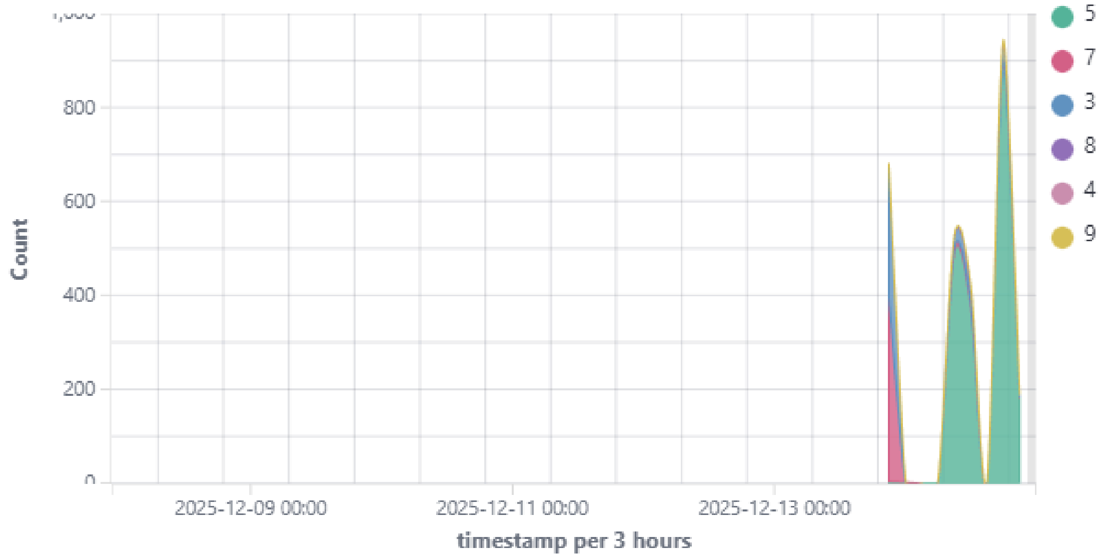
Threat hunting report

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

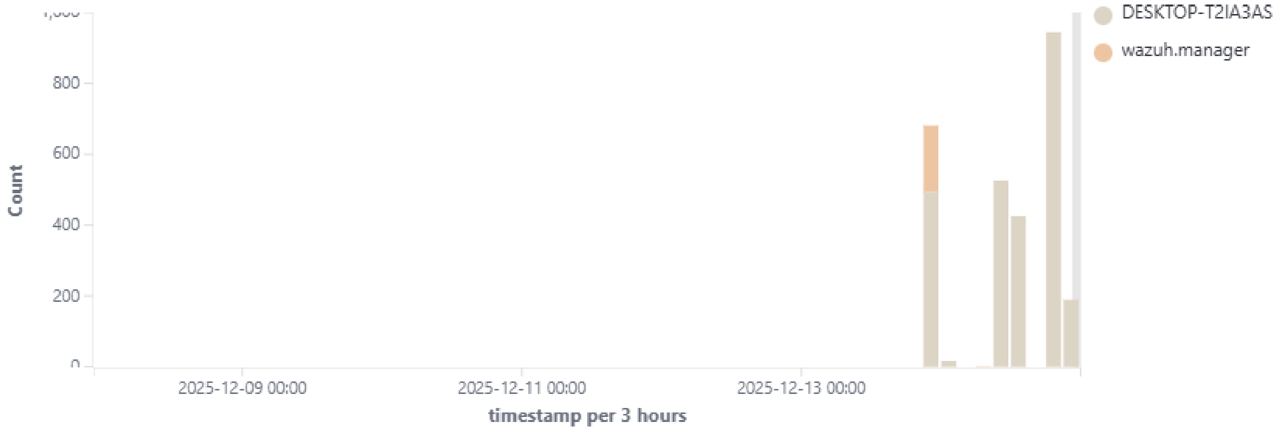
2025-12-07T22:27:23 to 2025-12-14T22:27:23

