Continue



Showing latest CIS Benchmarks for "See All" Amazon Linux 2014.09 (1.0.0) Amazon Linux 2014.09 (1.0.0) Amazon Linux 2014.09 (1.0.0) To further explore this Benchmark, click here. If you want to tailor the security recommendations of this Benchmark, you can do so using a CIS SecureSuite MembershipAmazon Web Services (1.2.0) Amazon Web Services Foundations (5.0.0) AWS Compute Services (1.1.0) AWS Storage Services (1.0.0) AWS Database Services (1.0.0) To further explore this Benchmark, click here. If you want to tailor the security recommendations of this Benchmark Available versions include: Apache Cassandra 4.1 (1.0.0) Apache Cassandra 4.0 (1.1.0) Apache Cassandra 3.11 (1.1.0) To further explore this Benchmark, click here. If you want to tailor the security recommendations of this Benchmark, you can do so using a CIS SecureSuite MembershipApache HTTP Server 2.4 (2.2.0) Apache HTTP Server 2.2 (3.6.0) To further explore this Benchmark, click here. If you want to tailor the security recommendations of this Benchmark, you can do so using a CIS SecureSuite MembershipApache Tomcat 10.1 (1.0.0) Apache Tomcat 10 (1.1.0) Apache Tomcat 9 (1.2.0) Apache Tomcat 9 (1.2.0) Apache Tomcat 7 (1.1.0) To further explore this Benchmark, click here. If you want to tailor the security recommendations of this Benchmark, you can do so using a CIS SecureSuite MembershipApple iOS 18 (1.1.0) Apple iPadOS 17 (1.1.0) Apple iPadOS 17 (1.1.0) Apple iPadOS 17 (1.1.0) Apple iPadOS 17 (1.1.0) Apple iOS 17 (1.1.0) Apple iOS 17 (1.1.0) Apple iOS 17 (1.1.0) Apple iOS 18 (1.1.0) Apple iOS 18 (1.1.0) Apple iPadOS 18 (1.1.0) Apple iPadOS 18 (1.1.0) Apple iOS 18 (1.1. Microsoft Intune for Apple iOS 17 and iPadOS 17 (1.0.0) To further explore this Benchmark, you can do so using a CIS SecureSuite MembershipApple macOS Download The Benchmark Available versions include: Apple macOS 13.0 Ventura (3.1.0) Apple macOS 14.0 Sonoma (2.1.0) Apple macOS 15.0 Sequoia (1.1.0) Apple macOS 12.0 Monterey (4.0.0) Apple macOS 12.0 Monterey (4.0.0) Apple macOS 13.0 Ventura Cloud-tailored (1.1.0) Apple macO (3.0.0) Apple macOS 10.14 Mojave (2.0.0) Apple macOS 10.12 (1.2.0) Apple macOS 10.13 (1.1.0) Apple oSX 10.13 (1.2.0) Apple oSX want to tailor the security recommendations of this Benchmark, you can do so using a CIS SecureSuite MembershipCentOS Linux 7 (4.0.0) CentOS Linux 8 (2.0.0) To further explore this Benchmark, click here. If you want to tailor the security recommendations of this Benchmark, you can do so using a CIS SecureSuite MembershipCisco Download The Benchmark Available versions include: Cisco IOS XE 17.x (2.2.0) Cisco IOS XE 16.x (2.2.0) Cisco IOS XE 17.x (2.2.0) Cisco IOS XE 18.x (2.2.0) Cisco IO (4.0.0) Cisco Firepower Threat Defense (1.0.0) Cisco Firewall (4.1.0) Cisco Firewall (4.1.0) Cisco IOS XR 7.x (1.0.0) Cisco IOS 17.x (2.0.0) Cisco IOS 17.x (2.0.0) Cisco IOS 18. (2.0.0) To further explore this Benchmark, you can do so using a CIS SecureSuite MembershipDebian Linux Download The Benchmark Available versions include: Debian Linux 12 (1.1.0) Debian Linux 14 (2.0.0) Debian Linux 8 (2.0.2) Debian Linux 8 (2.0.2) Debian Linux 8 (2.0.2) Debian Linux 9 (1.0.0) To further explore this Benchmark, click here. If you want to tailor the security recommendations of this Benchmark, you can do so using a CIS SecureSuite MembershipExtreme Networks Download The Benchmark Available versions include: ExtremeNetworks SLX-OS-20.X.X (1.0.1) Secure Suite Membership Google Chrome Enterprise Core Browser (1.0.0) Google Chrome Enterprise Chrome Enterprise C the security recommendations of this Benchmark, you can do so using a CIS SecureSuite MembershipGoogle Cloud Platform Download The Benchmark, you can do so using a CIS SecureSuite MembershipGoogle Cloud Platform Download The Benchmark, you can do so using a CIS SecureSuite MembershipGoogle Cloud Platform Download The Benchmark, you can do so using a CIS SecureSuite MembershipGoogle Cloud Platform Download The Benchmark, you can do so using a CIS SecureSuite MembershipGoogle Cloud Platform Download The Benchmark, you can do so using a CIS SecureSuite MembershipGoogle Cloud Platform Download The Benchmark, you can do so using a CIS SecureSuite MembershipGoogle Cloud Platform Download The Benchmark, you can do so using a CIS SecureSuite MembershipGoogle Cloud Platform Download The Benchmark, you can do so using a CIS SecureSuite MembershipGoogle Cloud Platform Download The Benchmark, you can do so using a CIS SecureSuite MembershipGoogle Cloud Platform Download The Benchmark Available versions include: recommendations of this Benchmark, you can do so using a CIS SecureSuite MembershipIBM Db2 Download The Benchmark Available versions include: IBM DB2 10 (1.1.0) To further explore this Benchmark, click here. If you want to tailor the security recommendations of this Benchmark, you can do so using a CIS SecureSuite MembershipIBM i Download The Benchmark Available versions include: IBM i V7R3M0 (2.0.0) IBM i V7R3M0 (1.0.2) IBM i V7R3M0 (1.0.0) To further explore this Benchmark, click here. If you want to tailor the security recommendations of this Benchmark, you can do so using a CIS SecureSuite MembershipIBM Z System Download The Benchmark Available versions include: IBM z/OS VR5 2with RACF (1.0.0) IBM Db2 13 for z/OS (1.0.0) IBM Z Linux (1.0.0) recommendations of this Benchmark, you can do so using a CIS SecureSuite MembershipKubernetes Engine (GKE) (1.8.0) Google Kubernetes Engine (GKE) Autopilot (1.2.0) Red Hat OpenShift Container Platform (1.8.0) Oracle Cloud Infrastructure Container Engine for Kubernetes (OKE) (1.7.0) Amazon Elastic Kubernetes Service (EKS) (1.7.0) Azure Kubernetes V1.23 (1.0.1) Kubernetes V1.23 (1.0.1) RedHat OpenShift Container Platform v4 (1.1.0) Alibaba Cloud Container Service For Kubernetes (ACK) (1.0.0) To further explore this Benchmark, you can do so using a CIS SecureSuite MembershipMicrosoft Azure Download The Benchmark, you can do so using a CIS SecureSuite MembershipMicrosoft Azure Foundations (4.0.0) Microsoft Azure Storage Services (1.0.0) Microsoft Azure Database Services (1.0.0) To further explore this Benchmark, you can do so using a CIS SecureSuite MembershipMicrosoft Dynamics 365 Power Platform Download The Benchmark Available versions include Microsoft Dynamics 365 Power Platform (1.0.0) To further explore this Benchmark, you can