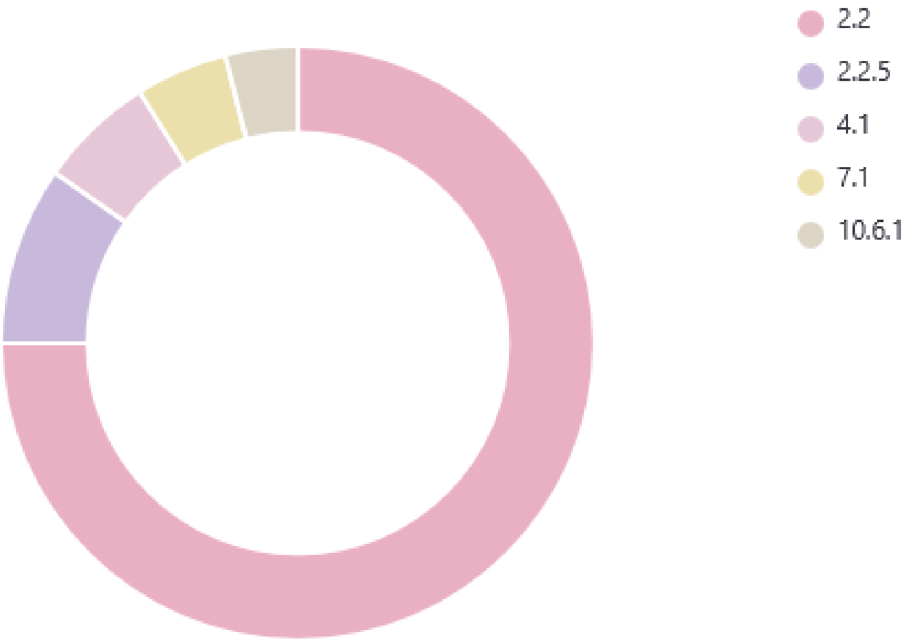
Top 5 alerts



Top 5 rule groups



Top 5 PCI DSS Requirements



289
- Total -

0
- Level 12 or above alerts -

0
- Authentication failure -

3
- Authentication success -

Alerts summary

Rule ID	Description	Level	Count
60106	Windows Logon Success	3	3
19008	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow Basic authentication' is set to 'Disabled'.	3	2
19008	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow unencrypted traffic' is set to 'Disabled'.	3	2
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Configure 'Accounts: Rename administrator account'.	7	1
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Configure 'Accounts: Rename guest account'.	7	1
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Configure 'Interactive logon: Message text for users attempting to log on'.	7	1
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Configure 'Interactive logon: Message title for users attempting to log on'.	7	1
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Disable IPv6 (Ensure TCPIP6 Parameter 'DisabledComponents' is set to '0xff (255)').	7	1
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Account lockout duration' is set to '15 or more minute(s)'.	7	1
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Account lockout threshold' is set to '5 or fewer invalid logon attempt(s), but not 0'.	7	1
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	1
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow Clipboard synchronization across devices' is set to 'Disabled'.	7	1
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow Cloud Search' is set to 'Enabled: Disable Cloud Search'.	7	1
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow Cortana above lock screen' is set to 'Disabled'.	7	1
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow Cortana' is set to 'Disabled'.	7	1
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	1
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow Message Service Cloud Sync' is set to 'Disabled'.	7	1
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow Microsoft accounts to be optional' is set to 'Enabled'.	7	1
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow Online Tips' is set to 'Disabled'.	7	1
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow Print Spooler to accept client connections' is set to 'Disabled'.	7	1
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow Remote Shell Access' is set to 'Disabled'.	7	1
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow UI Automation redirection' is set to 'Disabled'.	7	1
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow Use of Camera' is set to 'Disabled'.	7	1
19008	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Accounts: Administrator account status' is set to 'Disabled'.	3	1
19008	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Accounts: Guest account status' is set to 'Disabled'.	3	1
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	1
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	1

Rule ID	Description	Level	Count
19008	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow indexing of encrypted files' is set to 'Disabled'.	3	1
19008	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow remote server management through WinRM' is set to 'Disabled'.	3	1
19008	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow user control over installs' is set to 'Disabled'.	3	1
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	1
19008	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Always install with elevated privileges' is set to 'Disabled'.	3	1
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	1
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	1
19008	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Audit Audit Policy Change' is set to include 'Success'.	3	1
19008	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Audit Authentication Policy Change' is set to include 'Success'.	3	1
19008	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Audit Logoff' is set to include 'Success'.	3	1
19008	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Audit Logon' is set to 'Success and Failure'.	3	1
19008	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Audit Other System Events' is set to 'Success and Failure'.	3	1
19008	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Audit Security Group Management' is set to include 'Success'.	3	1
19008	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Audit Security State Change' is set to include 'Success'.	3	1
19009	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Configure Automatic Updates: Scheduled install day' is set to '0 - Every day'.	3	1
19009	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Download Mode' is NOT set to 'Enabled: Internet'.	3	1
19009	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Select when Quality Updates are received' is set to 'Enabled: 0 days'.	3	1
19009	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Support device authentication using certificate' is set to 'Enabled: Automatic'.	3	1
501	New wazuh agent connected.	3	1
503	Wazuh agent started.	3	1
506	Wazuh agent stopped.	3	1

Groups summary

Groups	Count
sca	394
authentication_success	3
ossec	3
windows	3
windows_security	3