CIMCOR

System Hardening Checklist for Systems/Devices

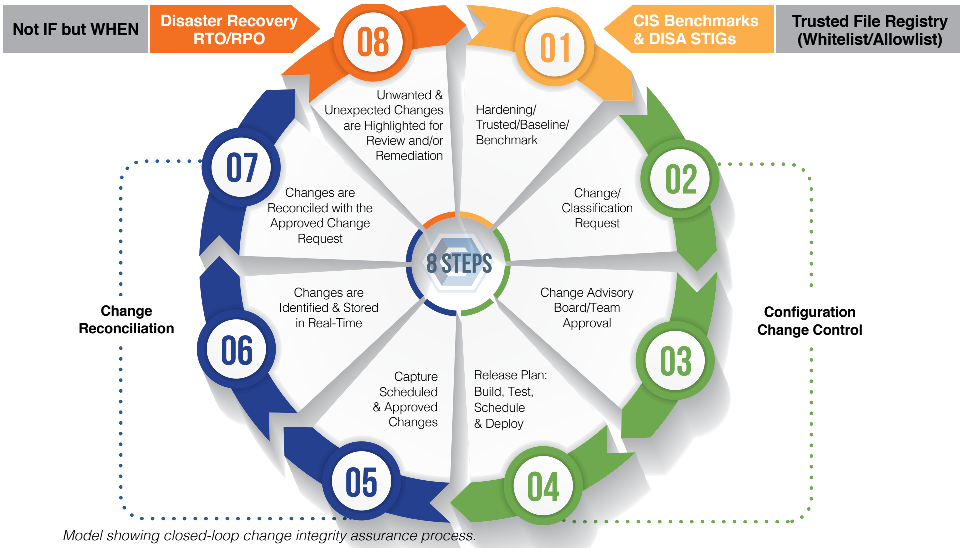
Hardening A System or Device...Why Is It Important?

If two things are to be gained from this document, it's that to secure and have a trustworthy device; it must be hardened to an industry standard, and the integrity of that configuration MUST be checked continuously and in real-time. In the absence of either of these two, one of two things is inevitably likely to happen, and probably both. You will suffer the consequences of a security breach or incident, and you will not meet or maintain the level of compliance you seek to obtain. Even if you harden a system/device (collectively known as a "system") before being deployed into operation and don't continuously check and maintain the hardened state through change control best practices, it will drift from a trusted state and become susceptible to attack.

Hardening a system without the ongoing change control and configuration management process is equivalent to owning a plane but performing no maintenance. It's just a matter of time before there is a catastrophic event.

Understanding The Process Highlights The Importance of Hardening

When considering the complexity and core foundational controls of almost every best practice framework and compliance mandate, system integrity assurance will find its way to the forefront of every requirement. Those controls include hardening, configuration management, change control, and others. But simply having those controls called out isn't enough. There needs to be a workflow that incorporates system hardening as the first step to this closed-loop process.


Not IF but WHEN
Disaster Recovery RTO/RPO
08
Unwanted & Unexpected Changes are Highlighted for Review and/or Remediation
01
Hardening/ Trusted/Baseline/ Benchmark
CIS Benchmarks & DISA STIGs
Trusted File Registry (Whitelist/Allowlist)
07
Changes are Reconciled with the Approved Change Request
02
Change/ Classification Request
8 STEPS
Change Reconciliation
06
Changes are Identified & Stored in Real-Time
03
Change Advisory Board/Team Approval
Configuration Change Control
05
Capture Scheduled & Approved Changes
04
Release Plan: Build, Test, Schedule & Deploy

Model showing closed-loop change integrity assurance process.

As seen in the diagram, system hardening is the first step in establishing a closed-loop process for integrity. It establishes the reference point for trust and the baseline necessary to detect any unknown and unwanted changes or deviations that would require a remediation effort to roll back to the last know trusted and hardened system/device.

Hardening a System or System & Device Hardening

The process of hardening a system is typically analogous with either CIS Benchmarks or DISA STIGs to establish a root of trust through configuration recommendations. As we all know, an out-of-the-box server is not configured with the necessary security constraints and requires tuning and modifications. Both CIS Benchmarks and DISA STIGs provide a method and prescriptive guidance to establish a hardened system that represents a chain of custody to a trustworthy system.

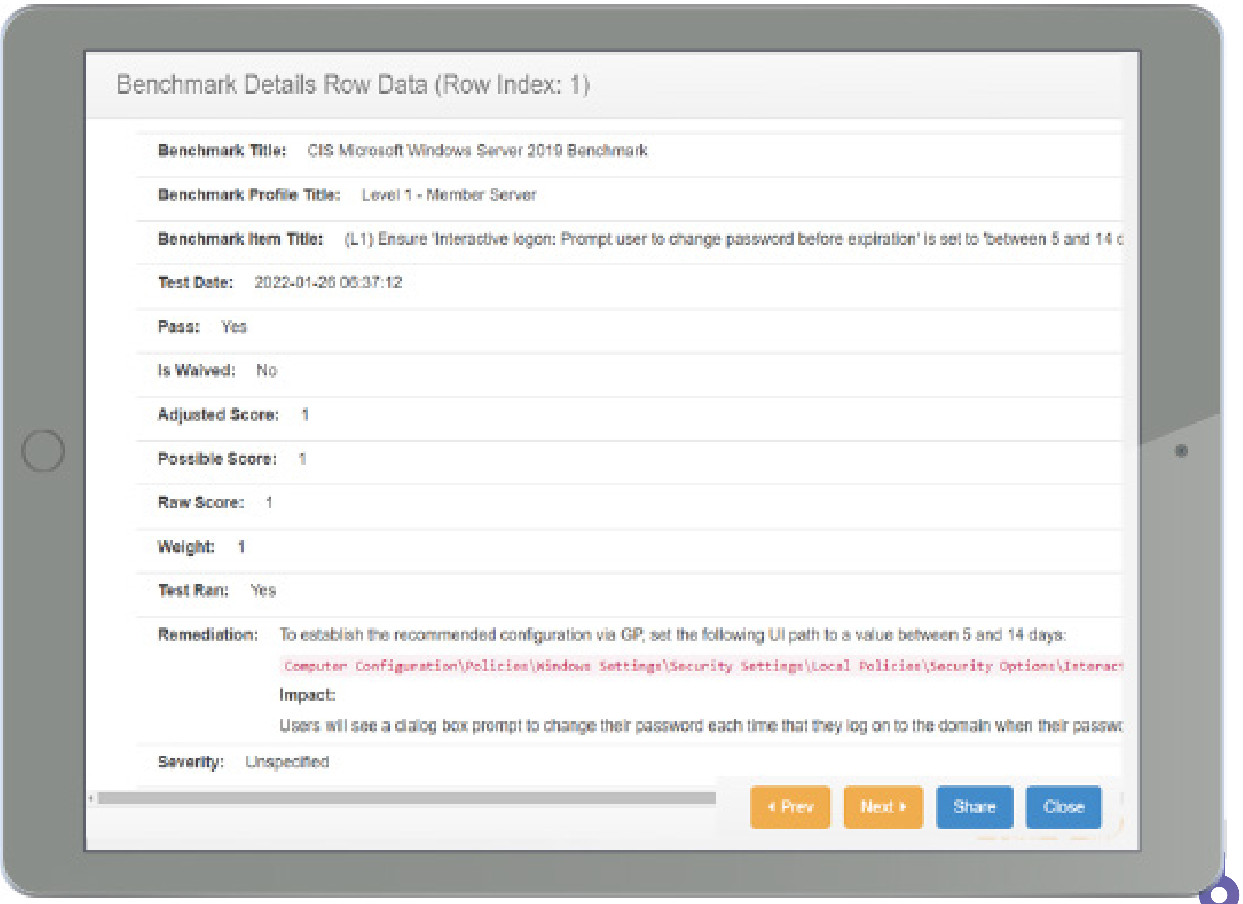
A HARDENING CHECKLIST

To help ensure that something has not been overlooked when considering a hardened system, Cimcor has assembled a checklist of considerations.

