

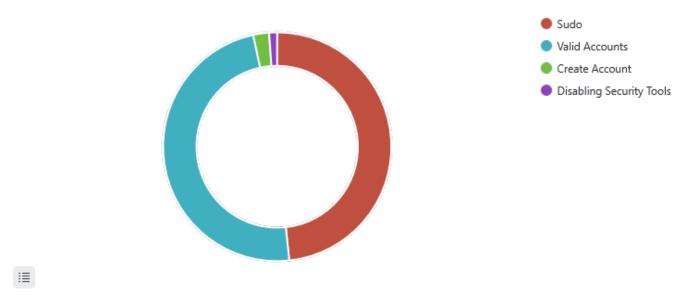
Security events report

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

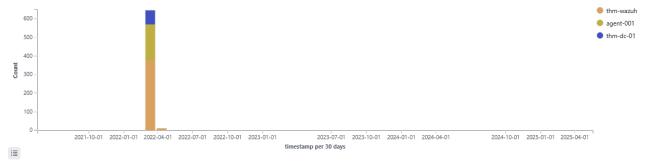
② 2021-05-18T11:29:52 to 2025-05-18T11:29:52

Q manager.name: thm-wazuh

Alerts

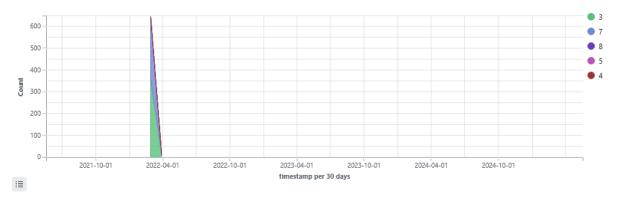


Alerts evolution Top 5 agents

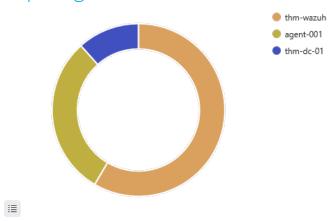




Alert level evolution



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



18008 CS Benchmark for Debian/Linux 10: Ensure HTTP Server is not enabled 3 2 18008 CS Benchmark for Debian/Linux 10: Ensure LTAP client is not installed 3 2 18008 CS Benchmark for Debian/Linux 10: Ensure NPS and RPC are not enabled 3 2 18008 CS Benchmark for Debian/Linux 10: Ensure NIS Server is not enabled 3 2 18008 CS Benchmark for Debian/Linux 10: Ensure NIS Server is not enabled 3 2 18008 CS Benchmark for Debian/Linux 10: Ensure NIS Server is not enabled 3 2 18008 CS Benchmark for Debian/Linux 10: Ensure SSH Server is not enabled 3 2 18008 CS Benchmark for Debian/Linux 10: Ensure SSH Legtevel is appropriate 3 2 18009 CS Benchmark for Debian/Linux 10: Ensure SSH Legtevel is appropriate 3 2 18000 CS Benchmark for Debian/Linux 10: Ensure base chains exist 3 2 18000 CS Benchmark for Debian/Linux 10: Ensure base chains exist 3 2 18000 CS Benchmark for Debian/Linux 10: Ensure base chains exist 3 2 18000 CS Benchmark for Debian/Linux 10: Ensure wire	Rule ID	Description	Level	Count
19008 CIS Benchmark for Debian/Linux 10. Ensure NTS and RPC are not enabled 3 2 19008 CIS Benchmark for Debian/Linux 10. Ensure NTS and RPC are not enabled 3 2 19008 CIS Benchmark for Debian/Linux 10. Ensure NTS and RPC are not enabled 3 2 19008 CIS Benchmark for Debian/Linux 10. Ensure NTS and RPC are not enabled 3 2 19008 CIS Benchmark for Debian/Linux 10. Ensure NTS 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 HostbasedAuthentication is disabled 3 2 19008 CIS Benchmark for Debian/Linux 10. Ensure SSH HostbasedAuthentication is disabled 3 2 19009 CIS Benchmark for Debian/Linux 10. Ensure SSH Logit-vell is appropriate 3 2 19009 CIS Benchmark for Debian/Linux 10. Ensure SSH Logit-vell is appropriate 3 2 19009 CIS Benchmark for Debian/Linux 10. Ensure a table exists 3 2 19009 CIS Benchmark for Debian/Linux 10. Ensure a table exists 3 2 19009 CIS Benchmark for Debian/Linux 10. Ensure configured 3 2 19009 CIS Benchmark for Debian/Linux 10. Ensure re pis configured 3 2 19009 CIS Benchmark for Debian/Linux 10. Ensure re pis configured 3 2 19009 CIS Benchmark for Debian/Linux 10. Ensure re pis configured 3 2 19009 CIS Benchmark for Debian/Linux 10. Ensure re pis configured 3 2 19009 CIS Benchmark for Debian/Linux 10. Ensure re pis configured 3 2 19009 CIS Benchmark for Debian/Linux 10. Ensure re pis configured 3 2 19009 CIS Benchmark for Debian/Linux 10. Ensure re pis configured 3 2 19009 CIS Benchmark for Debian/Linux 10. Ensure re pis configured 3 3 19009 CIS Benchmark for Debian/Linux 10. Ensure re pis configured 3 3 19009 CIS Benchmark for Debian/Linux 10. Ensure re pis configured 3 3 19009 CIS Benchmark for Debian/Linux 10. Ensure re pis configure CIP Conf	19008	CIS Benchmark for Debian/Linux 10: Ensure HTTP 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 SSH provided 3 3 2 19008 CIS Benchmark for Debian/Linux 10. Ensure SSH InsprecRhosts is enabled 3 2 19008 CIS Benchmark for Debian/Linux 10. Ensure SSH InsprecRhosts is enabled 3 2 19008 CIS Benchmark for Debian/Linux 10. Ensure SSH Logit-veil is appropriate 3 2 19008 CIS Benchmark for Debian/Linux 10. Ensure SSH Logit-veil is appropriate 3 2 19009 CIS Benchmark for Debian/Linux 10. Ensure SSH Logit-veil is appropriate 3 2 19009 CIS Benchmark for Debian/Linux 10. Ensure disprecable states of the state of th	19008	CIS Benchmark for Debian/Linux 10: Ensure LDAP client is not installed	3	2
19008 CIS Benchmark for Debiar/Linux 1D: Ensure NIS Client is not installed 3 2 19008 CIS Benchmark for Debiar/Linux 1D: Ensure NIS Client is not enabled 3 2 19008 CIS Benchmark for Debiar/Linux 1D: Ensure SNMP Server is not enabled 3 2 19008 CIS Benchmark for Debiar/Linux 1D: Ensure SNMP Server is not enabled 3 2 19008 CIS Benchmark for Debiar/Linux 1D: Ensure SSH HostbasedAuthentication is disabled 3 2 19008 CIS Benchmark for Debiar/Linux 1D: Ensure SSH I logit evel is appropriate 3 2 19009 CIS Benchmark for Debiar/Linux 1D: Ensure SSH I logit evel is appropriate 3 2 19009 CIS Benchmark for Debiar/Linux 1D: Ensure a table exists 3 2 19009 CIS Benchmark for Debiar/Linux 1D: Ensure a table exists 3 2 19009 CIS Benchmark for Debiar/Linux 1D: Ensure a table exists 3 2 19009 CIS Benchmark for Debiar/Linux 1D: Ensure default deny firewall policy 3 2 19009 CIS Benchmark for Debiar/Linux 1D: Ensure