manager.name: wazuh.manager

Top 10 Alert level evolution



Alerts evolution - Top 5 agents



2,783

- Total -

0

- Level 12 or above alerts -

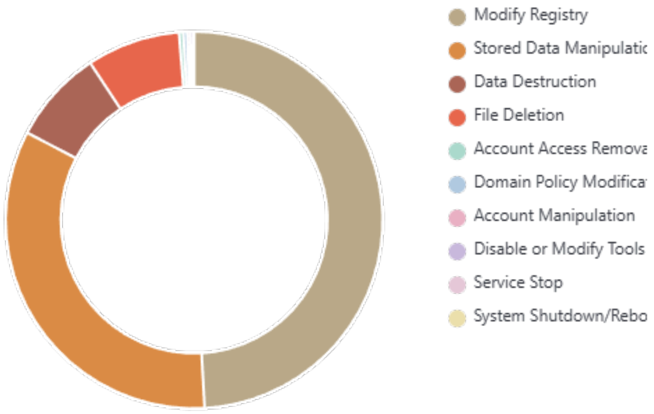
14

- Authentication failure -

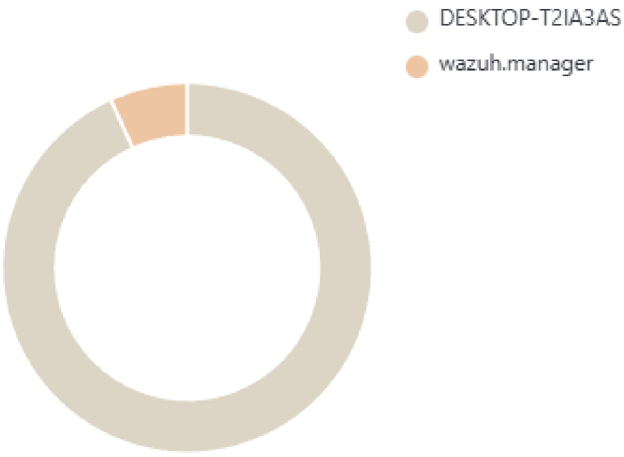
0

- Authentication success -

Top 10 MITRE ATT&CKS



Top 5 agents



Alerts summary

Rule ID	Description	Level	Count
750	Registry Value Integrity Checksum Changed	5	948
594	Registry Key Integrity Checksum Changed	5	351
752	Registry Value Entry Added to the System	5	245
751	Registry Value Entry Deleted.	5	241
598	Registry Key Entry Added to the System	5	64
597	Registry Key Entry Deleted.	5	61
60642	Software protection service scheduled successfully.	3	30
67022	Non network or service local logon.	3	23
67023	Non service account logged off.	3	21
60122	Logon Failure - Unknown user or bad password	5	14
67028	Special privileges assigned to new logon.	3	13
506	Wazuh agent stopped.	3	10
553	File deleted.	7	10
554	File added to the system.	5	10
60110	User account changed	8	10
503	Wazuh agent started.	3	9
60104	Windows audit failure event	5	8
61104	Service startup type was changed	3	8
550	Integrity checksum changed.	7	6
502	Wazuh server started.	3	4
19005	SCA summary: CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0: Score less than 30% (26)	9	3
60132	System time changed	5	3
60608	Summary event of the report's signatures.	4	3
19008	CIS Benchmark for Amazon Linux 2023 Benchmark v1.0.0.: Ensure permissions on /etc/passwd are configured.	3	2
19008	CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0: Ensure 'Allow Basic authentication' is set to 'Disabled'.	3	2
19008	CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0: Ensure 'Allow unencrypted traffic' is set to 'Disabled'.	3	2
60775	SessionEnv was unavailable to handle a notification event.	5	2
19003	SCA summary: CIS Benchmark for Amazon Linux 2023 Benchmark v1.0.0.: Score less than 80% (53)	5	2
60112	Windows Audit Policy changed	8	2
60668	The Windows search service started.	3	2
60669	The Windows search service stopped normally.	3	2
19007	CIS Benchmark for Amazon Linux 2023 Benchmark v1.0.0.: Ensure AIDE is installed.	7	1
19007	CIS Benchmark for Amazon Linux 2023 Benchmark v1.0.0.: Ensure VSFTP Server is not installed.	7	1
19007	CIS Benchmark for Amazon Linux 2023 Benchmark v1.0.0.:	7	1