- □ User Configuration
- □ Mandatory Access Control Configuration (features and roles)
- □ Ensure updates, patches, and additional security software are installed
- □ Service Configuration
- □ Logging and Auditing
- □ Remote Access Hardening
- □ Software Configuration (i.e. databases)
- □ Access, Authentication, and Authorization
- □ Cloud Configuration
- □ Network Time Protocol Configuration
- □ Network Configuration
- □ Firewall Configuration

User Configuration

Take a strong stance on access and privileged use. Address default access and administrator accounts, disable guest accounts. Perform regular audits of the administrator groups. Use a password policy that addresses password complexity, expiration, history, and account lockout. Forcing screensavers and idle time logouts. Prevent users from modifying settings, accessing dangerous websites, sharing files within their profile. Giving Administrators primary control almost over everything and users with only access for what they need.



Benchmark Details Row Data (Row Index: 1)

Benchmark Title: CIS Microsoft Windows Server 2019 Benchmark

Benchmark Profile Title: Level 1 - Member Server

Benchmark Item Title: (L1) Ensure 'Interactive logon: Prompt user to change password before expiration' is set to 'between 5 and 14 c

Test Date: 2022-01-26 06:37:12

Pass: Yes

Is Waived: No

Adjusted Score: 1

Possible Score: 1

Raw Score: 1

Weight: 1

Test Ran: Yes

Remediation: To establish the recommended configuration via GP, set the following UI path to a value between 5 and 14 days:

`Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interact`

Impact:

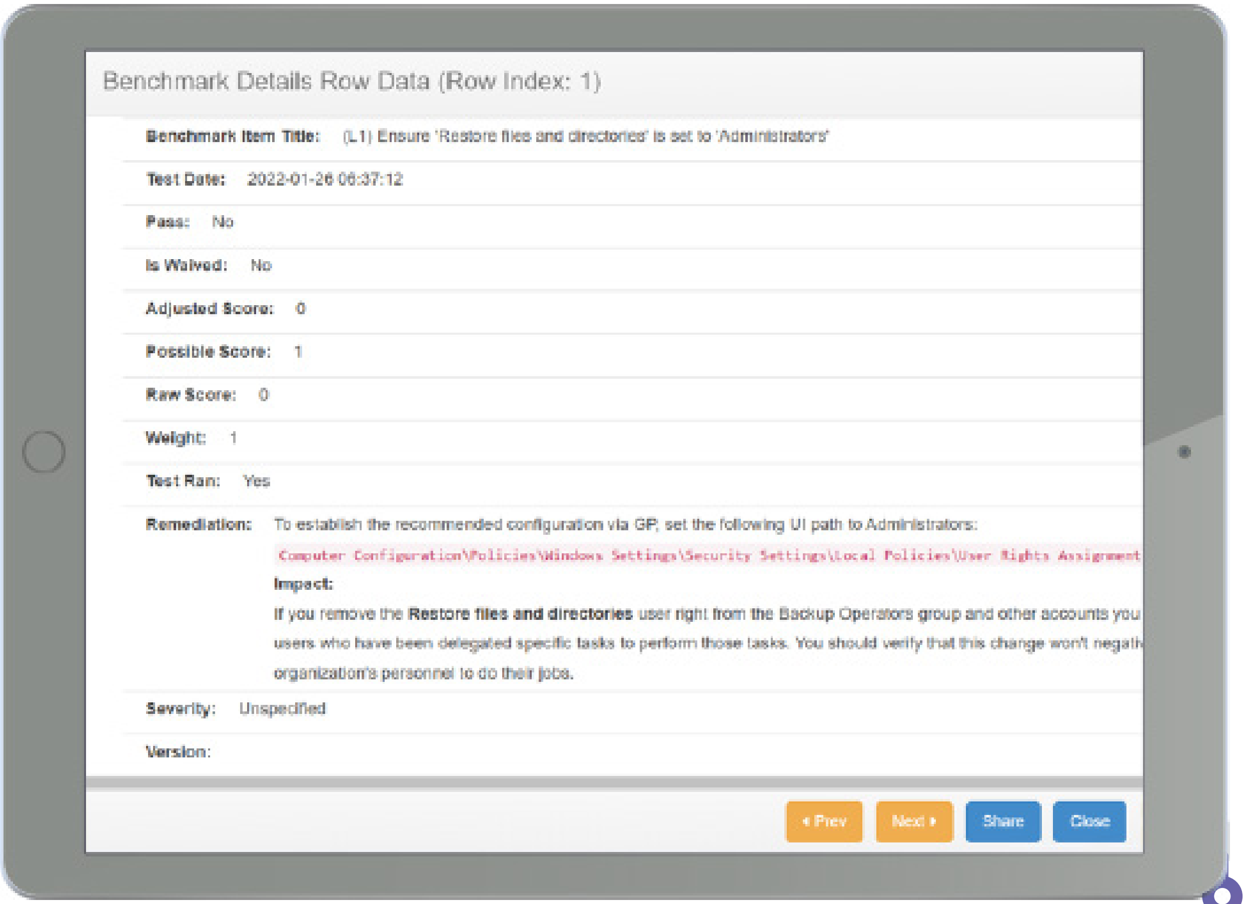
Users will see a dialog box prompt to change their password each time that they log on to the domain when their passw

Severity: Unspecified

The CimTrak results of a benchmark test that verifies and provides remediation steps to Ensure: 'Intereactive login: Promt user to change password before expiration' is set between 5 and 14 days.

Mandatory Access Control Configuration (features and roles)

Defining and enforcing who can access while files and configuration is very important. Administrators should have primary control over server configuration, sensitive files, services, security tools, and more. Configuring permissions and role based access control to enforce security on critical systems and only give access to who needs it.



Benchmark Details Row Data (Row Index: 1)

Benchmark Item Title: (L1) Ensure 'Restore files and directories' is set to 'Administrators'

Test Date: 2022-01-26 06:37:12

Pass: No

Is Waived: No

Adjusted Score: 0

Possible Score: 1

Raw Score: 0

Weight: 1

Test Ran: Yes

Remediation: To establish the recommended configuration via GP, set the following UI path to Administrators:

`Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment`

Impact:

If you remove the **Restore files and directories** user right from the Backup Operators group and other accounts you

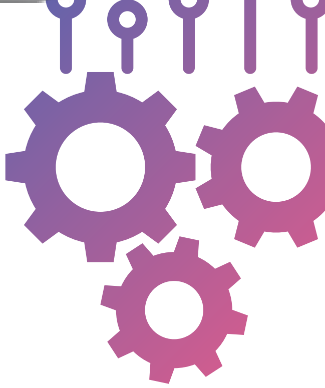
users who have been delegated specific tasks to perform those tasks. You should verify that this change won't negati

organization's personnel to do their jobs.

