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

Security events report

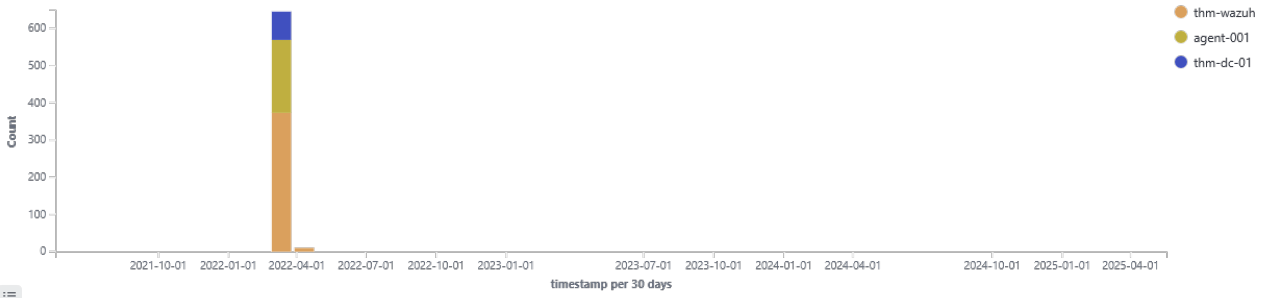
Browse through your security alerts, identifying issues and threats in your environment.

2021-05-18T11:29:52 to 2025-05-18T11:29:52

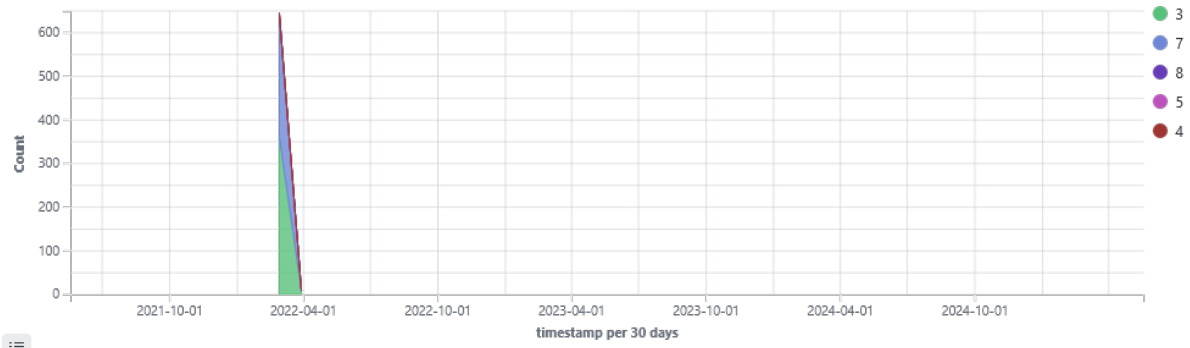
manager.name: thm-wazuh

Alerts

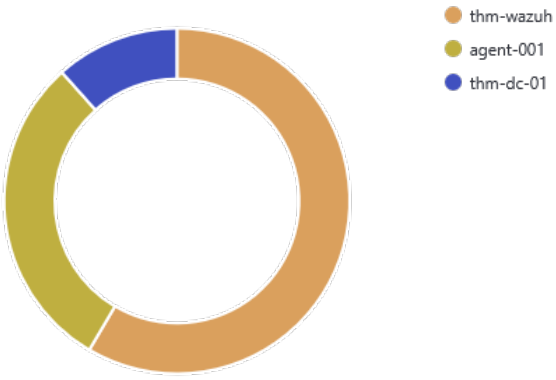
Alerts evolution Top 5 agents



Alert level evolution



Top 5 agents



Alerts summary

Rule ID	Description	Level	Count
5502	PAM: Login session closed.	3	46
5501	PAM: Login session opened.	3	43
5402	Successful sudo to ROOT executed.	3	40
2902	New dpkg (Debian Package) installed.	7	18
2904	Dpkg (Debian Package) half configured.	7	18
2901	New dpkg (Debian Package) requested to install.	3	15
19007	CIS Benchmark for Debian/Linux 10: Ensure default deny firewall policy	7	4
19007	CIS Benchmark for Debian/Linux 10: Ensure loopback traffic is configured	7	4
19004	SCA summary: CIS Benchmark for Debian/Linux 10: Score less than 50% (38)	7	4
502	Ossec server started.	3	3
19007	CIS Benchmark for Debian/Linux 10: Disable USB Storage	7	2
19007	CIS Benchmark for Debian/Linux 10: Ensure /tmp is configured	7	2
19007	CIS Benchmark for Debian/Linux 10: Ensure AIDE is installed	7	2
19007	CIS Benchmark for Debian/Linux 10: Ensure DCCP is disabled	7	2
19007	CIS Benchmark for Debian/Linux 10: Ensure ICMP redirects are not accepted	7	2
19007	CIS Benchmark for Debian/Linux 10: Ensure IP forwarding is disabled	7	2
19007	CIS Benchmark for Debian/Linux 10: Ensure IPv6 default deny firewall policy	7	2
19007	CIS Benchmark for Debian/Linux 10: Ensure IPv6 loopback traffic is configured	7	2
19007	CIS Benchmark for Debian/Linux 10: Ensure IPv6 router advertisements are not accepted	7	2
19007	CIS Benchmark for Debian/Linux 10: Ensure RDS is disabled	7	2
19007	CIS Benchmark for Debian/Linux 10: Ensure Reverse Path Filtering is enabled	7	2
19007	CIS Benchmark for Debian/Linux 10: Ensure SCTP is disabled	7	2
19007	CIS Benchmark for Debian/Linux 10: Ensure SSH AllowTcpForwarding is disabled	7	2
19007	CIS Benchmark for Debian/Linux 10: Ensure SSH Idle Timeout Interval is configured	7	2
19007	CIS Benchmark for Debian/Linux 10: Ensure SSH LoginGraceTime is set to one minute or less	7	2
19007	CIS Benchmark for Debian/Linux 10: Ensure SSH MaxAuthTries is set to 4 or less	7	2
19007	CIS Benchmark for Debian/Linux 10: Ensure SSH MaxStartups is configured	7	2
19007	CIS Benchmark for Debian/Linux 10: Ensure SSH X11 forwarding is disabled	7	2
19008	CIS Benchmark for Debian/Linux 10: Disable Automounting	3	2
19008	CIS Benchmark for Debian/Linux 10: Disable IPv6	3	2
19008	CIS Benchmark for Debian/Linux 10: Ensure AppArmor is enabled in the bootloader configuration	3	2
19008	CIS Benchmark for Debian/Linux 10: Ensure AppArmor is installed	3	2
19008	CIS Benchmark for Debian/Linux 10: Ensure Avahi Server is not enabled	3	2
19008	CIS Benchmark for Debian/Linux 10: Ensure CUPS is not enabled	3	2
19008	CIS Benchmark for Debian/Linux 10: Ensure DHCP Server is not enabled	3	2
19008	CIS Benchmark for Debian/Linux 10: Ensure DNS Server is not enabled	3	2
19008	CIS Benchmark for Debian/Linux 10: Ensure FTP Server is not enabled	3	2
19008	CIS Benchmark for Debian/Linux 10: Ensure HTTP Proxy Server is not enabled	3	2

