CornCon X

Strategic Endpoint Hardening with CIS

Zach Kromkowski
Co-Founder
Senteon Managed Endpoint Hardening

SENTEON
MANAGED ENDPOINT HARDENING

Are You Familiar with the CIS Controls?

What about the CIS Benchmarks?

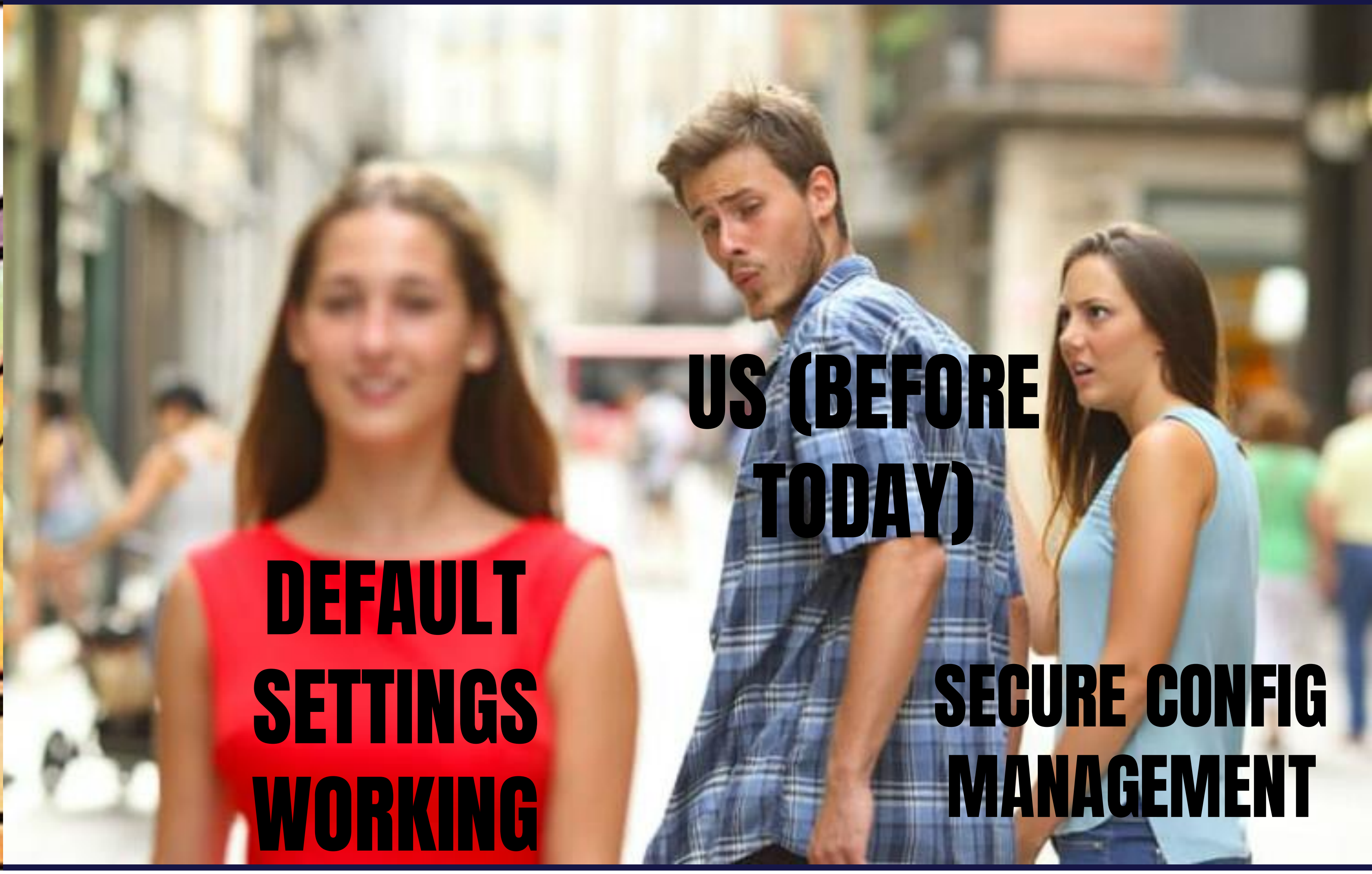
How many pages of documentation is it to harden a Win11 box? 1379 Pages

Is PowerShell a security tool?