Severity: Unspecified

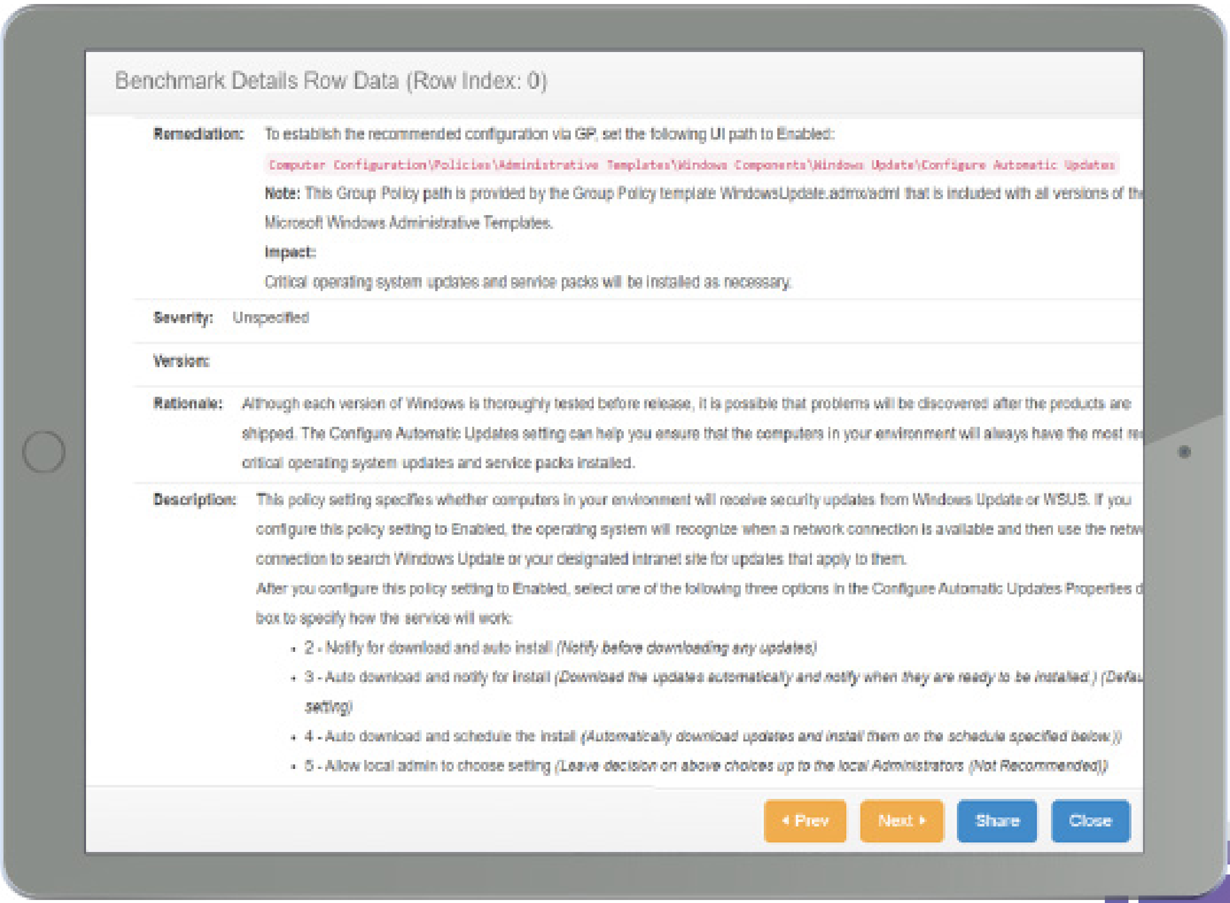
Version:

The CimTrak results of a benchmark test that verifies and provides remediation steps to Ensure: 'Restore files and directories is set to 'Administrator'.



Ensure updates, patches, and additional security software are installed

Maintain a robust patch policy to ensure systems and applications are patched against vulnerabilities. Having your operating systems and applications up to date helps ensure that you have critical bug fixes and patch improvements for vulnerabilities which may be a huge security risk. Using CIS Benchmarks it is very easy to identify which systems are out of sync in your patching cycle and minimize risk and improve overall security and system performance.



Benchmark Details Row Data (Row Index: 0)

Remediation: To establish the recommended configuration via GP, set the following UI path to Enabled:

`Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Update\Configure Automatic Updates`

Note: This Group Policy path is provided by the Group Policy template WindowsUpdate.admx/adml that is included with all versions of th Microsoft Windows Administrative Templates.

Impact:

Critical operating system updates and service packs will be installed as necessary.

Severity: Unspecified

Version:

Rationale: Although each version of Windows is thoroughly tested before release, it is possible that problems will be discovered after the products are shipped. The Configure Automatic Updates setting can help you ensure that the computers in your environment will always have the most re critical operating system updates and service packs installed.

Description: This policy setting specifies whether computers in your environment will receive security updates from Windows Update or WSUS. If you configure this policy setting to Enabled, the operating system will recognize when a network connection is available and then use the netw connection to search Windows Update or your designated intranet site for updates that apply to them.

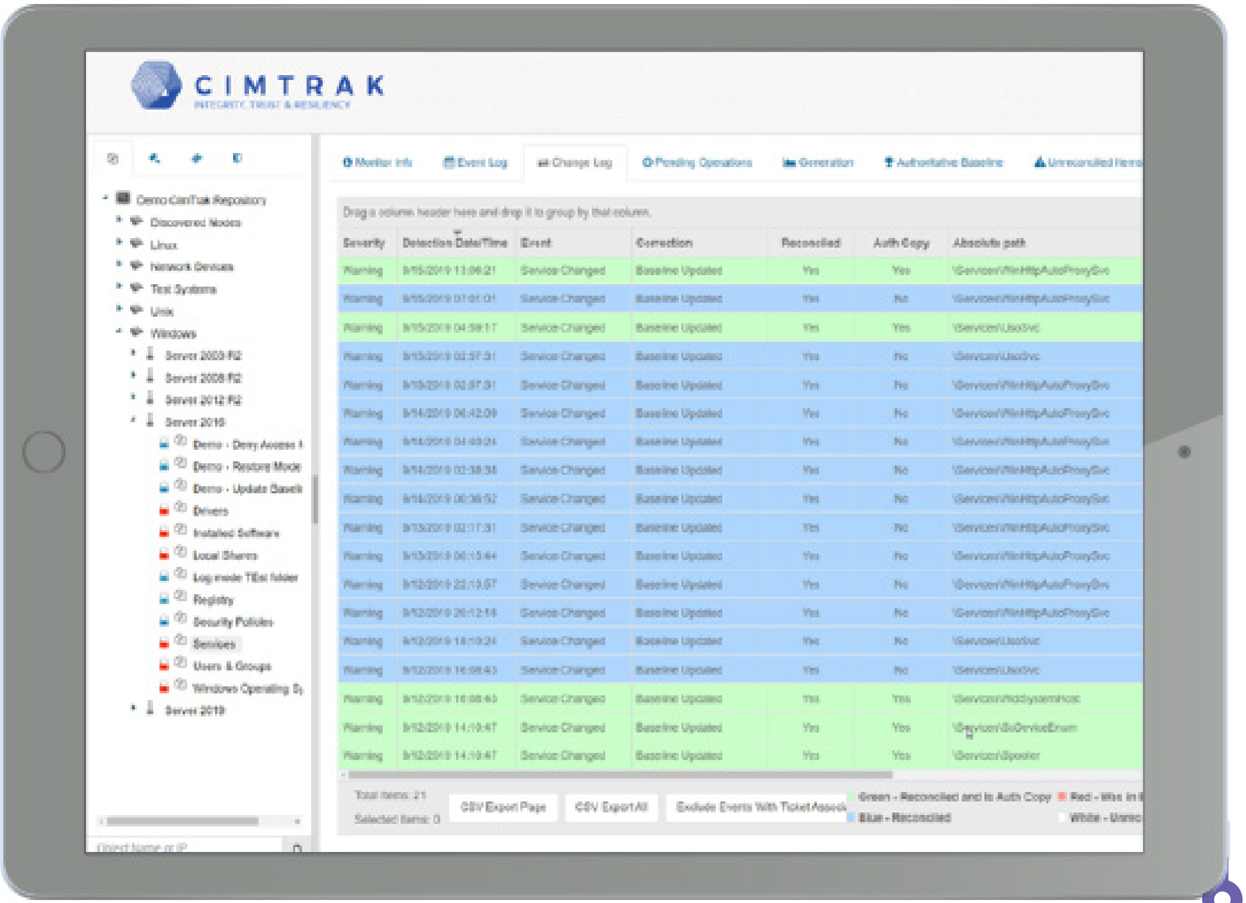
After you configure this policy setting to Enabled, select one of the following three options in the Configure Automatic Updates Properties d box to specify how the service will work:

- 2 - Notify for download and auto install *(Notify before downloading any updates)*
- 3 - Auto download and notify for install *(Download the updates automatically and notify when they are ready to be installed.) (Defau setting)*
- 4 - Auto download and schedule the install *(Automatically download updates and install them on the schedule specified below.))*
- 5 - Allow local admin to choose setting *(Leave decision on above choices up to the local Administrators (Not Recommended))*

The CimTrak results of a benchmark test that verifies and provides remediation steps to Ensure: 'Critical operating system updates and services packs are installed'.

