RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID:

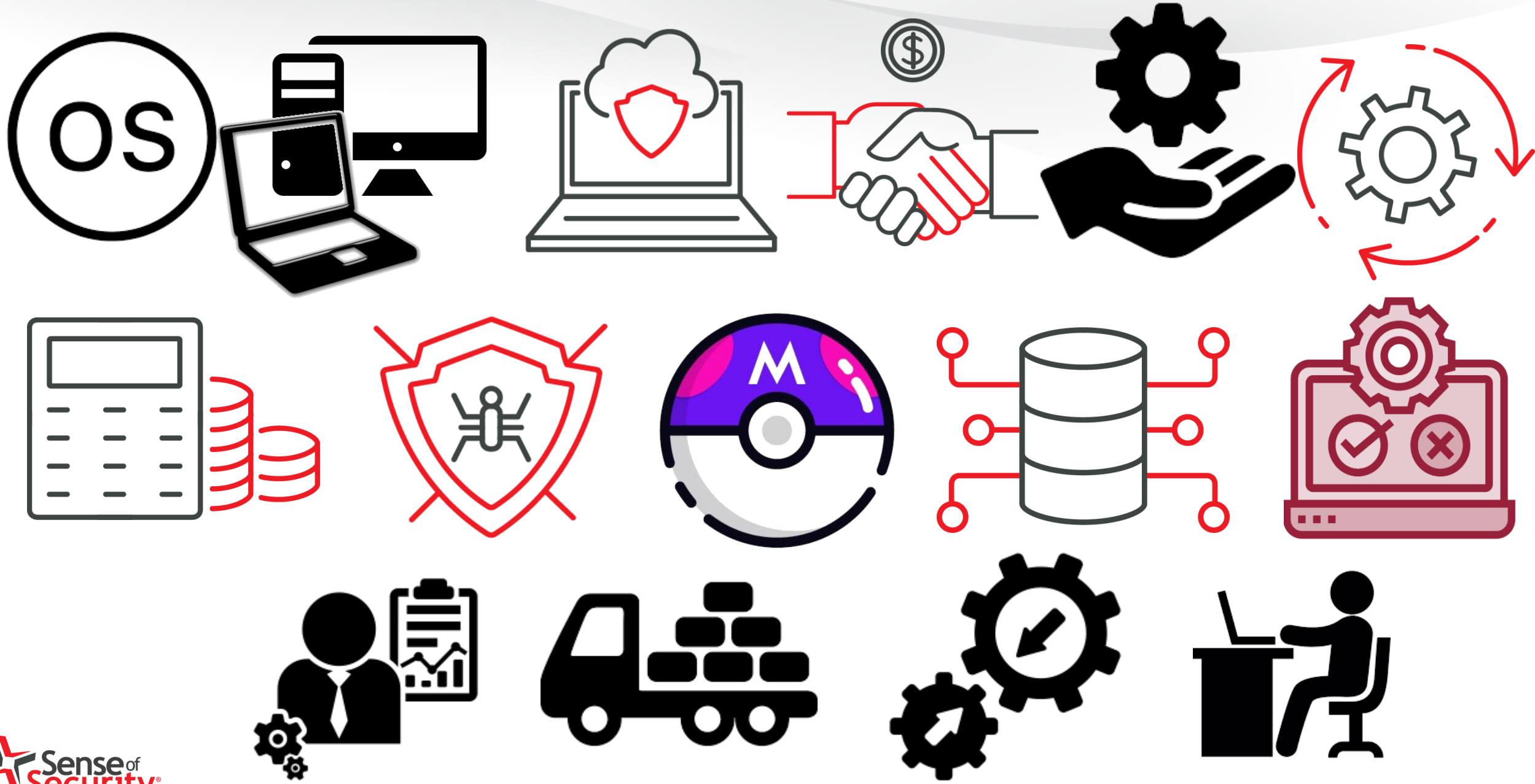
Preventing an Enterprise Win10 Rollout Being Remotely Controlled and Ransomed

Murray Goldschmidt

Chief Operating Officer
Sense of Security (a CyberCX Company)
@ITsecurityAU

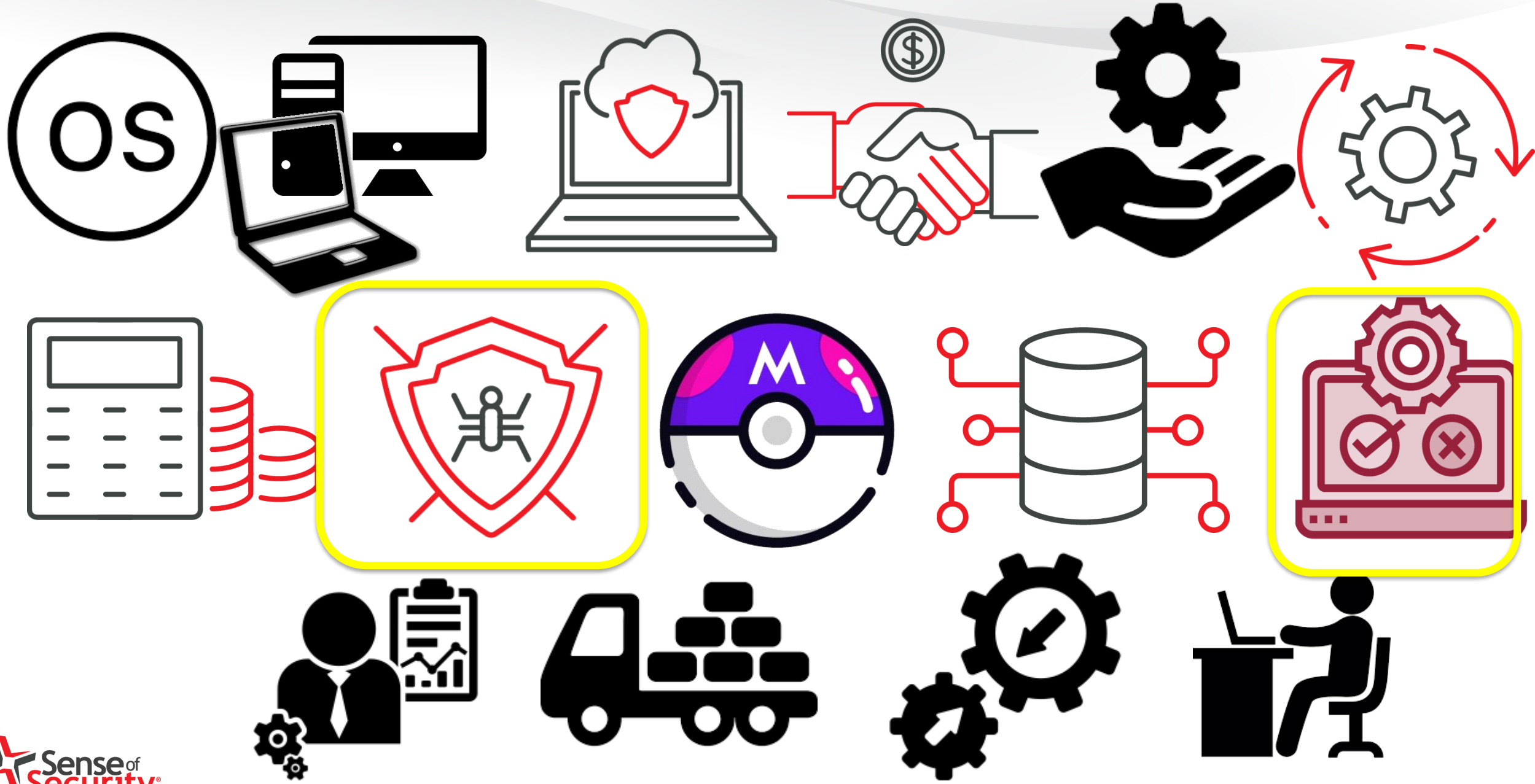
Concerned about this?

Enterprise Computer Rollout - Security



Sense of Security

A CyberCX company



Sense of Security

A CyberCX company

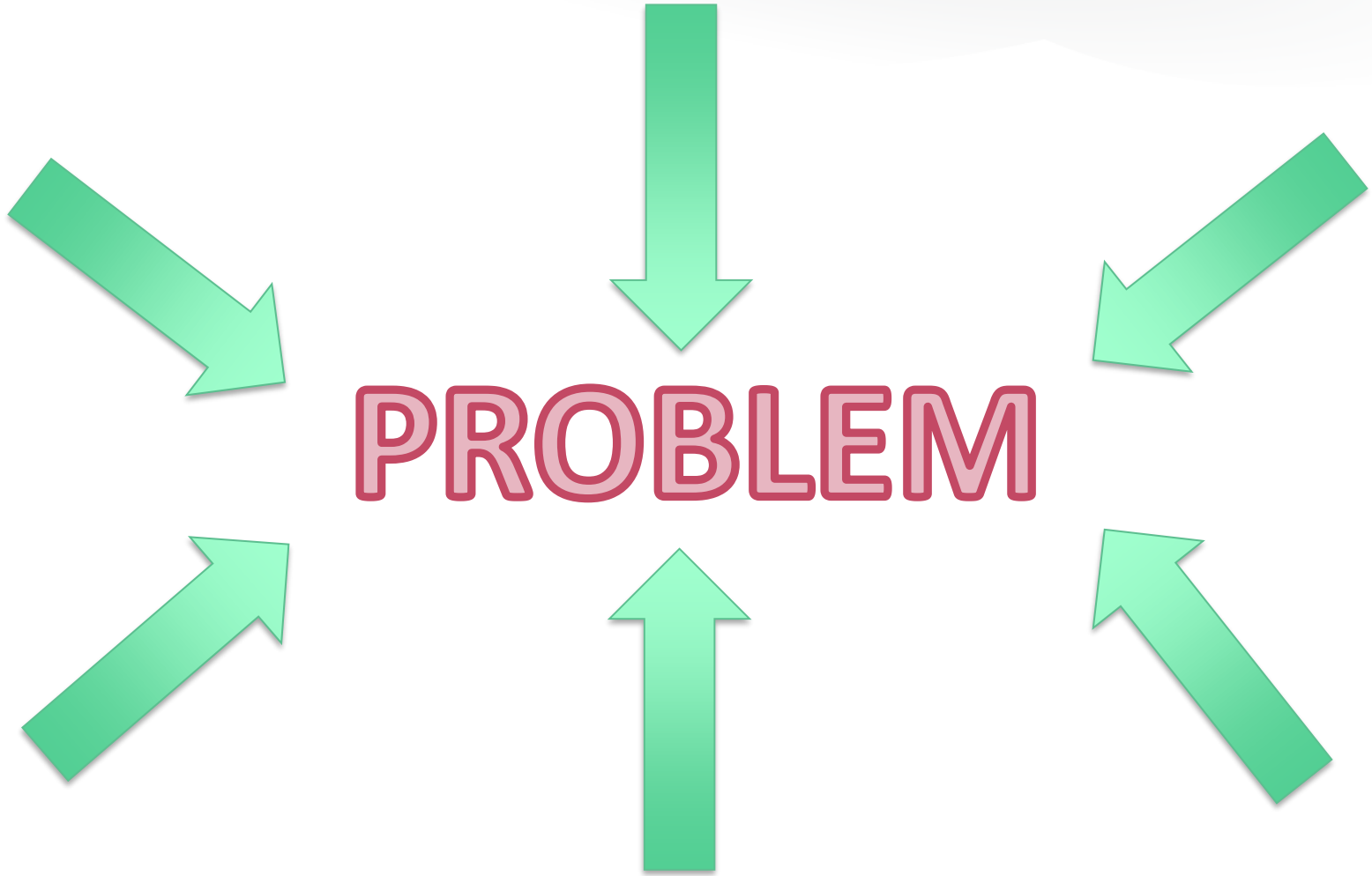
But not enough forward thinking ……

- Expensive Programs → Live with your decisions
- Long time-in-deployment (years)
- Address Compliance Requirements
- Address Corporate Policies (Push Down, Local Enforcement)
- Support Field Upgrades
- Deliver Cyber Resilience
- Avoid Catastrophic Situations (Losing control of your entire fleet)