default deny firewall policy 3 2 19009 CIS Benchmark for Debiar/Linux 1D: Ensure default deny firewall policy 3 2 19009 CIS Benchmark for Debiar/Linux 1D: Ensure mtp is configured 3 2 19009 CIS Benchmark for Debiar/Linux 1D: Ensure ntp is configured 3 2 19009 CIS Benchmark for Debiar/Linux 1D: Ensure mtp is configured 3 2 19009 CIS Benchmark for Debiar/Linux 1D: Ensure wireless interfaces are disabled 3 2 19009 CIS Benchmark for Debiar/Linux 1D: Ensure wireless interfaces are disabled 3 2 19009 CIS Benchmark for Windows audit: Ensure Silvays Install with elevated privileges is set to Tisabled 3 2 19009 CIS Benchmark for Windows audit: Ensure Silvays Install with elevated privileges is set to Tisabled 3 1 19009 Benchmark for Windows audit: Ensure Silvays prompt for password upon connection' is set to Finabled 3 1 19009 Benchmark for Windows audit: Ensure Silvays prompt for password upon connection' is set to Finabled 3 1 19009 Benchmark for Windows audit: Ensure Silvays prompt for password upon connection' is set to Tinabled 3 1 19009 Benchmark for Windows audit: Ensure Silvays prompt for password upo	19008	CIS Benchmark for Debian/Linux 10: Ensure LDAP server is not enabled	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 SSH Postbased/Authentication is disabled 3 2 19008 CIS Benchmark for Debian/Linux 10: Ensure SSH porcePhosts is enabled 3 2 19008 CIS Benchmark for Debian/Linux 10: Ensure SSH porcePhosts is enabled 3 2 19009 CIS Benchmark for Debian/Linux 10: Ensure SSH porcePhosts is enabled 3 2 19009 CIS Benchmark for Debian/Linux 10: Ensure SSH porcePhosts is enabled 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 date exists 3 2 19009 CIS Benchmark for Debian/Linux 10: Ensure chrony is configured 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 frewall policy 3 2 19009 CIS Benchmark for Debian/Linux 10: Ensure default deny frewall policy 3 2 19009 CIS Benchmark for Debian/Linux 10: Ensure default deny frewall policy 3 2 19009 CIS Benchmark for Debian/Linux 10: Ensure default deny frewall policy 3 2 19000 CIS Benchmark for Debian/Linux 10: Ensure wireless interfaces are disabled 3 2 19000 CIS Benchmark for Debian/Linux 10: Ensure wireless interfaces are disabled 3 2 19000 SCA summary: Benchmark for Windows audit: Score less than 80% (70) 5 2 19001 New ossec agent connected. 3 2 19001 New group added to the system. 8 2 19002 Renchmark for Windows audit: Ensure 'Always install with elevated privileges' 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 Solicited 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 'Don tallow drive redirection' is set to 'Disabled' 3 1 19009 Benchmark for Windows audit: Ensure 'Don tallow drive redirection' is set to 'Enabled'	19008	CIS Benchmark for Debian/Linux 10: Ensure NFS and RPC are 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 HostbasedAuthentication is disabled 3 2 19008 CIS Benchmark for Debian/Linux 10: Ensure SSH ling level is appropriate 3 2 19009 CIS Benchmark for Debian/Linux 10: Ensure SSH ling level is appropriate 3 2 19009 CIS Benchmark for Debian/Linux 10: Ensure GDM ling in 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 chrony is configured 3 2 19009 CIS Benchmark for Debian/Linux 10: Ensure chrony is configured 3 2 19009 CIS Benchmark for Debian/Linux 10: Ensure chrony is configured 3 2 19009 CIS Benchmark for Debian/Linux 10: Ensure chrony is configured 3 2 19009 CIS Benchmark for Debian/Linux 10: Ensure chrony is configured 3 2 19009 CIS Benchmark for Debian/Linux 10: Ensure chrony is configured 3 2 19009 CIS Benchmark for Debian/Linux 10: Ensure may be configured 3 2 19009 CIS Benchmark for Debian/Linux 10: Ensure wireless interfaces are disabled 3 2 19009 CIS Benchmark for Debian/Linux 10: Ensure wireless interfaces are disabled 3 2 19009 CIS Benchmark for Debian/Linux 10: Ensure wireless interfaces are disabled 3 2 19009 CIS Benchmark for Debian/Linux 10: Ensure wireless interfaces are disabled 3 2 19009 CIS Benchmark for Windows audit: Ensure Wildows 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 Solicited Remote Assistance' is set to "Disabled" 3 1 19009 Benchmark	19008	CIS Benchmark for Debian/Linux 10: Ensure NIS Client is not installed	3	2