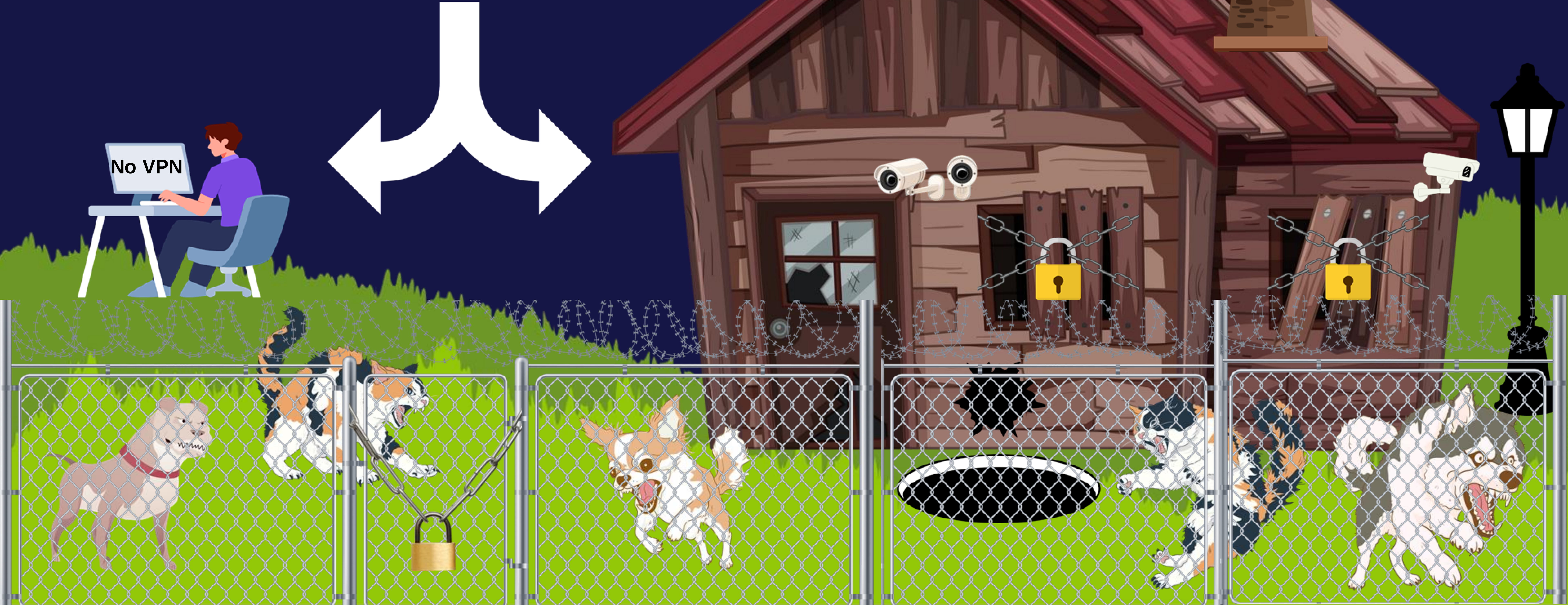
Features of Security Tools

Feature	PowerShell
Centralized Reporting and Auditing	✗
Role-Based Access Control (RBAC)	✗
Policy Management and Enforcement	✗
Encryption and Secure Data Handling	✗
Support and Maintenance Services	✗

