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

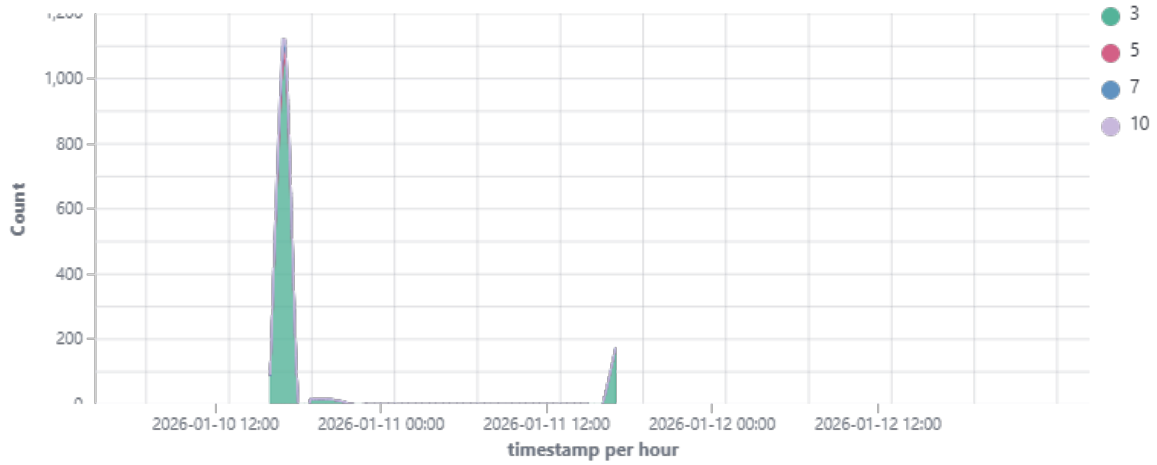
Threat hunting report

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

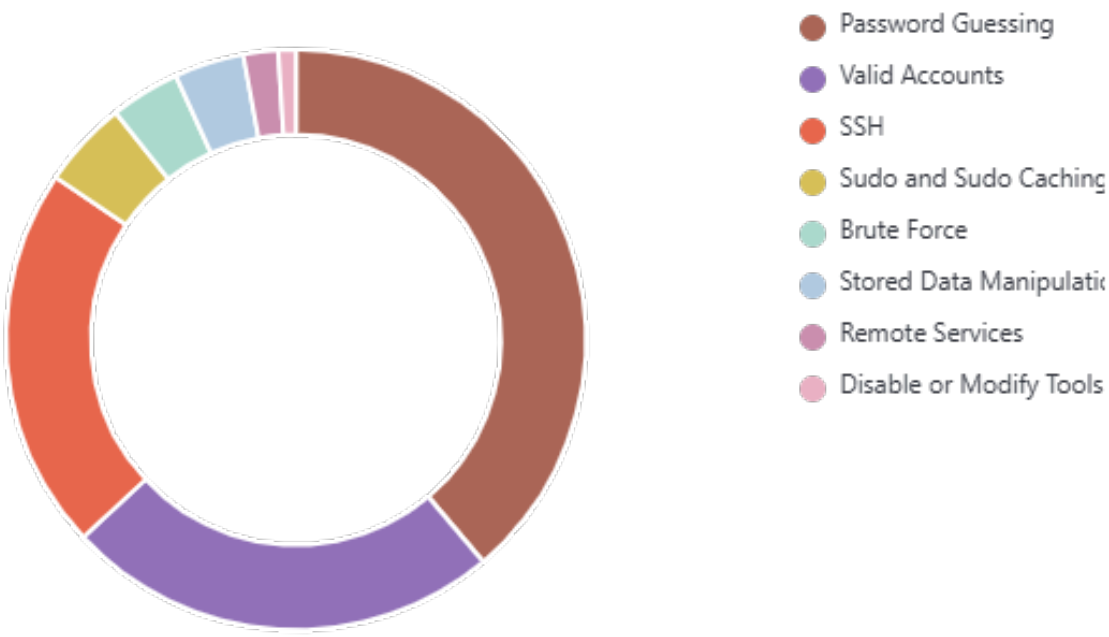
2026-01-10T03:22:38 to 2026-01-13T03:22:38