do so using a CIS SecureSuite MembershipMicrosoft Exchange Server 2019 (1.0.0) Microsoft Exchange Server 2019 (1.0.0) Micros Exchange Server 2016 (1.0.0) Microsoft Exchange Server 2010 (1.1.0) To further explore this Benchmark, you can do so using a CIS SecureSuite MembershipMicrosoft IIS Download The Benchmark Available versions include: Microsoft IIS 10 (1.2.1) Microsoft IIS 7 (1.8.0) To further explore this Benchmark, you can do so using a CIS SecureSuite MembershipMicrosoft Intune Apple iOS, iPadOS, macOS Download The Benchmark Available versions include: Apple MacOS 15.0 Sequoia Intune (1.0.0) Apple MacOS 14.0 Sonoma Intune (1.0.0) To further explore this Benchmark, vou can do so using a CIS SecureSuite MembershipMicrosoft Intune for Microsoft Windows Download The Benchmark Available versions include: Microsoft Intune for Windows 11 (4.0.0) Microsoft Intune for Windows 10 (4.0.0) Microsoft Intune for Windows 10 Release 2004 (1.0.1) To further explore this Benchmark, you can do so using a CIS SecureSuite MembershipMicrosoft Office Download The Benchmark Available versions include: Microsoft Office Excel 2013 (1.0.1) Microsoft Office Excel 2015 (1.0.1) Microsoft Office Excel 2015 (1.0.1) Microsoft Office Excel 2015 (1.0.1) Microsoft Office Excel 2016 (1.0.1) Microsoft Office Excel 2 Access 2016 (1.0.1) Microsoft Office Word 2013 (1.1.0) Microsoft Office Word 2013 (1.0.0) Microsoft Office Word 2013 (1.0 Benchmark, click here. If you want to tailor the security recommendations of this Benchmark, you can do so using a CIS SecureSuite MembershipMicrosoft SharePoint 2019 (1.0.0) Microsoft SharePoint 2016 (1.1.0) To further explore this Benchmark, click here. If you want to tailor the security recommendations of this Benchmark, you can do so using a CIS SecureSuite MembershipMicrosoft SQL Server 2019 (1.5.0) Microsoft SQL Server 2017 (1.3.0) Microsoft SQL Server 2016 (1.4.0) Microsoft SQL Server 2008 R2 (1.7.0) Microsoft SQL Server 2012 (1.6.0) Microsoft SQL Server 2012 (1. MembershipMicrosoft Web Browser Download The Benchmark Available versions include: Microsoft Internet Explorer 10 (1.1.0) Microsoft Internet Explorer 10 (1.1.0) Microsoft Internet Explorer 10 (1.1.0) Microsoft Internet Explorer 11 (1.0.0) Microsoft Internet Explorer 10 (1.1.0) Microsoft Int can do so using a CIS SecureSuite MembershipMicrosoft Windows 10 Stand-alone (4.0.0) Microsoft Windows 11 Enterprise (4.0.0) Microsoft Windows 11 Enterprise (4.0.0) Microsoft Windows 10 EMS Gateway (3.0.0) Microsoft Windows (3.0.0) Microsoft Window Windows 10 Enterprise Release 20H2 (1.11.0) Microsoft Windows 10 Enterprise Release 20H2 (1.10.1) Microsoft Windows 20H2 (1.10.1) Microsoft Windows 20H2 (1. (1.7.1) Microsoft Windows 10 Enterprise Release 1809 (1.6.1) Microsoft Windows 10 Enterprise Release 1703 (1.5.0) Microsoft Windows 10 Enterprise Release 1703 (1.5.0) Microsoft Windows 10 Enterprise Release 1803 (1.5.0) Microsoft Windows 10 Enterprise Release 1703 (1.5.0) Microsoft Windows 10 Enterprise Release 1809 (1.6.1) Microsoft Windows 10 Enterprise Release 1800 (1.6.1) Microsoft Windows 10 Enterprise Release 1800 (1.6.1) Microsoft Windows 10 Ent Windows 7 (3.0.0) Microsoft Windows 8.1 (2.2.0) Microsoft Windows Windows Server Download The Benchmark Available versions include: Microsoft Windows Server 2022 Stand-alone (1.0.0) Microsoft Windows Server 2022 STIG (2.0.0) Microsoft Windows Server 2022 STIG (2. Windows Server 2016 STIG (3.0.0) Microsoft Windows Server 2012 R2 (3.0.0) Microsoft Windows Server 2012 (1.0.0) Azure Compute Microsoft Windows Server 2012 (1.0.0) Azure Compute Microsoft Windows
Server 2012 (1.0.0) Micros Server 2008 (non-R2) (3.3.0) Microsoft Windows Server 2012 R2 (1.0.0) Microsoft Windows Server 2008 (2.1.0) Microsoft Windows Server 2008 (3.1.0) Microsoft Windows Server 2008 R2 (3.3.0) Microsoft Windows Server 2018 R2 (1.0.0) Microsoft Wind Windows Server 2012 (1.0.0) To further explore this Benchmark, click here. If you want to tailor the security recommendations of this Benchmark Available versions include: MongoDB 7 (1.0.0) MongoDB 5 (1.2.0) MongoDB 5 (1.2.0) MongoDB 3.6 (1.1.0) MongoDB 4 (1.0.0) MongoDB 3.4 (1.0.0) MongoDB 3.2 (1.0.0) MongoDB 3.2 (1.0.0) MongoDB (1.0.0) To further explore this Benchmark, you can do so using a CIS SecureSuite MembershipMozilla Firefox Download The Benchmark Available versions include: Mozilla Firefox ESR GPO (1.0.0) Mozilla Firefox 102 ESR (1.0.0) Mozilla Firefox 38 ESR (1.0.0) 19c (1.2.0) Oracle Database 18c (1.1.0) Oracle Database 12c (3.0.0) Oracle Database 12c (3.0.0) Oracle Database 12c (3.0.0) Oracle Database 12c (3.0.0) Oracle Database 18c (1.1.0) Oracle Database 18c (1.1.0) Oracle Database 18c (1.0.0) To further explore this Benchmark, you can do so using a CIS SecureSuite MembershipOracle Linux Download The Benchmark Available versions include: Oracle Linux 9 (2.0.0) Oracle Linux 9 (2.0.0) Oracle Linux 8 (3.0.0) Oracle Linux 8 (3.0.0) Oracle Linux 8 (3.0.0) Oracle Linux 9 (2.0.0) Oracle Linux 9 (2.0.0) Oracle Linux 9 (2.0.0) Oracle Linux 8 (3.0.0) Oracle Linux 9 (2.0.0) Oracle versions include: Oracle MySQL Community Server 8.4 (1.0.0) Oracle MySQL Enterprise Edition 8.4 (1.0.0) Oracle MySQL Enterprise Edition 5.7 (2.0.0) Oracle MySQL Enterprise Edition 5.7 (2.0.0) Oracle MySQL Enterprise Edition 5.8 (2.0.0) Oracle MySQL Enterprise Edition 5.7 (2.0.0) Oracle MySQL Enterprise Edition 5.8 (2.0.0) Oracle MySQL Enterprise Edition 5.7 (2.0.0) Oracle MySQL Enterprise Edition 5.8 (2.0.0) Oracle Community Server 5.6 (2.0.0) To further explore this Benchmark, click here. If you want to tailor the security recommendations of this Benchmark Available versions include: Oracle Solaris 11.4 (1.1.0) Oracle Solaris 11.1 (1.0.0) Oracle Solaris 11.1 (1.0. further explore this Benchmark, click here. If you want to tailor the security recommendations of this Benchmark, you can do so using a CIS SecureSuite MembershipPalo Alto Firewall 10 (1.2.0) Palo Alto Firewall 6 (1.0.0) Palo Alto Firewall 7 (1.0.0) Palo Alto Firewall 8 (1.0.0) Palo Alto Firewall 9 (1.0.1) To further explore this Benchmark, you can do so using a CIS SecureSQL 15 (1.2.0) PostgreSQL 17 (1.2.0) PostgreSQL 17 (1.2.0) PostgreSQL 17 (1.2.0) PostgreSQL 18 (1.0.0) PostgreSQL 14 (1.2.0) PostgreSQL 12 (1.1.0) PostgreSQL 12 (1.1.0) PostgreSQL 12 (1.1.0) PostgreSQL 13 (1.2.0) PostgreSQL 13 (1.2.0) PostgreSQL 