CIS Cisco NX OS Switch L2S STIG Benchmark

v1.0.0 - 08-22-2025

Terms of Use

Please see the below link for our current terms of use:

https://www.cisecurity.org/cis-securesuite/cis-securesuite-membership-terms-of-use/

For information on referencing and/or citing CIS Benchmarks in 3rd party documentation (including using portions of Benchmark Recommendations) please contact CIS Legal (legalnotices@cisecurity.org) and request guidance on copyright usage.

NOTE: It is ***NEVER*** acceptable to host a CIS Benchmark in ***ANY*** format (PDF, etc.) on a 3rd party (non-CIS owned) site.

Table of Contents

Overview

Target Technology Details

Cisco NX OS Switch L2S Secure Technical Implementation Guide (STIG)

Version: 3 Release: 2 Benchmark

Date: 24 Oct 2024

Intended Audience

This benchmark is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate Cisco NX OS Switch L2S and are looking to comply with the STIG guidance

Recommendation Definitions

The following defines the various components included in a CIS recommendation as applicable. If any of the components are not applicable it will be noted, or the component will not be included in the recommendation.

Title

Concise description for the recommendation's intended configuration.

Assessment Status

An assessment status is included for every recommendation. The assessment status indicates whether the given recommendation can be automated or requires manual steps to implement. Both statuses are equally important and are determined and supported as defined below:

Automated

Represents recommendations for which assessment of a technical control can be fully automated and validated to a pass/fail state. Recommendations will include the necessary information to implement automation.

Manual

Represents recommendations for which assessment of a technical control cannot be fully automated and requires all or some manual steps to validate that the configured state is set as expected. The expected state can vary depending on the environment.

Profile

A collection of recommendations (or rules) for securing a technology or a supporting platform. STIG Benchmark profiles are used to identify which Vulnerability Severity Category Code (CAT) each rule is associated with.

Description

The Rule Title from the STIG.

Rationale Statement

Detailed reasoning for the recommendation to provide the user a clear and concise understanding on the importance of the recommendation.

Audit Procedure

Systematic instructions for determining if the target system complies with the recommendation.

Remediation Procedure

Systematic instructions for applying recommendations to the target system to bring it into compliance according to the recommendation.

Additional Information

Supplementary information that does not correspond to any other field but may be useful to the user.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **SEVERITY: CAT I**

  Items in this profile exhibit one or more of the following characteristics:

  - are considered to be high severity
  - are intended for environments or use cases where following STIG based security guidance is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

  This profile is intended for servers and workstations.

- **SEVERITY: CAT II**

  Items in this profile exhibit one or more of the following characteristics:

  - are considered to be medium severity
  - are intended for environments or use cases where following STIG based security guidance is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

  This profile is intended for servers and workstations.

- **SEVERITY: CAT III**

  Items in this profile exhibit one or more of the following characteristics:

  - are considered to be low severity
  - are intended for environments or use cases where following STIG based security guidance is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

  This profile is intended for servers and workstations.

Acknowledgements

The Recommendations in this Benchmark are a representation of the Rules in the unclassified DISA STIG for Cisco NX OS Switch L2S.

Recommendations

1 STIG RULES

Cisco NX-OS

Cisco NX OS Switch L2S Secure Technical Implementation Guide (STIG)

Version: 3 Release: 2 Benchmark

Date: 24 Oct 2024

CLASSIFICATION unclassified

1.1 CISC-L2-000020 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The Cisco switch must uniquely identify all network-connected endpoint devices before establishing any connection.

```
GROUP ID: V-220675
RULE ID: SV-220675r539671
```

Rationale:

Controlling LAN access via 802.1x authentication can assist in preventing a malicious user from connecting an unauthorized PC to a switch port to inject or receive data from the network without detection.

Audit:

Verify if the switch configuration has 802.1x authentication implemented for all access switch ports connecting to LAN outlets (i.e., RJ-45 wall plates) or devices not located in the telecom room, wiring closets, or equipment rooms. MAC Authentication Bypass (MAB) must be configured on those switch ports connected to devices that do not support an 802.1x supplicant.

Step 1: Verify that 802.1x is configured on all host-facing interfaces as shown in the example below:

```
interface Ethernet1/1
 dot1x pae authenticator
 dot1x port-control auto
 dot1x host-mode single-host
 switchport access vlan 10
interface Ethernet1/2
 dot1x pae authenticator
 dot1x port-control auto
 dot1x host-mode single-host
 switchport access vlan 10
interface Ethernet1/3
 dot1x pae authenticator
 dot1x port-control auto
 dot1x host-mode single-host
 switchport access vlan 10
```

Note: Host-mode must be set to single-host, multi-domain (for VoIP phone + PC), or multi-auth (multiple PCs connected to a hub). Host-mode multi-host is not compliant with this requirement.

Step 2: Verify that 802.1x authentication is configured on the switch as shown in the example below:

```
aaa group server radius RADIUS_GROUP
 server 1.1.1.1
 server 1.2.1.1
…
…
…
aaa authentication dot1x default group RADIUS_GROUP
```

Step 3: Verify that the radius servers have been defined.

```
radius-server host 10.1.1.1 key 7 "xxxxxxxxxxx" authentication accounting
timeout 5 retransmit 1
radius-server host 10.2.1.1 key 7 " xxxxxxxxxxx" authentication accounting
timeout 5 retransmit 1
```

If 802.1x authentication or MAB is not configured on all access switch ports connecting to LAN outlets or devices not located in the telecom room, wiring closets, or equipment rooms, this is a finding.

Remediation:

Configure 802.1 x authentications on all host-facing access switch ports. To authenticate those devices that do not support 802.1x, MAC Authentication Bypass must be configured.

