Threat hunting report

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

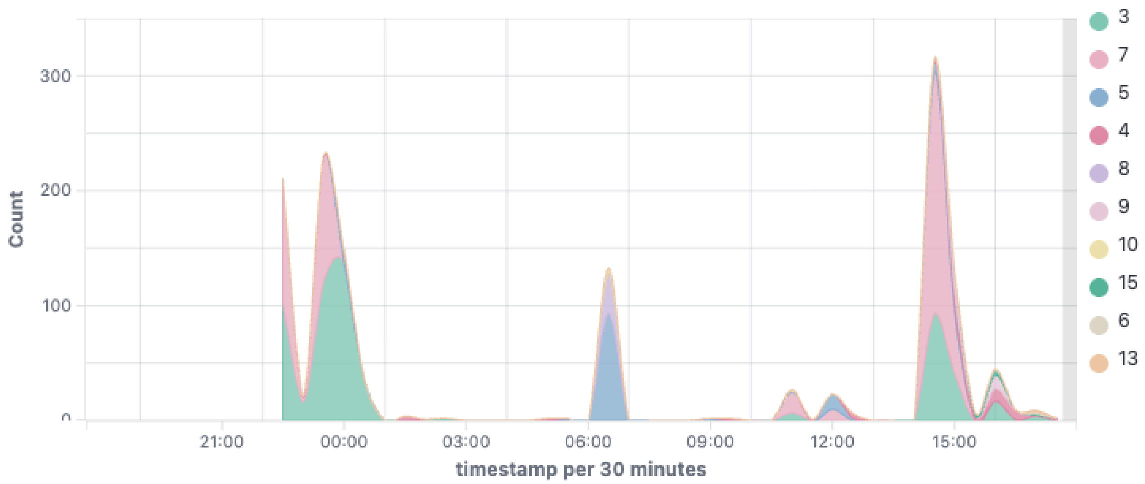
2025-11-27T17:39:37 to 2025-11-28T17:39:37

manager.name: ip-172-31-16-30 AND manager.name: ip-172-31-16-30 AND rule.level: 1-null

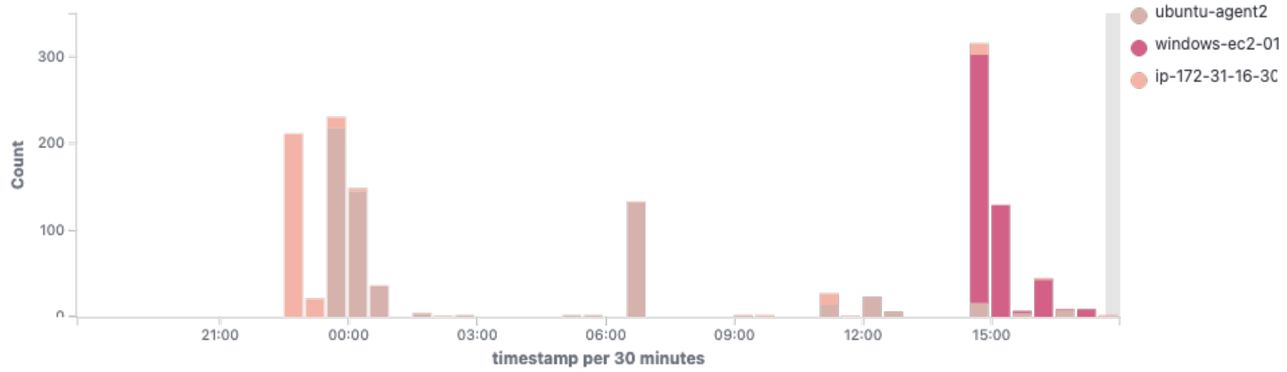
Top 3 agents with level 15 alerts

ID	Name	IP address	Version	Manager	Operating system	Registration date	Last keep alive
003	windows-ec2-01	172.31.40.70	Wazuh v4.14.1	ip-172-31-16-30	Microsoft Windows Server 2022 Datacenter 10.0.20348.4405	Nov 28, 2025 @ 19:53:54.000	Nov 28, 2025 @ 22:39:27.000