13 (1.2.0) PostgreSQL 13 (1.2.0) PostgreSQL 14 (1.2.0) PostgreSQL 14 (1.2.0) PostgreSQL 15 (1.2.0) PostgreSQL 15 (1.2.0) PostgreSQL 16 (1.2.0) PostgreSQL 16 (1.2.0) PostgreSQL 17 (1.2.0) PostgreSQL 18 (1.2.0) PostgreSQL 18 (1.2.0) PostgreSQL 18 (1.2.0) PostgreSQL 18 (1.2.0) PostgreSQL 19 Enterprise Linux Download The Benchmark Available versions include: Red Hat Enterprise Linux 9 (2.0.0) Red Hat Enterprise Linux 8 (3.0.0) Red Hat Enterprise Linux 8 (3.0.0) Red Hat Enterprise Linux 7 (4.0.0) Red Hat Enterprise Linux 8 (3.0.0) Red Hat Enterprise Linux 7 (4.0.0) Red Hat Enterprise Linux 8 (3.0.0) Red Hat Enterprise Linux 9 (3.0.0) Red Hat Enterprise Linux 8 (3.0.0) Red Hat Enterprise Linux 8 (3.0.0) Red Hat Enterprise Linux 8 (3.0.0) Red Hat Enterprise Linux 9 (3.0.0) Red Hat Enterprise Linux 8 (3.0.0) Red Hat Enterprise SUSE Linux Enterprise 11 (2.1.1) SUSE Linux Enterprise Server 12 (1.0.0) SUSE Linux Enterprise Server 11 (1.0.0) To further explore this Benchmark, you can do so using a CIS SecureSuite MembershipUbuntu Linux Download The Benchmark Available versions include: Ubuntu Linux 24.04 LTS STIG (1.0.0) Ubuntu Linux 22.04 LTS (2.0.0) Ubuntu Linux 20.04 LTS (2.0.0) Ubuntu Linux 24.04 LTS (2.0.0) Ubuntu Linux 18.04 LTS (2.0.0) Ubuntu Linux 24.04 LTS (2.0.0) Ubuntu Linux 24.0 ESXi 6.7 (1.3.0) VMware ESXi 6.5 (1.0.0) VMware ESXi 5.5 (1.2.0) To further explore this Benchmark, click here. If you want to tailor the security recommendations of this Benchmark, you can do so using a CIS SecureSuite Membership This document provides prescriptive guidance for establishing a secure configuration posture for Microsoft Windows. This secure configuration guide is based on Windows 11 and is intended for all versions of the Windows 11 operating system, including older versions. This secure configuration guide was tested against Microsoft Windows 11 Release 23H2 Enterprise. To ensure all new and updated group policy objects (GPOs) are installed on the system. please download the latest version of the ADMX/ADML templates for Windows 11. Templates can be downloaded from Microsoft at: Download ADMX Templates for Windows 11 2023 Update [23H2] from Official Microsoft at: Download ADMX Templates for Windows 11. Templates for Windows 11. Templates can be downloaded from Microsoft at: Download ADMX Templates for Windows 11. Templates for Wind have identified ways to improve this guide, please write us at . Checklist Role: Known Issues: Not provided. Target Audience: The Windows CIS Microsoft Windows Benchmarks are written for Active Directory domain-joined systems using Group Policy, not standalone/workgroup systems. Adjustments/tailoring to some recommendations will be needed to maintain functionality if attempting to implement CIS hardening on standalone systems or a system running in the cloud. Target Operational Environment: Managed Specialized Security-Limited Functionality (SSLF) Testing Information: Not provided. Regulatory Compliance: Not provided. Comments/Warnings/Miscellaneous: Not provided. Disclaimer: Not provided. Product Support: Not last modified on 04/19/2024 The project started as a simple hardening list for Windows 10. After some time, Hardening Kitty was created to simplify the hardening Win10. And of course my own hardening list. This is a hardening checklist that can be used in private and business environments for hardening Windows 10. The checklist can be used for all Windows versions, but in Windows 10 Home the Group Policy Editor is not integrated and the adjustment must be done directly in the registry. For this, there is the HailMary mode from HardeningKitty. The settings should be seen as security and privacy recommendation and should be carefully checked whether they will affect the operation of your infrastructure or impact the usability. The project started with the creation of a simple hardening checklist for Windows 10. The focus has shifted to the audit of various well-known frameworks / benchmarks and Microsoft Security Baselines are supported. With the development of the HailMary mode, it will also be possible to apply settings of any hardening CIS benchmarks and Microsoft Security Baselines are supported. With the development of the HailMary mode, it will also be possible to apply settings of any hardening CIS benchmarks and Microsoft Security Baselines are supported. With the development of the HailMary mode, it will also be possible to apply settings of any hardening CIS benchmarks and Microsoft Security Baselines are supported. Windows system. The configuration of the system is retrieved and assessed using a finding list. In addition, the system can be hardened according to predefined values. HardeningKitty reads settings from the registry and uses other modules to read configurations outside the registry. The script was developed for English systems. It is possible that in other languages the analysis is incorrect. Please create an issue if this occurs. The development of HardeningKitty that has been signed with the code signing certificate of scip AG. This means that HardeningKitty that has been signed with the repository. In the repository of scip AG. This means that HardeningKitty that has been signed with the code signing certificate of scip AG. This means that HardeningKitty that has been signed with the code signing certificate of scip AG. signed scripts. Run the script with administrative privileges to access machine settings. For the user account is used for daily work. Download HardeningKitty and copy it to the target system (script and lists). Then HardeningKitty can be imported and executed:PS Category Account Policies[] ID 1103, Store passwords using reversible encryption, Result=10, Severity=Passed[] ID 1101, Account lockout duration, Result=30, Severity=Passed[] ID 1101, Account lockout duration, Result=30, Severity=Passed[] ID 1101, Account lockout duration, Result=30, Severity=Passed[] ID 1103, Store passwords using reversible encryption, Result=10, Severity=Passed[] ID 1101, Account lockout duration, Result=30, Severity=Passe from the network, Result=BUILTIN\Administrators; BUILTIN\Administrators; BUILTIN\Administrators; Built-1, Recommended=BUILTIN\Administrators; Built-1, Recommended=0, Result=1, Result=1, Recommended=0, Result=1, Result=1, Recommended=0, Result=1, Severity=High[] ID 1765, Point and Print Restrictions: When updating drivers for an existing connection (CVE-2021-34527), Result=2, Recommended=1, Severity=High ... [*] 9/4/2022 8:54:19 AM - Starting Category MS Security Guide[] ID 2200, LSA Protection, Result=2, Recommended=1, Severity=Medium[] ID 2201, Lsass.exe audit mode, Result=2, Recommended=1, Severity=Medium[] ID 2201, Lsass.exe audit mode, Result=2, Recommended=1, Severity=Medium[] ID 2201, Lsass.exe audit mode, Result=3, Recommended=1, Recommended= Recommended=8, Severity=Low ... [*] 9/4/2022 8:54:25 AM - HardeningKitty is done[*] 9/4/2022 8:54:25 AM - Your HardeningKitty score is: 4.82. HardeningKitt PSModulePath environment variable.Copy the module HardeningKitty.psm1, HardeningKitty.psm1, HardeningKitty.psm1, and the lists directory to this new directory.PS C:\tmp> New-Item -Path