Step 1: Configure the radius servers as shown in the example below:

```
SW1(config)# radius-server host 10.1.1.1 key xxxx
SW1(config)# radius-server host 10.2.1.1 key xxxx
```

Step 2: Enable 802.1x authentication on the switch.

```
SW1(config)# aaa group server radius RADIUS_GROUP
SW1(config-radius)# server 10.1.1.1
SW1(config-radius)# server 10.2.1.1
SW1(config-radius)# exit
SW1(config)# aaa authentication dot1x default group RADIUS_GROUP
SW1(config)# exit
```

Step 3: Enable 802.1x on all host-facing interfaces as shown in the example below:

```
SW1(config)# int e1/1 - 80
SW1(config-if-range)# dot1x port-control auto
SW1(config-if-range)# dot1x host-mode single-host
SW1(config-if-range)# end
```

Note: Host-mode must be set to single-host, multi-domain (for VoIP phone + PC), or multi-auth (multiple PCs connected to a hub). Host-mode multi-host is not compliant with this requirement.

Additional Information:

CCI-000778 Uniquely identify organization-defined devices and/or types of devices before establishing a local, remote, and/or network connection.

- NIST SP 800-53::IA-3
- NIST SP 800-53A::IA-3.1 (ii)
- NIST SP 800-53 Revision 4::IA-3
- NIST SP 800-53 Revision 5::IA-3

1.2 CISC-L2-000030 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco switch must authenticate all VLAN Trunk Protocol (VTP) messages with a hash function using the most secured cryptographic algorithm available.

```
GROUP ID: V-220676
RULE ID: SV-220676r539671
```

Rationale:

VLAN Trunk Protocol (VTP) provides central management of VLAN domains, thus reducing administration in a switched network. When configuring a new VLAN on a VTP server, the VLAN is distributed through all switches in the domain. This reduces the need to configure the same VLAN everywhere. VTP pruning preserves bandwidth by preventing VLAN traffic (unknown MAC, broadcast, multicast) from being sent down trunk links when not needed, that is, there are no access switch ports in neighboring switches belonging to such VLANs. An attack can force a digest change for the VTP domain enabling a rogue device to become the VTP server, which could allow unauthorized access to previously blocked VLANs or allow the addition of unauthorized switches into the domain. Authenticating VTP messages with a cryptographic hash function can reduce the risk of the VTP domain's being compromised.

Audit:

Review the switch configuration to verify if VTP is enabled.

Step 1: Enter the show feature command to determine if vtp is enabled.

Step 2: Enter the show vtp status command to determine operating mode.

```
SW1# show vtp status
VTP Status Information
----------------------
VTP Version : 2 (capable)
Configuration Revision : 0
Maximum VLANs supported locally : 1005
Number of existing VLANs : 5
VTP Operating Mode : Transparent
VTP Domain Name : XXXXX
VTP Pruning Mode : Disabled (Operationally Disabled)
VTP V2 Mode : Disabled
VTP Traps Generation : Disabled
MD5 Digest : 0x0C 0x5E 0xC3 0x74 0x3F 0xB0 0x2F 0x49
```

If mode is set to anything other than off or transparent, verify that a password has been configured using the show vtp password command.

Note: VTP authenticates all messages using an MD5 hash that consists of the VTP version + The VTP Password + VTP Domain + VTP Configuration Revision.

If VTP is enabled on the switch and is not authenticating VTP messages with a hash function using a configured password, this is a finding.

Remediation:

Configure the switch to authenticate all VLAN Trunk Protocol (VTP) messages with a hash function using a configured password as shown in the example below:

```
SW1(config)# vtp password xxxxxxxxx
```

Additional Information:

CCI-000803 Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

- NIST SP 800-53::IA-7
- NIST SP 800-53A::IA-7.1
- NIST SP 800-53 Revision 4::IA-7
- NIST SP 800-53 Revision 5::IA-7

1.3 CISC-L2-000060 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco switch must be configured for authorized users to select a user session to capture.

```
GROUP ID: V-220677
RULE ID: SV-220677r1015266
```

Rationale:

Without the capability to select a user session to capture/record or view/hear, investigations into suspicious or harmful events would be hampered by the volume of information captured. The volume of information captured may also adversely impact the operation for the network. Session audits may include port mirroring, tracking websites visited, and recording information and/or file transfers.

Audit:

Verify that the switch is capable of capturing ingress and egress packets from any designated switch port for the purpose of monitoring a specific user session. The example configuration below will capture packets from interface Ethernet1/66 and replicate the packets to interface Ethernet1/68.

```
monitor session 1
 source interface Ethernet1/66 both
 destination interface Ethernet1/68
```

If the switch is not capable of capturing ingress and egress packets from a designated switch port, this is a finding.

Remediation:

Enable the feature or configure the switch so that it is capable of capturing ingress and egress packets from any designated switch port for the purpose of monitoring a specific user session. The example configuration below will capture packets from interface Ethernet1/66 and replicate the packets to Ethernet1/68.

```
SW1(config)# monitor session 1
SW1(config-monitor)# source interface ethernet 1/66
SW1(config-monitor)# destination interface ethernet 1/68
SW1(config-monitor)# end
```

Additional Information:

CCI-001919 Provide the capability for organization-defined users or roles to select a user session to record; view; hear; or log the content of a user session under organization-defined circumstances.

- NIST SP 800-53 Revision 4::AU-14
- NIST SP 800-53 Revision 5::AU-14 a

1.4 CISC-L2-000070 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco switch must be configured for authorized users to remotely view, in real time, all content related to an established user session from a component separate from The Cisco switch.

```
GROUP ID: V-220678
RULE ID: SV-220678r856487
```

Rationale:

Without the capability to remotely view/hear all content related to a user session, investigations into suspicious user activity would be hampered. Real-time monitoring allows authorized personnel to take action before additional damage is done. The ability to observe user sessions as they are happening allows for interceding in ongoing events that after-the-fact review of captured content would not allow.

Audit:

Verify that the switch is capable of capturing ingress and egress packets from any designated switch port for the purpose of remotely monitoring a specific user session. The example configuration below will capture packets from interface Ethernet1/66 and replicate the packets to interface Ethernet1/68.

```
monitor session 1
 source interface Ethernet1/66 both
 destination interface Ethernet1/68
```

If the switch is not capable of capturing ingress and egress packets from a designated switch port for the purpose of remotely monitoring a specific user session, this is a finding.