manager.name: ubuntulab

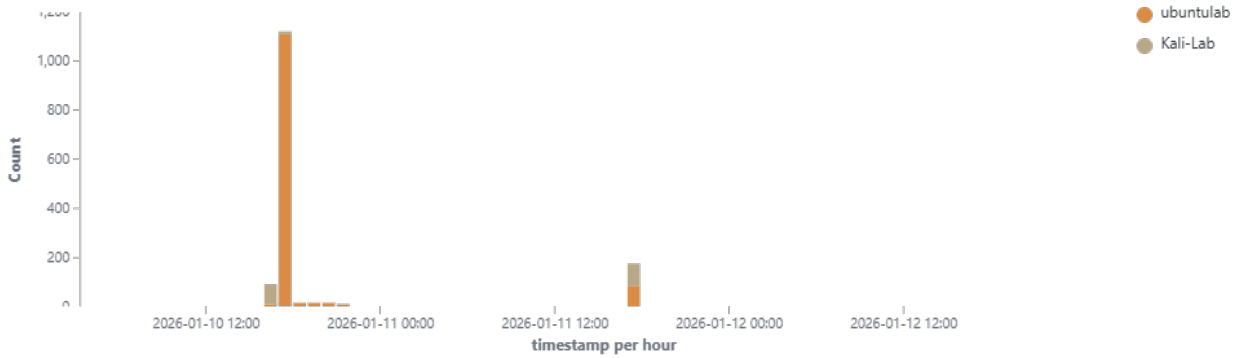
Top 10 Alert level evolution



Top 10 MITRE ATT&CKS



Alerts evolution - Top 5 agents



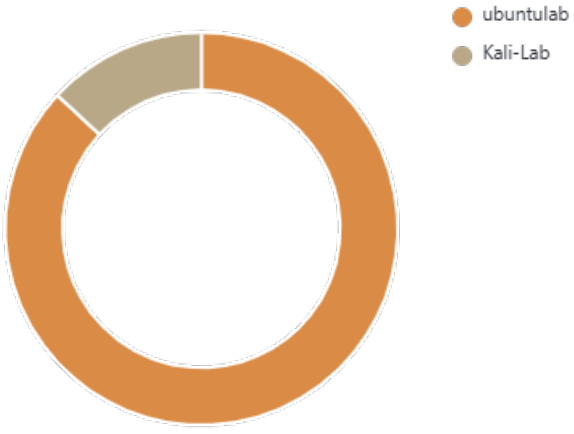
1,450
- Total -

0
- Level 12 or above alerts -

44
- Authentication failure -

25
- Authentication success -

Top 5 agents



Alerts summary

Rule ID	Description	Level	Count
86601	Suricata: Alert - GPL ICMP PING *NIX	3	803
86003	Docker: Error message	3	156
86601	Suricata: Alert - ET INFO Observed Discord Domain in DNS Lookup (discordapp .com)	3	83
86601	Suricata: Alert - ET INFO Observed Discord Domain (discordapp .com in TLS SNI)	3	71
86601	Suricata: Alert - ET INFO GNU/Linux APT User-Agent Outbound likely related to package management	3	65
86601	Suricata: Alert - ET INFO Possible Kali Linux hostname in DHCP Request Packet	3	59
651	Host Blocked by firewall-drop Active Response	3	32
86601	Suricata: Alert - ET SCAN Potential SSH Scan OUTBOUND	3	27
5501	PAM: Login session opened.	3	23
5760	sshd: authentication failed.	5	22
5503	PAM: User login failed.	5	18
510	Host-based anomaly detection event (rootcheck).	7	12
2904	Dpkg (Debian Package) half configured.	7	11
86601	Suricata: Alert - SURICATA SSH invalid banner	3	8
5502	PAM: Login session closed.	3	8
2902	New dpkg (Debian Package) installed.	7	7
5402	Successful sudo to ROOT executed.	3	5
86601	Suricata: Alert - SURICATA Applayer Detect protocol only one direction	3	4
550	Integrity checksum changed.	7	4
86601	Suricata: Alert - ET SCAN Potential SSH Scan	3	3
502	Wazuh server started.	3	3
503	Wazuh agent started.	3	3
5763	sshd: brute force trying to get access to the system. Authentication failed.	10	3
652	Host Unblocked by firewall-drop Active Response	3	3
86601	Suricata: Alert - ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack	3	2
86601	Suricata: Alert - SURICATA ICMPv4 unknown code	3	2
5715	sshd: authentication success.	3	2
86601	Suricata: Alert - ET INFO HTTP traffic on port 443 (POST)	3	1
86601	Suricata: Alert - ET INFO TLS Handshake Failure	3	1
86601	Suricata: Alert - ET SCAN NMAP OS Detection Probe	3	1
86601	Suricata: Alert - ET SCAN Potential VNC Scan 5800-5820	3	1
86601	Suricata: Alert - ET SCAN Suspicious inbound to MSSQL port 1433	3	1
86601	Suricata: Alert - ET SCAN Suspicious inbound to Oracle SQL port 1521	3	1

Rule ID	Description	Level	Count
86601	Suricata: Alert - ET SCAN Suspicious inbound to PostgreSQL port 5432	3	1
86601	Suricata: Alert - ET SCAN Suspicious inbound to mySQL port 3306	3	1
40704	Systemd: Service exited due to a failure.	5	1
506	Wazuh agent stopped.	3	1
5551	PAM: Multiple failed logins in a small period of time.	10	1