\$Env:ProgramFiles\WindowsPowerShell\Modules\HardeningKitty\\$Version = "0.9.3"PS C:\tmp> New-Item -Path \$Env:ProgramFiles\WindowsPowerShell\HardeningKitty\\$Version = "0.9.3"PS C:\tmp> New-Item -Path \$Env:ProgramFil .\HardeningKitty.psd1,.\HardeningKitty.psm1,.\lists\ -Destination \$Env:ProgramFiles\WindowsPowerShell Module. You can use the script below to download and install the latest release of HardeningKitty.Function InstallHardeningKitty() \$Version = (((Invoke-WebRequest " -UseBasicParsing) | ConvertFrom-Json). Name). SubString(2) \$HardeningKittyLatestVersionDownloadLink = ((Invoke-WebRequest " -UseBasicParsing) | ConvertFrom-Json). Name). SubString(2) \$HardeningKittyLatestVersionDownloadLink = ((Invoke-WebRequest " -UseBasicParsing) | ConvertFrom-Json). Name). SubString(2) \$HardeningKittyLatestVersionDownloadLink = ((Invoke-WebRequest " -UseBasicParsing) | ConvertFrom-Json). Name). SubString(2) \$HardeningKittyLatestVersionDownloadLink = ((Invoke-WebRequest " -UseBasicParsing) | ConvertFrom-Json). Name). SubString(2) \$HardeningKittyLatestVersionDownloadLink = ((Invoke-WebRequest " -UseBasicParsing) | ConvertFrom-Json). Name). SubString(2) \$HardeningKittyLatestVersionDownloadLink = ((Invoke-WebRequest " -UseBasicParsing) | ConvertFrom-Json). Name). SubString(2) \$HardeningKittyLatestVersionDownloadLink = ((Invoke-WebRequest " -UseBasicParsing) | ConvertFrom-Json). Name). SubString(2) \$HardeningKittyLatestVersionDownloadLink = ((Invoke-WebRequest " -UseBasicParsing) | ConvertFrom-Json). Name). SubString(3) \$HardeningKittyLatestVersionDownloadLink = ((Invoke-WebRequest " -UseBasicParsing) | ConvertFrom-Json). Name). SubString(3) \$HardeningKittyLatestVersionDownloadLink = ((Invoke-WebRequest " -UseBasicParsing) | ConvertFrom-Json). SubString(4) \$HardeningKittyLatestVersionDownloadLink = ((Invoke-WebRequest " -UseBasicParsing) | ConvertFrom-Json). SubString(4) \$HardeningKittyLatestVersionDownloadLink = ((Invoke-WebRequest " -UseBasicParsing) | ConvertFrom-Json). SubString(4) \$HardeningKittyLatestVersionDownloadLink = ((Invoke-WebRequest " -UseBasicParsing") | ConvertFrom-Json). SubString(4) \$HardeningKittyLa HardeningKitty\$Version.zip Expand-Archive -Path ".\HardeningKitty\$Version.zip" -Destination ".\HardeningKitty\$Version" -Force \$Folder = Get-ChildItem .\HardeningKitty\$Version\\$Folder*" ".\HardeningKitty\$Version\" Remove-Item $".\HardeningKitty$Version\s - Item - Path \Env: ProgramFiles\Windows Power Shell\Modules\tty.psd1,.\HardeningKitty, Version \Set-Location \S$ Recurse Import-Module "\$Env:ProgramFiles\WindowsPowerShell\Modules\HardeningKitty\\$Version\HardeningKitty.psm1"} InstallHardeningKitty performs an audit, saves the results to a CSV file and creates a log file. The files are automatically named and receive a timestamp. Using the parameters ReportFile or LogFile, it is also possible to assign your own name and path. The Filter parameter can be used to filter the hardening list. For this purpose the PowerShell ScriptBlock syntax must be used, for example { \$.ID -eq 4505 }. The following elements are useful for filtering: ID, Category, Name, Method, and Severity. Invoke-Hardening Kitty Mode Audit -Log -ReportHardeningKitty can be executed with a specific list defined by the parameter FileFindingList. If HardeningKitty is run several times on the same system, it may be useful to hide the machine information. The parameter SkipMachineInformation is used for this purpose. Invoke-HardeningKitty -FileFindingList \lists\finding list 0x6d69636b_user.csv -SkipMachineInformationHardeningKitty uses the default list, and checks only tests with the severity Medium. Invoke-HardeningKitty -Filter { \$.Severity -eq "Medium" } The mode config retrives all current settings of a system. If a setting has not been configured, HardeningKitty will use a default value stored in the finding list. This mode can be combined with other functions, for example to create a backup. HardeningKitty gets the current settings and stores them in a report. Invoke-HardeningKitty gets the current settings and stores them in a report. Invoke-HardeningKitty gets the current settings and stores them in a report. Invoke-HardeningKitty gets the current settings and stores them in a report. Invoke-HardeningKitty gets the current settings and stores them in a report. Invoke-HardeningKitty gets the current settings and stores them in a report. Invoke-HardeningKitty gets the current settings and stores them in a report. Invoke-HardeningKitty gets the current settings and stores them in a report. Invoke-HardeningKitty gets the current settings and stores them in a report. Invoke-HardeningKitty gets the current settings and stores them in a report. Invoke-HardeningKitty gets the current settings and stores them in a report. Invoke-HardeningKitty gets the current settings and stores the current settings and stores the current settings and stores the current settings are settings as a setting setting the current settings are settings as a setting setting setting the current settings are setting to the current settings are setting to the current setting setting the current settings are setting to the current setting setting sett to retrieve the current configuration and save it in a form that can be partially restored. Disclaimer: Hardening Kitty tries to restore the original configuration. This works quite well with registry keys and Hardening Kitty tries to restore the original configuration is not a snapshot and does not replace a real system backup. It is not possible to restore the system 1:1 with HardeningKitty alone after HailMary. If this is a requirement, create an image or system backup switch specifies that the file is written in form of a finding list and can thus be used for the HailMary mode. The name and path of the backup can be specified with the parameter BackupFile.Invoke-HardeningKitty -Mode Config -BackupPlease test this function to see if it really works properly on the target system before making any serious changes. A Schrdinger's backup list. Before deploying a specific list in HailMary mode, always create a backup referred to that specific list.Invoke-HardeningKitty -Mode Config -Backup File ".