Remediation:

Enable the feature or configure the switch so that it is capable of capturing ingress and egress packets from any designated switch port for the purpose of monitoring a specific user session. The example configuration below will capture packets from interface Ethernet1/66 and replicate the packets to Ethernet1/68.

```
SW1(config)# monitor session 1
SW1(config-monitor)# source interface ethernet 1/66
SW1(config-monitor)# destination interface ethernet 1/68
SW1(config-monitor)# end
```

Additional Information:

CCI-001920 Provide the capability for authorized users to remotely view and hear content related to an established user session in real time.

- NIST SP 800-53 Revision 4::AU-14 (3)
- NIST SP 800-53 Revision 5::AU-14 (3)

1.5 CISC-L2-000080 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco switch must authenticate all endpoint devices before establishing any connection.

```
GROUP ID: V-220679
RULE ID: SV-220679r856488
```

Rationale:

Without authenticating devices, unidentified or unknown devices may be introduced, thereby facilitating malicious activity.

For distributed architectures (e.g., service-oriented architectures), the decisions regarding the validation of authentication claims may be made by services separate from the services acting on those decisions. In such situations, it is necessary to provide authentication decisions (as opposed to the actual authenticators) to the services that need to act on those decisions.

This requirement applies to applications that connect either locally, remotely, or through a network to an endpoint device (including, but not limited to, workstations, printers, servers (outside a datacenter), VoIP Phones, and VTC CODECs). Gateways and SOA applications are examples of where this requirement would apply.

Device authentication is a solution enabling an organization to manage devices. It is an additional layer of authentication ensuring only specific pre-authorized devices can access the system.

Audit:

Verify if the switch configuration has 802.1x authentication implemented for all access switch ports connecting to LAN outlets (i.e., RJ-45 wall plates) or devices not located in the telecom room, wiring closets, or equipment rooms. MAC Authentication Bypass (MAB) must be configured on those switch ports connected to devices that do not provide an 802.1x supplicant.

Step 1: Verify that 802.1x is configured on all host-facing interfaces as shown in the example below:

```
interface Ethernet1/1
 dot1x pae authenticator
 dot1x port-control auto
 dot1x host-mode single-host
 switchport access vlan 10
interface Ethernet1/2
 dot1x pae authenticator
 dot1x port-control auto
 dot1x host-mode single-host
 switchport access vlan 10
interface Ethernet1/3
 dot1x pae authenticator
 dot1x port-control auto
 dot1x host-mode single-host
 switchport access vlan 10
```

Note: Host-mode must be set to single-host, multi-domain (for VoIP phone + PC), or multi-auth (multiple PCs connected to a hub). Host-mode multi-host is not compliant with this requirement.

Step 2: Verify that 802.1x authentication is configured on the switch as shown in the example below:

```
aaa group server radius RADIUS_GROUP
 server 1.1.1.1
 server 1.2.1.1
…
…
…
aaa authentication dot1x default group RADIUS_GROUP
```

Step 3: Verify that the radius servers have been defined.

```
radius-server host 10.1.1.1 key 7 "xxxxxxxxxxx" authentication accounting
timeout 5 retransmit 1
radius-server host 10.2.1.1 key 7 " xxxxxxxxxxx" authentication accounting
timeout 5 retransmit 1
```

If 802.1x authentication or MAB is not on configured on all access switch ports connecting to LAN outlets or devices not located in the telecom room, wiring closets, or equipment rooms, this is a finding.

Remediation:

Configure 802.1 x authentications on all host-facing access switch ports. To authenticate those devices that do not support 802.1x, MAC Authentication Bypass must be configured.

Step 1: Configure the radius servers as shown in the example below:

```
SW1(config)# radius-server host 10.1.1.1 key xxxx
SW1(config)# radius-server host 10.2.1.1 key xxxx
```

Step 2: Enable 802.1x authentication on the switch.

```
SW1(config)# aaa group server radius RADIUS_GROUP
SW1(config-radius)# server 10.1.1.1
SW1(config-radius)# server 10.2.1.1
SW1(config-radius)# exit
SW1(config)# aaa authentication dot1x default group RADIUS_GROUP
SW1(config)# exit
```

Step 3: Enable 802.1x on all host-facing interfaces as shown in the example below:

```
SW1(config)# int e1/1 - 80
SW1(config-if-range)# dot1x port-control auto
SW1(config-if-range)# dot1x host-mode single-host
SW1(config-if-range)# end
```

Note: Host-mode must be set to single-host, multi-domain (for VoIP phone + PC), or multi-auth (multiple PCs connected to a hub). Host-mode multi-host is not compliant with this requirement.

Additional Information:

CCI-001958 Authenticate organization-defined devices and/or types of devices before establishing a local, remote, and/or network connection.

- NIST SP 800-53 Revision 4::IA-3
- NIST SP 800-53 Revision 5::IA-3

1.6 CISC-L2-000090 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The Cisco switch must have Root Guard enabled on all switch ports connecting to access layer switches and hosts.

```
GROUP ID: V-220680
RULE ID: SV-220680r940009
```

Rationale:

Spanning Tree Protocol (STP) does not provide any means for the network administrator to securely enforce the topology of the switched network. Any switch can be the root bridge in a network. However, a more optimal forwarding topology places the root bridge at a specific predetermined location. With the standard STP, any bridge in the network with a lower bridge ID takes the role of the root bridge. The administrator cannot enforce the position of the root bridge but can set the root bridge priority to 0 in an effort to secure the root bridge position.

The root guard feature provides a way to enforce the root bridge placement in the network. If the bridge receives superior STP Bridge Protocol Data Units (BPDUs) on a root guard-enabled port, root guard moves this port to a root-inconsistent STP state and no traffic can be forwarded across this port while it is in this state. To enforce the position of the root bridge it is imperative that root guard is enabled on all ports where the root bridge should never appear.