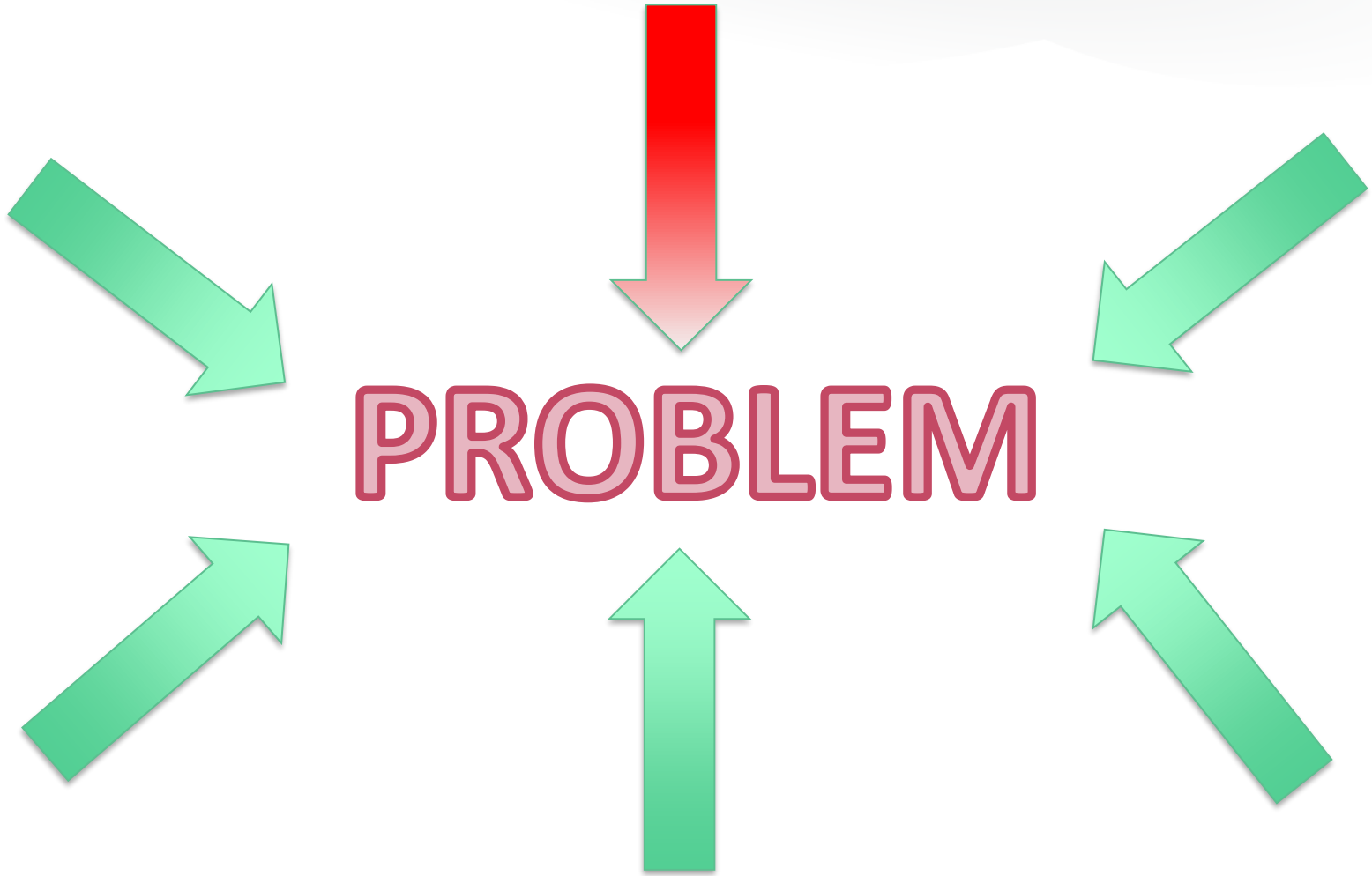
Coverage? Budget?


THINK
ABOUT
THINGS
DIFFERENTLY

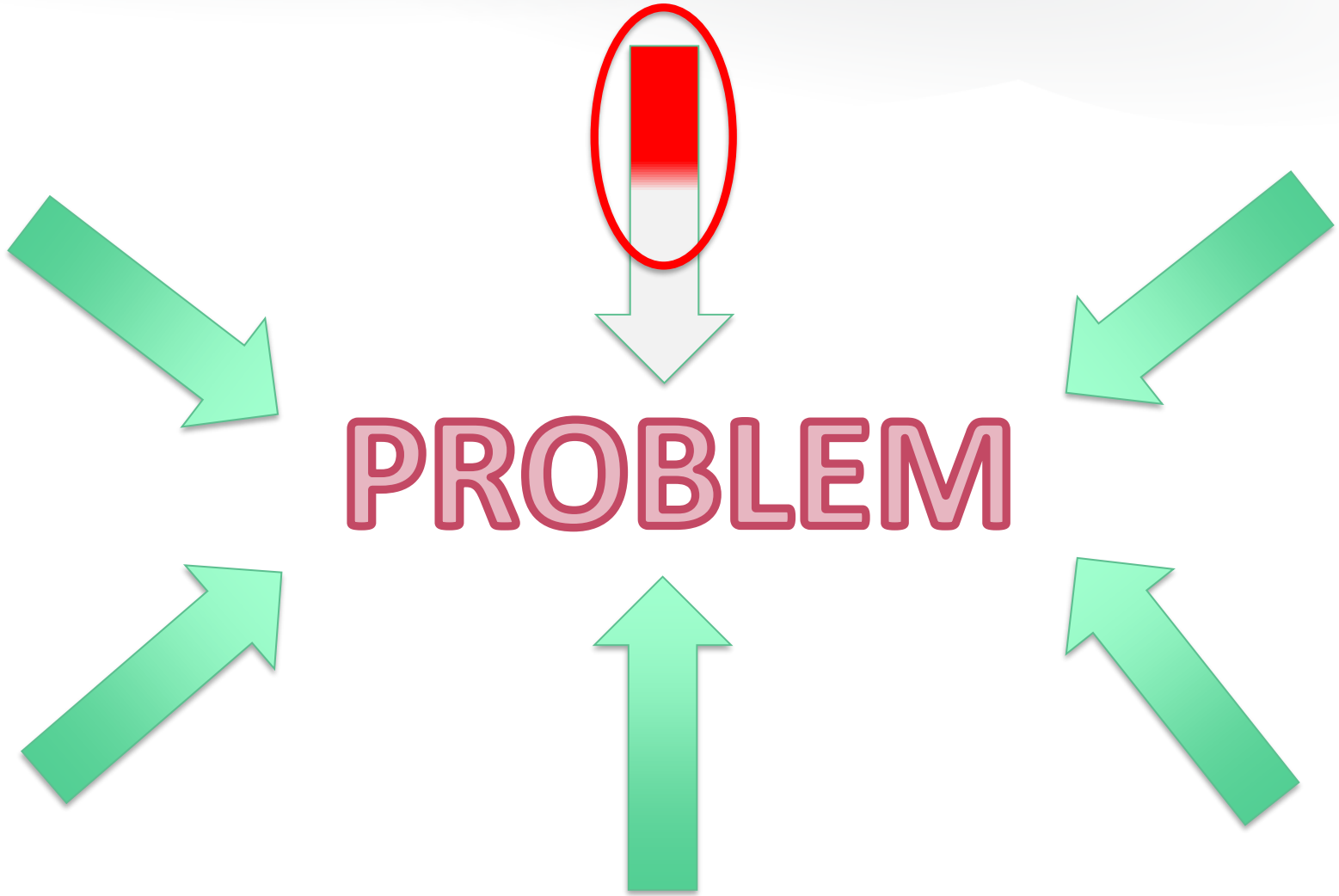
Explore the Options and Areas for Improvement