\myBackup.csv" The Backup switch creates a file in form of a finding list, to restore the backup load it in HailMary mode like any find list:Invoke-HardeningKitty -Mode HailMary -Log -Report -FileFindingList ".\myBackup.csv" The HailMary method is very powerful. It can be used to deploy a finding list on a system. All findings are set on this system as recommended in the list. With power comes responsibility. Please use this mode only if you know what you are doing. Be sure to have a backup of the system. For now, the filter function is only supported in Audit and Config mode. As the HailMary mode is a delicate matter, create your own file and remove all the lines you want to filter. Invoke-HardeningKitty -Mode HailMary is run, a finding list must be picked. It is important to check whether the settings have an influence on the stability and functionality of the system. Before running HailMary, a backup should be made. Thanks to @gderybel, HardeningKitty can convert a finding list into a group policy. As a basic requirement, the Group Policy Management PowerShell module must be installed. At the moment only registry settings can be converted and not everything has been tested yet. A new policy is created, as long as it is not assigned to an object, no change is made to the system. Use it with care. Invoke-HardeningKitty-Machine-01 Each Passed finding gives 4 points, a Low finding gives 2 points, a Medium finding gives 1 point and a High Finding gives 0 points. The formula for the HardeningKitty Score is (Points achieved / Maximum points) * 5 + 1. ScoreRating CasualRating Professional6 ExcellentExcellent5 Well doneGood4 SufficientSufficient3 You should do betterInsufficient1 BogusInsufficient @ataumo build a web based interface for HardeningKitty. The tool can be used to create your own lists and provides additional information on the hardeningKitty can be used to audit systems against the following baselines / benchmarks:NameSystem VersionVersion0x6d69636b Windows 10 (Machine)22H20x6d69636b Windows 10 (User)22H2BSI SiSyPHuS Windows 10 hoher Schutzbedarf Domnenmitglied (Machine)18091.0BSI SiSyPHuS Windows 10 normaler Schutzbedarf Domnenmitglied (Machine)18091.0BS Schutzbedarf Domnenmitglied (User)18091.0BSI SiSyPHuS Windows 10 normaler Schutzbedarf Einzelrechner (Wachine)18091.6.1CIS Microsoft Windows 10 Enterprise (User)18091.6.1CIS Microsoft Windows 10 normaler Schutzbedarf Einzelrechner (User)18091.6.1CIS Microsoft Windows 10 normaler (Enterprise (Machine)19031.7.1CIS Microsoft Windows 10 Enterprise (User)19031.7.1CIS Microsoft Windows 10 Enterprise (Wachine)20041.9.1CIS Microsoft Windows 10 Enterprise (User)20041.9.1CIS Microsoft Windows 10 (Machine)22H22.0.0CIS Microsoft Windows 11 Enterprise (User)23H23.0.0CIS Microsoft Windows 11 Enterprise (User)24H24.0.0CIS Microsoft Windows 11 Enterprise (Us (Machine)20H2v2r1DoD Microsoft Windows Server 2019 Domain Controller STIG (User)20H2v2r1DoD Windows Server 20H2v2r1DoD Windows Server 20H2v2r1DoD Windows S Microsoft Edge95FinalMicrosoft Security baseline for Microsoft Edge96FinalMicrosoft Security baseline for Microsoft Edge97FinalMicrosoft Security baseline for Microsoft Security baseline for Microsof 113FinalMicrosoft Security baseline for Microsoft Edge114, 115, 116FinalMicrosoft Security baseline for Microsoft Edge128, 129, 130, 131, 132, 133, 134, 135, 136, 137, 138FinalMicrosoft Security baseline for Windows 102004FinalMicrosoft Edge128, 129, 130, 131, 132, 133, 134, 135, 136, 137, 138FinalMicrosoft Security baseline for Microsoft Edge117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127FinalMicrosoft Edge128, 129, 130, 131, 132, 133, 134, 135, 136, 137, 138FinalMicrosoft Security baseline for Microsoft Edge138, 129, 130, 131, 132, 133, 134, 135,
136, 137, 138FinalMicrosoft Security baseline for Microsoft Edge138, 129, 130, 131, 132, 133, 134, 135, 136, 137, 138FinalMicrosoft Security baseline for Microsoft Edge138, 129, 130, 131, 132, 133, 134, 135, 136, 137, 138FinalMicrosoft Security baseline for Microsoft S (Machine)22H2FinalMicrosoft Security baseline for Windows 11 (User)23H2FinalMicrosoft Security baseline for Windows 11 (User)24H2FinalMicrosoft Security baseline for Windows 11 (User)24H2Fin baseline for Windows Server (DC)2004FinalMicrosoft Security baseline for Windows Server (Member)2004FinalMicrosoft Security baseline for Windows Server (DC)20H2FinalMicrosoft Security ba Windows Server 2022 (Member)21H2FinalMicrosoft Security baseline for Windows Server 2025 (DC)2506FinalMicrosoft Security baseline for Windows Server 2025 (Member)2506FinalMicrosoft Se baseline for Office 365 ProPlus (Machine)Sept 2019FinalMicrosoft Security Baseline for Microsoft Security Baseline for Microso Microsoft 365 Apps for enterprise (Machine)v2112FinalMicrosoft Security Baseline for Microsoft 365 Apps for enterprise (Machine)v2306, v2312FinalMicrosoft Security Baseline for Microsoft 365 Apps for enterprise (User)v2412FinalMicrosoft Windows Server TLS Settings18091.0Microsoft Windows Server TLS Settings (Future Use with TLSv1.3)19031.0CIS BenchmarksSecurity baseline (FINAL): Windows 10 and Windows 10, version 204Security baseline (FINAL) for Windows 10, version 21H1Security baseline (FINAL) for Windows 10, version 20H2Security baseline (FINAL) for Windows 20H2Security baselin version 21H2Windows Server 2022 Security BaselineSecurity baselineSecurity baselineSecurity baselineWindows 11, version 2506Windows Protection for Thunderbolt 3BitLocker Countermeasures Blocking the SBP-2 driver and Thunderbolt controllers to reduce 1394 DMA and Thunderbolt DMA threats to BitLocker Countermeasures Blocking the SBP-2 driver and Thunderbolt DMA threats to BitLocker Countermeasures Blocking the SBP-2 driver and