Audit:

Review the switch topology as well as the configuration to verify that Root Guard is enabled on all switch ports connecting to access layer switches.

```
interface Ethernet1/1
…
 …
 …
spanning-tree guard root
interface Ethernet1/2
…
 …
 …
spanning-tree guard root
interface Ethernet1/3
…
 …
 …
spanning-tree guard root
```

If the switch has not enabled Root Guard on all switch ports connecting to access layer switches, this is a finding

Remediation:

Configure the switch to have Root Guard enabled on all ports connecting to access layer switches.

```
SW1(config)# int e1/1 - 44
SW1(config-if-range)# spanning-tree guard root
SW1(config-if-range)# end
```

Additional Information:

CCI-002385 Protect against or limit the effects of organization-defined types of denial-of-service events.

- NIST SP 800-53 Revision 4::SC-5
- NIST SP 800-53 Revision 5::SC-5 a

1.7 CISC-L2-000100 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco switch must have BPDU Guard enabled on all user-facing or untrusted access switch ports.

```
GROUP ID: V-220681
RULE ID: SV-220681r856490
```

Rationale:

If a rogue switch is introduced into the topology and transmits a Bridge Protocol Data Unit (BPDU) with a lower bridge priority than the existing root bridge, it will become the new root bridge and cause a topology change, rendering the network in a suboptimal state. The STP PortFast BPDU guard enhancement allows network designers to enforce the STP domain borders and keep the active topology predictable. The devices behind the ports that have STP PortFast enabled are not able to influence the STP topology. At the reception of BPDUs, the BPDU guard operation disables the port that has PortFast configured. The BPDU guard transitions the port into errdisable state and sends a log message.

Audit:

Review the switch configuration to verify that BPDU Guard is enabled on all user-facing or untrusted access switch ports as shown in the configuration example below:

```
interface Ethernet1/1
…
 …
 …
spanning-tree bpduguard enable
interface Ethernet1/2
…
 …
 …
spanning-tree bpduguard enable
```

If the switch has not enabled BPDU Guard, this is a finding.

Remediation:

Configure the switch to have BPDU Guard enabled on all user-facing or untrusted access switch ports as shown in the configuration example below:

```
SW1(config)# int e1/1 -44
SW1(config-if-range)# spanning-tree bpduguard enable
```

Note: BPDU guard can also be enabled globally on all edge ports via the following command:

```
spanning-tree port type edge bpduguard default
```

Additional Information:

CCI-002385 Protect against or limit the effects of organization-defined types of denial-of-service events.

- NIST SP 800-53 Revision 4::SC-5
- NIST SP 800-53 Revision 5::SC-5 a

1.8 CISC-L2-000110 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco switch must have STP Loop Guard enabled.

```
GROUP ID: V-220682
RULE ID: SV-220682r856491
```

Rationale:

The Spanning Tree Protocol (STP) loop guard feature provides additional protection against STP loops. An STP loop is created when an STP blocking port in a redundant topology erroneously transitions to the forwarding state. In its operation, STP relies on continuous reception and transmission of BPDUs based on the port role. The designated port transmits BPDUs, and the non-designated port receives BPDUs. When one of the ports in a physically redundant topology no longer receives BPDUs, the STP conceives that the topology is loop free. Eventually, the blocking port from the alternate or backup port becomes a designated port and moves to a forwarding state. This situation creates a loop. The loop guard feature makes additional checks. If BPDUs are not received on a non-designated port and loop guard is enabled, that port is moved into the STP loop-inconsistent blocking state.

Audit:

Review the switch configuration to verify that STP Loop Guard is enabled as shown in the configuration example below:

```
hostname SW1
…
…
…
spanning-tree loopguard default
```

If STP Loop Guard is not enabled, this is a finding.

Remediation:

Configure the switch to have STP Loop Guard enabled via the spanning-tree loopguard default global command.

Additional Information:

CCI-002385 Protect against or limit the effects of organization-defined types of denial-of-service events.

- NIST SP 800-53 Revision 4::SC-5
- NIST SP 800-53 Revision 5::SC-5 a

1.9 CISC-L2-000120 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco switch must have Unknown Unicast Flood Blocking (UUFB) enabled.

```
GROUP ID: V-220683
RULE ID: SV-220683r856492
```

Rationale:

Access layer switches use the Content Addressable Memory (CAM) table to direct traffic to specific ports based on the VLAN number and the destination MAC address of the frame. When a router has an Address Resolution Protocol (ARP) entry for a destination host and forwards it to the access layer switch and there is no entry corresponding to the frame's destination MAC address in the incoming VLAN, the frame will be sent to all forwarding ports within the respective VLAN, which causes flooding. Large amounts of flooded traffic can saturate low-bandwidth links, causing network performance issues or complete connectivity outage to the connected devices. Unknown unicast flooding has been a nagging problem in networks that have asymmetric routing and default timers. To mitigate the risk of a connectivity outage, the Unknown Unicast Flood Blocking (UUFB) feature must be implemented on all access layer switches. The UUFB feature will block unknown unicast traffic flooding and only permit egress traffic with MAC addresses that are known to exit on the port.

Audit:

Review the switch configuration to verify that UUFB is enabled on all access switch ports as shown in the configuration example below:

```
interface Ethernet1/1
 switchport block unicast
interface Ethernet1/2
 switchport block unicast
…
…
…
interface Ethernet1/32
 switchport block unicast
```

If any access switch ports do not have UUFB enabled, this is a finding.

Remediation:

Configure the switch to have Unknown Unicast Flood Blocking (UUFB) enabled as shown in the configuration example below:

```
SW1(config)# int e1/1-32
SW1(config-if-range)# switchport block unicast
SW1(config-if-range)# end
```

Additional Information:

CCI-002385 Protect against or limit the effects of organization-defined types of denial-of-service events.

