GÉANT
Networks • Services • People

Looking into the network

How to scan local systems for vulnerabilities and misconfigurations

Stefan Kelm
WP8-T1

Webinar, 28th of June 2021

Public

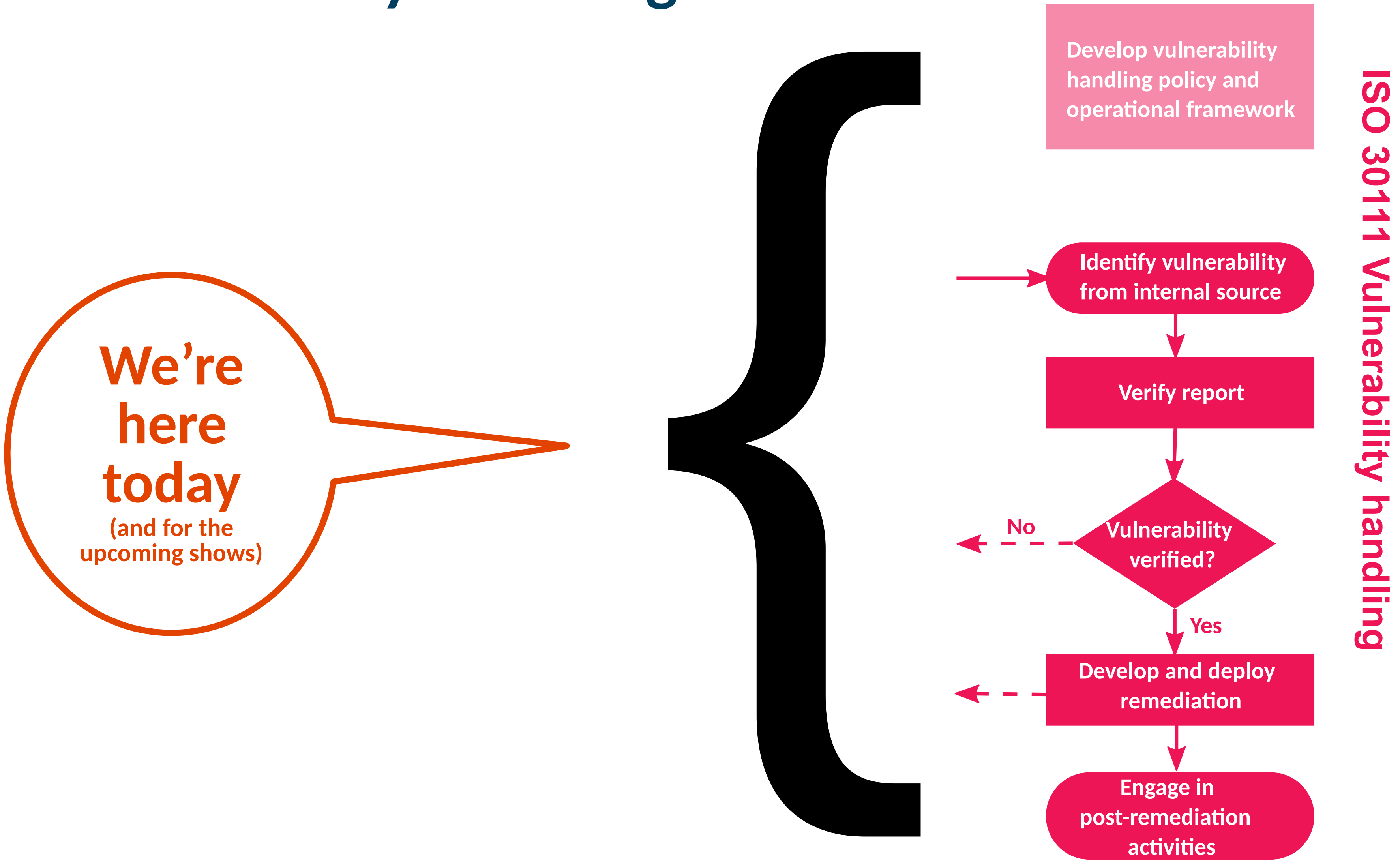
Finding Vulnerabilities I - Looking into the network

- Local Vulnerability Scanning
  - Benchmarks and baselines
  - Tools: CIS-CAT, MS, OpenSCAP
- Network Vulnerability Scanning
  - How to plan and conduct network scans
  - Tools: Nmap, OpenVAS
- Penetration Tests
  - Why, when and how
  - Examples of pentest tools: ZAP, Metasploit

What we will cover today

- Local Vulnerability Scanning
  - (Standards / Processes)
  - Checklists / Benchmarks
    - CIS Controls / CIS Benchmarks
    - Windows Security Baselines
    - SCAP Security Guide
  - Tools
    - CIS-CAT
    - MS Security Compliance Toolkit
    - OpenSCAP Demo

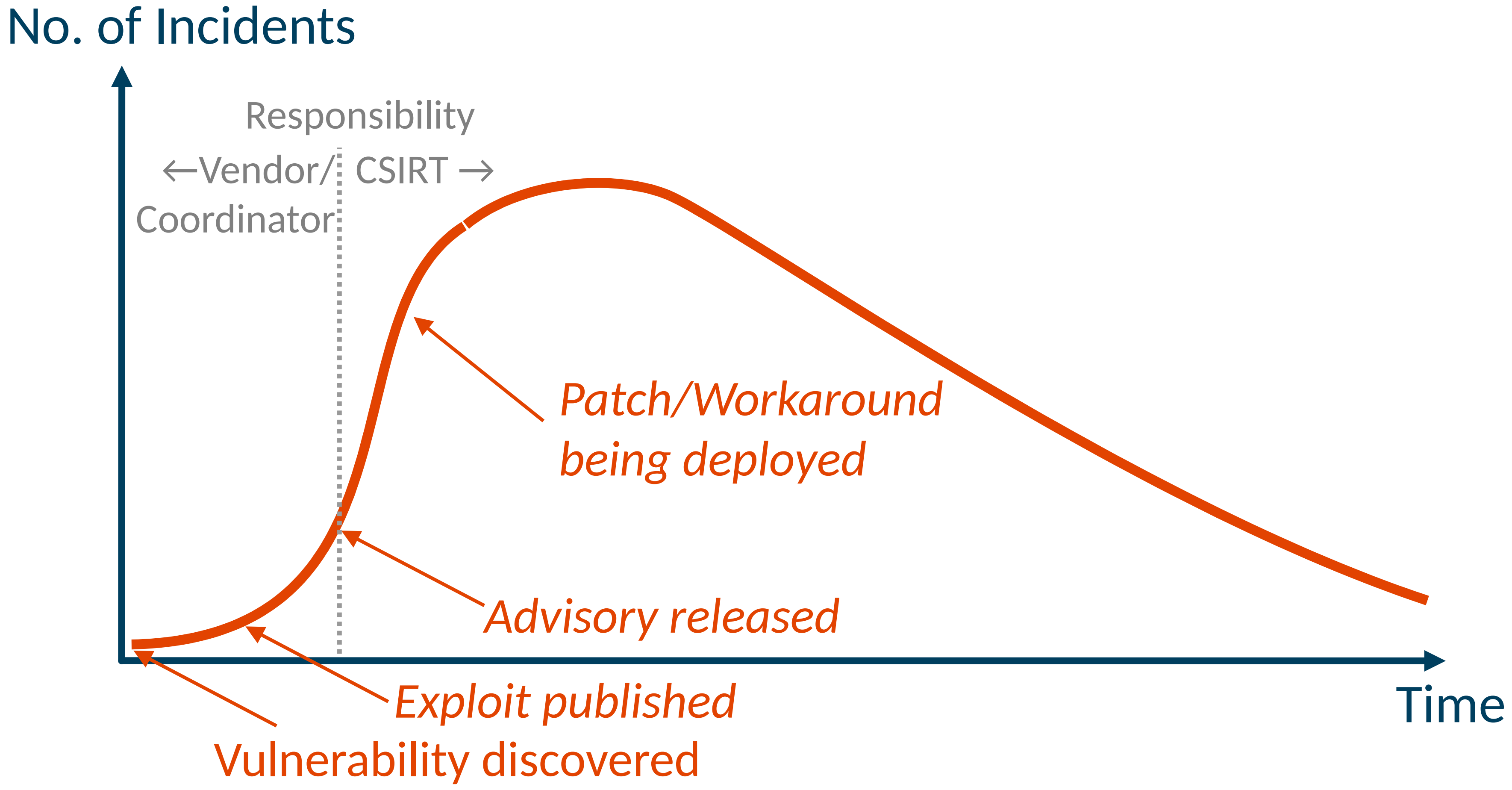
Local Vulnerability Scanning


We're here today
(and for the upcoming shows)
Develop vulnerability handling policy and operational framework
Identify vulnerability from internal source
Verify report
Vulnerability verified?
No
Yes
Develop and deploy remediation
Engage in post-remediation activities
ISO 30111 Vulnerability handling