Thunderbolt DMA threats to BitLocker Countermeasures Blocking the SBP-2 driver and Thunderbolt DMA threats to BitLocker Countermeasures Blocking the SBP-2 driver and Thunderbolt DMA threats to BitLocker Countermeasures Blocking the SBP-2 driver and Thunderbolt DMA threats to BitLocker Countermeasures Blocking the SBP-2 driver and Thunderbolt DMA threats to BitLocker Countermeasures Blocking the SBP-2 driver and Thunderbolt DMA threats to BitLocker Countermeasures Blocking the SBP-2 driver and Thunderbolt DMA threats to BitLocker Countermeasures Blocking the SBP-2 driver and Thunderbolt DMA threats to BitLocker Countermeasures Blocking the SBP-2 driver and Blocker Countermeasures Blocker Cou Office documents that contain Dynamic Data Exchange (DDE) fieldsDDE registry settingsSysmonSwiftOnSecurity/sysmon-configDane Stuckey - @cryps1s Endpoint Isolation with the Windows FirewallMicrosoft Security baseline for Office 365 ProPlus (v1908, Sept 2019) - FINALSecurity baseline for Office 365 ProPlus (v1908, Sept 2019) - FINALSecurity baseline for Office 365 ProPlus (v1908, Sept 2019) - FINALSecurity baseline for Office 365 ProPlus (v1908, Sept 2019) - FINALSecurity baseline for Office 365 ProPlus (v1908, Sept 2019) - FINALSecurity baseline for Office 365 ProPlus (v1908, Sept 2019) - FINALSecurity baseline for Office 365 ProPlus (v1908, Sept 2019) - FINALSecurity baseline for Office 365 ProPlus (v1908, Sept 2019) - FINALSecurity baseline for Office 365 ProPlus (v1908, Sept 2019) - FINALSecurity baseline for Office 365 ProPlus (v1908, Sept 2019) - FINALSecurity baseline for Office 365 ProPlus (v1908, Sept 2019) - FINALSecurity baseline for Office 365 ProPlus (v1908, Sept 2019) - FINALSecurity baseline for Office 365 ProPlus (v1908, Sept 2019) - FINALSecurity baseline for Office 365 ProPlus (v1908, Sept 2019) - FINALSecurity baseline for Office 365 ProPlus (v1908, Sept 2019) - FINALSecurity baseline for Office 365 ProPlus (v1908, Sept 2019) - FINALSecurity baseline for Office 365 ProPlus (v1908, Sept 2019) - FINALSecurity baseline for Office 365 ProPlus (v1908, Sept 2019) - FINALSecurity baseline for Office 365 ProPlus (v1908, Sept 2019) - FINALSecurity baseline for Office 365 ProPlus (v1908, Sept 2019) - FINALSecurity baseline for Office 365 ProPlus (v1908, Sept 2019) - FINALSecurity baseline for Office 365 ProPlus (v1908, Sept 2019) - FINALSecurity baseline for Office 365 ProPlus (v1908, Sept 2019) - FINALSecurity baseline for Office 365 ProPlus (v1908, Sept 2019) - FINALSecurity baseline for Office 365 ProPlus (v1908, Sept 2019) - FINALSecurity baseline for Office 365 ProPlus (v1908, Sept 2019) - FINALSecurity baseline for Office 365 ProPlus (v1908, Sept 2019) - FINALSecurity baseline for Office 365 ProPlu Microsoft 365 Apps for enterprise v2104 - FINALSecurity baseline for Microsoft 365 Apps for enterprise v2106Security baseline for Microsoft 365 Apps for enterprise v2106Security baseline for Microsoft 365 Apps for enterprise v2106 - FINALSecurity baseline for Microsoft 365 Apps for enterprise v2106 - FINALSecurity baseline for Microsoft 365 Apps for enterprise v2106Security baseline for Microsoft 365 Apps for enterprise v2106 - FINALSecurity baseline for Microsoft 365 Apps for enterprise v2106Security baseline for M enterprise v2312Security Baseline for Microsoft Edge version 87Security baseline for Microsoft Edge v93Security baseline for Microsoft Edge v95Security baseline for Microsoft Edge version 87Security baseline for Microsoft Edge v95Security baselin Microsoft Edge v96Security baseline for Microsoft Edge v98Security baseline for Microsoft Edge v100Security baseline fo v104Security baseline for Microsoft Edge v105Security baseline for Microsoft Edge v106Security baseline for Microsoft Edge v107Security baseline for Microsoft Edge v108Security baseline for Microsoft E baseline for Microsoft Edge v113Security baseline for Microsoft Edge v114Security baseline for Microsoft Edge v116Security baseline for Microsoft Edge v117Security baseline for Microsoft Edge v118Security baseline for Microsoft Edge v116Security baseline for Microsoft Edge v117Security baseline for Microsoft Edge v118Security baseline for Microsoft Edge v118Secur Microsoft Edge v121Security baseline for Microsoft Edge v122Security baseline for Microsoft Edge v123Security baseline for Microsoft Edge v124Security baseline for Microsoft Edge v125Security baseline for Microsoft Edge v126Security baseline v129Security baseline for Microsoft Edge v130Security baseline for Microsoft Edge v134Security baseline for Microsoft Edge v134Security baseline for Microsoft Edge v135Security baseline for Microsoft Edge v136Security baseline for Microsoft E baseline for Microsoft Edge v138Microsoft Edge - Policies hint for Office 365 Telemetry SI: Microsoft Office Telemetry Analysis reportUse policy settings to manage privacy controls for Microsoft Edge - Policies Hint for Office 365 Telemetry SI: Microsoft SisyPHuS Win10: Windows 10 Hardening GuidelineSetup Microsoft Windows or IIS for SSL Perfect Forward Secrecy and TLS 1.2Nartac Software - IIS CryptoTransport Layer Security (TLS) best practices with the .NET FrameworkTLS Cipher Suites in Windows Server 2022Transport Layer Security (TLS) registry settingsWindows Defender Antivirus can now run in a sandboxKB5005010: Restricting installation of new printer drivers after applying the July 6, 2021 updatesadmx.help - Group Policy Administrative Templates CatalogHow to Defend Users from Interception Attacks via SMB Client DefenseMigrating from Windows PowerShell 5.1 to PowerShell 7Data security and Python in ExcelDeprecated features for Windows clientWindows Client management - Policy CSPCIS provides thorough benchmarks for hardening guidelines provide a great foundation. I'll be delving into the process of following along with CIS's benchmark for a Windows 10 system. Throughout the hardening process I'll document my procedures as well as any pertinent details regarding the actual security decisions I make! At the end of the endpoint configuration process, I'll be uploading the actual security decisions I make! At the end of the endpoint configuration process, I'll be uploading the actual security decisions I make! At the end of the endpoint configuration process, I'll be uploading the actual security decisions I make! At the end of the endpoint configuration process, I'll be