19008 CIS Benchmark for Debian/Linux 10: Ensure SSH logtevells appropriate 3 2 19008 CIS Benchmark for Debian/Linux 10: Ensure SSH logtevells appropriate 3 2 19009 CIS Benchmark for Debian/Linux 10: Ensure SSH logtevells appropriate 3 2 19009 CIS Benchmark for Debian/Linux 10: Ensure SSH logtevells appropriate 3 2 19009 CIS Benchmark for Debian/Linux 10: Ensure a table exists 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 deal table exists 3 2 19009 CIS Benchmark for Debian/Linux 10: Ensure deal table exists 3 2 19009 CIS Benchmark for Debian/Linux 10: Ensure dispanded 3 2 19009 CIS Benchmark for Debian/Linux 10: Ensure dispanded 3 2 19009 CIS Benchmark for Debian/Linux 10: Ensure dispanded 3 2 19009 CIS Benchmark for Debian/Linux 10: Ensure wireless interfaces are disabled 3 2 19009 CIS Benchmark for Debian/Linux 10: Ensure wireless interfaces are disabled 3 2 19009 CIS Benchmark for Windows audit: Score less than 80% (70) 5 2 1900 SCA summary: Benchmark for Windows audit: Score less than 80% (70) 5 2 1900 New group added to the system. 8 2 1900 Senchmark for Windows audit: Ensure 'Always install with elevated privileges' is set to 'Disabled' 3 1 1900 Benchmark for Windows audit: Ensure 'Always prompt for password upon connection' is set to 'Enabled' 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 Solicited Remote Assistance' is set to 'Disabled' 3 1 19009 Benchmark for Windows audit: Ensure 'Devices: Allowed to format and eject removable media' is set to 'Enabled' Administrators' 19009 Benchmark for Windows audit: Ensure 'Devices: Allowed to format and eject removable media' is set to 'Enabled' Administrators' 19009 Benchmark for Windows audit: Ensure 'Devices: Allowed to format and eject removable media' is set to 'Enabled' Administrators' 19009 Benchmark	19008	CIS Benchmark for Debian/Linux 10: Ensure NIS Server is not 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 SSH LogLevel is appropriate 3 2 19009 CIS Benchmark for Debian/Linux 10: Ensure a table exists 3 2 19009 CIS Benchmark for Debian/Linux 10: Ensure a table exists 3 2 19009 CIS Benchmark for Debian/Linux 10: Ensure than sexist 3 2 19009 CIS Benchmark for Debian/Linux 10: Ensure than sexist 3 2 19009 CIS Benchmark for Debian/Linux 10: Ensure than sexist 3 2 19009 CIS Benchmark for Debian/Linux 10: Ensure than sexist 3 2 19009 CIS Benchmark for Debian/Linux 10: Ensure than sexist 3 2 19009 CIS Benchmark for Debian/Linux 10: Ensure than sexist 3 2 19009 CIS Benchmark for Debian/Linux 10: Ensure wireless interfaces are disabled 3 2 19000 CIS Benchmark for Debian/Linux 10: Ensure wireless interfaces are disabled 3 2 19000 CIS Benchmark for Debian/Linux 10: Ensure wireless interfaces are disabled 3 2 19000 CIS Benchmark for Debian/Linux 10: Ensure wireless interfaces are disabled 3 2 19000 CIS Benchmark for Debian/Linux 10: Ensure wireless interfaces are disabled 3 2 19000 CIS Benchmark for Windows audit: Ensure Vilvays install with elevated privileges is set to 'Disabled' 3 2 19000 Deschmark for Windows audit: Ensure Vilvays install with elevated privileges is set to 'Disabled' 3 1 19000 Benchmark for Windows audit: Ensure Configure Offer Remote Assistance' is set to 'Disabled' 3 1 19000 Benchmark for Windows audit: Ensure Configure Offer Remote Assistance' is set to 'Disabled' 3 1 19000 Benchmark for Windows audit: Ensure 'Devices: Allowed to format and eject removable media' is set to 'Enabled' 3 1 19000 Benchmark for Windows audit: Ensure 'Devices: Allowed to format and eject removable media' is set to 'Enabled' 3 1 19000 Benchmark for Windows audit: Ensure 'Devices: Allowed to format and eject removable media' is set to 'Enabled' 3 1 19000 Benchmark for Windows audit: Ensure 'Devices: Allowed to format and eject removable media' is set to 'Enabled' 3 1 19000 Benchmark for Windows audit:	19008	CIS Benchmark for Debian/Linux 10: Ensure SNMP Server is not enabled	3	2
19008 CIS Benchmark for Debian/Linux 10: Ensure SSH Logl evel is appropriate 3 2 19009 CIS Benchmark for Debian/Linux 10: Ensure at table exists 3 2 19009 CIS Benchmark for Debian/Linux 10: Ensure at 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 base chains exist 3 2 19009 CIS Benchmark for Debian/Linux 10: Ensure base chains exist 3 2 19009 CIS Benchmark for Debian/Linux 10: Ensure default deny firewall policy 3 2 19009 CIS Benchmark for Debian/Linux 10: Ensure of Ensure default deny firewall policy 3 2 19009 CIS Benchmark for Debian/Linux 10: Ensure of Ensure default deny firewall policy 3 2 19009 CIS Benchmark for Debian/Linux 10: Ensure of Ensure default deny firewall policy 3 2 19000 CIS Benchmark for Debian/Linux 10: Ensure expense of Ensure default deny firewall policy 3 2 19000 CIS Benchmark for Debian/Linux 10: Ensure expense of Ensure default deny firewall policy 3 2 19000 CIS Benchmark for Debian/Linux 10: Ensure expense of Ensure default deny firewall policy 3 2 19000 SCA summary: Benchmark for Windows audit: Score less than 80% (70) 5 2 19000 New sosec agent connected. 3 2 19000 New group added to the system. 8 2 19000 New group added to the system. 