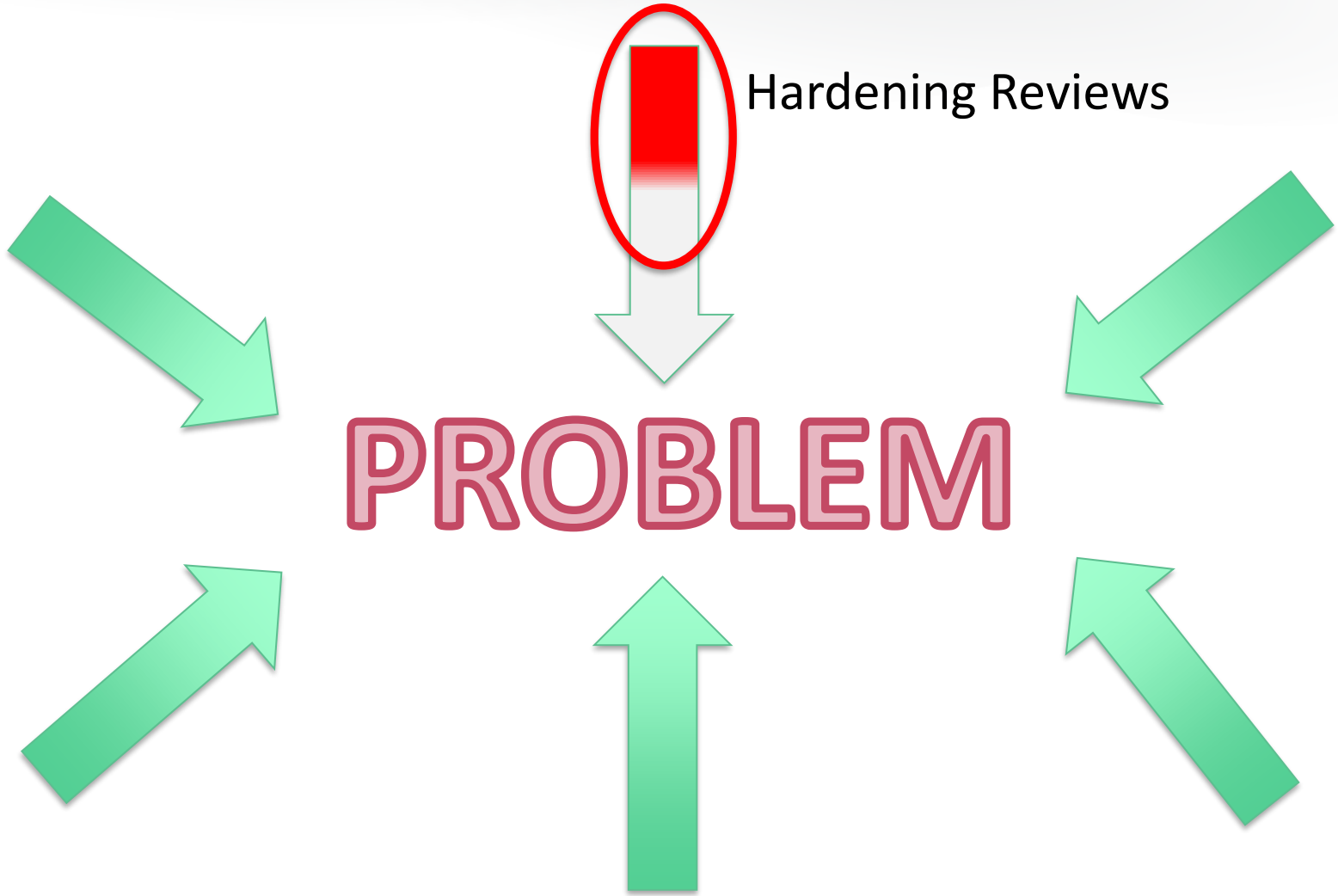
Explore the Options and Areas for Improvement

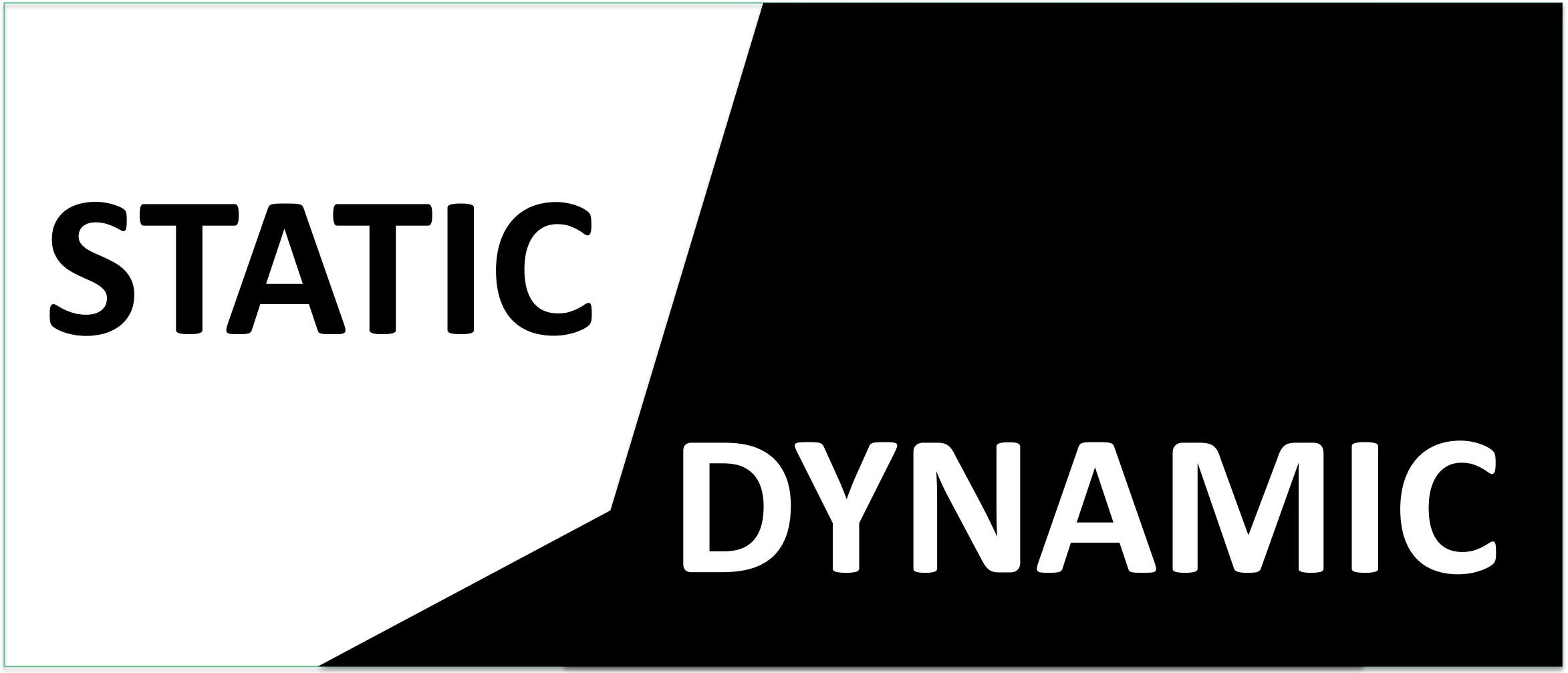


Explore the Options and Areas for Improvement



Explore the Options and Areas for Improvement

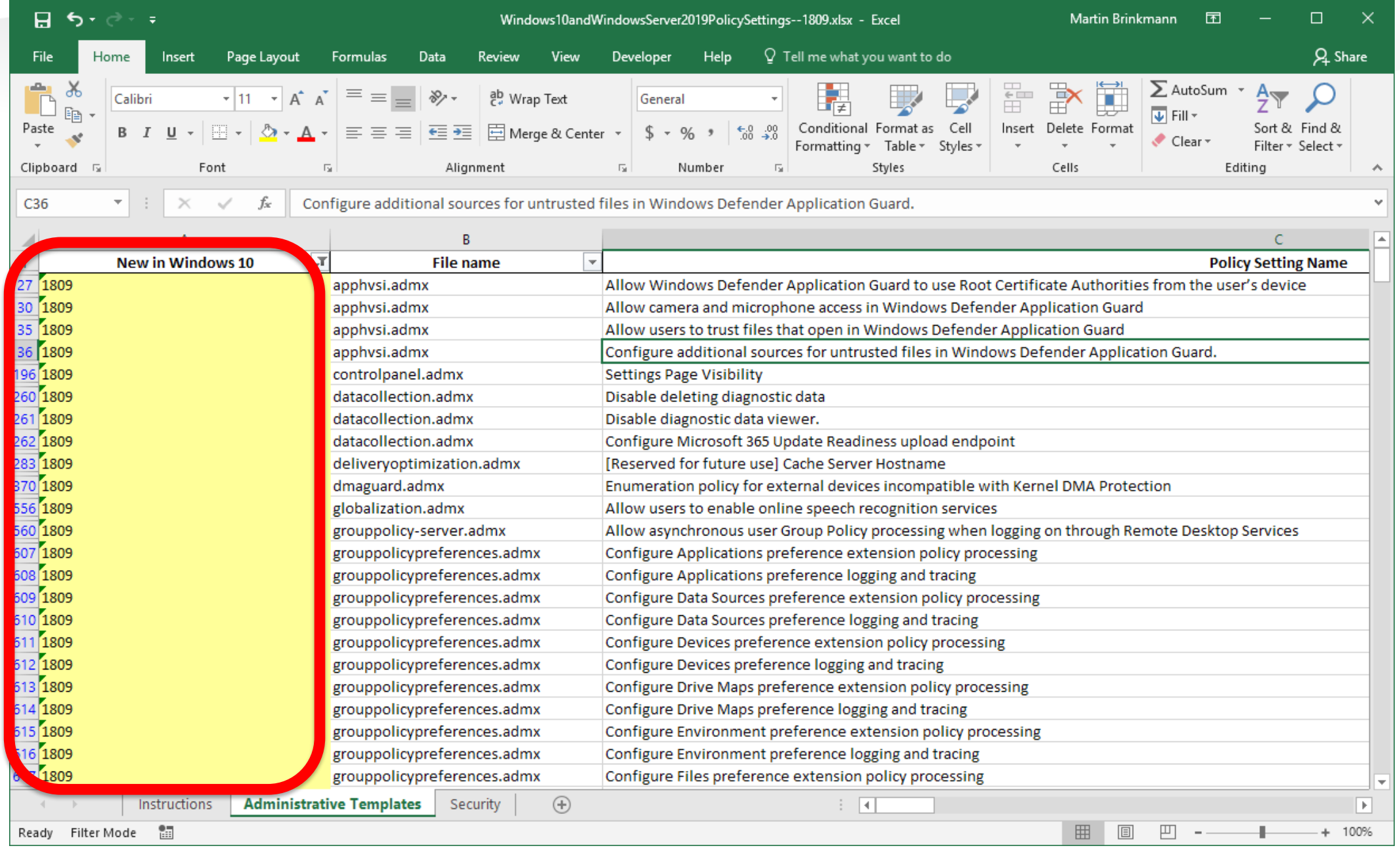



STATIC
DYNAMIC

Static Testing - Limitations

Checklist

Step	√	To Do	MFD	UT Note	Cat I	Cat II/III	Min Std
		Preparation and Installation					
1		If machine is a new install, protect it from hostile network traffic, until the operating system is installed and hardened.		§	!	!	4.5.1
2		Consider using the Security Configuration Wizard to assist in hardening the host.		§			
		Service Packs and Hotfixes					
3		Install the latest service packs and hotfixes from Microsoft.		§	!	!	4.5.2
4		Enable automatic notification of patch availability.		§	!	!	4.5.5
		User Account Policies					
5		Set minimum password length.	1.1.4	§	!	!	
6		Enable password complexity requirements.	1.1.5	§	!		
7		Do not store passwords using reversible encryption. (Default)	1.1.6	§	!	!	



Windows10andWindowsServer2019PolicySettings--1809.xlsx - Excel — Martin Brinkmann

File Home Insert Page Layout Formulas Data Review View Developer Help Tell me what you want to do Share

Paste Clipboard Calibri 11 Font Wrap Text Merge & Center Alignment General Number Conditional Formatting Format as Table Cell Styles Styles Insert Delete Format Cells AutoSum Fill Clear Sort & Filter Find & Select Editing

C36 Configure additional sources for untrusted files in Windows Defender Application Guard.