Rule ID	Description	Level	Count
	Ensure accounts in /etc/passwd use shadowed passwords.		
19007	CIS Benchmark for Amazon Linux 2023 Benchmark v1.0.0.: Ensure actions as another user are always logged.	7	1
19007	CIS Benchmark for Amazon Linux 2023 Benchmark v1.0.0.: Ensure at is restricted to authorized users.	7	1
19007	CIS Benchmark for Amazon Linux 2023 Benchmark v1.0.0.: Ensure at least one nftables table exists.	7	1
19007	CIS Benchmark for Amazon Linux 2023 Benchmark v1.0.0.: Ensure auditd is installed.	7	1
19007	CIS Benchmark for Amazon Linux 2023 Benchmark v1.0.0.: Ensure changes to system administration scope (sudoers) is collected.	7	1
19007	CIS Benchmark for Amazon Linux 2023 Benchmark v1.0.0.: Ensure cron is restricted to authorized users.	7	1
19007	CIS Benchmark for Amazon Linux 2023 Benchmark v1.0.0.: Ensure events that modify date and time information are collected.	7	1
19007	CIS Benchmark for Amazon Linux 2023 Benchmark v1.0.0.: Ensure events that modify the system's Mandatory Access Controls are collected.	7	1
19007	CIS Benchmark for Amazon Linux 2023 Benchmark v1.0.0.: Ensure events that modify the system's network environment are collected.	7	1
19007	CIS Benchmark for Amazon Linux 2023 Benchmark v1.0.0.: Ensure events that modify user/group information are collected.	7	1
19007	CIS Benchmark for Amazon Linux 2023 Benchmark v1.0.0.: Ensure file deletion events by users are collected.	7	1
19007	CIS Benchmark for Amazon Linux 2023 Benchmark v1.0.0.: Ensure gpgcheck is globally activated.	7	1
19007	CIS Benchmark for Amazon Linux 2023 Benchmark v1.0.0.: Ensure inactive password lock is 30 days or less.	7	1
19007	CIS Benchmark for Amazon Linux 2023 Benchmark v1.0.0.: Ensure kernel module loading unloading and modification is collected.	7	1
19007	CIS Benchmark for Amazon Linux 2023 Benchmark v1.0.0.: Ensure local login warning banner is configured properly.	7	1
19007	CIS Benchmark for Amazon Linux 2023 Benchmark v1.0.0.: Ensure login and logout events are collected.	7	1
19007	CIS Benchmark for Amazon Linux 2023 Benchmark v1.0.0.: Ensure minimum days between password changes is 7 or more.	7	1
19008	CIS Benchmark for Amazon Linux 2023 Benchmark v1.0.0.: Ensure Avahi Server is not installed.	3	1
19008	CIS Benchmark for Amazon Linux 2023 Benchmark v1.0.0.: Ensure CUPS is not installed.	3	1
19008	CIS Benchmark for Amazon Linux 2023 Benchmark v1.0.0.: Ensure DHCP Server is not installed.	3	1
19008	CIS Benchmark for Amazon Linux 2023 Benchmark v1.0.0.: Ensure DNS Server is not installed.	3	1
19008	CIS Benchmark for Amazon Linux 2023 Benchmark v1.0.0.:	3	1