- NIST SP 800-53 Revision 4::SC-5
- NIST SP 800-53 Revision 5::SC-5 a

1.10 CISC-L2-000130 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco switch must have DHCP snooping for all user VLANs to validate DHCP messages from untrusted sources.

```
GROUP ID: V-220684
RULE ID: SV-220684r856493
```

Rationale:

In an enterprise network, devices under administrative control are trusted sources. These devices include the switches, routers, and servers in the network. Host ports and unknown DHCP servers are considered untrusted sources. An unknown DHCP server on the network on an untrusted port is called a spurious DHCP server, any device (PC, Wireless Access Point) that is loaded with DHCP server enabled. The DHCP snooping feature determines whether traffic sources are trusted or untrusted. The potential exists for a spurious DHCP server to respond to DHCPDISCOVER messages before the real server has time to respond. DHCP snooping allows switches on the network to trust the port a DHCP server is connected to and not trust the other ports.

The DHCP snooping feature validates DHCP messages received from untrusted sources and filters out invalid messages as well as rate-limits DHCP traffic from trusted and untrusted sources. DHCP snooping feature builds and maintains a binding database, which contains information about untrusted hosts with leased IP addresses, and it utilizes the database to validate subsequent requests from untrusted hosts. Other security features, such as IP Source Guard and Dynamic Address Resolution Protocol (ARP) Inspection (DAI), also use information stored in the DHCP snooping binding database. Hence, it is imperative that the DHCP snooping feature is enabled on all VLANs.

Audit:

Step 1: Review the switch configuration and verify that DHCP snooping is enabled on a per-VLAN basis as shown in the example below:

```
vlan 1,4,6-10
ip dhcp snooping
…
…
…
ip dhcp snooping vlan 4,6-10
```

Note: Switchports assigned to a user VLAN would have drops in the area where the user community would reside; hence, the "untrusted" term is used. Server and printer VLANs would not be applicable. By default, DHCP snooping is disabled on all VLANs.

If the switch does not have DHCP snooping enabled for all user VLANs to validate DHCP messages from untrusted sources, this is a finding.

Remediation:

Step 1: Enable the DHCP feature.

```
SW1(config)# feature dhcp
```

Step 2: Configure the switch to have DHCP snooping for all user VLANs to validate DHCP messages from untrusted sources as shown in the example below:

```
SW1(config)# ip dhcp snooping
SW1(config)# ip dhcp snooping vlan 4,6-10
```

Additional Information:

CCI-002385 Protect against or limit the effects of organization-defined types of denial-of-service events.

- NIST SP 800-53 Revision 4::SC-5
- NIST SP 800-53 Revision 5::SC-5 a

1.11 CISC-L2-000140 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco switch must have IP Source Guard enabled on all user-facing or untrusted access switch ports.

```
GROUP ID: V-220685
RULE ID: SV-220685r856494
```

Rationale:

IP Source Guard provides source IP address filtering on a Layer 2 port to prevent a malicious host from impersonating a legitimate host by assuming the legitimate host's IP address. The feature uses dynamic DHCP snooping and static IP source binding to match IP addresses to hosts on untrusted Layer 2 access ports. Initially, all IP traffic on the protected port is blocked except for DHCP packets. After a client receives an IP address from the DHCP server, or after static IP source binding is configured by the administrator, all traffic with that IP source address is permitted from that client. Traffic from other hosts is denied. This filtering limits a host's ability to attack the network by claiming a neighbor host's IP address.

Audit:

Review the switch configuration to verify that IP Source Guard is enabled on all user-facing or untrusted access switch ports as shown in the example below:

```
interface Ethernet1/1
 ip verify source dhcp-snooping-vlan
interface Ethernet1/2
 ip verify source dhcp-snooping-vlan
…
…
…
interface Ethernet1/32
 ip verify source dhcp-snooping-vlan
```

Note: the IP Source Guard feature depends on the entries in the DHCP snooping database or static IP-MAC-VLAN configuration commands to verify IP-to-MAC address bindings.

If the switch does not have IP Source Guard enabled on all untrusted access switch ports, this is a finding.

Remediation:

Configure the switch to have IP Source Guard enabled on all user-facing or untrusted access switch ports.

```
SW1(config)# int e1/1-32
SW1(config-if-range)# ip verify source dhcp-snooping-vlan
```

Additional Information:

CCI-002385 Protect against or limit the effects of organization-defined types of denial-of-service events.

- NIST SP 800-53 Revision 4::SC-5
- NIST SP 800-53 Revision 5::SC-5 a

1.12 CISC-L2-000150 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco switch must have Dynamic Address Resolution Protocol (ARP) Inspection (DAI) enabled on all user VLANs.

```
GROUP ID: V-220686
RULE ID: SV-220686r856495
```

Rationale:

DAI intercepts Address Resolution Protocol (ARP) requests and verifies that each of these packets has a valid IP-to-MAC address binding before updating the local ARP cache and before forwarding the packet to the appropriate destination. Invalid ARP packets are dropped and logged. DAI determines the validity of an ARP packet based on valid IP-to-MAC address bindings stored in the DHCP snooping binding database. If the ARP packet is received on a trusted interface, the switch forwards the packet without any checks. On untrusted interfaces, the switch forwards the packet only if it is valid.

Audit:

Review the switch configuration to verify that Dynamic Address Resolution Protocol (ARP) Inspection (DAI) feature is enabled on all user VLANs.

```
hostname SW2
…
…
…
ip arp inspection vlan 2,4-8,11
```

Note: DAI depends on the entries in the DHCP snooping binding database to verify IP-to-MAC address bindings in incoming ARP requests and ARP responses.

If DAI is not enabled on all user VLANs, this is a finding.

Remediation:

Configure the switch to have Dynamic Address Resolution Protocol (ARP) Inspection (DAI) enabled on all user VLANs as shown in the example below:

```
SW1(config)# ip arp inspection vlan 2,4-8,11
```

Additional Information:

CCI-002385 Protect against or limit the effects of organization-defined types of denial-of-service events.

- NIST SP 800-53 Revision 4::SC-5
- NIST SP 800-53 Revision 5::SC-5 a

1.13 CISC-L2-000160 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The Cisco switch must have Storm Control configured on all host-facing switchports.

```
GROUP ID: V-220687
RULE ID: SV-220687r539671
```

Rationale:

A traffic storm occurs when packets flood a LAN, creating excessive traffic and degrading network performance. Traffic storm control prevents network disruption by suppressing ingress traffic when the number of packets reaches a configured threshold levels. Traffic storm control monitors ingress traffic levels on a port and drops traffic when the number of packets reaches the configured threshold level during any one-second interval.