	A	B	C
	New in Windows 10	File name	Policy Setting Name
27	1809	apphvsi.admx	Allow Windows Defender Application Guard to use Root Certificate Authorities from the user's device
30	1809	apphvsi.admx	Allow camera and microphone access in Windows Defender Application Guard
35	1809	apphvsi.admx	Allow users to trust files that open in Windows Defender Application Guard
36	1809	apphvsi.admx	Configure additional sources for untrusted files in Windows Defender Application Guard.
196	1809	controlpanel.admx	Settings Page Visibility
260	1809	datacollection.admx	Disable deleting diagnostic data
261	1809	datacollection.admx	Disable diagnostic data viewer.
262	1809	datacollection.admx	Configure Microsoft 365 Update Readiness upload endpoint
283	1809	deliveryoptimization.admx	[Reserved for future use] Cache Server Hostname
370	1809	dmaguard.admx	Enumeration policy for external devices incompatible with Kernel DMA Protection
556	1809	globalization.admx	Allow users to enable online speech recognition services
560	1809	grouppolicy-server.admx	Allow asynchronous user Group Policy processing when logging on through Remote Desktop Services
607	1809	grouppolicypreferences.admx	Configure Applications preference extension policy processing
608	1809	grouppolicypreferences.admx	Configure Applications preference logging and tracing
609	1809	grouppolicypreferences.admx	Configure Data Sources preference extension policy processing
610	1809	grouppolicypreferences.admx	Configure Data Sources preference logging and tracing
611	1809	grouppolicypreferences.admx	Configure Devices preference extension policy processing
612	1809	grouppolicypreferences.admx	Configure Devices preference logging and tracing
613	1809	grouppolicypreferences.admx	Configure Drive Maps preference extension policy processing
614	1809	grouppolicypreferences.admx	Configure Drive Maps preference logging and tracing
615	1809	grouppolicypreferences.admx	Configure Environment preference extension policy processing
616	1809	grouppolicypreferences.admx	Configure Environment preference logging and tracing
6	1809	grouppolicypreferences.admx	Configure Files preference extension policy processing

Instructions | Administrative Templates | Security

Ready Filter Mode 100%

Australian Government
Australian Signals Directorate

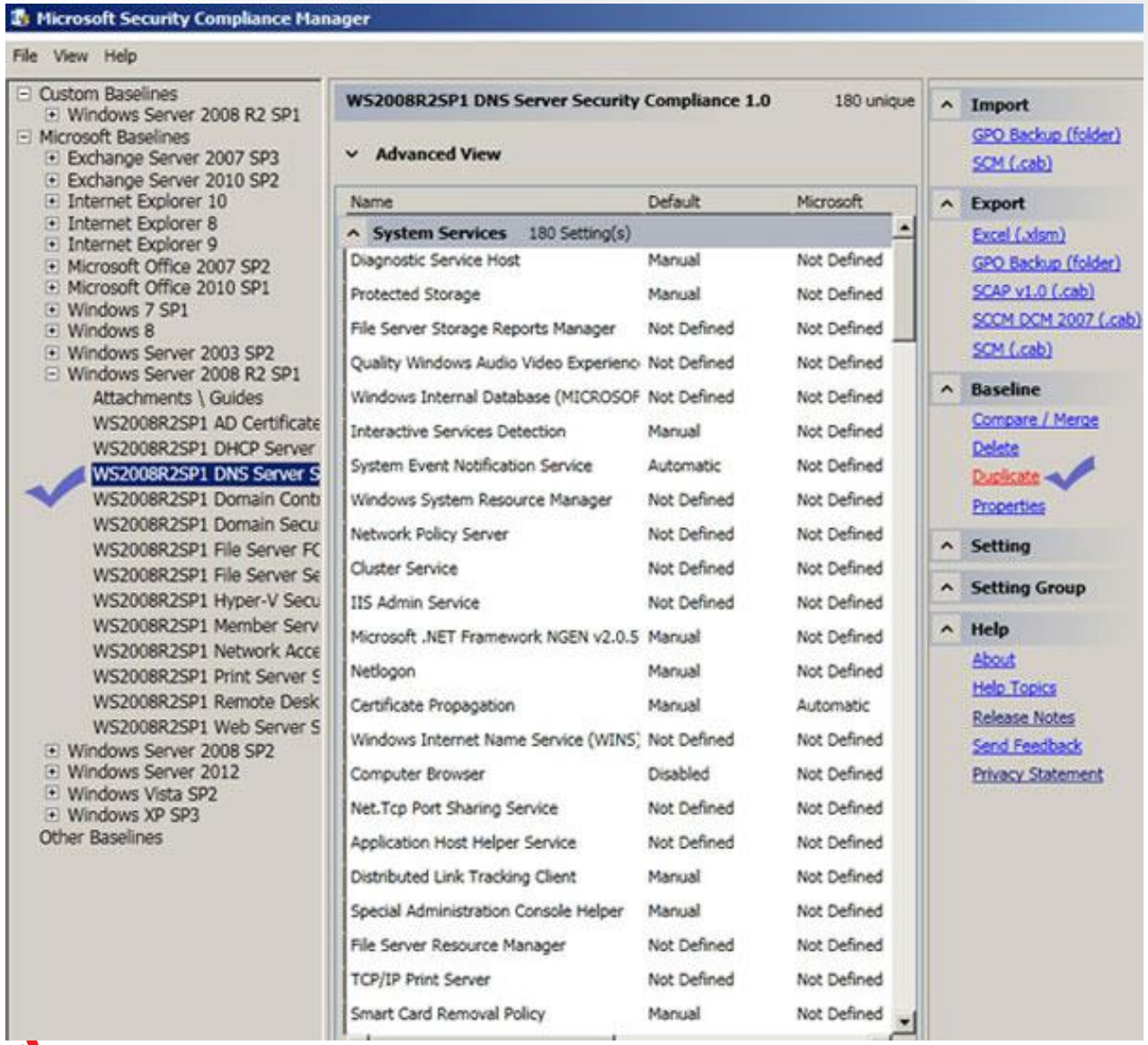
ACSC Australian Cyber Security Centre

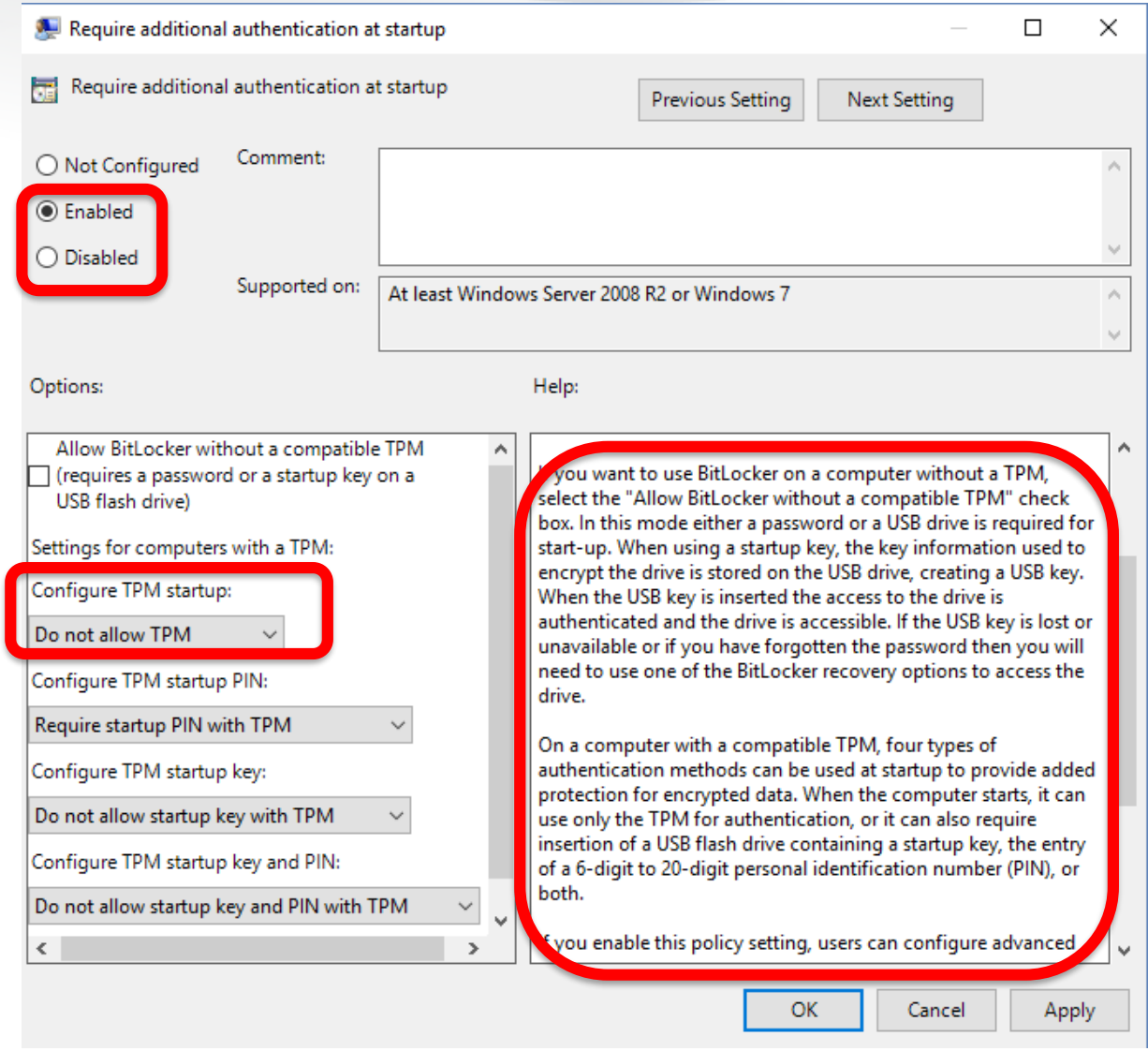
https://www.cyber.gov.au/publications/hardening-microsoft-windows-10-version-1709-workstations