Top 10 Alert level evolution



Alerts evolution - Top 5 agents



1,367

- Total -

8

- Level 12 or above alerts -

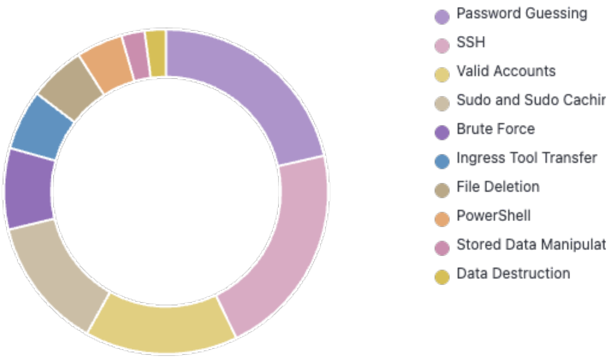
159

- Authentication failure -

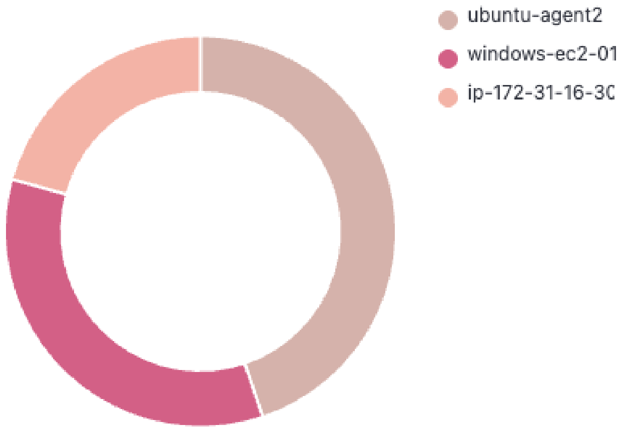
80

- Authentication success -

Top 10 MITRE ATT&CKS



Top 5 agents



Alerts summary

Rule ID	Description	Level	Count
5710	sshd: Attempt to login using a non-existent user	5	111
5502	PAM: Login session closed.	3	79
5501	PAM: Login session opened.	3	76
5402	Successful sudo to ROOT executed.	3	65
5758	Maximum authentication attempts exceeded.	8	36
92205	Powershell process created an executable file in Windows root folder	9	24
92066	C:\\Windows\\SysWOW64\\SecEdit.exe binary in a suspicious location launched by C:\\Windows\\SysWOW64\\WindowsPowerShell\\v1.0\\powershell.exe	4	20
92021	Powershell was used to delete files or directories	3	18
5762	sshd: connection reset	4	16
554	File added to the system.	5	13
5740	sshd: connection reset by peer	4	13
550	Integrity checksum changed.	7	12
553	File deleted.	7	11
92031	Discovery activity executed	3	8
92213	Executable file dropped in folder commonly used by malware	15	7
2501	syslog: User authentication failure.	5	6
503	Wazuh agent started.	3	6
506	Wazuh agent stopped.	3	6
5712	sshd: brute force trying to get access to the system. Non existent user.	10	5
19004	SCA summary: CIS Ubuntu Linux 22.04 LTS Benchmark v2.0.0.: Score less than 50% (45)	7	3
5403	First time user executed sudo.	4	3
5715	sshd: authentication success.	3	3
92027	Powershell process spawned powershell instance	4	3
19007	CIS Ubuntu Linux 22.04 LTS Benchmark v2.0.0.: Ensure /tmp is a separate partition.	7	2
19007	CIS Ubuntu Linux 22.04 LTS Benchmark v2.0.0.: Ensure AIDE is installed.	7	2
19007	CIS Ubuntu Linux 22.04 LTS Benchmark v2.0.0.: Ensure a nftables table exists.	7	2
19007	CIS Ubuntu Linux 22.04 LTS Benchmark v2.0.0.: Ensure access to bootloader config is configured.	7	2
19007	CIS Ubuntu Linux 22.04 LTS Benchmark v2.0.0.: Ensure access to the su command is restricted.	7	2
19007	CIS Ubuntu Linux 22.04 LTS Benchmark v2.0.0.: Ensure audit tools owner is configured.	7	2
19007	CIS Ubuntu Linux 22.04 LTS Benchmark v2.0.0.: Ensure bootloader password is set.	7	2