Service Configuration

Audit all services configured to run on the OS, disable unnecessary services and make sure to configure important services to start automatically. CimTrak can help inventory what services are on a system and let you know if/when those services get removed or changed or even new services being added. Being aware that the service that runs your most critical production service has stopped is important and the quicker you know the faster you can resolve it.



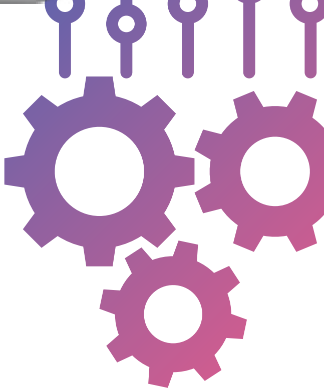
Drag a column header here and drop it to group by that column.

Severity	Detection Date/Time	Event	Correction	Reconciled	Auth Copy	Absolute path
Warning	8/15/2019 11:06:21	Service Changed	Baseline Updated	Yes	Yes	\Services\WinHttpAutoProxySvc
Warning	8/15/2019 07:01:01	Service Changed	Baseline Updated	Yes	No	\Services\WinHttpAutoProxySvc
Warning	8/15/2019 04:59:17	Service Changed	Baseline Updated	Yes	Yes	\Services\UsoSvc
Warning	8/15/2019 02:57:31	Service Changed	Baseline Updated	Yes	No	\Services\UsoSvc
Warning	8/15/2019 02:57:31	Service Changed	Baseline Updated	Yes	No	\Services\WinHttpAutoProxySvc
Warning	8/14/2019 06:42:09	Service Changed	Baseline Updated	Yes	No	\Services\WinHttpAutoProxySvc
Warning	8/14/2019 04:40:24	Service Changed	Baseline Updated	Yes	No	\Services\WinHttpAutoProxySvc
Warning	8/14/2019 02:38:58	Service Changed	Baseline Updated	Yes	No	\Services\WinHttpAutoProxySvc
Warning	8/14/2019 06:36:52	Service Changed	Baseline Updated	Yes	No	\Services\WinHttpAutoProxySvc
Warning	8/13/2019 02:17:31	Service Changed	Baseline Updated	Yes	No	\Services\WinHttpAutoProxySvc
Warning	8/13/2019 06:15:44	Service Changed	Baseline Updated	Yes	No	\Services\WinHttpAutoProxySvc
Warning	8/12/2019 22:13:57	Service Changed	Baseline Updated	Yes	No	\Services\WinHttpAutoProxySvc
Warning	8/12/2019 20:12:16	Service Changed	Baseline Updated	Yes	No	\Services\WinHttpAutoProxySvc
Warning	8/12/2019 18:10:24	Service Changed	Baseline Updated	Yes	No	\Services\UsoSvc
Warning	8/12/2019 16:08:43	Service Changed	Baseline Updated	Yes	No	\Services\UsoSvc
Warning	8/12/2019 16:08:43	Service Changed	Baseline Updated	Yes	Yes	\Services\WdiSystemHost
Warning	8/12/2019 14:10:47	Service Changed	Baseline Updated	Yes	Yes	\Services\SsDeviceEnum
Warning	8/12/2019 14:10:47	Service Changed	Baseline Updated	Yes	Yes	\Services\Spooler

Total Items: 21
Selected Items: 0

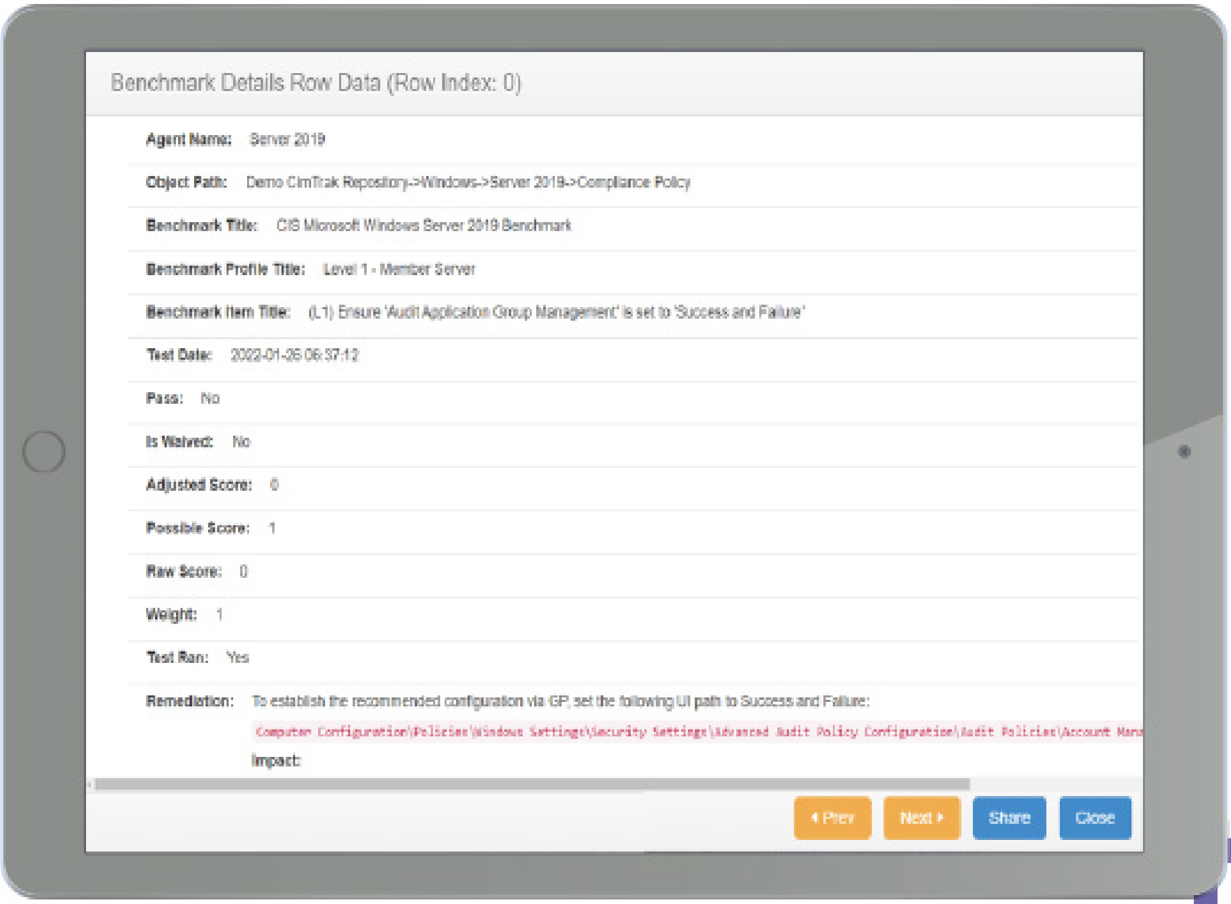
🟩 Green - Reconciled and is Auth Copy
🟥 Red - Was in
🟦 Blue - Reconciled
⬜ White - Unrec

The CimTrak results highlighting new services that were added, modified, or deleted.