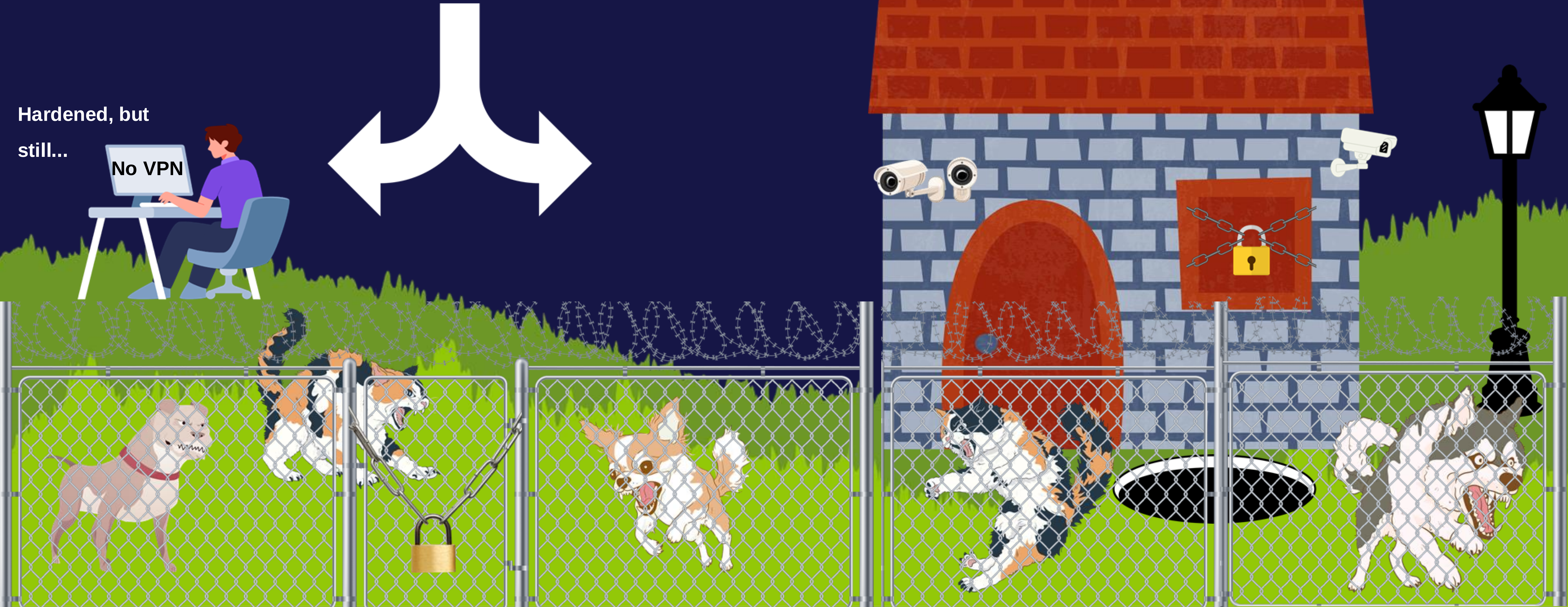
Functional Does Not Mean Secure



Do You Know Where Your Data Is?