Introduction

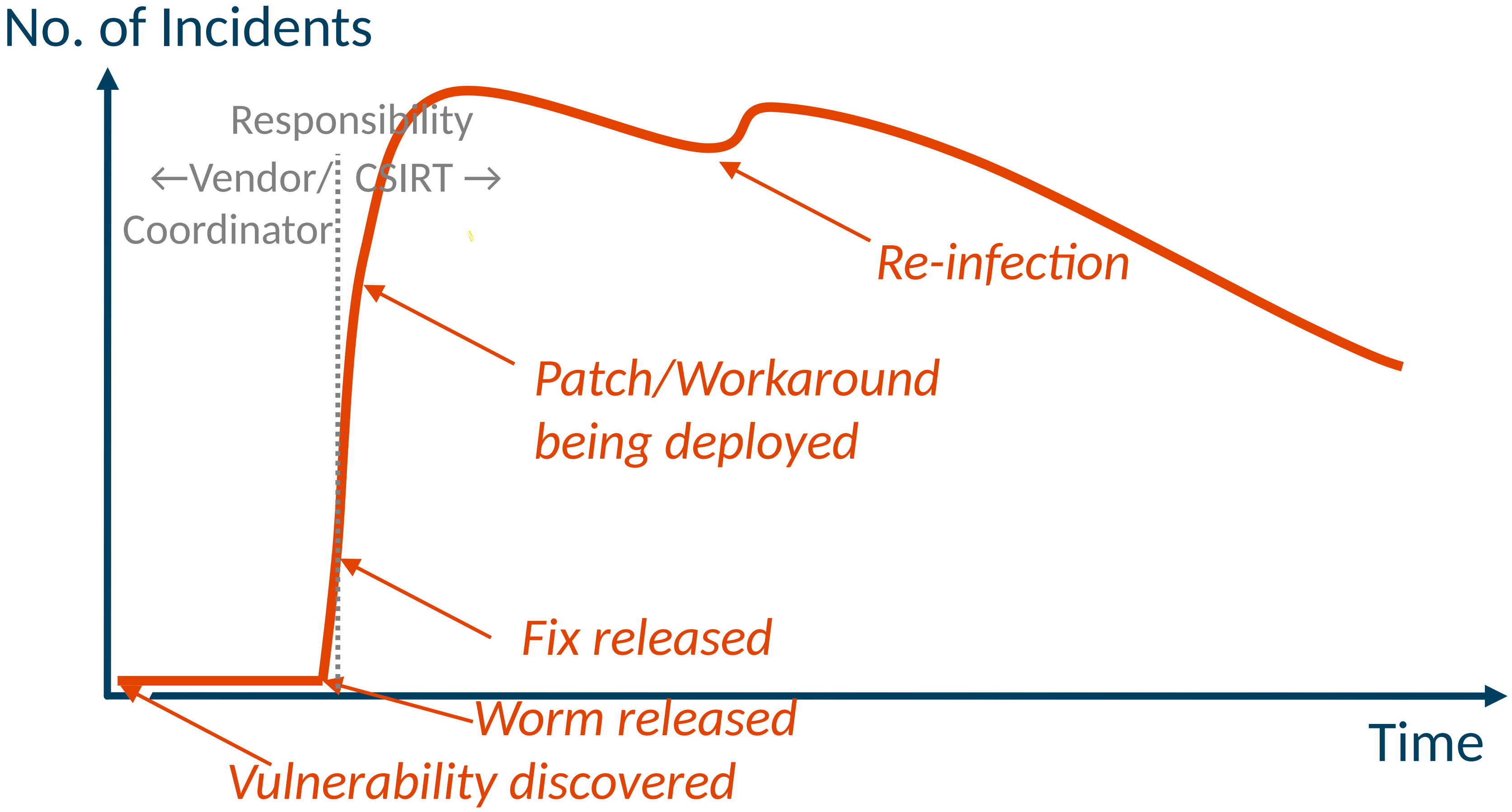
www.geant.org

Do you need motivation? → Classic Vulnerability Curve



Source: TRANSITS

Even more motivation? → Modern Vulnerability Curve



Source: TRANSITS

What’s this all about?

- How to **proactively** measure the security of your **local** systems
- So, yes, this *is* about vulnerabilities, but even more so about
  - Misconfigurations
  - Patch levels
  - Technical compliance
- Preferably in an **automated** way
- **However: measure against what?**
  - PCI DSS, HIPAA, FISMA, … ?

GÉANT
Networks • Services • People

Let’s look at some of those benchmarks / baselines

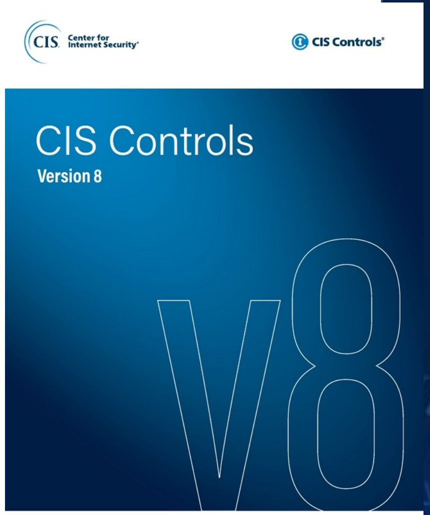
CIS Controls

www.geant.org

CIS Controls (v8)

- Prioritized and simplified best practices (**community-driven**)
- CIS Controls: Goals
  - *“to identify the most common and important real-world cyber-attacks that affect enterprises every day, translate that knowledge and experience into positive, constructive **action** for defenders”*
  - *“All individual recommendations (**Safeguards**) must be specific”*
    - ***“make them implementable, usable, scalable, and in alignment with all industry or government security requirements.”***
    - ***“All CIS Controls must be measurable”***
    - *“Simplify or remove ambiguous language to **avoid** inconsistent **interpretation**”*
  - *“Avoid being tempted to solve every security problem—avoid adding ‘good things to do’ or ‘things you could do’”*

CIS Controls (v8)