Sense of Security
A CyberCX company

Sense of Security

A CyberCX company


Microsoft Security Compliance Manager
File View Help
Custom Baselines
Windows Server 2008 R2 SP1
Microsoft Baselines
Exchange Server 2007 SP3
Exchange Server 2010 SP2
Internet Explorer 10
Internet Explorer 8
Internet Explorer 9
Microsoft Office 2007 SP2
Microsoft Office 2010 SP1
Windows 7 SP1
Windows 8
Windows Server 2003 SP2
Windows Server 2008 R2 SP1
Attachments \ Guides
WS2008R2SP1 AD Certificate
WS2008R2SP1 DHCP Server
WS2008R2SP1 DNS Server S
WS2008R2SP1 Domain Contr
WS2008R2SP1 Domain Secu
WS2008R2SP1 File Server FC
WS2008R2SP1 File Server Se
WS2008R2SP1 Hyper-V Secu
WS2008R2SP1 Member Serv
WS2008R2SP1 Network Acce
WS2008R2SP1 Print Server S
WS2008R2SP1 Remote Desk
WS2008R2SP1 Web Server S
Windows Server 2008 SP2
Windows Server 2012
Windows Vista SP2
Windows XP SP3
Other Baselines
WS2008R2SP1 DNS Server Security Compliance 1.0
180 unique
Advanced View
Name
Default
Microsoft
System Services 180 Setting(s)
Diagnostic Service Host Manual Not Defined
Protected Storage Manual Not Defined
File Server Storage Reports Manager Not Defined Not Defined
Quality Windows Audio Video Experienc Not Defined Not Defined
Windows Internal Database (MICROSOF Not Defined Not Defined
Interactive Services Detection Manual Not Defined
System Event Notification Service Automatic Not Defined
Windows System Resource Manager Not Defined Not Defined
Network Policy Server Not Defined Not Defined
Cluster Service Not Defined Not Defined
IIS Admin Service Not Defined Not Defined
Microsoft .NET Framework NGEN v2.0.5 Manual Not Defined
Netlogon Manual Not Defined
Certificate Propagation Manual Automatic
Windows Internet Name Service (WINS) Not Defined Not Defined
Computer Browser Disabled Not Defined
Net.Tcp Port Sharing Service Not Defined Not Defined
Application Host Helper Service Not Defined Not Defined
Distributed Link Tracking Client Manual Not Defined
Special Administration Console Helper Manual Not Defined
File Server Resource Manager Not Defined Not Defined
TCP/IP Print Server Not Defined Not Defined
Smart Card Removal Policy Manual Not Defined
Import
GPO Backup (folder)
SCM (.cab)
Export
Excel (.xlsm)
GPO Backup (folder)
SCAP v1.0 (.cab)
SCCM DCM 2007 (.cab)
SCM (.cab)
Baseline
Compare / Merge
Delete
Duplicate
Properties
Setting
Setting Group
Help
About
Help Topics
Release Notes
Send Feedback
Privacy Statement


Require additional authentication at startup
Require additional authentication at startup
Previous Setting
Next Setting
Not Configured
Enabled
Disabled
Comment:
Supported on:
At least Windows Server 2008 R2 or Windows 7
Options:
Help:
Allow BitLocker without a compatible TPM (requires a password or a startup key on a USB flash drive)
Settings for computers with a TPM:
Configure TPM startup:
Do not allow TPM
Configure TPM startup PIN:
Require startup PIN with TPM
Configure TPM startup key:
Do not allow startup key with TPM
Configure TPM startup key and PIN:
Do not allow startup key and PIN with TPM
If you want to use BitLocker on a computer without a TPM, select the "Allow BitLocker without a compatible TPM" check box. In this mode either a password or a USB drive is required for start-up. When using a startup key, the key information used to encrypt the drive is stored on the USB drive, creating a USB key. When the USB key is inserted the access to the drive is authenticated and the drive is accessible. If the USB key is lost or unavailable or if you have forgotten the password then you will need to use one of the BitLocker recovery options to access the drive.
On a computer with a compatible TPM, four types of authentication methods can be used at startup to provide added protection for encrypted data. When the computer starts, it can use only the TPM for authentication, or it can also require insertion of a USB flash drive containing a startup key, the entry of a 6-digit to 20-digit personal identification number (PIN), or both.
If you enable this policy setting, users can configure advanced
OK
Cancel
Apply

Top recommendations

OS security updates	Install the latest security updates	+72 points
Exploit Guard ⓘ	Turn on Attack Surface Reduction rules	+33 points
Exploit Guard ⓘ	Set controlled folder access to enabled...	+32 points
Antivirus	Fix antivirus reporting and get emerge...	+19 points
Credential Guard ⓘ	Turn on Credential Guard	+17 points
BitLocker ⓘ	Ensure drive compatibility ⓘ	+17 points
BitLocker ⓘ	Encrypt all supported drives	+8 points
Windows Hello ⓘ	Encourage all users to use Windows He...	+7 points

Assessing Hardening - Problems

- Generally where most SOE/Image tests start & end
- Static assessments cost more than they are worth
- Results in constraints of budget. Money spent in the wrong places
- Done ineffectively through manual means
- **Scope ineffective (generally trying to match benchmark stds only)**
- **Then cut out items in the "too hard basket"**
- Seldom cover broad ranges of controls
  - Full Disk Encryption (no excuse its built in!)
  - App Whitelisting (its built in – but more complicated to get right)
  - File Integrity Monitoring (much more accessible in Vuln Mgt)

Assessing Hardening – Increasing the Scope

- Assess for seemingly benign configs that can be trojaned
- Examples:
  - PDF controls
    - BADPDF: Stealing Windows Credentials via PDF Files
      - The fundamental issue has been fixed CVE-2018-4993
      - Huge number of orgs remain susceptible to this (**points to s/w supply chain issue**)
  - Understanding Appref.MS Config Files
    - Windows 10 victim host - Fully patched with Windows Defender enabled
    - See http://i.blackhat.com/USA-19/Wednesday/us-19-Burke-ClickOnce-And-Youre-In-When-Appref-Ms-Abuse-Is-Operating-As-Intended-wp.pdf
    - **Points to S/W and Services Supply Chain Issues & Config Mgt Issues & Vuln Mgt Issues**

The .appref-ms file can be ran to check for updates and run the application. This is the crux of the malicious deployment mechanism, as an .appref-ms file can be ran even if the application was not previously installed. Upon execution it will connect with the deployment server to install and run

By selecting "The application should check for updates" the application will always check in with the deployment server to see if there is a more recent version of the application. By setting "Before the application starts" it can be specified that the application will force install any established updates before running the application should they be found. As long as the user approved of the initial application installation, any updates to the application will not require user approval. In this section a minimum version number can also be specified for updates, in addition to specifying a separate location where the update is located if required.

As the .appref-ms filetype is not flagged as malicious by Gmail or Outlook, you could attach it directly to an e-mail to gain initial access upon code execution on the end user's host. However, to further give credence to the social engineering aspects of phishing it may be prudent to use the .appref-ms file as an OLE within a Word document.

maketecheasier.com/send-file-extensions-blocked-from-outlook/

Apps Klik USB 3.0 to Giga...

maketecheasier H

Ads by Google

Microsoft Bans 38 File Extensions from Web Outlook

By Simon Batt – Posted on Oct 9, 2019 in Internet

maketecheasier.com/send-file-extensions-blocked-from-outlook/

Apps Klik USB 3.0 to Giga...

maketecheasier H

Ads by Google

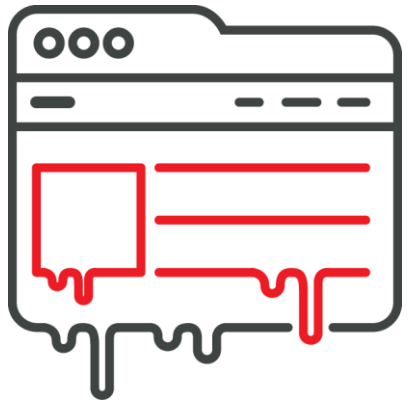
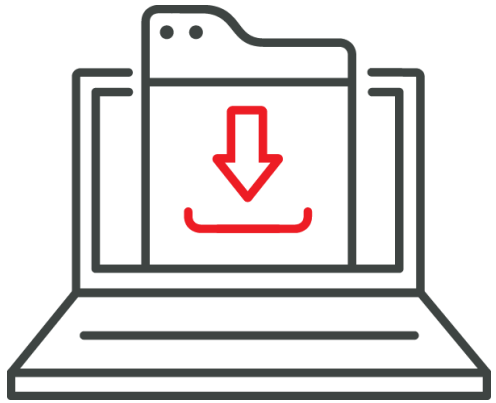
Microsoft Bans 38 File Extensions from Web Outlook – Here's How to Send Them

By Simon Batt – Posted on Oct 9, 2019 in Internet

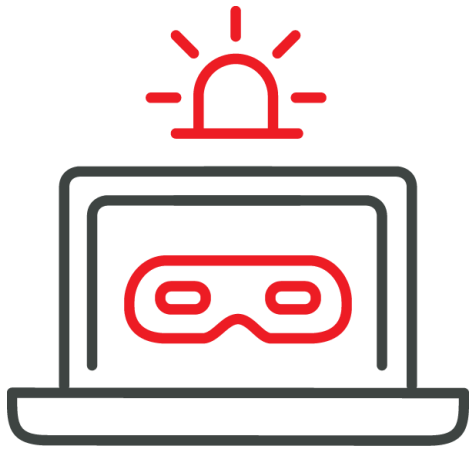
As per the announcement announcing this change, Microsoft has listed the exact file extensions that are now blocked. These include:

- Files related to the Python scripting language (".py," ".pyc," ".pyo," ".pyw," ".pyz," and ".pyzw")
- Files related to the PowerShell scripting language (".ps1," ".ps1xml," ".ps2," ".ps2xml," ".psc1," ".psc2," ".psd1," ".psdm1," ".cdxml," and ".pssc")
- Java Files (".jar" and ".jnlp")
- Digital Certificate Files (".cer," ".crt," ".der")
- Windows ClickOnce Files (".appref-ms")
- Microsoft Data Access Components (".udl")
- Windows Sandbox files (".wsb")
- Files used by "various applications" as stated by Microsoft (".appcontent-ms," ".settingcontent-ms," ".cnt," ".hpj," ".website," ".webpnp," ".mcf," ".printerexport," ".pl," ".theme," ".vbp," ".xbap," ".xll," ".xnk," ".msu," ".diagcab," and ".grp")

Scenario for Total Loss of Control of Computer Fleet



Sense of Security
A CyberCX company

Assessing Hardening - Improvements

- Still important, must be more effective.
- Adopt Automation!
- Strive towards Continuous Monitoring.
  - Hardening profiles change over time.
  - You need to review WHAT you are checking for and UPDATE as the landscape changes
  - Hardening is more than core OS hardening. Need to check for configuration of crypto/app whitelisting and configs that will cause problems @ run time (appref.ms)
  - **Hardening reviews are next to useless if performed once off**