Rule ID	Description	Level	Count
19007	CIS Ubuntu Linux 22.04 LTS Benchmark v2.0.0.: Ensure events that modify user/group information are collected.	7	2
19007	CIS Ubuntu Linux 22.04 LTS Benchmark v2.0.0.: Ensure filesystem integrity is regularly checked.	7	2
19007	CIS Ubuntu Linux 22.04 LTS Benchmark v2.0.0.: Ensure ftp client is not installed.	7	2
19007	CIS Ubuntu Linux 22.04 LTS Benchmark v2.0.0.: Ensure iptables packages are installed.	7	2
19007	CIS Ubuntu Linux 22.04 LTS Benchmark v2.0.0.: Ensure login and logout events are collected.	7	2
19007	CIS Ubuntu Linux 22.04 LTS Benchmark v2.0.0.: Ensure nftables service is enabled.	7	2
19007	CIS Ubuntu Linux 22.04 LTS Benchmark v2.0.0.: Ensure nodev option set on /var/log partition.	7	2
19007	CIS Ubuntu Linux 22.04 LTS Benchmark v2.0.0.: Ensure nodev option set on /var/tmp partition.	7	2
19007	CIS Ubuntu Linux 22.04 LTS Benchmark v2.0.0.: Ensure noexec option set on /tmp partition.	7	2
19007	CIS Ubuntu Linux 22.04 LTS Benchmark v2.0.0.: Ensure noexec option set on /var/log partition.	7	2
19007	CIS Ubuntu Linux 22.04 LTS Benchmark v2.0.0.: Ensure nosuid option set on /home partition.	7	2
19007	CIS Ubuntu Linux 22.04 LTS Benchmark v2.0.0.: Ensure nosuid option set on /tmp partition.	7	2
19007	CIS Ubuntu Linux 22.04 LTS Benchmark v2.0.0.: Ensure nosuid option set on /var/log partition.	7	2
19008	CIS Microsoft Windows Server 2022 Benchmark v2.0.0: Ensure 'Allow Basic authentication' is set to 'Disabled'.	3	2
19008	CIS Microsoft Windows Server 2022 Benchmark v2.0.0: Ensure 'Allow unencrypted traffic' is set to 'Disabled'.	3	2
19008	CIS Ubuntu Linux 22.04 LTS Benchmark v2.0.0.: Ensure X window server services are not in use.	3	2
19008	CIS Ubuntu Linux 22.04 LTS Benchmark v2.0.0.: Ensure access to /etc/motd is configured.	3	2
19008	CIS Ubuntu Linux 22.04 LTS Benchmark v2.0.0.: Ensure audit configuration files owner is configured.	3	2
19008	CIS Ubuntu Linux 22.04 LTS Benchmark v2.0.0.: Ensure autofs services are not in use.	3	2
19008	CIS Ubuntu Linux 22.04 LTS Benchmark v2.0.0.: Ensure avahi daemon services are not in use.	3	2
19008	CIS Ubuntu Linux 22.04 LTS Benchmark v2.0.0.: Ensure dns server services are not in use.	3	2
19008	CIS Ubuntu Linux 22.04 LTS Benchmark v2.0.0.: Ensure group root is the only GID 0 group.	3	2
19008	CIS Ubuntu Linux 22.04 LTS Benchmark v2.0.0.: Ensure ldap client is not installed.	3	2
19008	CIS Ubuntu Linux 22.04 LTS Benchmark v2.0.0.: Ensure ldap server services are not in use.	3	2
19008	CIS Ubuntu Linux 22.04 LTS Benchmark v2.0.0.: Ensure message	3	2