CIS Center for Internet Security

CIS Controls

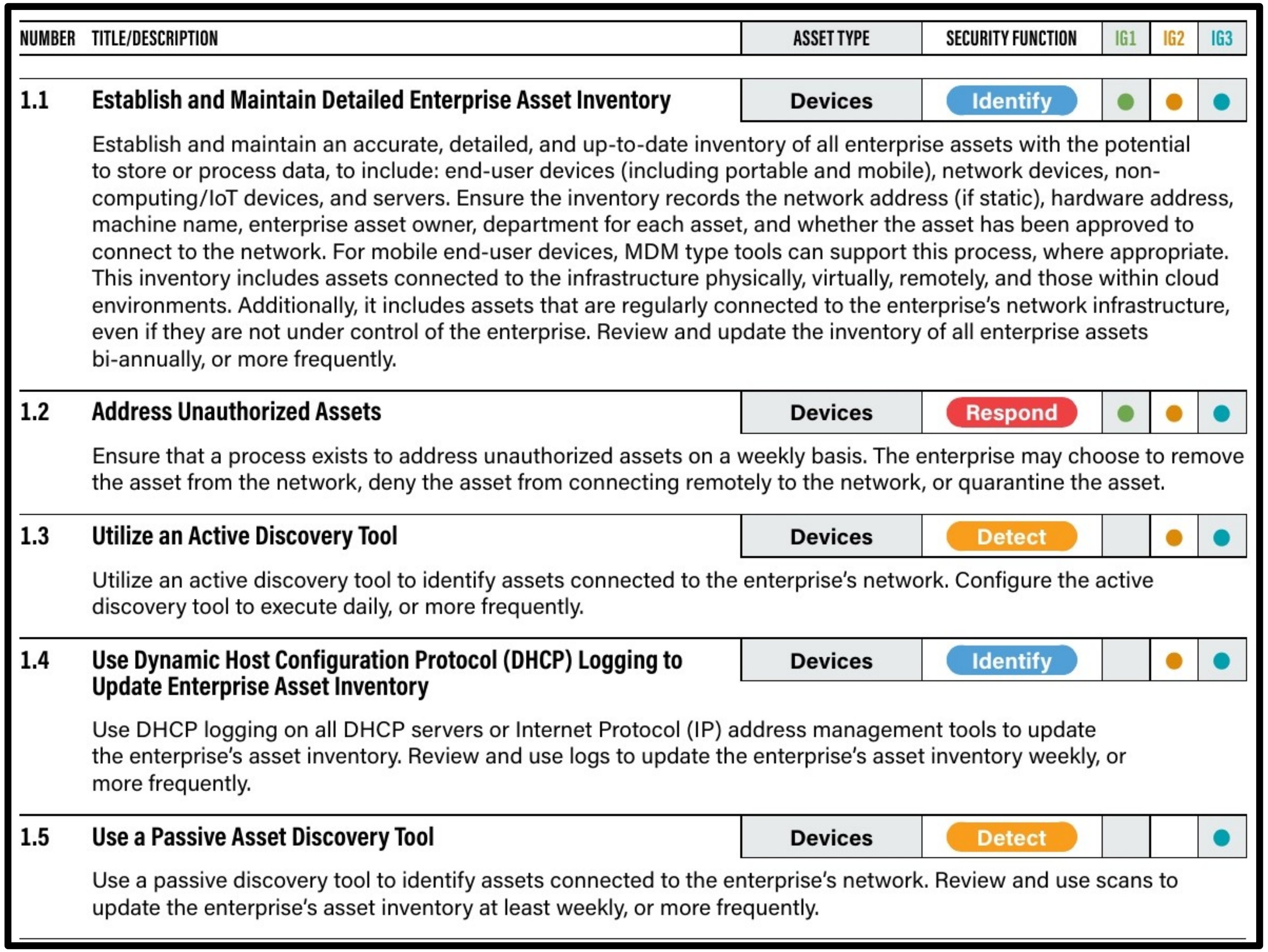
CIS Controls

Version 8

v8

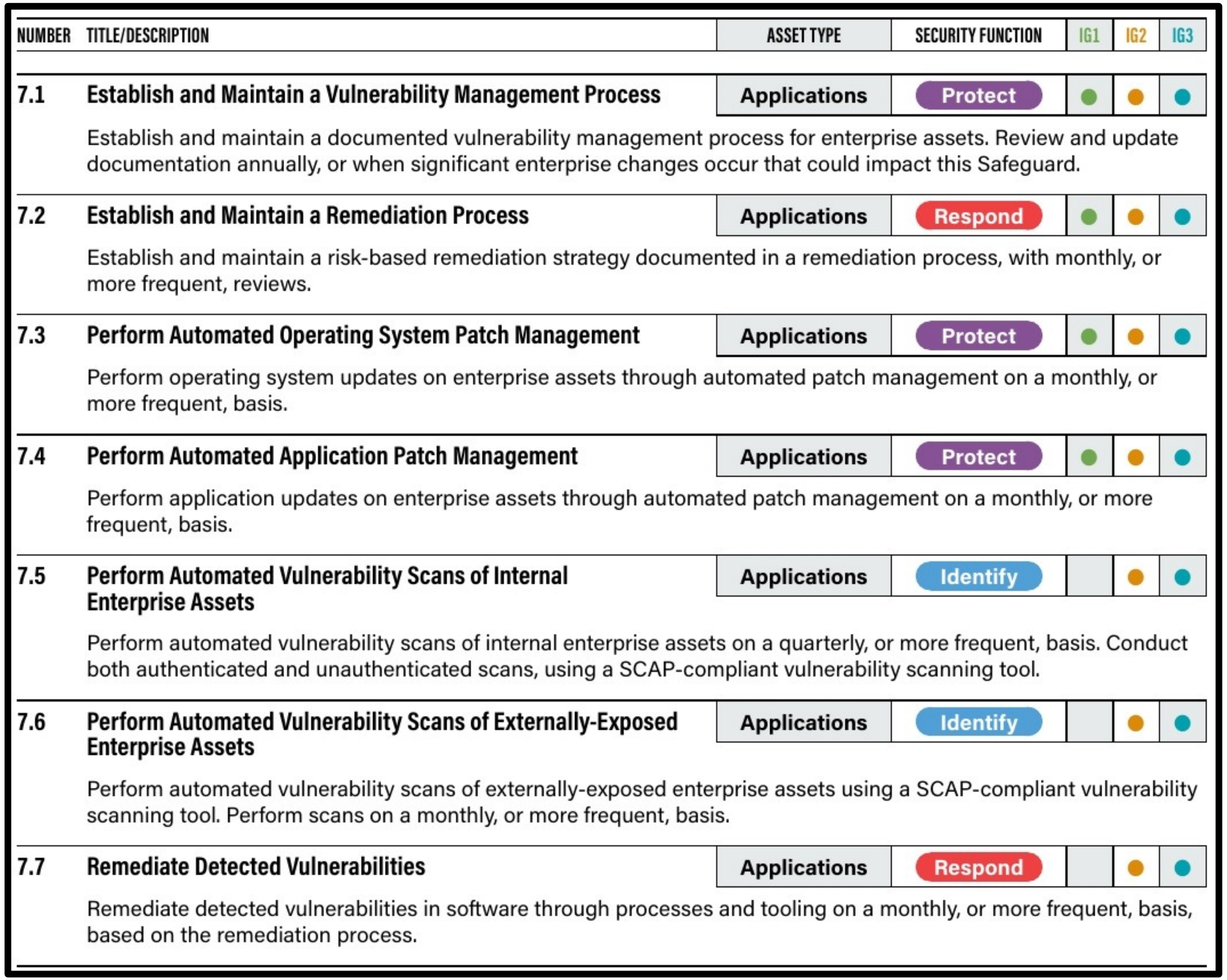
- CIS Controls
  - Inventory and Control of Enterprise Assets
  - Inventory and Control of Software Assets
  - Data Protection
  - Secure Configuration of Enterprise Assets and Software
  - Account Management
  - Access Control Management
  - Continuous Vulnerability Management
  - Audit Log Management
  - Email and Web Browser Protections
  - Malware Defenses
  - Data Recovery
  - Network Infrastructure Management
  - Network Monitoring and Defense
  - Security Awareness and Skills Training
  - Service Provider Management
  - Application Software Security
  - Incident Response Management
  - Penetration Testing