Logging and Auditing

Logging needs to be reviewed as we often find that logging may be disabled, log file max size is too small to be useful, and ensure that all logs are backed up locally or to a centralized management platform. If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected.



Benchmark Details Row Data (Row Index: 0)

Agent Name: Server 2019

Object Path: Demo CimTrak Repository->Windows->Server 2019->Compliance Policy

Benchmark Title: CIS Microsoft Windows Server 2019 Benchmark

Benchmark Profile Title: Level 1 - Member Server

Benchmark Item Title: (L1) Ensure 'Audit Application Group Management' is set to 'Success and Failure'

Test Date: 2022-01-26 06:37:12

Pass: No

Is Waived: No

Adjusted Score: 0

Possible Score: 1

Raw Score: 0

Weight: 1

Test Ran: Yes

Remediation: To establish the recommended configuration via GP, set the following UI path to Success and Failure:

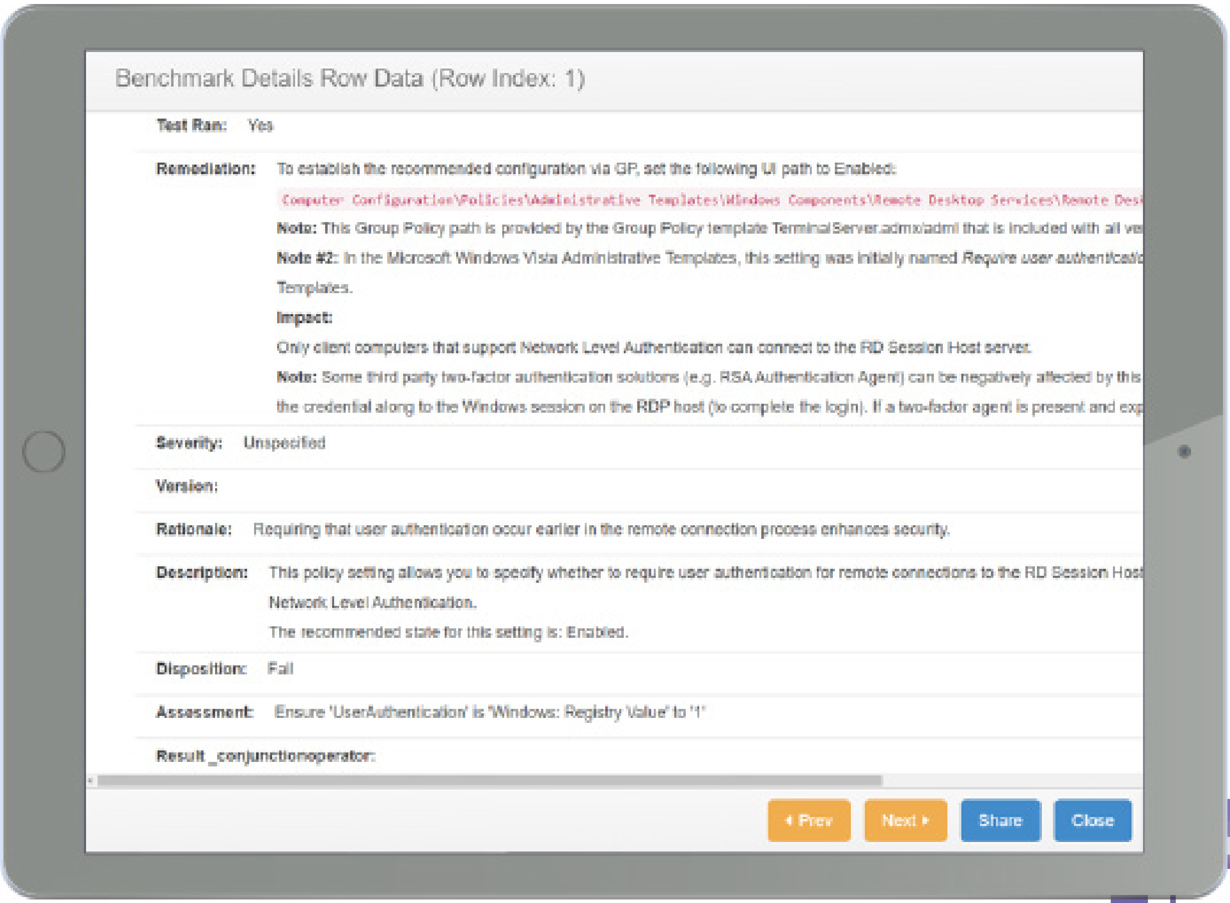
```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Mana
```

Impact:

The CimTrak results of a benchmark test that verifies and provides remediation steps to Ensure: 'Audit Application Group Managment is set to 'Success and Failure'.

Remote Access Hardening

Restrict remote access to an “as needed” basis. Enforce strict password requirements. Secure and monitor SSH, disable elevated privileges where possible, and use a non-elevated account when possible.



Benchmark Details Row Data (Row Index: 1)

Test Ran: Yes

Remediation: To establish the recommended configuration via GP, set the following UI path to Enabled:

`Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desk`

Note: This Group Policy path is provided by the Group Policy template TerminalServer.admx/adml that is included with all ve

Note #2: In the Microsoft Windows Vista Administrative Templates, this setting was initially named *Require user authenticatio*

Templates.

Impact:

Only client computers that support Network Level Authentication can connect to the RD Session Host server.

Note: Some third party two-factor authentication solutions (e.g. RSA Authentication Agent) can be negatively affected by this

the credential along to the Windows session on the RDP host (to complete the login). If a two-factor agent is present and exp

Severity: Unspecified

Version:

Rationale: Requiring that user authentication occur earlier in the remote connection process enhances security.

Description: This policy setting allows you to specify whether to require user authentication for remote connections to the RD Session Host

Network Level Authentication.

The recommended state for this setting is: Enabled.