8 2 19000 Benchmark for Windows audit: Ensure 'Always install with elevated privileges' is set to 'Disabled' 3 1 19000 Benchmark for Windows audit: Ensure 'Configure Offer Remote Assistance' is set to 'Disabled' 3 1 19000 Benchmark for Windows audit: Ensure 'Configure Offer Remote Assistance' is set to 'Disabled' 3 1 19000 Benchmark for Windows audit: Ensure 'Configure registry policy processing: Do not apply during periodic background 3 1 19000 Benchmark for Windows audit: Ensure 'Devices: Allowed to format and eject removable media' is set to 'Enabled' 3 1 19000 Benchmark for Windows audit: Ensure 'Devices: Allowed to format and eject removable media' is set to 'Enabled' 3 1 19000 Benchmark for Windows audit: Ensure 'Enable Rev Endpoint Mapper Client Authenticatio	19008	CIS Benchmark for Debian/Linux 10: Ensure SSH HostbasedAuthentication is disabled	3	2
19009 CIS Benchmark for Debian/Linux 10: Ensure a table exists 3 2 19009 CIS Benchmark for Debian/Linux 10: Ensure a table exists 3 2 19009 CIS Benchmark for Debian/Linux 10: Ensure a table exists 3 2 19009 CIS Benchmark for Debian/Linux 10: Ensure chrony is configured 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 default deny firewall policy 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 19003 SCA summary: Benchmark for Windows audit: Score less than 80% (70) 5 2 19004 New ossec agent connected. 3 2 19005 CIS Benchmark for Windows audit: Score less than 80% (70) 5 2 19006 New group added to the system. 8 2 19009 Benchmark for Windows audit: Ensure Wilways install with elevated privileges' is set to 'Disabled' 3 1 19009 Benchmark for Windows audit: Ensure Wilways 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 a processing is set to Enabled: ALSI Seanchmark for Windows audit: Ensure 'Do not allow drive redirection' is set to 'Enabled' 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 drive redirection' is set to 'Enabled' 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 'MSS: (DisablelPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing' is set to 'Enabled Highes	19008	CIS Benchmark for Debian/Linux 10: Ensure SSH IgnoreRhosts is enabled	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 default deny fiverwall policy 3 2 19009 CIS Benchmark for Debian/Linux 10: Ensure default deny fiverwall policy 3 2 19009 CIS Benchmark for Debian/Linux 10: Ensure default deny fiverwall policy 3 2 19009 CIS Benchmark for Debian/Linux 10: Ensure of default deny fiverwall policy 3 2 19009 CIS Benchmark for Debian/Linux 10: Ensure of the sconfigured 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 19004 CIS Benchmark for Windows audit: Score less than 80% (70) 5 2 19005 CIS Benchmark for Windows audit: Score less than 80% (70) 6 2 19006 CIS Benchmark for Windows audit: Ensure Mayays install with elevated privileges' is set to "Disabled" 3 2 19009 Enchmark for Windows audit: Ensure Mayays install with elevated privileges' is set to "Disabled" 3 1 19009 Benchmark for Windows audit: Ensure Mayays 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 "Finabled: Final Ensure "Configure registry policy processing: Do not apply during periodic background and processing" is set to "Finabled: Final Ensure" Do not allow drive redirection' is set to "Enabled" 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 drive redirection' is set to "Enabled" 3 1 19009 Benchmark for Windows audit: Ensure "Do not allow drive redirection' is set to "Enabled" 3 1 19009 Benchmark for W	19008	CIS Benchmark for Debian/Linux 10: Ensure SSH LogLevel is appropriate	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 not pis configured 3 2 19009 CIS Benchmark for Debian/Linux 10: Ensure not pis configured 3 2 19000 CIS Benchmark for Debian/Linux 10: Ensure not pis configured 3 2 19000 CIS Benchmark for Debian/Linux 10: Ensure wireless interfaces are disabled 3 2 19000 SCA summary. Benchmark for Windows audit: Score less than 80% (70) 5 2 19000 SCA summary. Benchmark for Windows audit: Score less than 80% (70) 5 2 19000 New ossec agent connected. 3 2 19001 New group added to the system. 4 2 19002 New group added to the system. 8 2 19002 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 'Configure Offer Remote Assistance' is set to 'Disabled' 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 registry policy processing: Do not apply during periodic background 3 1 19009 Benchmark for Windows audit: Ensure 'Configure registry policy processing: Do not apply during periodic background 3 1 19009 Benchmark for Windows audit: Ensure 'Devices: Allowed to format and eject removable media' is set to 'Enabled' 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 drive redirection' 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 'Enable RPC Endpoint Mapper Client Authentication' is set to 'Enabled' 3 1 19009 Benchmark for Windows audit: Ensure 'Basse (DisablelPSourceRouting) in Source routing p	19009	CIS Benchmark for Debian/Linux 10: Ensure GDM login banner is configured	3	2