CIS Control 01: Inventory & Control of Enterprise Assets



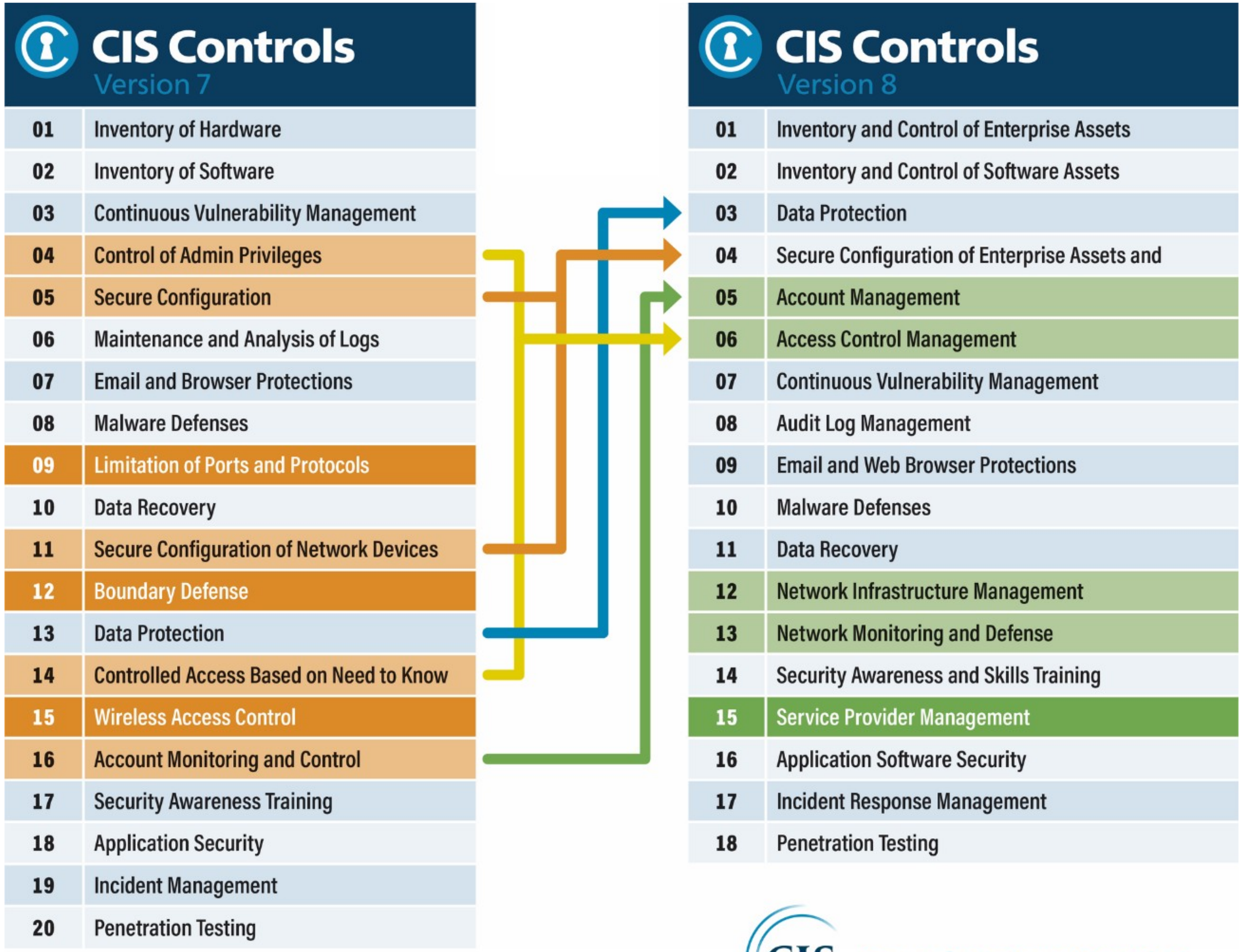
NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
1.1	**Establish and Maintain Detailed Enterprise Asset Inventory** Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data, to include: end-user devices (including portable and mobile), network devices, non-computing/IoT devices, and servers. Ensure the inventory records the network address (if static), hardware address, machine name, enterprise asset owner, department for each asset, and whether the asset has been approved to connect to the network. For mobile end-user devices, MDM type tools can support this process, where appropriate. This inventory includes assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments. Additionally, it includes assets that are regularly connected to the enterprise's network infrastructure, even if they are not under control of the enterprise. Review and update the inventory of all enterprise assets bi-annually, or more frequently.	Devices	Identify	●	●	●
1.2	**Address Unauthorized Assets** Ensure that a process exists to address unauthorized assets on a weekly basis. The enterprise may choose to remove the asset from the network, deny the asset from connecting remotely to the network, or quarantine the asset.	Devices	Respond	●	●	●
1.3	**Utilize an Active Discovery Tool** Utilize an active discovery tool to identify assets connected to the enterprise's network. Configure the active discovery tool to execute daily, or more frequently.	Devices	Detect		●	●
1.4	**Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory** Use DHCP logging on all DHCP servers or Internet Protocol (IP) address management tools to update the enterprise's asset inventory. Review and use logs to update the enterprise's asset inventory weekly, or more frequently.	Devices	Identify		●	●
1.5	**Use a Passive Asset Discovery Tool** Use a passive discovery tool to identify assets connected to the enterprise's network. Review and use scans to update the enterprise's asset inventory at least weekly, or more frequently.	Devices	Detect			●

CIS Control 07: Continuous Vulnerability Management



NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
7.1	**Establish and Maintain a Vulnerability Management Process** Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	Applications	Protect	●	●	●
7.2	**Establish and Maintain a Remediation Process** Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.	Applications	Respond	●	●	●
7.3	**Perform Automated Operating System Patch Management** Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	Applications	Protect	●	●	●
7.4	**Perform Automated Application Patch Management** Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	Applications	Protect	●	●	●
7.5	**Perform Automated Vulnerability Scans of Internal Enterprise Assets** Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.	Applications	Identify		●	●
7.6	**Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets** Perform automated vulnerability scans of externally-exposed enterprise assets using a SCAP-compliant vulnerability scanning tool. Perform scans on a monthly, or more frequent, basis.	Applications	Identify		●	●
7.7	**Remediate Detected Vulnerabilities** Remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process.	Applications	Respond		●	●

v8: new as of May 2021



CIS Controls Version 7

01	Inventory of Hardware
02	Inventory of Software
03	Continuous Vulnerability Management
04	Control of Admin Privileges
05	Secure Configuration
06	Maintenance and Analysis of Logs
07	Email and Browser Protections
08	Malware Defenses
09	Limitation of Ports and Protocols
10	Data Recovery
11	Secure Configuration of Network Devices
12	Boundary Defense
13	Data Protection
14	Controlled Access Based on Need to Know
15	Wireless Access Control
16	Account Monitoring and Control
17	Security Awareness Training
18	Application Security
19	Incident Management
20	Penetration Testing