Hardening Endpoints ++



Control 1: Inventory and Control of Enterprise Assets

Control 2: Inventory and Control of Software Assets

Control 3: Data Protection

Control 4: Secure Configuration of Enterprise Assets and Soft

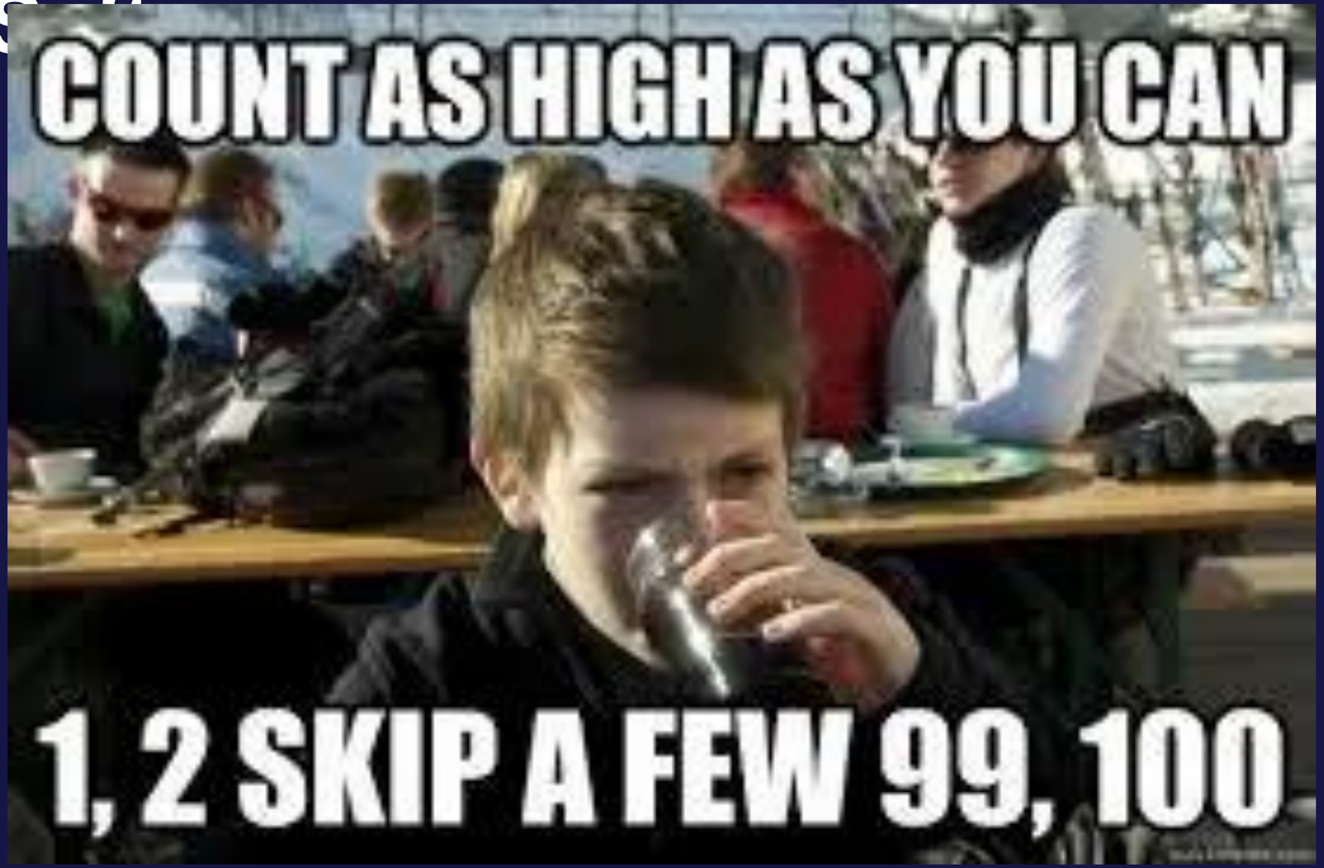
…

Control 07. Continuous Vulnerability Management