19009 CIS Benchmark for Debian/Linux 10: Ensure chrony is configured CIS Benchmark for Debian/Linux 10: Ensure default deny firewall policy CIS Benchmark for Debian/Linux 10: Ensure default deny firewall policy CIS Benchmark for Debian/Linux 10: Ensure mp is configured 3 2 19009 CIS Benchmark for Debian/Linux 10: Ensure wireless interfaces are disabled 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 19004 New group added to the system. 8 2 19005 New group 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 and processing' is set to 'Enabled' Administrators' 19009 Benchmark for Windows audit: Ensure 'Devices: Allowed to format and eject removable media' is set to 'Enabled' Administrators' 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 'NSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)' is set to 'Disabled' 5 protectis against packet spoofing' is set to 'Enabled: Highest protection, source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disab	19009	CIS Benchmark for Debian/Linux 10: Ensure a table exists	3	2
19009 CIS Benchmark for Debian/Linux 10: Ensure default deny firewall policy 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 19003 SCA summary: Benchmark for Windows audit: Score less than 80% (70) 5 2 19003 SCA summary: Benchmark for Windows audit: Score less than 80% (70) 5 2 19003 SCA summary: Benchmark for Windows audit: Score less than 80% (70) 6 2 19004 New ossec agent connected. 3 2 19005 First time user executed sudo. 4 2 19006 New group added to the system. 8 2 19007 New group added to the system. 8 2 19008 Benchmark for Windows audit: Ensure 'Always install with elevated privileges' is set to 'Disabled' 3 1 19009 Benchmark for Windows audit: Ensure 'Ways 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 registry policy processing: Do not apply during periodic background a processing' is set to 'Enabled' A'dministrators' 19009 Benchmark for Windows audit: Ensure 'Devices: Allowed to format and eject removable media' is set to 'Enabled' 3 1 19009 Benchmark for Windows audit: Ensure 'Devices: Allowed to format and eject removable media' is set to 'Enabled' 3 1 19009 Benchmark for Windows audit: Ensure 'Devices: Allowed to format and eject removable media' is set to 'Enabled' 3 1 19009 Benchmark for Windows audit: Ensure 'Poeices: Allowed to format and eject removable media' is set to 'Enabled' 3 1 19009 Benchmark for Windows audit: Ensure 'Poeices: Allowed to format and eject removable media' is set to 'Enabled' 3 1 19009 Benchmark for Windows audit: Ensure 'Poeices: Allowed to format and eject removable media' is set to 'Enabled' 3 1 19009 Benchmark for Windows audit: Ensure 'MSS: (DisablelPSourceRouting IPv6) IP source routing protection level (protects against pa	19009	CIS Benchmark for Debian/Linux 10: Ensure base chains exist	3	2
19009 CIS Benchmark for Debian/Linux 10: Ensure ntp is configured 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 2 502 503 First time user executed sudo. 4 2 5090 New group added to the system. 8 2 5090 New user added to the system. 8 2 5090 Benchmark for Windows audit: Ensure 'Always install with elevated privileges' is set to 'Disabled' 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 Configure Conf	19009	CIS Benchmark for Debian/Linux 10: Ensure chrony is configured	3	2
19009 CIS Benchmark for Debian/Linux 10: Ensure wireless interfaces are disabled SCA summary: Benchmark for Windows audit: Score less than 80% (70) SCA summary: Benchmark for Windows audit: Score less than 80% (70) New ossec agent connected. Rew ossec agent connected. New group added to the system. Reg 2 Sepol New group added to the system. Reg 2 Sepol New user added to the system. Reg 3 New user added to the system. Reg 4 Sepol New user added to the system. Reg 5 Sepol New user added to the system. Reg 6 Sepol New user added to the system. Reg 7 Sepol New user added to the system. Reg 7 Sepol New user added to the system. Reg 8 Sepol New user added to the system. Reg 8 Sepol New user added to the system. Reg 9 Sepol New user added to the system. Reg 9 Sepol New user added to the system. Reg 9 Sepol New user added to the system. Reg 9 Sepol New user added to the system. Reg 9 Sepol New user added to the system. Reg 9 Sepol New user added to the system. Reg 9 Sepol New user added to the system. Reg 9 Sepol New user added to the system. Reg 9 Sepol New user added to the system. Reg 9 Sepol New user added to the system. Reg 9 Reg 19 Sepol New user added to the system. Reg 9 Reg 19 Sepol New user added to the system. Reg 9 Reg 19 Sepol New user added to the system. Reg 9 Reg 19 Sepol New user added to the system. Reg 9 Reg 19 Sepol New user added to the system. Reg 9 Reg 19 Sepol New user added to the system. Reg 9 Reg 19 Re	19009	CIS Benchmark for Debian/Linux 10: Ensure default deny firewall policy	3	2
