Sentinel Security Pack

Security Controls Reference

Safeguard Name	Description	Remediation
Antivirus Presence	Determines if anti-virus software is detected	
Audit Changes To Firewall Settings Enabled	Determines if the policies that cause events to be logged when changes are made to the Windows firewall are enabled	Available in Sentinel Pro
Audit Group Membership Changes Enabled	Determines if the policies that cause events to be logged when changes are made to group membership are enabled	Available in Sentinel Pro
Audit Logon Events Enabled	Determines if the policies that cause events to be logged when users log in are enabled	Available in Sentinel Pro
Audit Object Access Enabled	Determines if the policies that cause events to be logged when objects are accessed are enabled	Available in Sentinel Pro
Audit Of Account Creation Enabled	Determines if the policies that cause events to be logged when accounts are created are enabled	Available in Sentinel Pro
Audit Printer Events Enabled	Determines if auditing of printer events is enabled	Available in Sentinel Pro
DHCP Lease Duration	Determines if the DHCP lease duration is configured correctly	
Disabled Accounts	Determines if there is any account that is disabled and has not been logged into over the last 365 days	Available in Sentinel Pro
Do Not Allow Auto Logon	Determines if auto log in is disabled	Available in Sentinel Pro
Do Not Display Last Login Name	Determines if the name of the last user to log in is displayed at the logon screen	Available in Sentinel Pro
Event Log Permissions	Determines if only authorized accounts have full control of the event log folder	Available in Sentinel Pro
FIPS Encryption Enabled	Determines if FIPS-compliant encryption algorithms are in use	Available in Sentinel Pro
Guest Account Disabled	Determines if the Guest account is disabled	Available in Sentinel Pro
Inactive Accounts	Determines if there is any account that has not been logged into over the last 60 days	Available in Sentinel Pro
Inactive Automatic Logoff	Determines if there exists a scheduled task to log off users if the device has been inactive for up to 90 minutes	Available in Sentinel Pro
Login Notice Enabled	Determines if the login notice is enabled	Available in Sentinel Pro

Safeguard Name	Description	Remediation
Logon Failure Lockout Enabled	Determines if account lockout is enabled after too many incorrect log in attempts	Available in Sentinel Pro
Maintain Password History	Determines if passwords can be re-used for a set number of generations (4 for regular users, 6 for administrators)	Available in Sentinel Pro
Maximum Password Age	Determines if passwords have a maximum age (90 days for regular users, 60 for administrators)	Available in Sentinel Pro
Minimum NTLM Security Level	Determines if the minimum required session security level for NTLM SSP-based network connections is being enforced	Available in Sentinel Pro
Network Session Auto Disconnect	Determines if the LAN Manager session auto-disconnect setting is enabled	Available in Sentinel Pro
Operating System Supported	Determines if the current operating system is supported by the operating system vendor	
Password Complexity	Whether the password complexity policy is enabled	Available in Sentinel Pro
Password Length	Determines if the password length policy only allows passwords of 8 or more characters	Available in Sentinel Pro
Password Must Be Changed At First Login	Determines if users are required to change their password during their first login	Available in Sentinel Pro
Password Must Be Re-entered When Changing	Determines if the current password must be re-entered when changing it	
Passwords Are Hidden	Determines if passwords are hidden when entered	
Require CHAP Encryption Authentication	Determines if CHAP, and not PAP, is used for encryption and security	
Require Full Disk Encryption	Determines if full disk encryption is required for mobile devices	
Screen Saver Idle Time	Determines if a short idle time has been set for screensavers	Available in Sentinel Pro
Screen Saver Passwords	Determines if screensavers for all users are password-protected	Available in Sentinel Pro
Shares Disallow Everyone Group	Determines if network shares disallow the Everyone group	Available in Sentinel Pro
System Clock Sync	Determines if the system clock is set to be synchronized regularly	Available in Sentinel Pro
Unique Group Names	Determines if groups have unique names	
Unique User Names	Determines if users have unique names	
Use Kerberos For Network Access	Determines if Kerboros is used to enable user privilege/resources to access the organization's network	
WannaCry Ransonware	Determines if system is vulnerable to the WannaCrypt ransomware by checking patch version	
Windows Firewall Auto Start	Determines if the Windows firewall is set to start automatically	Available in Sentinel Pro
Windows Firewall Enabled For All Profiles	Determines if the Windows firewall is enabled for all profiles	Available in Sentinel Pro
Windows Firewall Running	Determines if the Windows firewall is running	Available in Sentinel Pro

Additional Controls available in Silect Sentinel Pro Security Pack

In addition to remediation capabilities for the controls identified above, the following additional controls are available in Silect Sentinel Pro Security Pack:

Safeguard Name	Description	Remediation
Certificates Valid	Determine if all installed certificates have a valid path to a trusted root certificate and not be revoked	✓
Detect Java	Determines if Java has been detected	
Disallow Remote Admin Share Access	Determines if administrative shares can be accessed remotely using local accounts	✓
Maximum Certificate Lifespan	Determines if PKI certificates have lifespans that do not exceed 3 years	✓
Require Sealed Secure Channel	Determines if outgoing secure channel traffic is set to be encrypted whenever possible	✓
Require Securable File System	Determines if securable file system is used for storage media	
Require Secure Boot	Determines if Secure Boot is in use	
Require Signed Or Sealed Secure Channel	Determines if secure channel communications be either digitally signed or encrypted	✓
Require Signed Secure Channel	Determines if outgoing secure channel traffic is set to be digitally signed when possible	✓
Web Browser Blocks Java	Determines if Java (if installed) is blocked by the web browser	✓