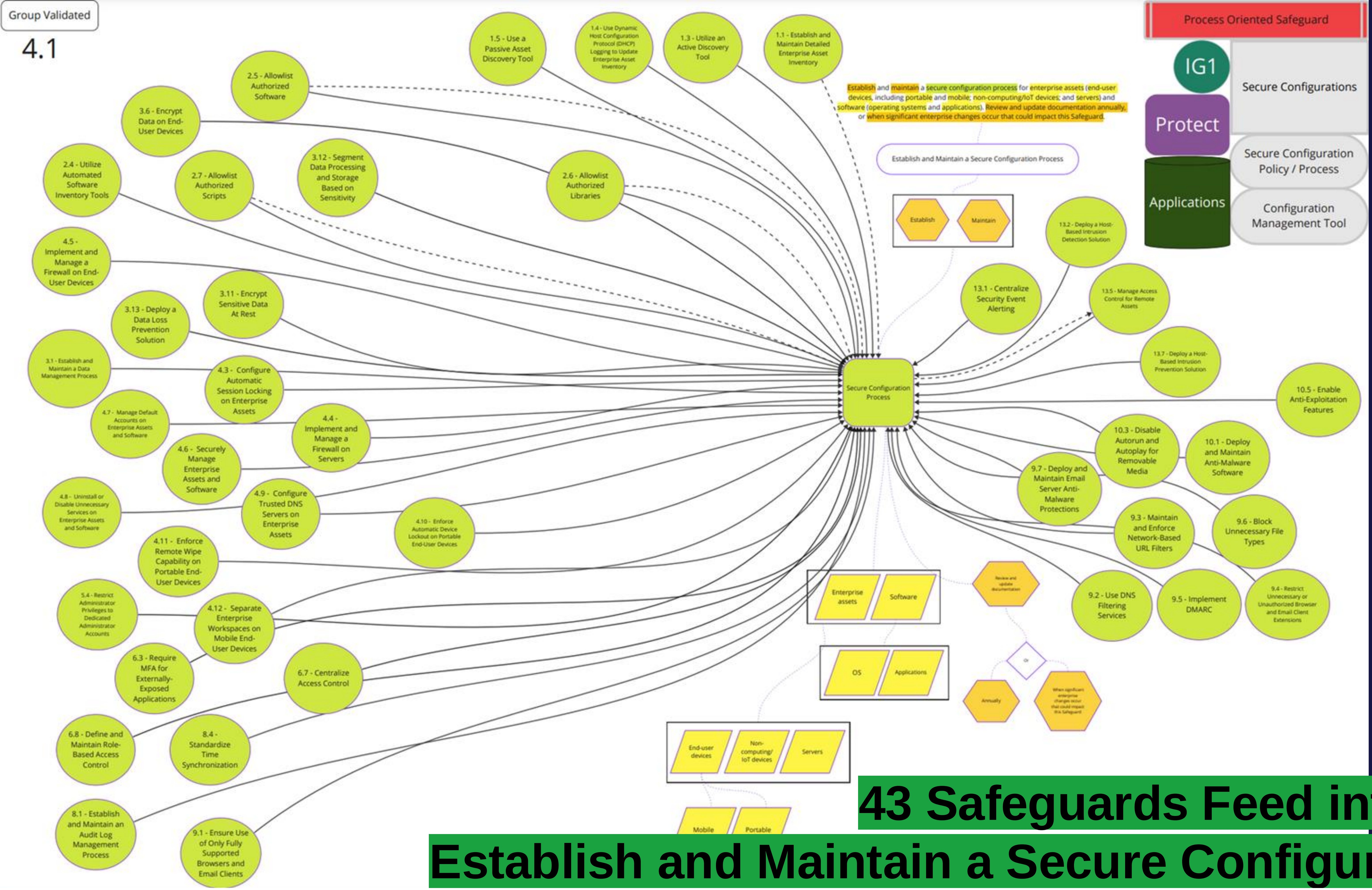
Control 10. Malware Defenses

Control 13. Network Monitoring and Defense

> “The CIS 18 are prioritized, easy to understand, and extremely cost-effective for small to mid-size organizations looking to prove they are secure enough to do business in today’s marketplace.”
>
> - CIS Website