SCA summary: Benchmark for Windows audit: Score less than 80% (70) 5 2	19009	CIS Benchmark for Debian/Linux 10: Ensure ntp is configured	3	2
501New ossec agent connected.325403First time user executed sudo.425901New group added to the system.825902New user added to the system.8219009Benchmark for Windows audit: Ensure 'Always install with elevated privileges' is set to 'Disabled'3119009Benchmark for Windows audit: Ensure 'Always prompt for password upon connection' is set to 'Enabled'3119009Benchmark for Windows audit: Ensure 'Configure Offer Remote Assistance' is set to 'Disabled'3119009Benchmark for Windows audit: Ensure 'Configure registry policy processing: Do not apply during periodic background processing' is set to 'Enabled'3119009Benchmark for Windows audit: Ensure 'Devices: Allowed to format and eject removable media' is set to 'Administrators'3119009Benchmark for Windows audit: Ensure 'Devices: Allowed to format and eject removable media' is set to 'Enabled'3119009Benchmark for Windows audit: Ensure 'Do not allow drive redirection' is set to 'Enabled'3119009Benchmark for Windows audit: Ensure 'Do not allow passwords to be saved' is set to 'Enabled'3119009Benchmark for Windows audit: Ensure 'MSS: (DisablelPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disabled'3119009Benchmark for Windows audit: Ensure 'MSS: (DisablelPSourceRouting) IP source routing is completely disabled'3119009Benchm	19009	CIS Benchmark for Debian/Linux 10: Ensure wireless interfaces are disabled	3	2
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 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 'MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)' is set to 'Disabled' 1 19009 Benchmark for Windows audit: Ensure 'MSS: (DisablelPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disabled' 1 19009 Benchmark for Windows audit: Ensure 'MSS: (DisablelPSourceRouting) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disabled' 1 19009 Benchmark for Windows audit: Ensure 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)' is set to 'Enabled' 1 19009 Benchmark for Windows audit: Ensure 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)' is set to 'Enabled' 1	19003	SCA summary: Benchmark for Windows audit: Score less than 80% (70)	5	2
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 'Configure Offer Remote Assistance' is set to 'Disabled' 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' 19009 Benchmark for Windows audit: Ensure 'Devices: Allowed to format and eject removable media' is set to 'Administrators' 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 'Do not allow passwords to be saved' is set to 'Enabled' 3 1 19009 Benchmark for Windows audit: Ensure 'MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)' is set to 'Disabled' 19009 Benchmark for Windows audit: Ensure 'MSS: (DisablelPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disabled' 19009 Benchmark for Windows audit: Ensure 'MSS: (DisablelPSourceRouting) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disabled' 19009 Benchmark for Windows audit: Ensure 'MSS: (SafeDilSearchMode) Enable Safe DLL search mode (recommended)' is set to 'Enabled' 19009 Benchmark for Windows audit: Ensure 'MSS: (SafeDilSearchMode) Enable Safe DLL search mode (recommended)' is set t	501	New ossec agent connected.	3	2
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' 19009 Benchmark for Windows audit: Ensure 'Devices: Allowed to format and eject removable media' is set to 'Administrators' 19009 Benchmark for Windows audit: Ensure 'Devices: Allowed to format and eject removable media' 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 'Po 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' 19009 Benchmark for Windows audit: Ensure 'MSS: (DisablelPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disabled' 19009 Benchmark for Windows audit: Ensure 'MSS: (DisablelPSourceRouting) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disabled' 19009 Benchmark for Windows audit: Ensure 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)' is set to 'Enabled' 19009 Benchmark for Windows audit: Ensure 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)' is set to	5403	First time user executed sudo.	4	2