Disposition: Fail

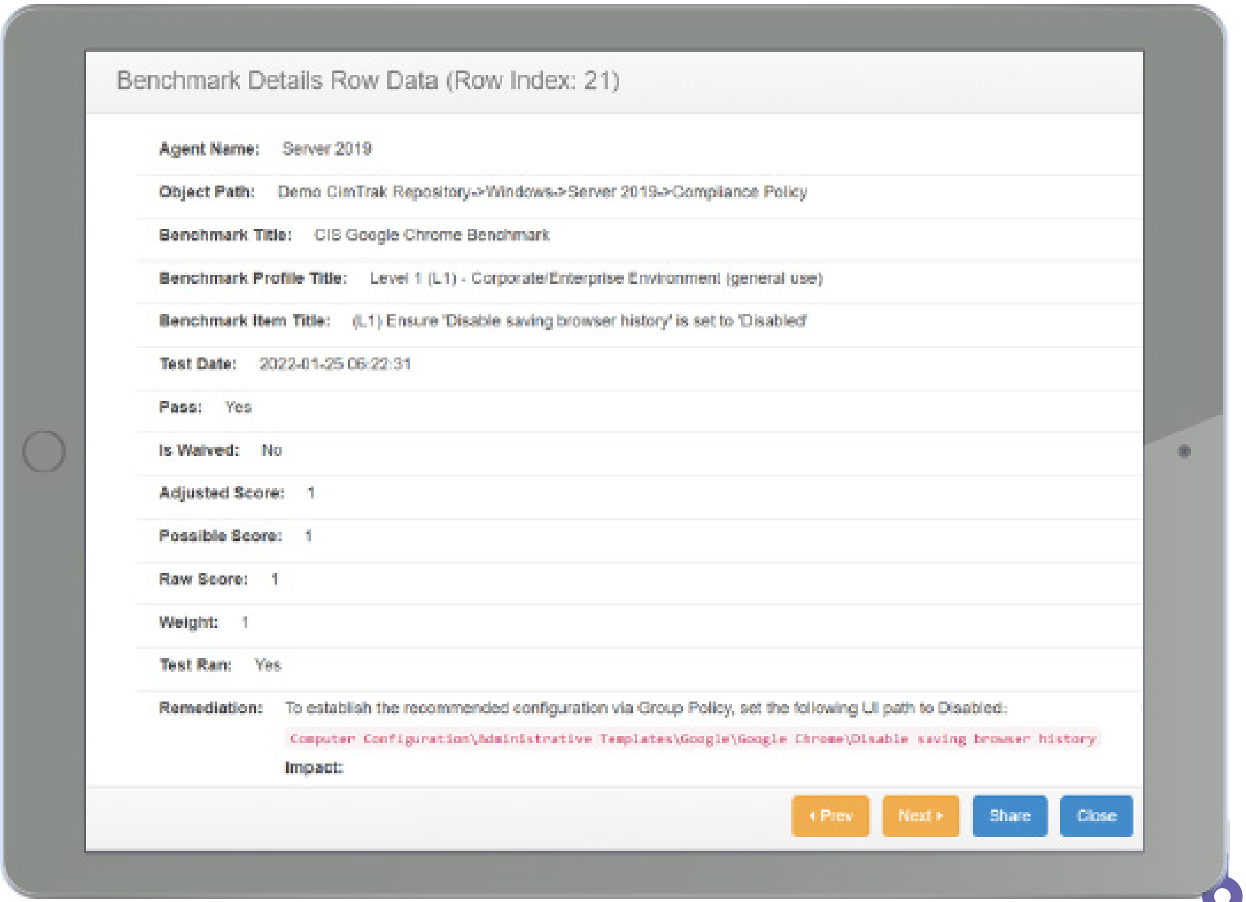
Assessment: Ensure 'UserAuthentication' is 'Windows: Registry Value' to '1'

Result_conjunctionoperator:

Only administrators who manage the systems should have access or other users who may require the use of that system. Having lenient settings for remote access may allow unauthorized users or attackers to gain access to the system and wreak havoc on the registry remotely or even gain RDP or SSH access. Some environments create multiple “jump” environments in different subnets that act as portals to access their segregated systems to prevent unauthorized access.

Software Configuration (i.e. Databases)

Restrict administrative privileges, implement role-based access, and maintain regular software update practices. There are benchmarks for many applications such as Google Chrome, Microsoft Office, SQL Server, Oracle Database, PostgreSQL, NGINX, Acrobat Reader, IIS, Internet Explorer, McAfee, DotNet Framework and more. Most of these applications are not secure out of the box. Hardening these applications are just as important as hardening the OS itself as they both are the backbone of your production environment.



Benchmark Details Row Data (Row Index: 21)

Agent Name: Server 2019

Object Path: Demo CimTrak Repository->Windows->Server 2019->Compliance Policy

Benchmark Title: CIS Google Chrome Benchmark

Benchmark Profile Title: Level 1 (L1) - Corporate/Enterprise Environment (general use)

Benchmark Item Title: (L1) Ensure 'Disable saving browser history' is set to 'Disabled'

Test Date: 2022-01-25 06:22:31

Pass: Yes

Is Waived: No

Adjusted Score: 1

Possible Score: 1

Raw Score: 1

Weight: 1

Test Ran: Yes

Remediation: To establish the recommended configuration via Group Policy, set the following UI path to Disabled:

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Disable saving browser history
```

Impact:

The CimTrak results of a benchmark test that verifies and provides remediation steps to Ensure: 'Disable saving browser history is set to Disabled'.

□ Access, Authentication, and Authorization

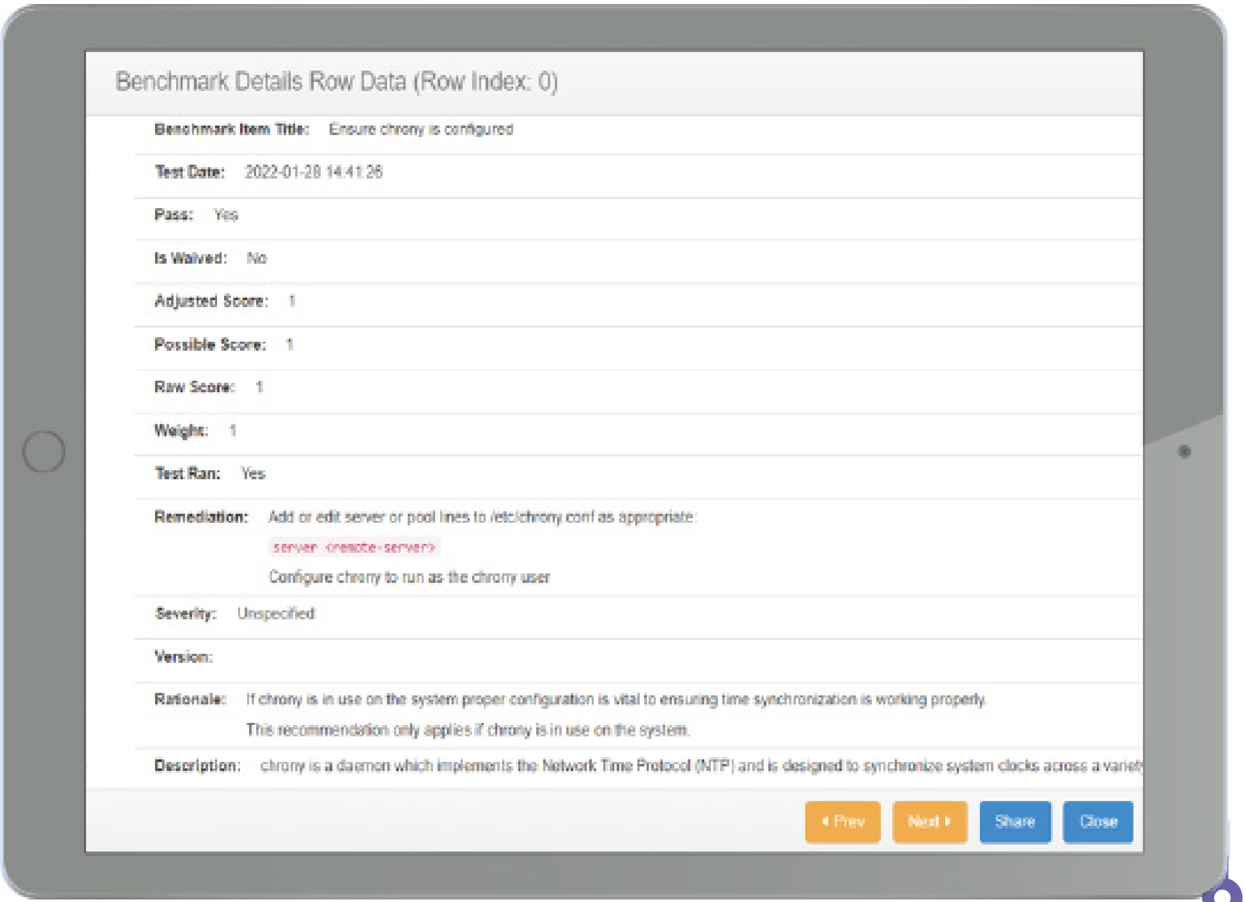
Ensure the systems are physically secured. Set up custom roles and strong passwords. Delete unnecessary operating system users, and avoid the use of root or “super admin” accounts with excessive privileges. Limit membership of admin groups. Grant elevated privileges on an as-needed basis. Consider multi factor authentication access.

□ Cloud Configuration

Use the cloud to your advantage, compartmentalize your infrastructure. Lock down your security groups and limit all ingress and egress traffic as needed. Use private subnets unless access to the internet is absolutely necessary. Imagine if the security groups for your AWS instances have changed, would you know? Getting alerted that ports are being open on your server is critical. Settings and configurations that exist OUTSIDE your system within these cloud interfaces need to be tracked and monitored as well for awareness of your environment and possible changes that could bring it down. Even volume changes or hardware changes that may suddenly impact a system’s performance. CimTrak can help monitor for these types of changes in Google Cloud, Amazon AWS, and Microsoft Azure.

Network Time Protocol Configuration

Minimize your attack exposure by making sure you have reviewed your NTP configuration and have removed or disabled any unnecessary NTP servers.   Incorrect configuration can cause systems to not communicate at all and possibly ruin production or disruptions to user access. Keeping systems in sync is critical for keeping them all online and available but also humans need to know the correct time within their domain.



Benchmark Details Row Data (Row Index: 0)

Benchmark Item Title: Ensure chrony is configured

Test Date: 2022-01-28 14:41:26

Pass: Yes

Is Waived: No

Adjusted Score: 1

Possible Score: 1

Raw Score: 1

Weight: 1

Test Ran: Yes

Remediation: Add or edit server or pool lines to /etc/chrony.conf as appropriate:

```
server <remote-server>
```

Configure chrony to run as the chrony user

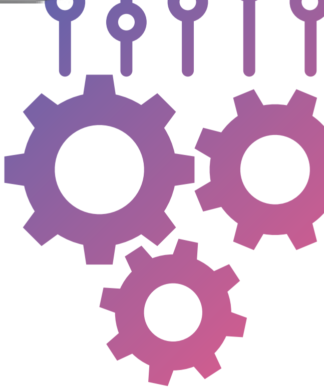
Severity: Unspecified

Version:

Rationale: If chrony is in use on the system proper configuration is vital to ensuring time synchronization is working properly.
This recommendation only applies if chrony is in use on the system.

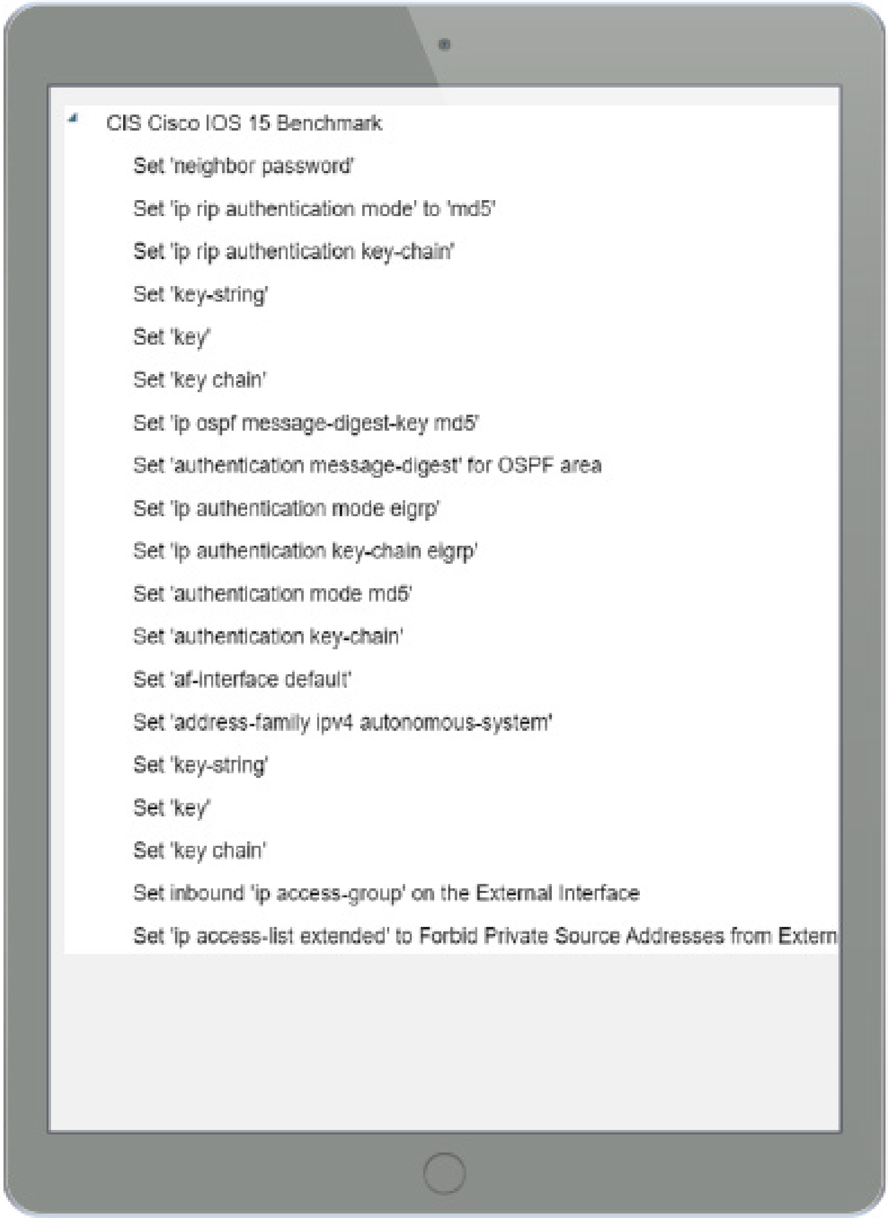
Description: chrony is a daemon which implements the Network Time Protocol (NTP) and is designed to synchronize system clocks across a variety

The CimTrak results of a benchmark test that verifies and provides remediation steps to Ensure: 'Chrony is configured' correctly.



Network Configuration

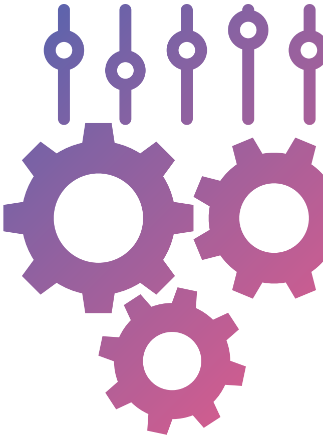
Most operating systems and network devices, including routers and switches, come equipped with services turned on when they are received from the manufacturer. Disabled services cannot be exploited by an adversary therefore, all unnecessary services should be disabled if they cannot be turned off considering blocking them at the firewall. Ensure DNS redundancy. Using CIS Benchmark guidelines can help provide a secure configuration posture for firewalls, switches, and routers which are the first line of defense of your network environment.



CIS Cisco IOS 15 Benchmark

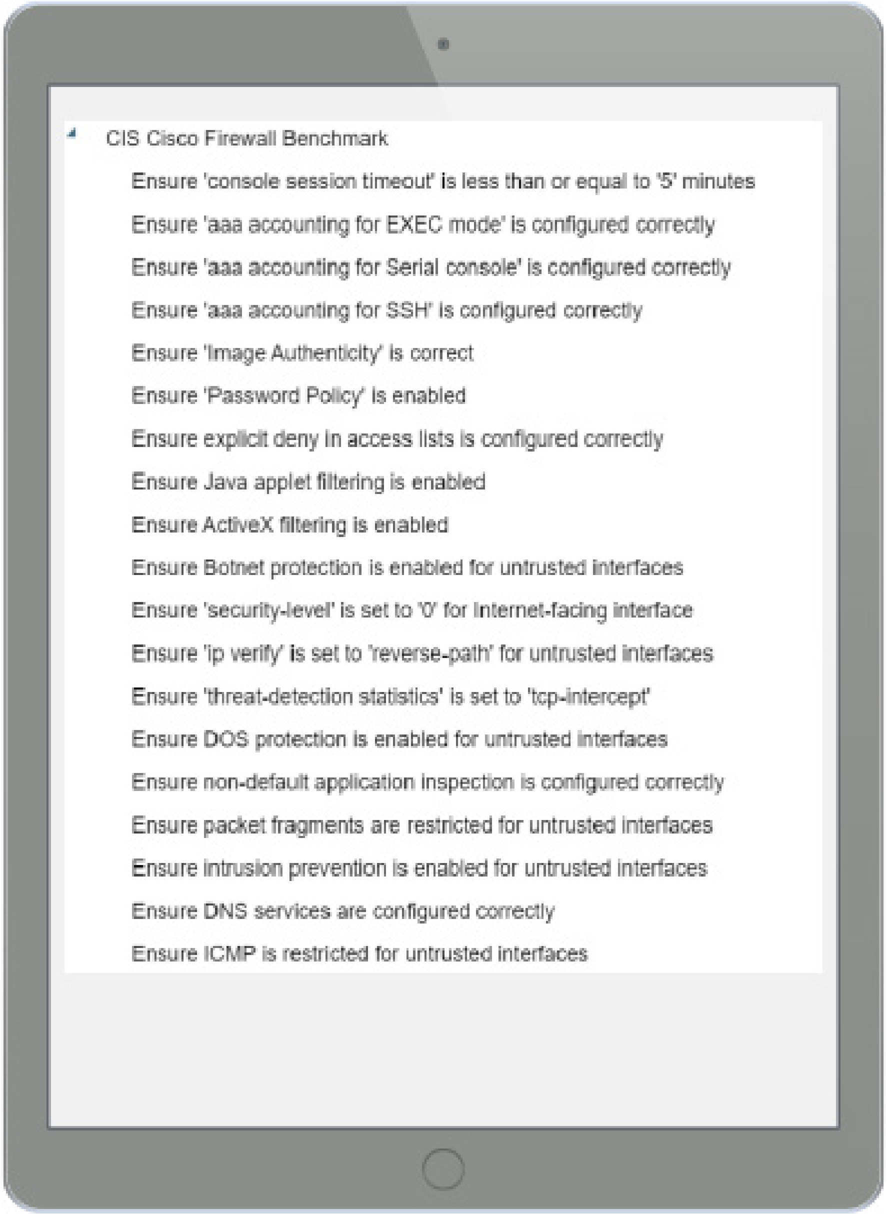
- Set 'neighbor password'
- Set 'ip rip authentication mode' to 'md5'
- Set 'ip rip authentication key-chain'
- Set 'key-string'
- Set 'key'
- Set 'key chain'
- Set 'ip ospf message-digest-key md5'
- Set 'authentication message-digest' for OSPF area
- Set 'ip authentication mode eigrp'
- Set 'ip authentication key-chain eigrp'
- Set 'authentication mode md5'
- Set 'authentication key-chain'
- Set 'af-interface default'
- Set 'address-family ipv4 autonomous-system'
- Set 'key-string'
- Set 'key'
- Set 'key chain'
- Set inbound 'ip access-group' on the External Interface
- Set 'ip access-list extended' to Forbid Private Source Addresses from Extern

CimTrak monitors and remediates the configurations and settings for network devices to ensure they have not deviated from an expected state of operation.



Firewall Configuration

Keep your Firewalls up to date. Make sure you have configured strong non-default passwords, audit account access regularly and remove unnecessary access. Make sure you have all your rules set to log and perform regular rule-base audits to remove unused or un-necessary rules. Using CIS Benchmark guidelines can help provide a secure configuration posture for firewalls, switches, and routers which are the first line of defense of your network environment.



CIS Cisco Firewall Benchmark

- Ensure 'console session timeout' is less than or equal to '5' minutes
- Ensure 'aaa accounting for EXEC mode' is configured correctly
- Ensure 'aaa accounting for Serial console' is configured correctly
- Ensure 'aaa accounting for SSH' is configured correctly
- Ensure 'Image Authenticity' is correct
- Ensure 'Password Policy' is enabled
- Ensure explicit deny in access lists is configured correctly
- Ensure Java applet filtering is enabled