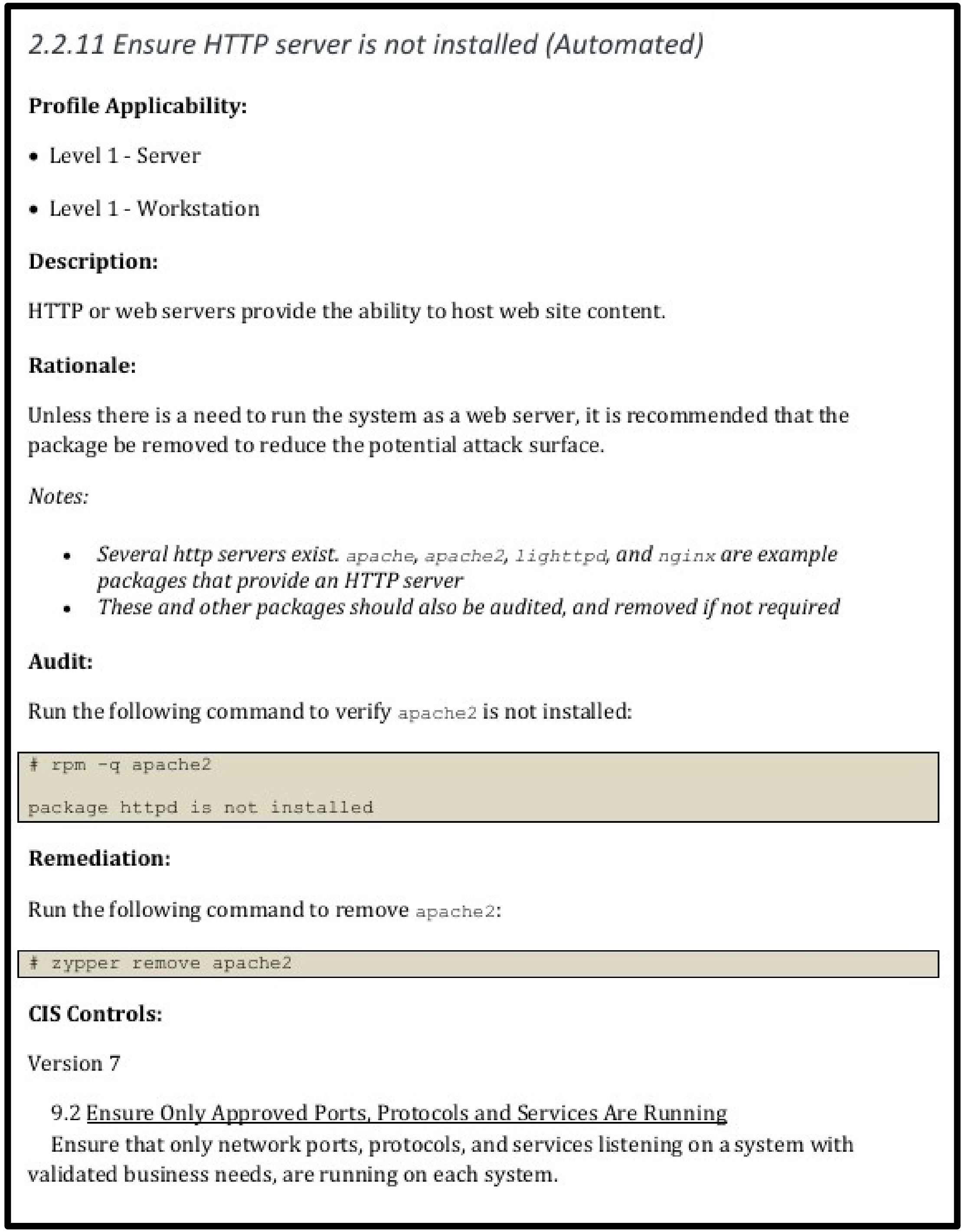
CIS Controls Version 8

01	Inventory and Control of Enterprise Assets
02	Inventory and Control of Software Assets
03	Data Protection
04	Secure Configuration of Enterprise Assets and
05	Account Management
06	Access Control Management
07	Continuous Vulnerability Management
08	Audit Log Management
09	Email and Web Browser Protections
10	Malware Defenses
11	Data Recovery
12	Network Infrastructure Management
13	Network Monitoring and Defense
14	Security Awareness and Skills Training
15	Service Provider Management
16	Application Software Security
17	Incident Response Management
18	Penetration Testing

CIS. Center for Internet Security®

CIS Benchmarks

- Q: how do you “translate” the (more general) Safeguards from CIS Controls into actionable items - how do you “make them implementable”?
  - CIS Benchmarks: vendor-neutral **configuration guidelines**
- 100+ benchmarks available
  - 25+ vendor product families
  - sometimes more than 1000 pages strong…
  - Implemented in applications
- Supported by **many** security vendors



2.2.11 Ensure HTTP server is not installed (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

HTTP or web servers provide the ability to host web site content.

Rationale:

Unless there is a need to run the system as a web server, it is recommended that the package be removed to reduce the potential attack surface.

Notes:

- *Several http servers exist.* `apache`, `apache2`, `lighttpd`, *and* `nginx` *are example packages that provide an HTTP server*
- *These and other packages should also be audited, and removed if not required*

Audit:

Run the following command to verify `apache2` is not installed:

```
# rpm -q apache2

package httpd is not installed
```

Remediation:

Run the following command to remove `apache2`:

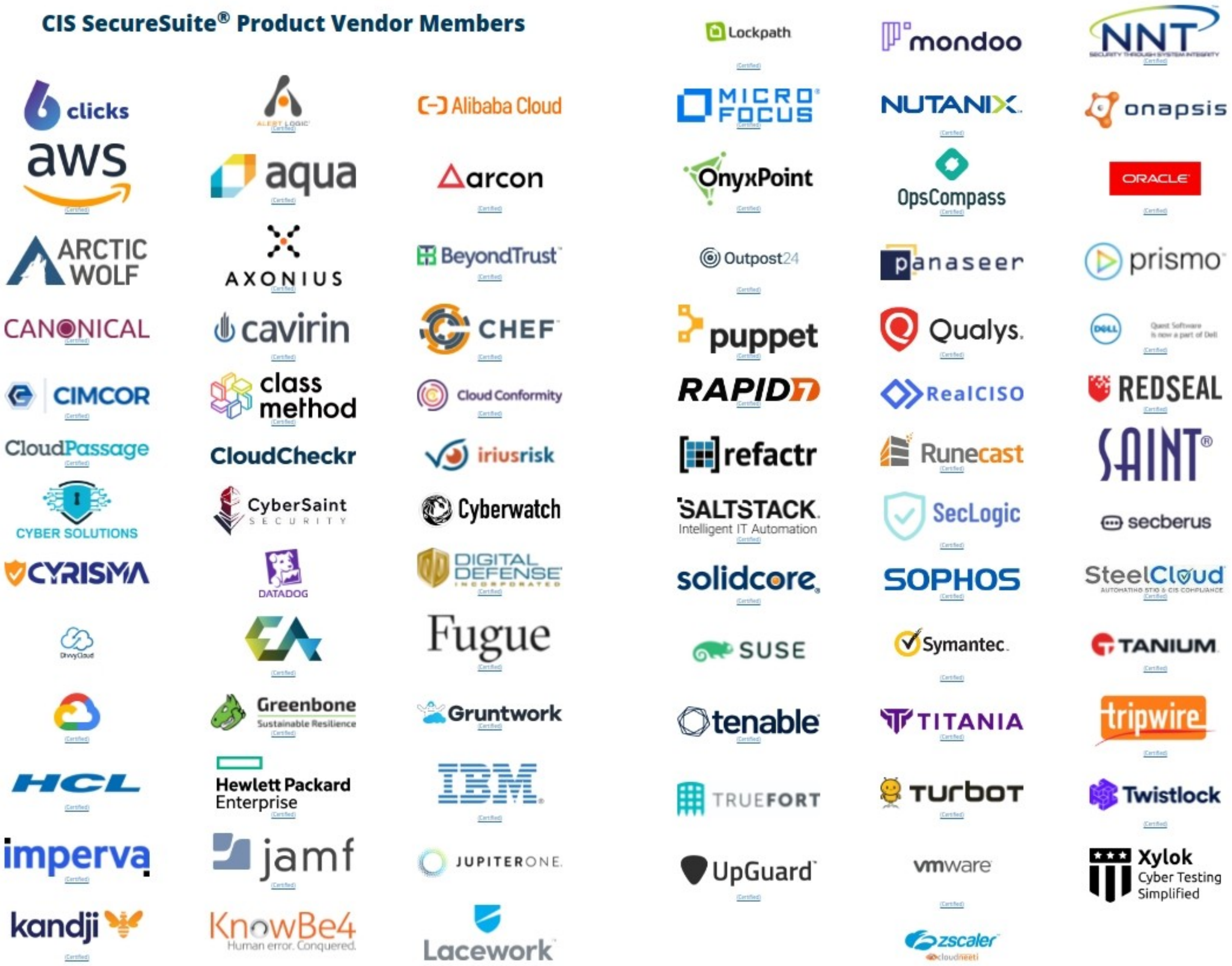
```
# zypper remove apache2
```

CIS Controls:

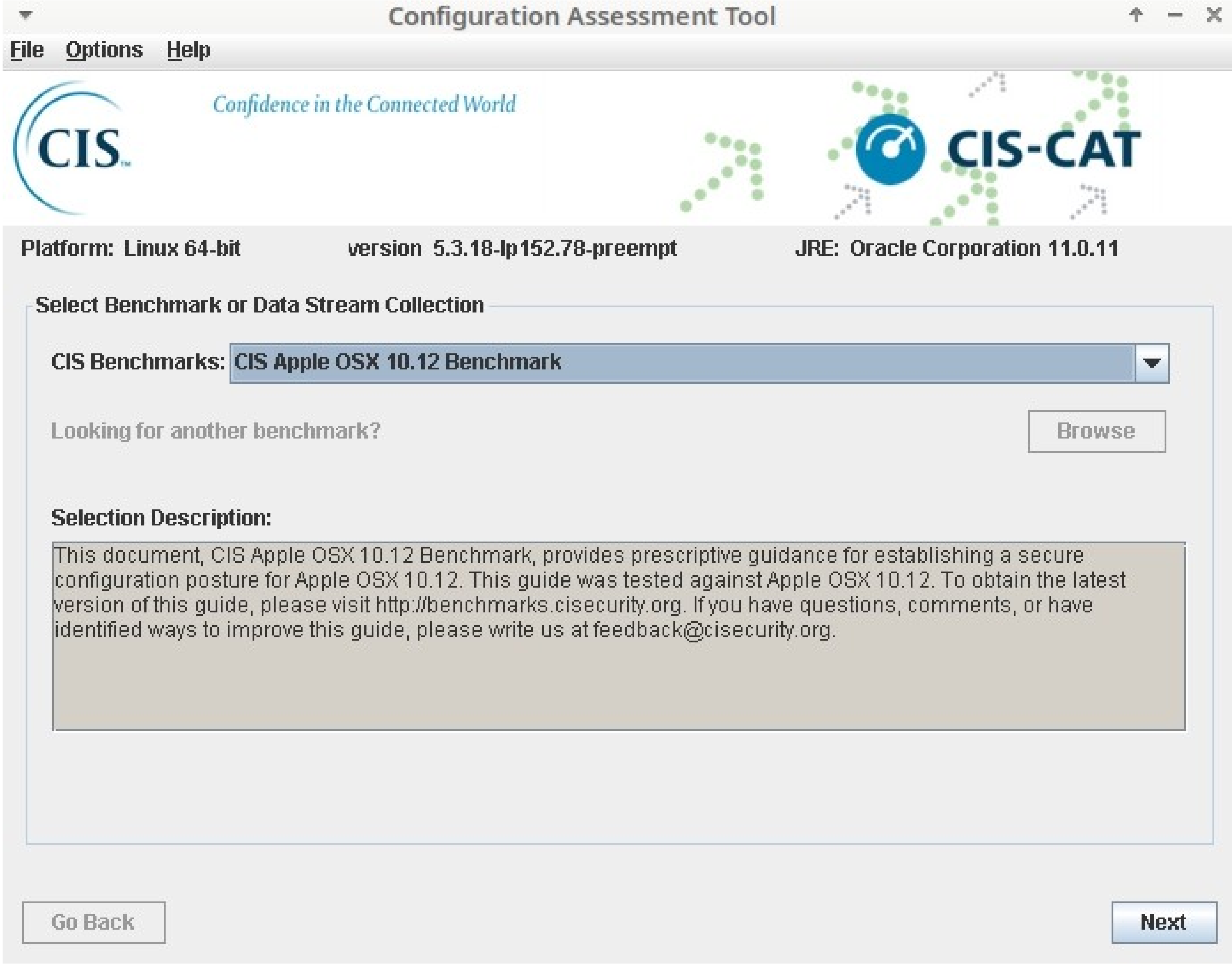
Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

Implemented by many vendors



CIS-CAT (Lite)


Configuration Assessment Tool
File
Options
Help
Confidence in the Connected World
CIS
CIS-CAT

Platform: Linux 64-bit   version 5.3.18-lp152.78-preempt   JRE: Oracle Corporation 11.0.11

Select Benchmark or Data Stream Collection

CIS Benchmarks: CIS Apple OSX 10.12 Benchmark

Looking for another benchmark?
Browse

Selection Description:

This document, CIS Apple OSX 10.12 Benchmark, provides prescriptive guidance for establishing a secure configuration posture for Apple OSX 10.12. This guide was tested against Apple OSX 10.12. To obtain the latest version of this guide, please visit http://benchmarks.cisecurity.org. If you have questions, comments, or have identified ways to improve this guide, please write us at feedback@cisecurity.org.

GÉANT
Networks • Services • People

Microsoft

www.geant.org

The Microsoft ecosystem

- MS Security Compliance Toolkit (SCT)
  - *"allow enterprise security administrators to download, analyze, test, edit, and store Microsoft-recommended **security configuration baselines** for Windows and other Microsoft products."*
  - *"administrators can compare their current GPOs with **Microsoft-recommended GPO baselines or other baselines**, edit them, store them in GPO backup file format"*
  - *"apply them broadly through Active Directory or individually through local policy."*

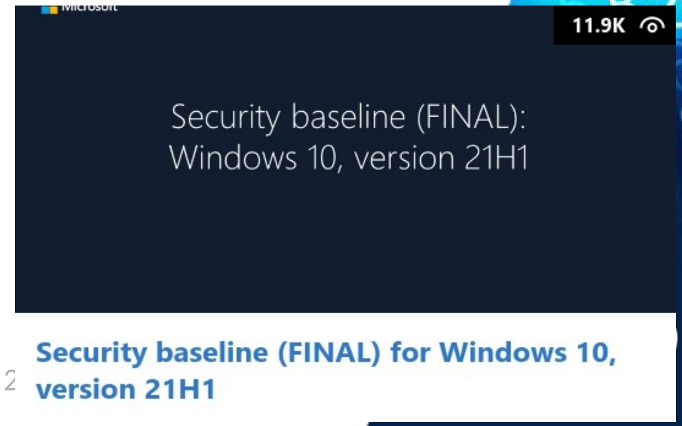
SCT: a set of tools

- **Policy Analyzer** tool: analyzing and comparing sets of GPOs
  - Highlight when a set of Group Policies has redundant settings or internal inconsistencies
  - Highlight the differences between versions or sets of Group Policies
  - Compare GPOs against current local policy and local registry settings
  - Capture a baseline and then compare it to a later one
- **Local Group Policy Object** (LGPO) tool
  - automate management of Local Group Policy
  - useful for managing non-domain-joined systems
- **Set Object Security** tool
- **GPO to Policy Rules** tool
- … as well as a number of PowerShell scripts …