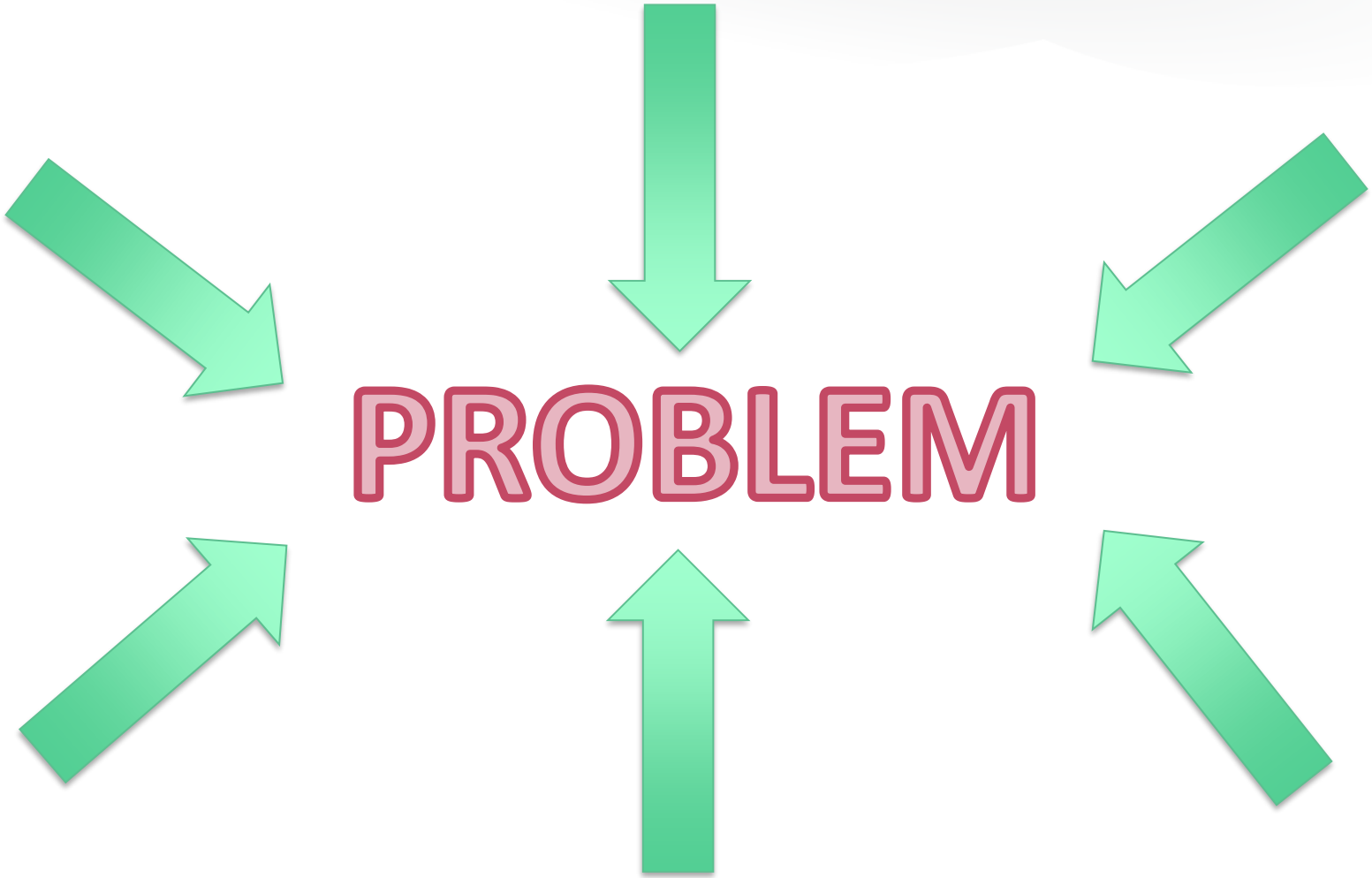
Assessing Hardening - Improvements

Summary

- Hardening Validation is part of Config/Vuln Mgt
  - should be ongoing operational activity – not capital expense.
- If hardening validation is BAU will represent a small portion of security budget for SOE/Rollout Programs
- Creates room for **Dynamic Testing**

Root Cause of Problems: Configuration Mgt

Explore the Options and Areas for Improvement



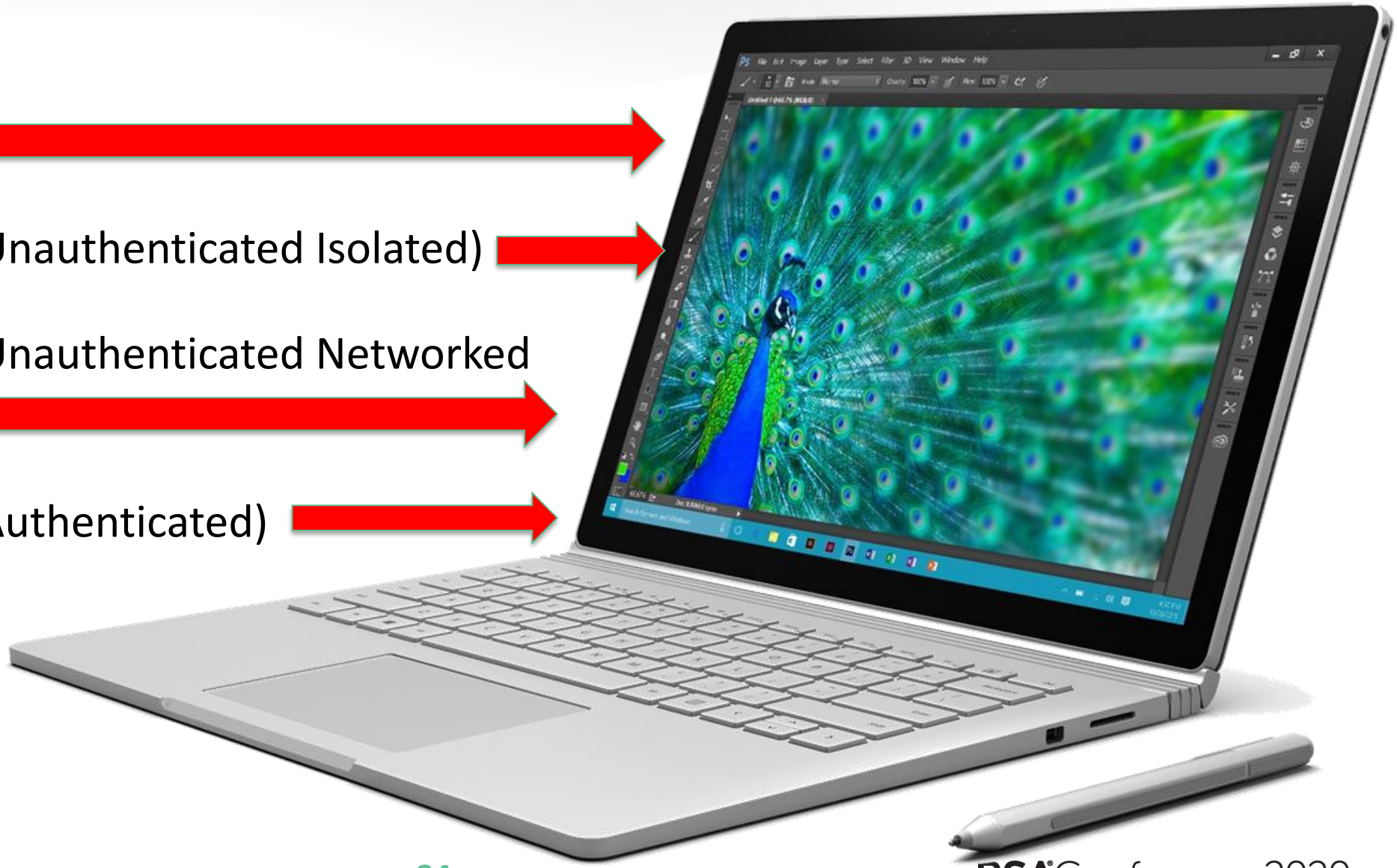
Dynamic Testing Variants

Pre Boot Testing

Post Boot Testing (Unauthenticated Isolated)

Post Boot Testing (Unauthenticated Networked (WLAN/LAN)

Post Boot Testing (Authenticated)



Pre Boot Security Testing

- Looking to exploit issues in:
  - BIOS Config
    - E.g. boot from alternative OS (USB etc)
  - Full Disk Encryption (FDE)
    - Limitations of FDE relying on TPM only and no PIN
      - Windows 10 users can update their BitLocker PINs and passwords themselves, without administrator credentials.
      - But PIN is **not** the default.
      - https://www.moderndeployment.com/require-startup-tpmpin-for-bitlocker-encryption-enterprise-security/

BitLocker authentication methods

Authentication method	Requires user interaction	Description
TPM only	No	TPM validates early boot components.
TPM + PIN	Yes	TPM validates early boot components. The user must enter the correct PIN before the start-up process can continue, and before the drive can be unlocked. The TPM will enter lockout if the incorrect PIN is entered repeatedly to protect the PIN from brute force attacks. The number of repeated attempts that will trigger a lockout is variable.
TPM + Network key	No	The TPM successfully validates early boot components, and a valid encrypted network key has been provided from the WDS server. This authentication method provides automatic unlock of operating system volumes at system reboot while still maintaining multifactor authentication.
TPM + startup key	Yes	The TPM successfully validates early boot components, and a USB flash drive containing the startup key has been inserted.
Startup key only	Yes	The user is prompted to insert the USB flash drive that holds the recovery key and/or startup key and reboot the computer.

- Network Unlock
  - **Network Unlock enables BitLocker-protected PCs to start automatically when connected to a wired corporate network on which Windows Deployment Services runs. ???????**
  - https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-device-encryption-overview-windows-10

Read the Fine Print – for the Countermeasures

Attacker with skill and lengthy physical access

Targeted attack with plenty of time; this attacker will open the case, will solder, and will use sophisticated hardware or software.

Mitigation:

- Pre-boot authentication set to TPM with a PIN protector (with a sophisticated alphanumeric PIN to help the TPM anti-hammering mitigation).

  -And-

- Disable Standby power management and shut down or hibernate the device before it leaves the control of an authorized user. This can be set using Group Policy:
  - Computer Configuration|Policies|Administrative Templates|Windows Components|File Explorer|Show hibernate in the power options menu
  - Computer Configuration|Policies|Administrative Templates|System|Power Management|Sleep Settings|Allow standby states (S1-S3) when sleeping (plugged in)
  - Computer Configuration|Policies|Administrative Templates|System|Power Management|Sleep Settings|Allow standby states (S1-S3) when sleeping (on battery)

These settings are **Not configured** by default.