Audit:

Review the switch configuration to verify that storm control is enabled on all host-facing interfaces as shown in the example below:

```
interface GigabitEthernet0/3
 switchport access vlan 12
 storm-control unicast unicast level 50.00
 storm-control broadcast broadcast level 40
```

If storm control is not enabled at a minimum for broadcast traffic, this is a finding.

Remediation:

Configure storm control for each host-facing interface as shown in the example below:

```
SW1(config)#int range e0/2 - 8
SW1(config-if-range)# storm-control unicast level 50
SW1(config-if-range)# storm-control broadcast level 40
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.14 CISC-L2-000170 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The Cisco switch must have IGMP or MLD Snooping configured on all VLANs.

```
GROUP ID: V-220688
RULE ID: SV-220688r539671
```

Rationale:

IGMP and MLD snooping provides a way to constrain multicast traffic at Layer 2. By monitoring the IGMP or MLD membership reports sent by hosts within a VLAN, the snooping application can set up Layer 2 multicast forwarding tables to deliver specific multicast traffic only to interfaces connected to hosts interested in receiving the traffic, thereby significantly reducing the volume of multicast traffic that would otherwise flood the VLAN.

Audit:

Review the switch configuration to verify that IGMP or MLD snooping has been configured for IPv4 and IPv6 multicast traffic respectively. The example below are the steps to verify that IGMP snooping is enabled for each VLAN.

Step 1: Verify that IGMP or MLD snooping is enabled globally. By default, IGMP snooping is enabled globally; hence, the following command should not be in the switch configuration:

```
no ip igmp snooping
```

Step 2: Verify that IGMP snooping is not disabled for any VLAN as shown in the example below:

```
no ip igmp snooping vlan 11
```

Note: When globally enabled, it is also enabled by default on all VLANs, but can be disabled on a per-VLAN basis. If global snooping is disabled, VLAN snooping cannot be enabled. If global snooping is enabled, VLAN snooping cannot be enabled or disabled.

If the switch is not configured to implement IGMP or MLD snooping for each VLAN, this is a finding.

Remediation:

Configure IGMP or MLD snooping for IPv4 and IPv6 multicast traffic respectively globally.

```
SW1(config)# ip igmp snooping
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.15 CISC-L2-000190 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco switch must enable Unidirectional Link Detection (UDLD) to protect against one-way connections.

```
GROUP ID: V-220689
RULE ID: SV-220689r917685
```

Rationale:

In topologies where fiber optic interconnections are used, physical misconnections can occur that allow a link to appear to be up when there is a mismatched set of transmit/receive pairs. When such a physical misconfiguration occurs, protocols such as STP can cause network instability. UDLD is a layer 2 protocol that can detect these physical misconfigurations by verifying that traffic is flowing bidirectionally between neighbors. Ports with UDLD enabled periodically transmit packets to neighbor devices. If the packets are not echoed back within a specific time frame, the link is flagged as unidirectional and the interface is shut down.

Audit:

If any of the switch ports have fiber optic interconnections with neighbors, review the switch configuration to verify that either UDLD is enabled globally or not explicitly disabled on a per interface basis as shown in the examples below.

```
hostname SW1
…
…
…
feature udld
```

or

```
interface GigabitEthernet0/3
udld disabled
```

Note: By default, UDLD is enabled on all interfaces with fiber optic connections. An alternative implementationwhen UDLD is not supported by connected device is to deploy a single member Link Aggregation Group (LAG) via IEEE 802.3ad Link Aggregation Control Protocol (LACP).

If the switch has fiber optic interconnections with neighbors and UDLD is not enabled, this is a finding.

Remediation:

Configure the switch to enable Unidirectional Link Detection (UDLD) to protect against one-way connections.

```
SW1(config)# feature udld
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.16 CISC-L2-000210 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco switch must have all disabled switch ports assigned to an unused VLAN.

```
GROUP ID: V-220690
RULE ID: SV-220690r991946
```

Rationale:

It is possible that a disabled port that is assigned to a user or management VLAN becomes enabled by accident or by an attacker and as a result gains access to that VLAN as a member.

Audit:

Step 1: Review the switch configurations and examine all access switch ports. Each access switch port not in use should have membership to an inactive VLAN.

```
interface Ethernet1/81
 shutdown
 switchport access vlan 999
interface Ethernet1/82
 shutdown
 switchport access vlan 999
interface Ethernet1/83
 shutdown
 switchport access vlan 999
```

Step 2: Verify that traffic from the inactive VLAN is not allowed on any trunk links as shown in the example below:

```
interface Ethernet1/1
 switchport mode trunk
 switchport trunk allowed vlan 1-998,1000-4094
```

Note: Switch ports configured for 802.1x are exempt from this requirement.

If there are any access switch ports not in use and not in an inactive VLAN, this is a finding.

Remediation:

Assign all switch ports not in use to an inactive VLAN.

Step 1: Assign the disabled interfaces to an inactive VLAN.

```
SW1(config)# int e1/81-128
SW1(config-if-range)# switchport access vlan 999
SW1(config-if-range)# end
```

Step 2: Configure trunk links to not allow traffic from the inactive VLAN.

```
SW1(config-if)# switchport trunk allowed vlan except 999
SW1(config-if)# end
```

Additional Information:

CCI-004891 Implement physically or logically separate subnetworks to isolate organization-defined critical system components and functions.

- NIST SP 800-53 Revision 5::SC-7 (29)

1.17 CISC-L2-000240 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco switch must not use the default VLAN for management traffic.