- Ensure ActiveX filtering is enabled
- Ensure Botnet protection is enabled for untrusted interfaces
- Ensure 'security-level' is set to '0' for Internet-facing interface
- Ensure 'ip verify' is set to 'reverse-path' for untrusted interfaces
- Ensure 'threat-detection statistics' is set to 'tcp-intercept'
- Ensure DOS protection is enabled for untrusted interfaces
- Ensure non-default application inspection is configured correctly
- Ensure packet fragments are restricted for untrusted interfaces
- Ensure intrusion prevention is enabled for untrusted interfaces
- Ensure DNS services are configured correctly
- Ensure ICMP is restricted for untrusted interfaces

CimTrak monitors and remediates firewall configurations to ensure they have not deviated from an expected state of operation.

Supported Platforms

CimTrak for Servers, Critical Workstations & POS Systems

WINDOWS: XP, Vista, 7, 8, 10, Embedded for Point of Service (WEPOS), POSReady, Windows 10 IoT Enterprise
WINDOWS SERVER: 2003, 2008, 2012, 2016, 2019
LINUX: Amazon, CentOS, ClearOS, Debian, Fedora, Oracle, Red Hat, SUSE, Ubuntu, others
SUN SOLARIS: x86, SPARC
MAC: Intel, Power PC
HP-UX: Itanium, PA-RISC
AIX

Windows Parameters Monitored

FILE ADDITIONS, DELETIONS, MODIFICATIONS, AND READS
ATTRIBUTES: compressed, hidden, offline, read-only, archive, reparse point
Creation time, DACL information, Drivers, File opened/read, File Size, File type, Group security information, Installed software, Local groups, Local security policy, Modify time, Registry (keys and values), Services, User groups

UNIX Parameters Monitored

FILE ADDITIONS, DELETIONS, AND MODIFICATIONS
Access Control List, Attributes: read-only, archive, Creation time, File Size, File type, Modify time, User and Group ID

Supported Platforms CimTrak For Network Devices

Cisco, Check Point, Extreme, F5, Fortinet, HP, Juniper, Netgear, NetScreen, Palo Alto, others

Supported Platforms CimTrak For Databases

Oracle, IBM DB2, Microsoft SQL Server, MySQL
PARAMETERS MONITORED: Default Rules, Full-text indexes, Functions, Groups, Index definitions, Roles, Stored Procedures, Table definitions, Triggers, User defined data types, Users, Views

Supported Hypervisors

Microsoft Hyper-V, VMware ESXi 3x, 4x, 5x, 6x, 7x

Supported Cloud Platforms

Google Cloud, Amazon AWS, Microsoft Azure

Supported Container & Orchestration Integrations

Docker, Docker Enterprise, Kubernetes, Google Kubernetes Engine (GKE), Amazon Elastic Kubernetes Service (EKS)

Supported Ticketing Integrations

CA ServiceDesk, Atlassian Jira, ServiceNow, BMC Remedy

Supported SIEM Integrations

IBM QRadar, McAfee Event Security Manager, Splunk, LogRhythm, Microfocus Arcsight, others

CIMCOR

CIMTRAK

Cimcor develops innovative, next-generation, file integrity monitoring software. The CimTrak Integrity Suite monitors and protects a wide range of physical, network, cloud, and virtual IT assets in real-time, while providing detailed forensic information about all changes. Securing your infrastructure with CimTrak helps you get compliant and stay that way.

CIMCOR.COM | FOLLOW US @CIMTRAK