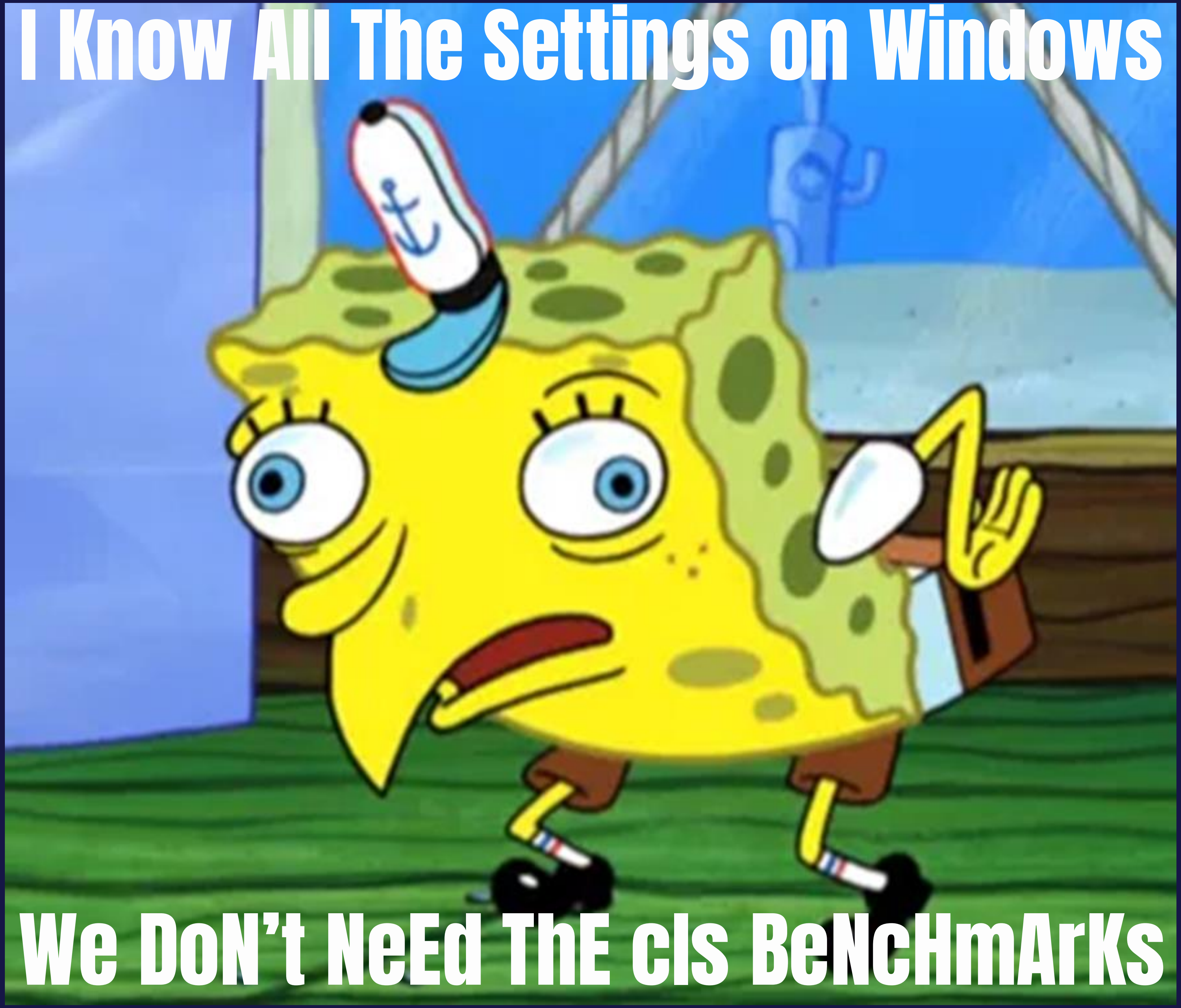


43 Safeguards Feed into Control 4.1: Establish and Maintain a Secure Configuration Process

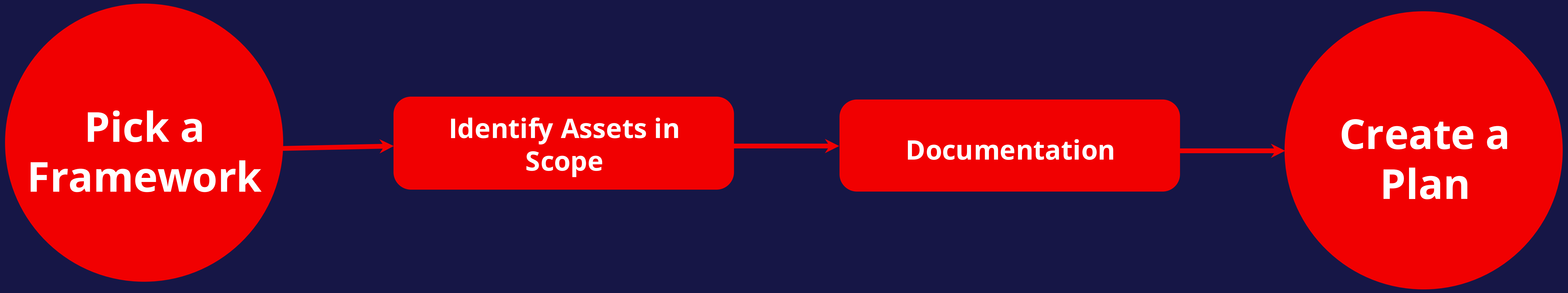

Group Validated
4.1
Process Oriented Safeguard
IG1
Secure Configurations
Protect
Secure Configuration Policy / Process
Applications
Configuration Management Tool
Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile; non-computing/IoT devices; and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
Establish and Maintain a Secure Configuration Process
Establish
Maintain
Secure Configuration Process
Enterprise assets
Software
OS
Applications
End-user devices
Non-computing/ IoT devices
Servers
Mobile
Portable
Review and update documentation
Or
Annually
When significant enterprise changes occur that could impact this Safeguard
1.5 - Use a Passive Asset Discovery Tool
1.4 - Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory
1.3 - Utilize an Active Discovery Tool
1.1 - Establish and Maintain Detailed Enterprise Asset Inventory
2.5 - Allowlist Authorized Software
3.6 - Encrypt Data on End-User Devices
2.4 - Utilize Automated Software Inventory Tools
2.7 - Allowlist Authorized Scripts
3.12 - Segment Data Processing and Storage Based on Sensitivity
2.6 - Allowlist Authorized Libraries
4.5 - Implement and Manage a Firewall on End-User Devices
3.11 - Encrypt Sensitive Data At Rest
3.13 - Deploy a Data Loss Prevention Solution
3.1 - Establish and Maintain a Data Management Process
4.3 - Configure Automatic Session Locking on Enterprise Assets
4.7 - Manage Default Accounts on Enterprise Assets and Software
4.4 - Implement and Manage a Firewall on Servers
4.6 - Securely Manage Enterprise Assets and Software