```
GROUP ID: V-220693
RULE ID: SV-220693r991949
```

Rationale:

Switches use the default VLAN (i.e., VLAN 1) for in-band management and to communicate with directly connected switches using Spanning-Tree Protocol (STP), Dynamic Trunking Protocol (DTP), VLAN Trunking Protocol (VTP), and Port Aggregation Protocol (PAgP)—all untagged traffic. As a consequence, the default VLAN may unwisely span the entire network if not appropriately pruned. If its scope is large enough, the risk of compromise can increase significantly.

Audit:

Review the switch configuration and verify that the default VLAN is not used to access the switch for management.

```
interface Vlan1
interface Vlan44
 description Management VLAN
 ip address 10.1.12.1/24
```

If the default VLAN is being used for management access to the switch, this is a finding.

Remediation:

Configure the switch for management access to use a VLAN other than the default VLAN.

```
SW1(config)# interface vlan 44
SW1(config-if)# ip add 10.1.12.1/24
SW1(config-if)# end
```

Additional Information:

CCI-004931 Establish organization-defined alternate communications paths for system operations organizational command and control.

- NIST SP 800-53 Revision 5::SC-47

1.18 CISC-L2-000220 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco switch must not have the default VLAN assigned to any host-facing switch ports.

```
GROUP ID: V-220691
RULE ID: SV-220691r991947
```

Rationale:

In a VLAN-based network, switches use the default VLAN (i.e., VLAN 1) for in-band management and to communicate with other networking devices using Spanning-Tree Protocol (STP), Dynamic Trunking Protocol (DTP), VLAN Trunking Protocol (VTP), and Port Aggregation Protocol (PAgP)—all untagged traffic. As a consequence, the default VLAN may unwisely span the entire network if not appropriately pruned. If its scope is large enough, the risk of compromise can increase significantly.

Audit:

Review the switch configurations and verify that no access switch ports have been assigned membership to the default VLAN (i.e., VLAN 1). VLAN assignments can be verified via the show vlan command. In the example below, interfaces 1/1 and 1/2 are trunk links.

```
SW1# show vlan

VLAN Name Status Ports
---- -------------------------------- --------- -------------------------------
--
1 default active Eth1/1, Eth1/2
10 VLAN0010 active Eth1/1, Eth1/2, Eth1/3, Eth1/4
 Eth1/5, Eth1/6, Eth1/7, Eth1/8
 Eth1/9, Eth1/10, Eth1/11
 Eth1/12, Eth1/13, Eth1/14
 Eth1/15, Eth1/16, Eth1/17
 Eth1/18, Eth1/19, Eth1/20
 Eth1/21, Eth1/22, Eth1/23
 Eth1/24, Eth1/25, Eth1/26
 Eth1/27, Eth1/28, Eth1/29
 Eth1/30
11 VLAN0011 active Eth1/1, Eth1/2, Eth1/31
 Eth1/32, Eth1/33, Eth1/34
 Eth1/35, Eth1/36, Eth1/37
 Eth1/38, Eth1/39, Eth1/40
```

If there are access switch ports assigned to the default VLAN, this is a finding.

Remediation:

Remove the assignment of the default VLAN from all access switch ports.

Additional Information:

CCI-004891 Implement physically or logically separate subnetworks to isolate organization-defined critical system components and functions.

- NIST SP 800-53 Revision 5::SC-7 (29)

1.19 CISC-L2-000230 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco switch must have the default VLAN pruned from all trunk ports that do not require it.

```
GROUP ID: V-220692
RULE ID: SV-220692r991948
```

Rationale:

The default VLAN (i.e., VLAN 1) is a special VLAN used for control plane traffic such as Spanning-Tree Protocol (STP), Dynamic Trunking Protocol (DTP), VLAN Trunking Protocol (VTP), and Port Aggregation Protocol (PAgP). VLAN 1 is enabled on all trunks and ports by default. With larger campus networks, care needs to be taken about the diameter of the STP domain for the default VLAN. Instability in one part of the network could affect the default VLAN, thereby influencing control-plane stability and therefore STP stability for all other VLANs.

Audit:

Review the switch configuration and verify that the default VLAN is pruned from trunk links that do not require it.

```
SW1# show interface trunk
--------------------------------------------------------------------------------
---
Port Native Status Port
 Vlan Channel
--------------------------------------------------------------------------------
---
Eth1/1 1 trunking --
Eth1/2 1 trunking --

--------------------------------------------------------------------------------
---
Port Vlans Allowed on Trunk
--------------------------------------------------------------------------------
---
Eth1/1 1-998,1000-4094
Eth1/2 1-998,1000-4094
```

If the default VLAN is not pruned from trunk links that should not be transporting frames for the VLAN, this is a finding.

Remediation:

Step 1: Prune VLAN 1 from any trunk links as necessary.

```
SW1(config)# int e1/2
SW1(config-if)# switchport trunk allowed vlan except 1, 999
SW1(config-if)# end
```

Step 2: Verify VLAN 1 is not allowed on the trunk link.

```
SW1# show interface trunk

--------------------------------------------------------------------------------
---
Port Native Status Port
 Vlan Channel
--------------------------------------------------------------------------------
---
Eth1/1 1 trunking --
Eth1/2 1 trunking --

--------------------------------------------------------------------------------
---
Port Vlans Allowed on Trunk
--------------------------------------------------------------------------------
---
Eth1/1 1-998,1000-4094
Eth1/2 2-998,1000-4094
```

Additional Information:

CCI-004891 Implement physically or logically separate subnetworks to isolate organization-defined critical system components and functions.

- NIST SP 800-53 Revision 5::SC-7 (29)

1.20 CISC-L2-000250 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco switch must have all user-facing or untrusted ports configured as access switch ports.

```
GROUP ID: V-220694
RULE ID: SV-220694r991951
```

Rationale:

Double encapsulation can be initiated by an attacker who has access to a switch port belonging to the native VLAN of the trunk port. Knowing the victim's MAC address and with the victim attached to a different switch belonging to the same trunk group, thereby requiring the trunk link and frame tagging, the malicious user can begin the attack by sending frames with two sets of tags. The outer tag that will have the attacker's VLAN ID (probably the well-known and omnipresent default VLAN) is stripped off by the switch, and the inner tag that will have the victim's VLAN ID is used by the switch as the next hop and sent out the trunk port.

Audit:

Review the switch configurations and examine all user-facing or untrusted switchports. The example below depicts both access and trunk ports.