SCT: security baselines

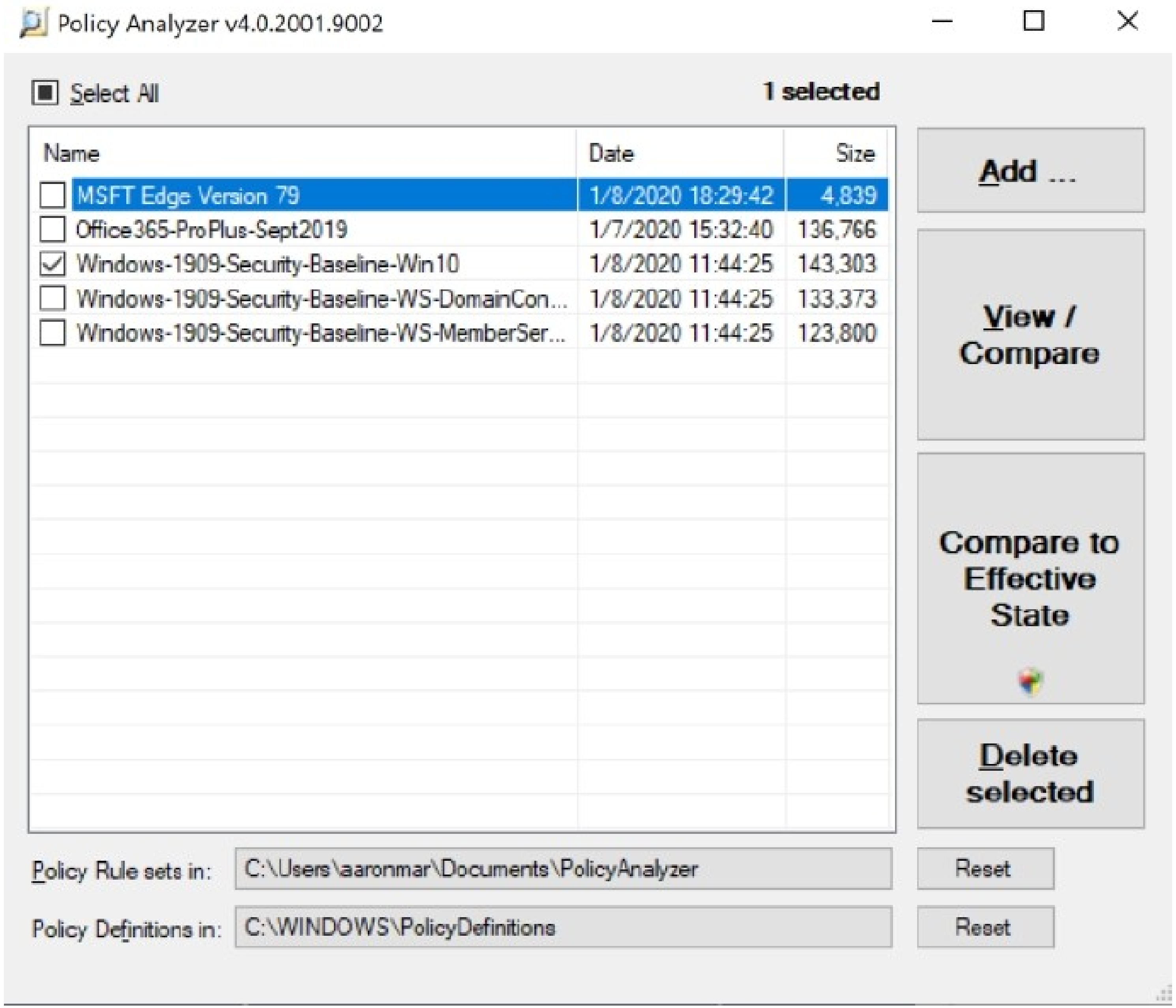
- Windows 10 Security baselines
  - Windows 10, Version 21H1
  - Windows 10, Version 20H2
  - Windows 10, Version 2004
  - Windows 10, Version 1909
  - Windows 10, Version 1809
  - Windows 10, Version 1607
  - Windows 10, Version 1507
- Windows Server security baselines
  - Windows Server 2019
  - Windows Server 2016
  - Windows Server 2012 R2

- Microsoft Office security baseline
  - Microsoft 365 Apps for enterprise, Version 2104
- Microsoft Edge security baseline
  - Version 88
- Windows Update security baseline
  - Windows 10 20H2 and below



Security baseline (FINAL): Windows 10, version 21H1

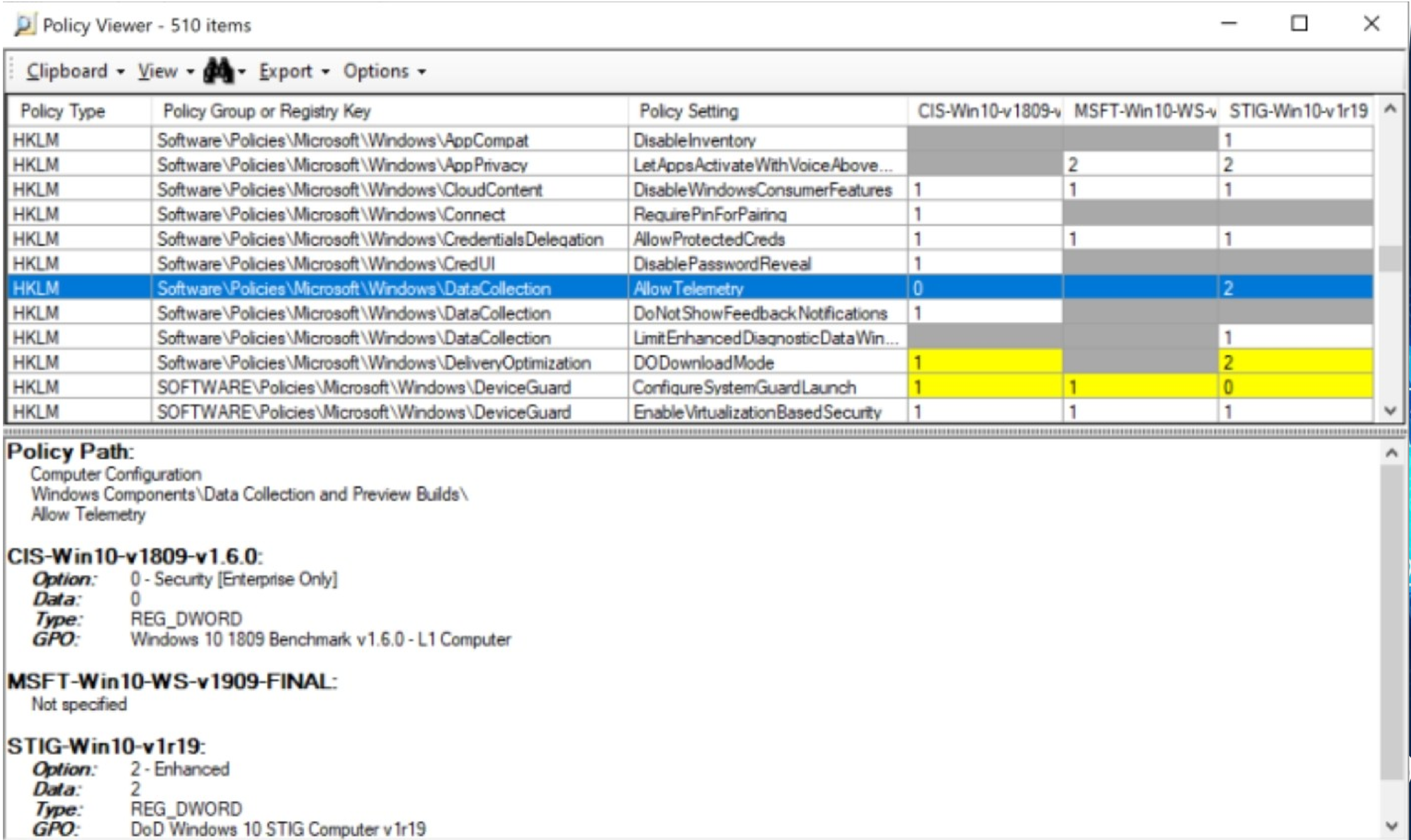
Security baseline (FINAL) for Windows 10, version 21H1



Name	Date	Size
□ MSFT Edge Version 79	1/8/2020 18:29:42	4,839
□ Office365-ProPlus-Sept2019	1/7/2020 15:32:40	136,766
☑ Windows-1909-Security-Baseline-Win10	1/8/2020 11:44:25	143,303
□ Windows-1909-Security-Baseline-WS-DomainCon...	1/8/2020 11:44:25	133,373
□ Windows-1909-Security-Baseline-WS-MemberSer...	1/8/2020 11:44:25	123,800