4.8 - Uninstall or Disable Unnecessary Services on Enterprise Assets and Software
4.9 - Configure Trusted DNS Servers on Enterprise Assets
4.10 - Enforce Automatic Device Lockout on Portable End-User Devices
4.11 - Enforce Remote Wipe Capability on Portable End-User Devices
5.4 - Restrict Administrator Privileges to Dedicated Administrator Accounts
4.12 - Separate Enterprise Workspaces on Mobile End-User Devices
6.3 - Require MFA for Externally-Exposed Applications
6.7 - Centralize Access Control
6.8 - Define and Maintain Role-Based Access Control
8.4 - Standardize Time Synchronization
8.1 - Establish and Maintain an Audit Log Management Process
9.1 - Ensure Use of Only Fully Supported Browsers and Email Clients
13.2 - Deploy a Host-Based Intrusion Detection Solution
13.1 - Centralize Security Event Alerting
13.5 - Manage Access Control for Remote Assets
13.7 - Deploy a Host-Based Intrusion Prevention Solution
10.5 - Enable Anti-Exploitation Features
10.3 - Disable Autorun and Autoplay for Removable Media
10.1 - Deploy and Maintain Anti-Malware Software
9.7 - Deploy and Maintain Email Server Anti-Malware Protections
9.3 - Maintain and Enforce Network-Based URL Filters
9.6 - Block Unnecessary File Types
9.2 - Use DNS Filtering Services
9.5 - Implement DMARC
9.4 - Restrict Unnecessary or Unauthorized Browser and Email Client Extensions

https://cybermattlee.com/wp-content/uploads/2024/05/CIS-V8-Mapping-Visuals-Per-Safeguard-v1.0.pdf

Major Data Loss
System Vulnerabilities
Skipping Control 4


I Know All The Settings on Windows
We DoN't NeEd ThE cIs BeNcHmArKs

First Steps for All



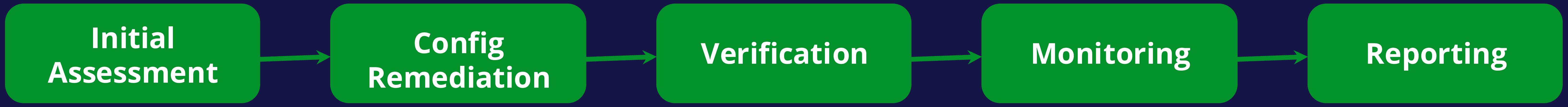
Pick a Framework

Identify Assets in Scope

Documentation

Create a Plan

But... What goes into a plan?