```
interface Ethernet1/1
 switchport
 switchport mode trunk
 switchport trunk allowed vlan 1-998,1000-4094
interface Ethernet1/2
 switchport
 switchport mode trunk
 switchport trunk allowed vlan 2-998,1000-4094
interface Ethernet1/3
interface Ethernet1/4
 switchport access vlan 10
```

Note: Switchport mode access is the default and hence will not be shown in the configuration.

If any of the user-facing switch ports are configured as a trunk, this is a finding.

Remediation:

Disable trunking on all user-facing or untrusted switch ports.

```
SW1(config)# int e1/3-128
SW1(config-if)# switchport mode access
SW1(config-if)# end
```

Additional Information:

CCI-004891 Implement physically or logically separate subnetworks to isolate organization-defined critical system components and functions.

- NIST SP 800-53 Revision 5::SC-7 (29)

1.21 CISC-L2-000260 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Cisco switch must have the native VLAN assigned to an ID other than the default VLAN for all 802.1q trunk links.

```
GROUP ID: V-220695
RULE ID: SV-220695r991952
```

Rationale:

VLAN hopping can be initiated by an attacker who has access to a switch port belonging to the same VLAN as the native VLAN of the trunk link connecting to another switch that the victim is connected to. If the attacker knows the victim's MAC address, it can forge a frame with two 802.1q tags and a layer 2 header with the destination address of the victim. Since the frame will ingress the switch from a port belonging to its native VLAN, the trunk port connecting to the victim's switch will simply remove the outer tag because native VLAN traffic is to be untagged. The switch will forward the frame on to the trunk link unaware of the inner tag with a VLAN ID of which the victim's switch port is a member.

Audit:

Review the switch configurations and examine all trunk links. Verify the native VLAN has been configured to a VLAN ID other than the ID of the default VLAN (i.e. VLAN 1) as shown in the example below:

```
interface Ethernet0/1
switchport
switchport mode trunk
switchport trunk native vlan 44
```

Note: An alternative to configuring a dedicated native VLAN is to ensure that all native VLAN traffic is tagged. This will mitigate the risk of VLAN hopping since there will always be an outer tag for native traffic as it traverses an 802.1q trunk link.

If the native VLAN has the same VLAN ID as the default VLAN, this is a finding.

Remediation:

To ensure the integrity of the trunk link and prevent unauthorized access, the ID of the native VLAN of the trunk port must be changed from the default VLAN (i.e., VLAN 1) to its own unique VLAN ID.

```
SW1(config)#int e0/1
SW1(config-if)#switchport trunk native vlan 44
```

Note: The native VLAN ID must be the same on both ends of the trunk link; otherwise, traffic could accidentally leak between broadcast domains.

Additional Information:

CCI-004891 Implement physically or logically separate subnetworks to isolate organization-defined critical system components and functions.

- NIST SP 800-53 Revision 5::SC-7 (29)

1.22 CISC-L2-000270 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The Cisco switch must not have any switchports assigned to the native VLAN.

```
GROUP ID: V-220696
RULE ID: SV-220696r991953
```

Rationale:

Double encapsulation can be initiated by an attacker who has access to a switch port belonging to the native VLAN of the trunk port. Knowing the victim's MAC address and with the victim attached to a different switch belonging to the same trunk group, thereby requiring the trunk link and frame tagging, the malicious user can begin the attack by sending frames with two sets of tags. The outer tag that will have the attacker's VLAN ID (probably the well-known and omnipresent default VLAN) is stripped off by the switch, and the inner tag that will have the victim's VLAN ID is used by the switch as the next hop and sent out the trunk port.

Audit:

Review the switch configurations and examine all access switch ports. Verify that they do not belong to the native VLAN as shown in the example below:

```
interface Ethernet0/1
switchport
switchport mode trunk
switchport trunk native vlan 44
interface Ethernet0/2
 switchport
 switchport access vlan 11
interface Ethernet0/3
 switchport
 switchport access vlan 12
```

If any access switch ports have been assigned to the same VLAN ID as the native VLAN, this is a finding.

Remediation:

Configure all access switch ports to a VLAN other than the native VLAN.

Additional Information:

CCI-004891 Implement physically or logically separate subnetworks to isolate organization-defined critical system components and functions.

- NIST SP 800-53 Revision 5::SC-7 (29)

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	**STIG RULES**		
1.1	CISC-L2-000020 (Manual)	☐	☐
1.2	CISC-L2-000030 (Manual)	☐	☐
1.3	CISC-L2-000060 (Manual)	☐	☐
1.4	CISC-L2-000070 (Manual)	☐	☐
1.5	CISC-L2-000080 (Manual)	☐	☐
1.6	CISC-L2-000090 (Manual)	☐	☐
1.7	CISC-L2-000100 (Manual)	☐	☐
1.8	CISC-L2-000110 (Manual)	☐	☐
1.9	CISC-L2-000120 (Manual)	☐	☐
1.10	CISC-L2-000130 (Manual)	☐	☐
1.11	CISC-L2-000140 (Manual)	☐	☐
1.12	CISC-L2-000150 (Manual)	☐	☐
1.13	CISC-L2-000160 (Manual)	☐	☐
1.14	CISC-L2-000170 (Manual)	☐	☐
1.15	CISC-L2-000190 (Manual)	☐	☐
1.16	CISC-L2-000210 (Manual)	☐	☐
1.17	CISC-L2-000240 (Manual)	☐	☐
1.18	CISC-L2-000220 (Manual)	☐	☐
1.19	CISC-L2-000230 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.20	CISC-L2-000250 (Manual)	☐	☐
1.21	CISC-L2-000260 (Manual)	☐	☐
1.22	CISC-L2-000270 (Manual)	☐	☐

Appendix: Change History

Date	Version	Changes for this version
Aug 22, 2025	1.0.0	Initial CIS Release