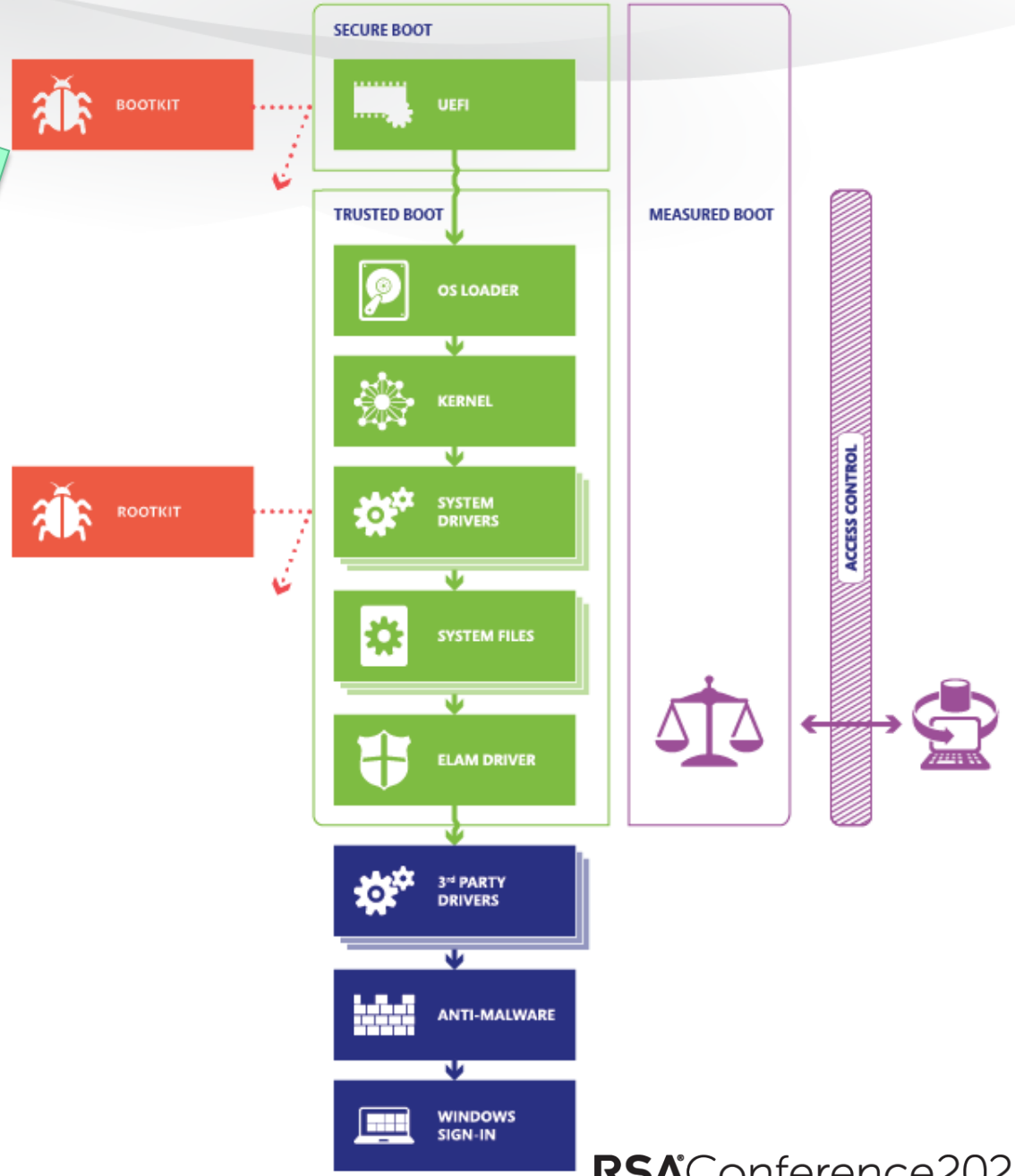
https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-countermeasures

Securing the Boot Process

- Secure Boot, a component of Trusted Boot, is a security feature supported by Microsoft Windows 10 version 1709 and motherboards with an UEFI2
  - Relevant to new fleets of computers
  - Not so much for refresh of old fleets
  - This is why testing how different computers in the fleet may respond to different attack scenarios is relevant.
  - https://docs.microsoft.com/en-us/windows/security/information-protection/secure-the-windows-10-boot-process

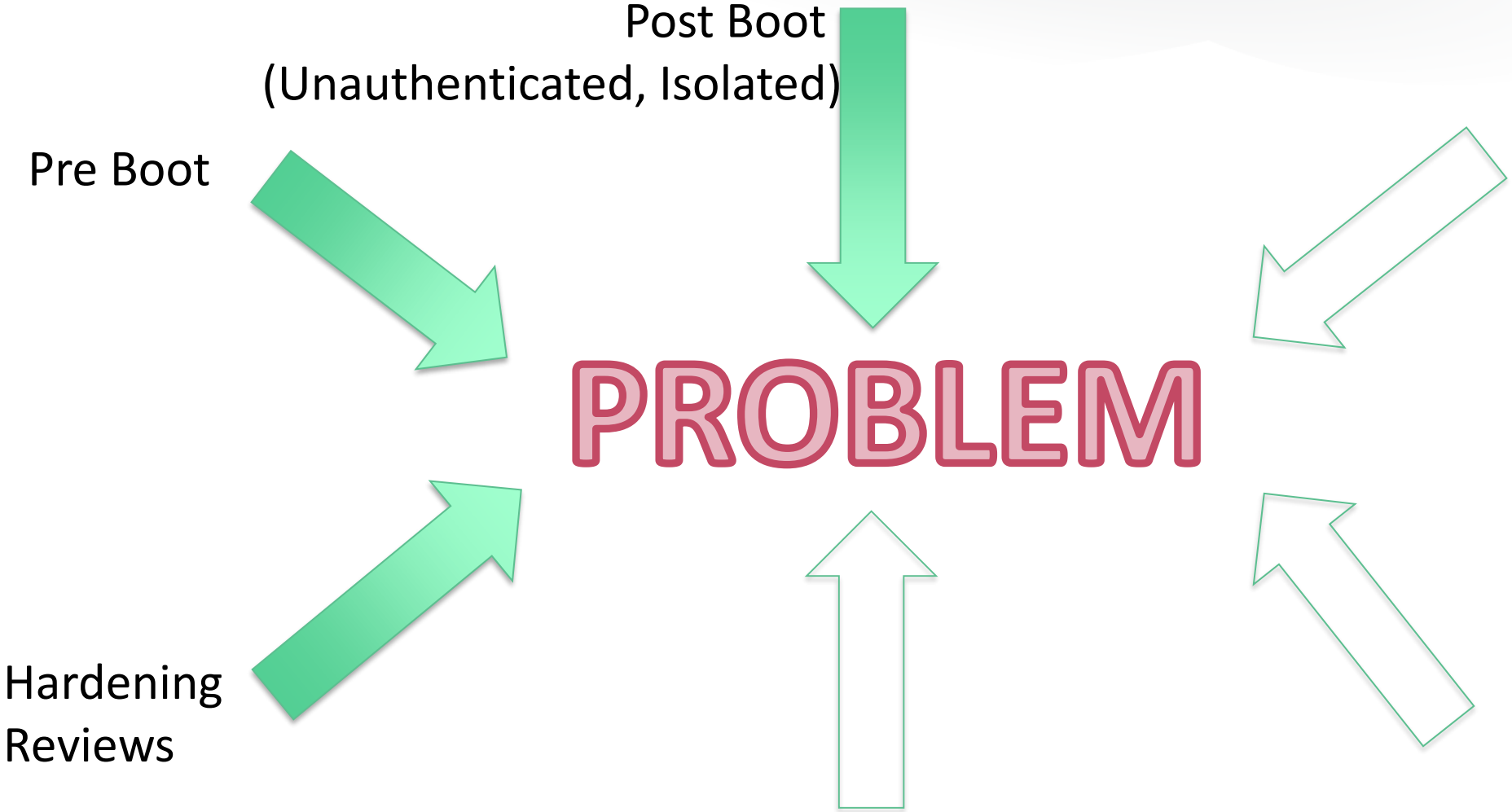
Because part of your fleet may be susceptible to **bootkits**

and **rootkits**



Microsoft Windows 10 version 1709 and motherboards with an UEFI2

Explore the Options and Areas for Improvement



Post Boot – Unauthenticated, Isolated

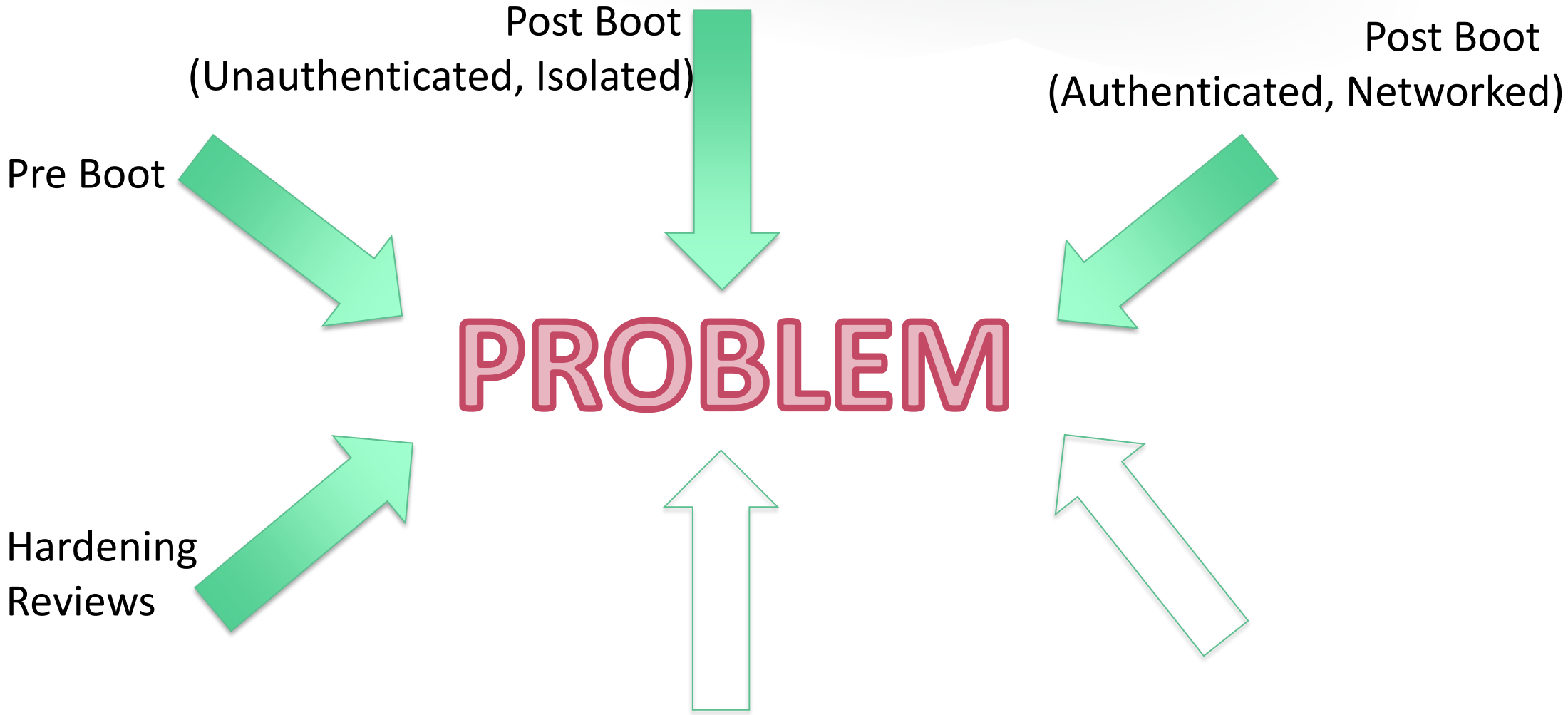
Post Boot – Unauthenticated, Isolated

- Problems
  - Relying on OS Authentication Controls
  - Account Guessing/Brute Forcing
    - Local Accounts
    - Domain Accounts (Cached)
    - Therefore testing of the laptop on and off network is required.
- Other components of the footprint are:
  - USB
  - Bluetooth
  - Ethernet
  - Any service that is operational on the OS and can be connected to if on the network (e.g. remote desktop, SNMP or other protocols)