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 3 1 19009 Benchmark for Windows audit: Ensure 'Devices: Allowed to format and eject removable media' is set to 'Enabled' 3 1 19009 Benchmark for Windows audit: Ensure 'Devices: Allowed to format and eject removable media' is set to 'Enabled' 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 'MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)' is set to 'Disabled' 1 19009 Benchmark for Windows audit: Ensure 'MSS: (DisablelPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disabled' 1 19009 Benchmark for Windows audit: Ensure 'MSS: (DisablelPSourceRouting) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disabled' 1 19009 Benchmark for Windows audit: Ensure 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)' is 3 1 19009 Benchmark for Windows audit: Ensure 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)' is 3 1 19009 Benchmark for Windows audit: Ensure 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)' is 3 1	5901	New group added to the system.	8	2
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 3 1 19009 Benchmark for Windows audit: Ensure 'Devices: Allowed to format and eject removable media' is set to 'Enabled' 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' 1 19009 Benchmark for Windows audit: Ensure 'MSS: (DisablelPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disabled' 1 19009 Benchmark for Windows audit: Ensure 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)' is 3 1 19009 Benchmark for Windows audit: Ensure 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)' is 3 1 19009 Benchmark for Windows audit: Ensure 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)' is 3 1	5902	New user added to the system.	8	2
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 3 1 19009 Benchmark for Windows audit: Ensure 'Devices: Allowed to format and eject removable media' is set to 'Administrators' 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: (DisablelPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disabled' 19009 Benchmark for Windows audit: Ensure 'MSS: (DisablelPSourceRouting) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disabled' 19009 Benchmark for Windows audit: Ensure 'MSS: (SafeDIISearchMode) Enable Safe DLL search mode (recommended)' is 3 1 20009 Benchmark for Windows audit: Ensure 'MSS: (SafeDIISearchMode) Enable Safe DLL search mode (recommended)' is 3 1 20009 Benchmark for Windows audit: Ensure 'MSS: (SafeDIISearchMode) Enable Safe DLL search mode (recommended)' is 3 1	19009	Benchmark for Windows audit: Ensure 'Always install with elevated privileges' is set to 'Disabled'	3	1
Benchmark for Windows audit: Ensure 'Configure Solicited Remote Assistance' is set to 'Disabled' Benchmark for Windows audit: Ensure 'Configure registry policy processing: Do not apply during periodic background processing' is set to 'Enabled: FALSE' Benchmark for Windows audit: Ensure 'Devices: Allowed to format and eject removable media' is set to 'Administrators' Benchmark for Windows audit: Ensure 'Do not allow drive redirection' is set to 'Enabled' Benchmark for Windows audit: Ensure 'Do not allow passwords to be saved' is set to 'Enabled' Benchmark for Windows audit: Ensure 'Enable RPC Endpoint Mapper Client Authentication' is set to 'Enabled' Benchmark for Windows audit: Ensure 'MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)' is set to 'Disabled' Benchmark for Windows audit: Ensure 'MSS: (DisablelPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disabled' Benchmark for Windows audit: Ensure 'MSS: (SafeDIISearchMode) Enable Safe DLL search mode (recommended)' is 3 1 set to 'Enabled' Sossec agent started. 3 1	19009	Benchmark for Windows audit: Ensure 'Always prompt for password upon connection' is set to 'Enabled'	3	1
Benchmark for Windows audit: Ensure 'Configure registry policy processing: Do not apply during periodic background processing' is set to 'Enabled: FALSE' 19009 Benchmark for Windows audit: Ensure 'Devices: Allowed to format and eject removable media' is set to 'Administrators' 19009 Benchmark for Windows audit: Ensure 'Do not allow drive redirection' is set to 'Enabled' 19009 Benchmark for Windows audit: Ensure 'Do not allow passwords to be saved' is set to 'Enabled' 19009 Benchmark for Windows audit: Ensure 'Enable RPC Endpoint Mapper Client Authentication' is set to 'Enabled' 19009 Benchmark for Windows audit: Ensure 'MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)' is set to 'Disabled' 19009 Benchmark for Windows audit: Ensure 'MSS: (DisablelPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disabled' 19009 Benchmark for Windows audit: Ensure 'MSS: (DisablelPSourceRouting) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disabled' 19009 Benchmark for Windows audit: Ensure 'MSS: (DisablelPSourceRouting) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disabled' 19009 Benchmark for Windows audit: Ensure 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)' is set to 'Enabled' 19009 Benchmark for Windows audit: Ensure 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)' is set to 'Enabled'	19009	Benchmark for Windows audit: Ensure 'Configure Offer Remote Assistance' is set to 'Disabled'	3	1