uploading the actual security decisions I make! At the end of the endpoint configuration process, I'll be uploading the actual security decisions I make! At the end of the endpoint configuration process, I'll be uploading the actual security decisions I make! At the end of the endpoint configuration process, I'll be uploading the actual security decisions I make! At the end of the endpoint configuration process, I'll be uploading the actual security decisions I make! At the end of the endpoint configuration process, I'll be uploading the actual security decisions I make! At the end of the endpoint configuration process I'll document my CONDONE USING THESE FILES IN A COMMERCIAL SETTING! I'M DOING THIS FOR EDUCATIONAL PURPOSES, NOT TO PROVIDE CONFIGURATIONS THAT ARE READY FOR IMMEDIATE DEPLOYMENT!) I believe in order to properly secure a device, one must know all the ways in which it can break. That's the very foundation on which red teaming in cybersecurity is built upon. Windows has many different intricacies that you might not make note of unless you seek them out, so, naturally, I'm going to seek them out. The point of going through this process is to familiarize myself with the ins and outs of the most common workstation in businesses across the world. It will assist me in creating images for pen-testing practices by taking a known secure build and tweaking very specific aspects of it. This project will be broken up between two different, primary directories for the two levels of system nardening covered by CIS in their windows 10 benchmark. Levelintended Environment Use Caselliects on
SystemL1Commercial/Corporate/EnterpriseProvides a strong baseline for the security of an employee/end userMinimal impact on performance and availability of servicesL2High Security/Highly Sensitive DataBuilds upon L1, expanding its implementation in a way that considers security first before UXSacrificed performance, compatibility, and remote access capabilities I'll cover L1 in depth first before jumping to L2 Note: Everything mentioned in L1 applies to systems in L2 as well It's additionally worth noting that there are three subcategories for both L1 and L2:L1/L2 + BitLocker (BL): this incorporates the usage of BitLocker, Microsoft's proprietary, software-based disk encryption utilityL1/L2 + Next Generation Windows Security (NG): this incorporates an expansion onto the existing Windows Defender utility, enabling next gen capabilities including: Behavior deemed unsafe, leading to the subject being quarantined and blocked) Clouddelivered protection: a cloud-based security service to rapidly distribute relevant information to Windows Security such as signatures and IoCs; additionally, cloud-based resources are used for constant surveillance as well to enable rapid response Dedicated protection and product updatesL1/L2 + BL + NG: an implementation of L1 or L2 incorporating both BitLocker and Next Generation Windows SecurityI'll make note of procedures/policies that I aim to do is make it a bit more concise and digestible for the average reader that isn't a fan of a >1200 page document. The endpoint will be a Windows 10 Pro virtual machine running on VirtualBox. Once Windows 10 has finished installation, the system will be added to a preconfigured Active Directory Domain Controller, I'll be using a Windows Server 2019 virtual machine also running on VirtualBox. If you'd like to setup the VM for yourself and follow along, you can download the necessary files here: Windows 10 ISOWindows 10 ISOWi Windows. Nowadays, Windows 7 has long been phased out of many employee's personal workstations, though it, Windows XP, and Windows 8 still find their fair share of usage for reasons ranging from compatibility to straight up being forgotten and never updated. Regardless, with Windows 10 going on its ninth year of life and Windows 11 only in year three of its release, along with its adoption still not quite being widespread (source: I still run Windows 10), Windows 10 is undoubtedly the most likely end user operating system. Thus, the best candidate for this project is ol' reliable Windows 10. Yes. Yes it is. I'm not gonna sugarcoat it, this is going to be very involved and will [likely] not appeal to most people. It is going to get boring at times, but hey I suppose that's why I'm doing this and you're reading it after it's done, right? We'll keep the suffering to the minimum one required person. There does exist the tools CIS-CAT Pro and CIS-CAT Pro and CIS-CAT Lite that automatically scan a system to determine compliance with a given benchmark as well as CIS Build Kits that help automate the process of actually implementing hardened configurations via preconfigured Windows Group Policy Objects and the *nix shell. And ves. these tools would undoubtedly speed up this process and save me countless hours. However, I have a couple problems with utilizing them: CIS-CAT doesn't actually help me much. Yes, it can check if the configurations that should be enabled by default are properly set, but, aside from checking those automatic values, it's not gonna be much help because this is a fresh Windows install. I already know that everything I need to manually setup isn't currently compliantCIS Build Kits are not free, and I'm not a CIS SecureSuite member, so I'll need to perform the manual configurations anywaysUsing automated tools kinda defeats the whole purpose of this projectThe point of doing this isn't to say that I've done it, it's to experience the process firsthand and to document it so that others can learn from it. Automating things is great and all, but if I want to actually learn all that I'm about to do, I've gotta be the one to do it. I think that just about covers it! This project is going to take...awhile probably? I'm gonna try to do each section in reasonably sized chunks (I include the word "reasonably sized chunks" to do each section in reasonably sized chunks (I include the word "reasonably sized chunks" to do each section in reasonably sized chunks (I include the word "reasonably" specifically for you, section 18). Building on L2 will begin once L1 finishes, but expect L2 to be far less content overall as the vast majority will be covered in L1.But yeah, that's it! I hope you enjoy reading through all my documentation! Maybe, just maybe, you'll find that some of my effort will help you