Rule ID	Description	Level	Count
	of the day is configured properly.		
19008	CIS Ubuntu Linux 22.04 LTS Benchmark v2.0.0.: Ensure network file system services are not in use.	3	2
19008	CIS Ubuntu Linux 22.04 LTS Benchmark v2.0.0.: Ensure nis server services are not in use.	3	2
19008	CIS Ubuntu Linux 22.04 LTS Benchmark v2.0.0.: Ensure nosuid option set on /dev/shm partition.	3	2
19008	CIS Ubuntu Linux 22.04 LTS Benchmark v2.0.0.: Ensure password failed attempts lockout includes root account.	3	2
19008	CIS Ubuntu Linux 22.04 LTS Benchmark v2.0.0.: Ensure password failed attempts lockout is configured.	3	2
19008	CIS Ubuntu Linux 22.04 LTS Benchmark v2.0.0.: Ensure permissions on /etc/passwd- are configured.	3	2
19008	CIS Ubuntu Linux 22.04 LTS Benchmark v2.0.0.: Ensure permissions on SSH public host key files are configured.	3	2
19008	CIS Ubuntu Linux 22.04 LTS Benchmark v2.0.0.: Ensure rsync services are not in use.	3	2
19009	CIS Ubuntu Linux 22.04 LTS Benchmark v2.0.0.: Ensure audit log files group owner is configured.	3	2
19009	CIS Ubuntu Linux 22.04 LTS Benchmark v2.0.0.: Ensure chrony is enabled and running.	3	2
19009	CIS Ubuntu Linux 22.04 LTS Benchmark v2.0.0.: Ensure cryptographic mechanisms are used to protect the integrity of audit tools.	3	2
19009	CIS Ubuntu Linux 22.04 LTS Benchmark v2.0.0.: Ensure journald Compress is configured.	3	2
19009	CIS Ubuntu Linux 22.04 LTS Benchmark v2.0.0.: Ensure journald ForwardToSyslog is disabled.	3	2
19009	CIS Ubuntu Linux 22.04 LTS Benchmark v2.0.0.: Ensure journald Storage is configured.	3	2
19009	CIS Ubuntu Linux 22.04 LTS Benchmark v2.0.0.: Ensure password complexity is configured.	3	2
19009	CIS Ubuntu Linux 22.04 LTS Benchmark v2.0.0.: Ensure password maximum sequential characters is configured.	3	2
19009	CIS Ubuntu Linux 22.04 LTS Benchmark v2.0.0.: Ensure password quality is enforced for the root user.	3	2
19009	CIS Ubuntu Linux 22.04 LTS Benchmark v2.0.0.: Ensure password same consecutive characters is configured.	3	2
19009	CIS Ubuntu Linux 22.04 LTS Benchmark v2.0.0.: Ensure systemd-journal-remote authentication is configured.	3	2
19005	SCA summary: CIS Microsoft Windows Server 2022 Benchmark v2.0.0: Score less than 30% (26)	9	2
2901	New dpkg (Debian Package) requested to install.	3	2
2902	New dpkg (Debian Package) installed.	7	2
2904	Dpkg (Debian Package) half configured.	7	2
501	New wazuh agent connected.	3	2
502	Wazuh server started.	3	2
60109	User account enabled or created	8	2

Rule ID	Description	Level	Count
60160	Domain Users Group Changed	5	2
60170	Users Group Changed	5	2
60642	Software protection service scheduled successfully.	3	2
61138	New Windows Service Created	5	2
67028	Special privileges assigned to new logon.	3	2
23502	The CVE-2023-49721 that affected lxd was solved due to an update in the agent or feed.	3	1
23502	The CVE-2024-6219 that affected lxd was solved due to an update in the agent or feed.	3	1
23502	The CVE-2025-54287 that affected lxd was solved due to an update in the agent or feed.	3	1
23502	The CVE-2025-54288 that affected lxd was solved due to an update in the agent or feed.	3	1
23502	The CVE-2025-54289 that affected lxd was solved due to an update in the agent or feed.	3	1
23502	The CVE-2025-54290 that affected lxd was solved due to an update in the agent or feed.	3	1
23502	The CVE-2025-54291 that affected lxd was solved due to an update in the agent or feed.	3	1
23504	CVE-2023-49721 affects lxd	7	1
23504	CVE-2025-54287 affects lxd	7	1
23504	CVE-2025-54288 affects lxd	7	1
23504	CVE-2025-54290 affects lxd	7	1
23504	CVE-2025-54291 affects lxd	7	1
23503	CVE-2024-6219 affects lxd	5	1