Rule ID	Description	Level	Count
	Ensure FTP client is not installed.		
19008	CIS Benchmark for Amazon Linux 2023 Benchmark v1.0.0.: Ensure GNOME Display Manager is removed.	3	1
19008	CIS Benchmark for Amazon Linux 2023 Benchmark v1.0.0.: Ensure HTTP Proxy Server is not installed.	3	1
19008	CIS Benchmark for Amazon Linux 2023 Benchmark v1.0.0.: Ensure IMAP and POP3 server is not installed.	3	1
19008	CIS Benchmark for Amazon Linux 2023 Benchmark v1.0.0.: Ensure LDAP client is not installed.	3	1
19008	CIS Benchmark for Amazon Linux 2023 Benchmark v1.0.0.: Ensure NIS server is not installed.	3	1
19008	CIS Benchmark for Amazon Linux 2023 Benchmark v1.0.0.: Ensure SELinux is installed.	3	1
19008	CIS Benchmark for Amazon Linux 2023 Benchmark v1.0.0.: Ensure SETroubleshoot is not installed.	3	1
19008	CIS Benchmark for Amazon Linux 2023 Benchmark v1.0.0.: Ensure SNMP Server is not installed.	3	1
19008	CIS Benchmark for Amazon Linux 2023 Benchmark v1.0.0.: Ensure Samba is not installed.	3	1
19008	CIS Benchmark for Amazon Linux 2023 Benchmark v1.0.0.: Ensure TFTP Server is not installed.	3	1
19008	CIS Benchmark for Amazon Linux 2023 Benchmark v1.0.0.: Ensure TFTP client is not installed.	3	1
19008	CIS Benchmark for Amazon Linux 2023 Benchmark v1.0.0.: Ensure a web server is not installed.	3	1
19009	CIS Benchmark for Amazon Linux 2023 Benchmark v1.0.0.: Disable USB Storage.	3	1
19009	CIS Benchmark for Amazon Linux 2023 Benchmark v1.0.0.: Ensure /dev/shm is a separate partition.	3	1
19009	CIS Benchmark for Amazon Linux 2023 Benchmark v1.0.0.: Ensure /tmp is a separate partition.	3	1
19009	CIS Benchmark for Amazon Linux 2023 Benchmark v1.0.0.: Ensure SELinux is not disabled in bootloader configuration.	3	1
19009	CIS Benchmark for Amazon Linux 2023 Benchmark v1.0.0.: Ensure SELinux policy is configured.	3	1
19009	CIS Benchmark for Amazon Linux 2023 Benchmark v1.0.0.: Ensure SSH AllowTcpForwarding is disabled.	3	1
19009	CIS Benchmark for Amazon Linux 2023 Benchmark v1.0.0.: Ensure SSH HostbasedAuthentication is disabled.	3	1
19009	CIS Benchmark for Amazon Linux 2023 Benchmark v1.0.0.: Ensure SSH Idle Timeout Interval is configured.	3	1
19009	CIS Benchmark for Amazon Linux 2023 Benchmark v1.0.0.: Ensure SSH IgnoreRhosts is enabled.	3	1
19009	CIS Benchmark for Amazon Linux 2023 Benchmark v1.0.0.: Ensure SSH LogLevel is appropriate.	3	1
19009	CIS Benchmark for Amazon Linux 2023 Benchmark v1.0.0.: Ensure SSH LoginGraceTime is set to one minute or less.	3	1
19009	CIS Benchmark for Amazon Linux 2023 Benchmark v1.0.0.: Ensure SSH MaxAuthTries is set to 4 or less.	3	1

Rule ID	Description	Level	Count
19009	CIS Benchmark for Amazon Linux 2023 Benchmark v1.0.0.: Ensure SSH MaxSessions is set to 10 or less.	3	1
19009	CIS Benchmark for Amazon Linux 2023 Benchmark v1.0.0.: Ensure SSH MaxStartups is configured.	3	1
19009	CIS Benchmark for Amazon Linux 2023 Benchmark v1.0.0.: Ensure SSH PAM is enabled.	3	1
19009	CIS Benchmark for Amazon Linux 2023 Benchmark v1.0.0.: Ensure SSH PermitEmptyPasswords is disabled.	3	1
19009	CIS Benchmark for Amazon Linux 2023 Benchmark v1.0.0.: Ensure SSH PermitUserEnvironment is disabled.	3	1
19009	CIS Benchmark for Amazon Linux 2023 Benchmark v1.0.0.: Ensure SSH X11 forwarding is disabled.	3	1
19009	CIS Benchmark for Amazon Linux 2023 Benchmark v1.0.0.: Ensure SSH access is limited.	3	1
19009	CIS Benchmark for Amazon Linux 2023 Benchmark v1.0.0.: Ensure SSH root login is disabled.	3	1
60775	WSearch was unavailable to handle a notification event.	5	1
19010	CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0: Ensure 'Audit Account Lockout' is set to include 'Failure'.: Status changed from failed to passed	3	1
501	New wazuh agent connected.	3	1
60137	Windows User Logoff	3	1
60610	Windows installer began an installation process.	3	1
60635	Windows installer reconfigured the product.	3	1
60702	The VSS service is shutting down due to idle timeout.	5	1
60716	Skipped creation of restore point for C:\\WINDOWS\\system32\\lpksetup.exe -Embedding, Language Pack Removal as there is a previous restore point available.	4	1
60776	SessionEnv was unavailable to handle a critical notification event.	7	1
61102	Windows System error event	5	1
61109	Name resolution for the name t-ring-fdv2.msedge.net timed out	5	1