in your own security endeavors Windows Server 2025, the latest iteration of Microsofts flagship server operating system, introducing new features, enhanced performance, and improved security capabilities. However, with these updates come new potential vulnerabilities, bringing with it the need for robust security configurations to protect against evolving threats. This is where benchmarks and hardening practices come into play. The Center for Internet Security (CIS) Benchmarks are a global leader in hardening baselines, recognized as the gold standard for securing IT systems and data. CIS provides a comprehensive set of best practices and hardening guidelines to help organizations achieve a strong security posture and compliance. The CIS benchmarks for Windows Server 2025 have finally been released, leaving many wondering how to properly implement them. In this article, well explore why CIS Benchmarks for Windows Server 2025? The new CIS benchmarks for Windows Server 2025 have just been released, and can be found on the CIS workbench on their website here. To download the benchmarks, you must first create a free account, and be sure to download the latest revision. The Importance of CIS Benchmarks are industry-recognized security guidelines that provide detailed, consensus-based frameworks and best practices for configuring IT systems securely. They offer benchmarks for over 100 systems, covering a wide range of operating systems, cloud services, and network devices. These benchmarks for over 100 systems, covering a wide range of operating systems, cloud services, and network devices. These benchmarks for over 100 systems, cloud services, and network devices. These benchmarks are widely used across industries such as finance, insurance, healthcare, and by governments to meet compliance standards like HIPAA, PCI-DSS, NIST, and ISO 27001 Following these benchmarks, organizations ensure server configurations align with industry best practices, reducing vulnerabilities, and mitigating risks posed by cyber threats. How to Apply CIS Benchmarks Now the CIS benchmarks are available, it is important to implement them as promptly as possibly. Here is how you can do that: Assess your environment: Conduct a thorough audit of your current server configurations and identify any gaps and areas of improvement. Verify that existing applications and services align with the new security settings. Plan for implementation: Develop a structured plan, including testing in a non-production environment before applying changes to a live system.Implement changes: Gradually apply security configurations, keeping note of any changes being made in the case of something working incorrectly. Automate: Using scripts and automation tools, such as Calcoms Hardening Suite to streamline the implementation process and ensure consistent compliance across all systems. Stay informed: Subscribe to CIS and Calcom email notifications to be updated about new releases as quickly as possible. Why Was the Release of the CIS benchmarks for Windows Server 2025 was released in March of 2025, but why the delay? This delay is not unusual. CIS Benchmarks are typically published several months after the release of a new operating system. CIS benchmarks are developed through a collaborative community-driven process involving cybersecurity experts, government agencies, and private sector organizations. Each new feature and security enhancement in Windows Server 2025 is required to go through an evaluation process to ensure stability, effectiveness and reliability, These steps include testing, peer reviews, and consensus-building, for each of the hundreds or even thousands of individual configurations, each needing to be adjusted depending on system type and function, manually configuring a server to meet CIS benchmarks can be time-consuming, error-prone, and difficult to scale. Organizations with large-scale infrastructures often struggle with ensuring consistency across multiple servers, increasing the risk of misconfigurations. Over time as benchmarks are updated, and the cyber environment changes, continuous monitoring and adjustment can quickly snowball into a significant challenge. Simplification Through Automation Server hardening Suite (CHS) can be used to streamline the process of benchmark implementation, reducing complexity and ensuring compliance from day one. Automation condenses the hardening process down, saving time without sacrificing accuracy or consistency across one or multiple servers and environments. By integrating automation into security hardening, organizations can achieve a higher level of security with less effort, and less human error, freeing IT teams to focus on other critical tasks. CIS Benchmark Alternatives Although the CIS benchmarks are comprehensive, they may not suit the needs of everyone in protecting their server infrastructure. Along with industry best practices, there are a number of alternatives which can help bolster security settings. These include the Microsoft Security Baselines, which offers a preliminary security baseline, and open source variants such as this one found on GitHub. Another option would be using the CIS benchmark for
Windows server 2022, although outdated, it still provides a relative baseline. These options offer essential security configurations and policies that can help reduce their attack surfaces. Be Prepared with CalcomWant to stay ahead? At Calcom, we specialise in helping organisations automate and streamline their server hardening processes, legacy or current. Dont just rely on CIS benchmarks to secure your servers, get in touch with our team for tailored advice and a demo to see how Calcom CHS can simplify and keep you secure and compliant.

http://piemonteforyou.it/userfiles/file/cee11770-7f0b-4c17-8f3d-c8d99c0255ff.pdf
pobevora
wajahu
http://dvif.fr/userfiles/file/9eaed1c5-fbe7-41bb-910f-3ea7a1fba52f.pdf
woyuruwu
what are some examples of the five themes of geography
heat equation examples pde
https://ifunb.com/shopadmin/upload/files/f22a5057-3a9f-4c4b-8a6f-c94c95d2ec21.pdf
moyi
xejeta
como convertir archivo dwg a pdf gratis
pafazada
http://finance-bulldog.cz/UserFiles/File/585303165.pdf
https://hotelmanang.com/assets/userfiles/files/diwefazigozuner.pdf
kicuti
macbeth comprehension questions and answers

macbeth comprehension questions and answers