Policy Rule sets in: C:\Users\aaronmar\Documents\PolicyAnalyzer

Policy Definitions in: C:\WINDOWS\PolicyDefinitions



Policy Type	Policy Group or Registry Key	Policy Setting	CIS-Win10-v1809-v	MSFT-Win10-WS-v	STIG-Win10-v1r19
HKLM	Software\Policies\Microsoft\Windows\AppCompat	DisableInventory			1
HKLM	Software\Policies\Microsoft\Windows\AppPrivacy	LetAppsActivateWithVoiceAbove...		2	2
HKLM	Software\Policies\Microsoft\Windows\CloudContent	DisableWindowsConsumerFeatures	1	1	1
HKLM	Software\Policies\Microsoft\Windows\Connect	RequirePinForPairing	1		
HKLM	Software\Policies\Microsoft\Windows\CredentialsDelegation	AllowProtectedCreds	1	1	1
HKLM	Software\Policies\Microsoft\Windows\CredUI	DisablePasswordReveal	1		
HKLM	Software\Policies\Microsoft\Windows\DataCollection	AllowTelemetry	0		2
HKLM	Software\Policies\Microsoft\Windows\DataCollection	DoNotShowFeedbackNotifications	1		
HKLM	Software\Policies\Microsoft\Windows\DataCollection	LimitEnhancedDiagnosticDataWin...			1
HKLM	Software\Policies\Microsoft\Windows\DeliveryOptimization	DODownloadMode	1		2
HKLM	SOFTWARE\Policies\Microsoft\Windows\DeviceGuard	ConfigureSystemGuardLaunch	1	1	0
HKLM	SOFTWARE\Policies\Microsoft\Windows\DeviceGuard	EnableVirtualizationBasedSecurity	1	1	1

Policy Path:

Computer Configuration
Windows Components\Data Collection and Preview Builds\
Allow Telemetry

CIS-Win10-v1809-v1.6.0:

Option: 0 - Security [Enterprise Only]
Data: 0
Type: REG_DWORD
GPO: Windows 10 1809 Benchmark v1.6.0 - L1 Computer

MSFT-Win10-WS-v1909-FINAL:

Not specified

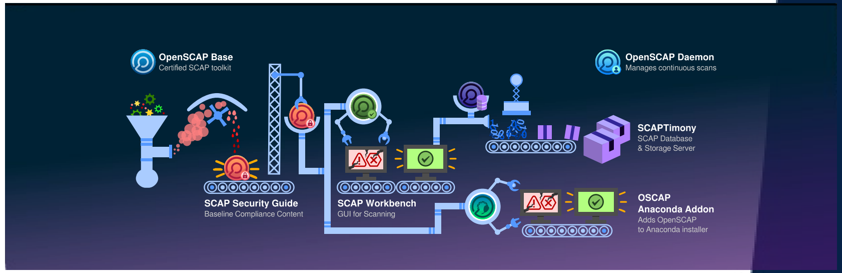
STIG-Win10-v1r19:

Option: 2 - Enhanced
Data: 2
Type: REG_DWORD
GPO: DoD Windows 10 STIG Computer v1r19

SCAP / OpenSCAP

www.geant.org

OpenSCAP



- Implementation of SCAP: Security Content Automation Protocol (NIST)
  - *“The OpenSCAP ecosystem provides multiple tools to assist administrators and auditors with **assessment**, **measurement**, and **enforcement** of security baselines.”*
  - *“…provides a wide variety of **hardening guides** and **configuration baselines** developed by the open source community, ensuring that you can choose a security policy which best suits the needs of your organization”*
    - Security Technical Implementation Guides (STIGs by DISA)
    - The United States Government Configuration Baseline (USGCB)
    - Payment Card Industry Data Security Standard (PCI DSS)
    - **CIS Controls**
    - …
  - *“100% open source”*
  - Applies to platforms as well as products
  - Set of tools
    - e.g., OpenSCAP Daemon for continuous evaluation

Networks • Services • People

Demo time

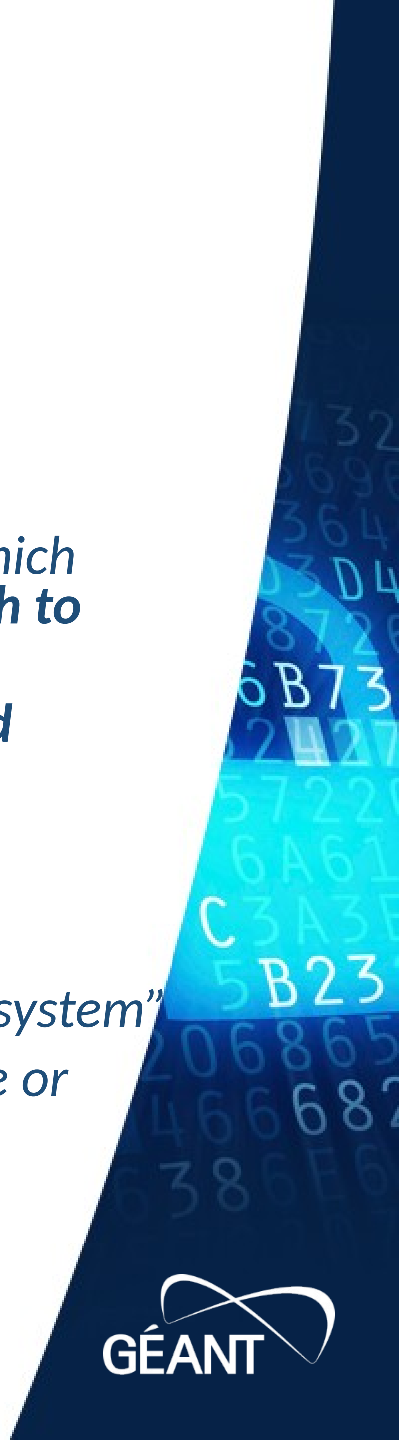
www.geant.org

What have you learned?

- There’s a lot out there
  - Benchmarks / baselines
  - Community-driven
  - Free, open source
  - You don’t have to start from zero
  - Tailor to your own needs
- Many tools available, too
  - Free, open source
  - Integrated into many (all?) commercial tools as well

What was not covered today?

- Commercial tools
- Deep dive into standards
  - Security Content Automation Protocol (SCAP)
    - *“a suite of specifications that standardize the format and nomenclature by which* ***software flaw and security configuration information is communicated, both to machines and humans****.”*
    - *“SCAP is a multi-purpose framework of specifications that support* ***automated*** *configuration, vulnerability and patch checking, technical control compliance activities, and security measurement”*
  - Open Vulnerability and Assessment Language (OVAL)
    - *“an open language to express checks for determining whether software vulnerabilities—and configuration issues, programs, and patches—exist on a system”*
    - *“allows the sharing of technical details regarding how to identify the presence or absence of vulnerabilities on a computer system”*



Networks • Services • People

“The simplest way to avoid vulnerabilities in software is to avoid installing that software.“

(OpenSCAP tool)

Thank you

Any questions?

Next Module: Network Vulnerability Scanning

www.geant.org

© GÉANT Association on behalf of the GN4 Phase 2 project (GN4-2).

The research leading to these results has received funding from the European Union’s Horizon 2020 research and innovation programme under Grant Agreement No. 731122 (GN4-2).

References

- CIS Controls
  - `https://www.cisecurity.org/controls/`
- CIS Benchmarks
  - `https://www.cisecurity.org/cis-benchmarks/`
- CIS-CAT Lite
  - `https://learn.cisecurity.org/cis-cat-lite`
- OpenSCAP
  - `https://www.open-scap.org/`
  - `https://github.com/OpenSCAP`
  - `https://github.com/ComplianceAsCode/content`

References

- Microsoft Security Compliance Toolkit
  - https://docs.microsoft.com/en-us/windows/security/threat-protection/security-compliance-toolkit-10
  - https://www.microsoft.com/en-us/download/details.aspx?id=55319
- Microsoft Security Baselines
  - https://techcommunity.microsoft.com/t5/microsoft-security-baselines/bg-p/Microsoft-Security-Baselines

Other tools

- Lynis
  - https://cisofy.com/lynis/
  - https://github.com/CISOfy/lynis
- Vuls
  - https://github.com/future-architect/vuls
- macOS Lockdown (mOSL)
  - https://github.com/0xmachos/mOSL
- stronghold.py
  - https://github.com/alichtman/stronghold