Initial Assessment

Config Remediation

Verification

Monitoring

Reporting

Step	InTune	Group Policy	PowerShell

Step	InTune	Group Policy	PowerShell
Initial Assessment	- Limited Built-in Tools - 3rd Party Required	- Manual Effort - Not Centralized	- Custom Scripting - Learning Curve

Step	InTune	Group Policy	PowerShell
Initial Assessment	- Limited Built-in Tools - 3rd Party Required	- Manual Effort - Not Centralized	- Custom Scripting - Learning Curve
Config Remediation	- Complex to Configure - Limited Granularity - Understanding Intune	- Conflicting Policies - Difficult at Scale - Version Control?	- Highly Customizable - Error Prone - Time Consuming

Step	InTune	Group Policy	PowerShell
Initial Assessment	- Limited Built-in Tools - 3rd Party Required	- Manual Effort - Not Centralized	- Custom Scripting - Learning Curve
Config Remediation	- Complex to Configure - Limited Granularity - Understanding Intune	- Conflicting Policies - Difficult at Scale - Version Control?	- Highly Customizable - Error Prone - Time Consuming
Verification	- Difficult to Verify - No Native Rollback	- Manual Checking - No Real Visibility - Third Party Needed	- Manual Script Checks - No Verification - Need Output Scripts

Step	InTune	Group Policy	PowerShell
Initial Assessment	- Limited Built-in Tools - 3rd Party Required	- Manual Effort - Not Centralized	- Custom Scripting - Learning Curve
Config Remediation	- Complex to Configure - Limited Granularity - Understanding Intune	- Conflicting Policies - Difficult at Scale - Version Control?	- Highly Customizable - Error Prone - Time Consuming
Verification	- Difficult to Verify - No Native Rollback	- Manual Checking - No Real Visibility - Third Party Needed	- Manual Script Checks - No Verification - Need Output Scripts
Monitoring	- Limited Real-Time - Not Designed to Continuously Monitor	- Nothing Built-in - Requires additional tools	- More Custom Scripts - All Periodic Checks

Step	InTune	Group Policy	PowerShell
Initial Assessment	- Limited Built-in Tools - 3rd Party Required	- Manual Effort - Not Centralized	- Custom Scripting - Learning Curve
Config Remediation	- Complex to Configure - Limited Granularity - Understanding Intune	- Conflicting Policies - Difficult at Scale - Version Control?	- Highly Customizable - Error Prone - Time Consuming
Verification	- Difficult to Verify - No Native Rollback	- Manual Checking - No Real Visibility - Third Party Needed	- Manual Script Checks - No Verification - Need Output Scripts
Monitoring	- Limited Real-Time - Not Designed to Continuously Monitor	- Nothing Built-in - Requires additional tools	- More Custom Scripts - All Periodic Checks
Reporting	- Limited Reporting - Not Detailed for Compliance	- Basic Reporting - Difficult to Generate Comprehensiveness	- More Custom Scripts - No Standardization - Very Manual

Goal

Preventing Unauthorized Access

Reducing the Attack Surface

Improving System Performance

Governance to Ensure Compliance

Assisting Settings

- Access this computer from the network
- User Account Control: Behavior of the elevation prompt for standard users
- Network access: Restrict anonymous access to Named Pipes and Shares

- SMB1 Client Driver
- WDigest Authentication
- Enable Structured Exception Handling Overwrite Protection (SEHOP)

- Configure Windows spotlight on lock screen
- Do not suggest third-party content in Windows spotlight
- Allow network connectivity during connected-standby (on battery)

- Minimum Password Length
- Store Passwords using Reversible Encryption
- Block Microsoft Accounts

“We know a thing or two, because we've seen a thing or two” - Farmers

Video editing software gaining access to “Lock pages in memory” without user knowledge.

Built in solutions claiming successful changes in settings, but the machine never actually making the change locally.

Xbox Settings becoming randomly available and auto turned on by windows updates.

SMB1…

Just SMB1 Everywhere...

Beginner

Understand the Basics

Start Small

Use Available Resources

Intermediate

Expand Scope

Automate Processes

Monitor Continuously

Advanced

Optimize Security

Integrate Advanced Tools

Regular Reviews

PROGRESSIVE
PROGRESSIVE
PROGRESSIVE

Learn to Explain the Benefit

You: You want to harden your assets?

Leadership: No, not really.

You: Yeah you’re right, things get secured, operations are smoother, improved security culture…

Leadership: Actually, I’m in!

You: Yeah you are...

CIS Benchmark Compliance Crosswalk

(Free after sign up, not mobile friendly)

General Hardening Resources

CIS Benchmark Downloads

Thank You!

Zach Kromkowski
zkromkowski@senteon.co
Co-Founder at Senteon