Rule ID	Description	Level	Count
19008	CIS Benchmark for Debian/Linux 10: Ensure HTTP Server is not enabled	3	2
19008	CIS Benchmark for Debian/Linux 10: Ensure LDAP client is not installed	3	2
19008	CIS Benchmark for Debian/Linux 10: Ensure LDAP server is not enabled	3	2
19008	CIS Benchmark for Debian/Linux 10: Ensure NFS and RPC are not enabled	3	2
19008	CIS Benchmark for Debian/Linux 10: Ensure NIS Client is not installed	3	2
19008	CIS Benchmark for Debian/Linux 10: Ensure NIS Server is not enabled	3	2
19008	CIS Benchmark for Debian/Linux 10: Ensure SNMP Server is not enabled	3	2
19008	CIS Benchmark for Debian/Linux 10: Ensure SSH HostbasedAuthentication is disabled	3	2
19008	CIS Benchmark for Debian/Linux 10: Ensure SSH IgnoreRhosts is enabled	3	2
19008	CIS Benchmark for Debian/Linux 10: Ensure SSH LogLevel is appropriate	3	2
19009	CIS Benchmark for Debian/Linux 10: Ensure GDM login banner is configured	3	2
19009	CIS Benchmark for Debian/Linux 10: Ensure a table exists	3	2
19009	CIS Benchmark for Debian/Linux 10: Ensure base chains exist	3	2
19009	CIS Benchmark for Debian/Linux 10: Ensure chrony is configured	3	2
19009	CIS Benchmark for Debian/Linux 10: Ensure default deny firewall policy	3	2
19009	CIS Benchmark for Debian/Linux 10: Ensure ntp is configured	3	2
19009	CIS Benchmark for Debian/Linux 10: Ensure wireless interfaces are disabled	3	2
19003	SCA summary: Benchmark for Windows audit: Score less than 80% (70)	5	2
501	New ossec agent connected.	3	2
5403	First time user executed sudo.	4	2
5901	New group added to the system.	8	2
5902	New user added to the system.	8	2
19009	Benchmark for Windows audit: Ensure 'Always install with elevated privileges' is set to 'Disabled'	3	1
19009	Benchmark for Windows audit: Ensure 'Always prompt for password upon connection' is set to 'Enabled'	3	1
19009	Benchmark for Windows audit: Ensure 'Configure Offer Remote Assistance' is set to 'Disabled'	3	1
19009	Benchmark for Windows audit: Ensure 'Configure Solicited Remote Assistance' is set to 'Disabled'	3	1
19009	Benchmark for Windows audit: Ensure 'Configure registry policy processing: Do not apply during periodic background processing' is set to 'Enabled: FALSE'	3	1
19009	Benchmark for Windows audit: Ensure 'Devices: Allowed to format and eject removable media' is set to 'Administrators'	3	1
19009	Benchmark for Windows audit: Ensure 'Do not allow drive redirection' is set to 'Enabled'	3	1
19009	Benchmark for Windows audit: Ensure 'Do not allow passwords to be saved' is set to 'Enabled'	3	1
19009	Benchmark for Windows audit: Ensure 'Enable RPC Endpoint Mapper Client Authentication' is set to 'Enabled'	3	1
19009	Benchmark for Windows audit: Ensure 'MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)' is set to 'Disabled'	3	1
19009	Benchmark for Windows audit: Ensure 'MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disabled'	3	1
19009	Benchmark for Windows audit: Ensure 'MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disabled'	3	1
19009	Benchmark for Windows audit: Ensure 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)' is set to 'Enabled'	3	1
503	Ossec agent started.	3	1
506	Ossec agent stopped.	3	1

Rule ID	Description	Level	Count
5407	Successful sudo executed.	3	1