processing' is set to 'Enabled: FALSE' 19009 Benchmark for Windows audit: Ensure 'Devices: Allowed to format and eject removable media' is set to 'Administrators' 19009 Benchmark for Windows audit: Ensure 'Do not allow drive redirection' is set to 'Enabled' 19009 Benchmark for Windows audit: Ensure 'Do not allow passwords to be saved' is set to 'Enabled' 19009 Benchmark for Windows audit: Ensure 'Enable RPC Endpoint Mapper Client Authentication' is set to 'Enabled' 19009 Benchmark for Windows audit: Ensure 'MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)' is set to 'Disabled' 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' 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' 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' 19009 Benchmark for Windows audit: Ensure 'MSS: (SafeDIISearchMode) Enable Safe DLL search mode (recommended)' is set to 'Enabled' 19009 Benchmark for Windows audit: Ensure 'MSS: (SafeDIISearchMode) Enable Safe DLL search mode (recommended)' is set to 'Enabled'	19009	Benchmark for Windows audit: Ensure 'Configure Solicited Remote Assistance' is set to 'Disabled'	3	1
'Administrators' 19009 Benchmark for Windows audit: Ensure 'Do not allow drive redirection' is set to 'Enabled' 19009 Benchmark for Windows audit: Ensure 'Do not allow passwords to be saved' is set to 'Enabled' 19009 Benchmark for Windows audit: Ensure 'Enable RPC Endpoint Mapper Client Authentication' is set to 'Enabled' 19009 Benchmark for Windows audit: Ensure 'MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)' is set to 'Disabled' 19009 Benchmark for Windows audit: Ensure 'MSS: (DisablelPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disabled' 19009 Benchmark for Windows audit: Ensure 'MSS: (DisablelPSourceRouting) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disabled' 19009 Benchmark for Windows audit: Ensure 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)' is set to 'Enabled' 503 Ossec agent started. 3 1	19009		3	1
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' 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' 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' 19009 Benchmark for Windows audit: Ensure 'MSS: (SafeDIISearchMode) Enable Safe DLL search mode (recommended)' is set to 'Enabled' 503 Ossec agent started. 3 1	19009		3	1
Benchmark for Windows audit: Ensure 'Enable RPC Endpoint Mapper Client Authentication' is set to 'Enabled' Benchmark for Windows audit: Ensure 'MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)' is set to 'Disabled' 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' 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' Benchmark for Windows audit: Ensure 'MSS: (SafeDIISearchMode) Enable Safe DLL search mode (recommended)' is set to 'Enabled' Sossec agent started.	19009	Benchmark for Windows audit: Ensure 'Do not allow drive redirection' is set to 'Enabled'	3	1
Benchmark for Windows audit: Ensure 'MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)' is set to 'Disabled' 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' 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' Benchmark for Windows audit: Ensure 'MSS: (SafeDIISearchMode) Enable Safe DLL search mode (recommended)' is set to 'Enabled' Ossec agent started.	19009	Benchmark for Windows audit: Ensure 'Do not allow passwords to be saved' is set to 'Enabled'	3	1
to 'Disabled' 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' 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' 19009 Benchmark for Windows audit: Ensure 'MSS: (SafeDIISearchMode) Enable Safe DLL search mode (recommended)' is set to 'Enabled' 503 Ossec agent started. 3 1 1 2 3 1	19009	Benchmark for Windows audit: Ensure 'Enable RPC Endpoint Mapper Client Authentication' is set to 'Enabled'	3	1
(protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disabled' 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' 19009 Benchmark for Windows audit: Ensure 'MSS: (SafeDIISearchMode) Enable Safe DLL search mode (recommended)' is set to 'Enabled' 503 Ossec agent started. 3 1	19009		3	1
against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disabled' 19009 Benchmark for Windows audit: Ensure 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)' is set to 'Enabled' 503 Ossec agent started. 3 1	19009		3	1
set to 'Enabled' 503 Ossec agent started. 3 1	19009		3	1
	19009		3	1
506 Ossec agent stopped. 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