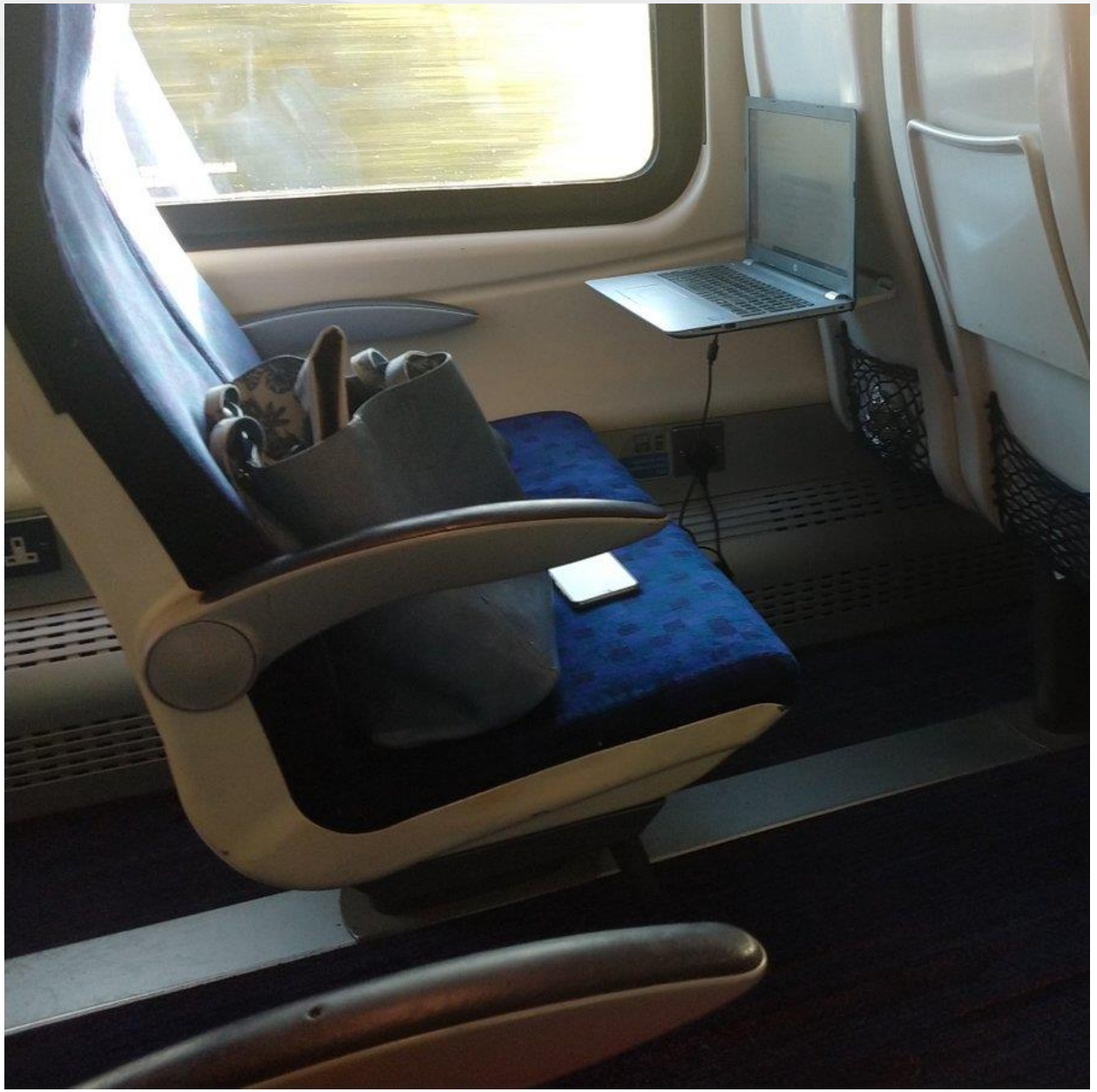
Post Boot – Unauthenticated, Isolated

- Testing
  - Local Password Attacks
  - Wireless Stimulation – assisted with OSINT/SE (Credential Leakage)
  - Perform attacks against online device, when connected to client premises/LAN
  - Perform attacks against online device, under normal use, i.e. as a remote worker
- Improvements
  - Smart Card, Biometric Access Controls – for Auth
  - Effective Password Policies (Local and Domain, LAPS)
  - Peripherals Security
  - Run Once Protections/App Whitelisting

Explore the Options and Areas for Improvement



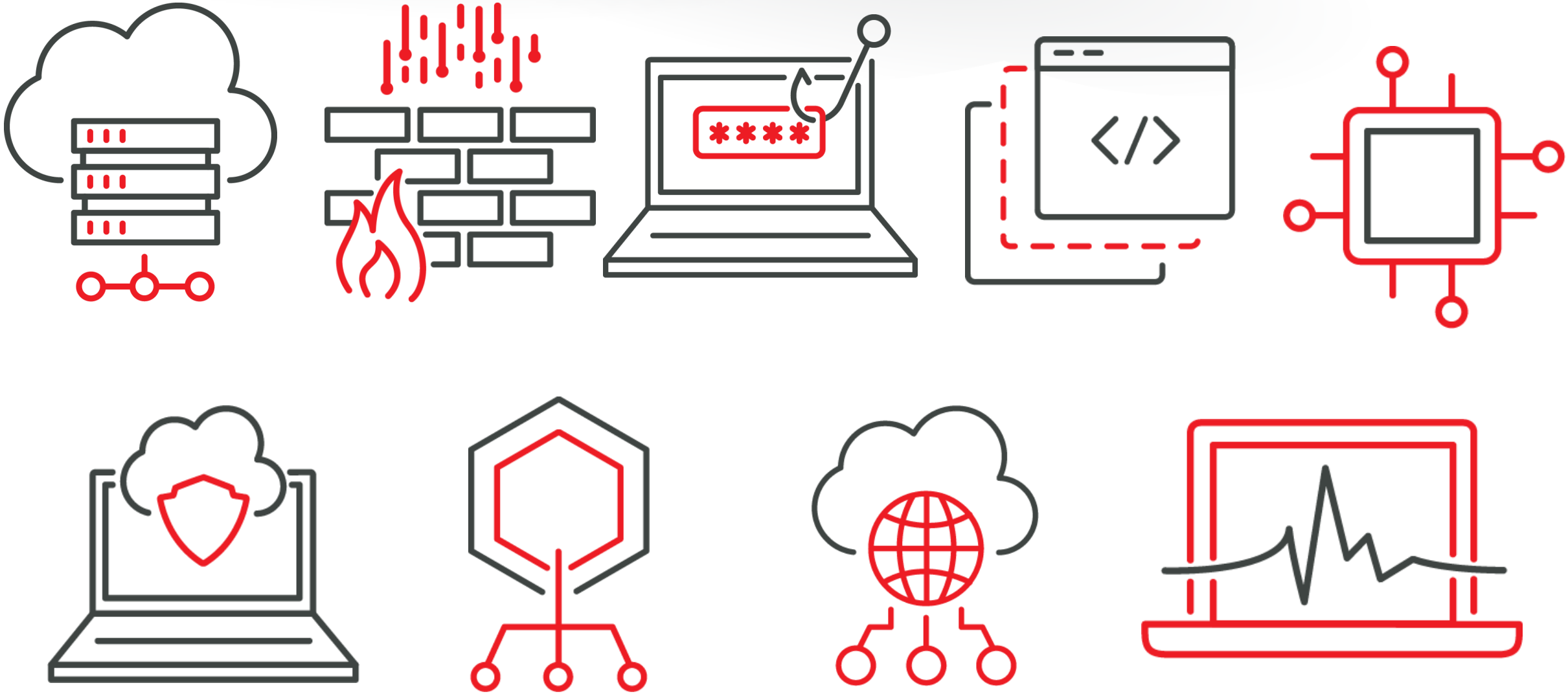
Post Boot - Authenticated



Sense of Security
A CyberCX company

The General Corporate User Case ….

Enterprise Breach Assessment Break-Out Penetration Test

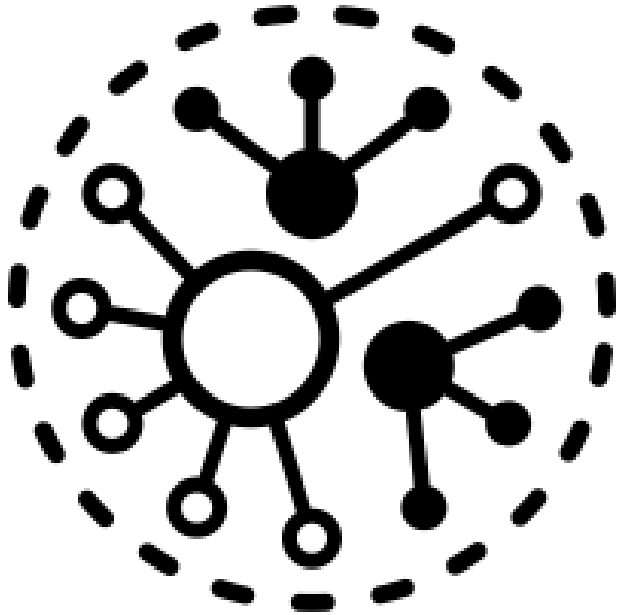


Sense of Security

A CyberCX company

Unvalidated Controls

But we hired a security guard!

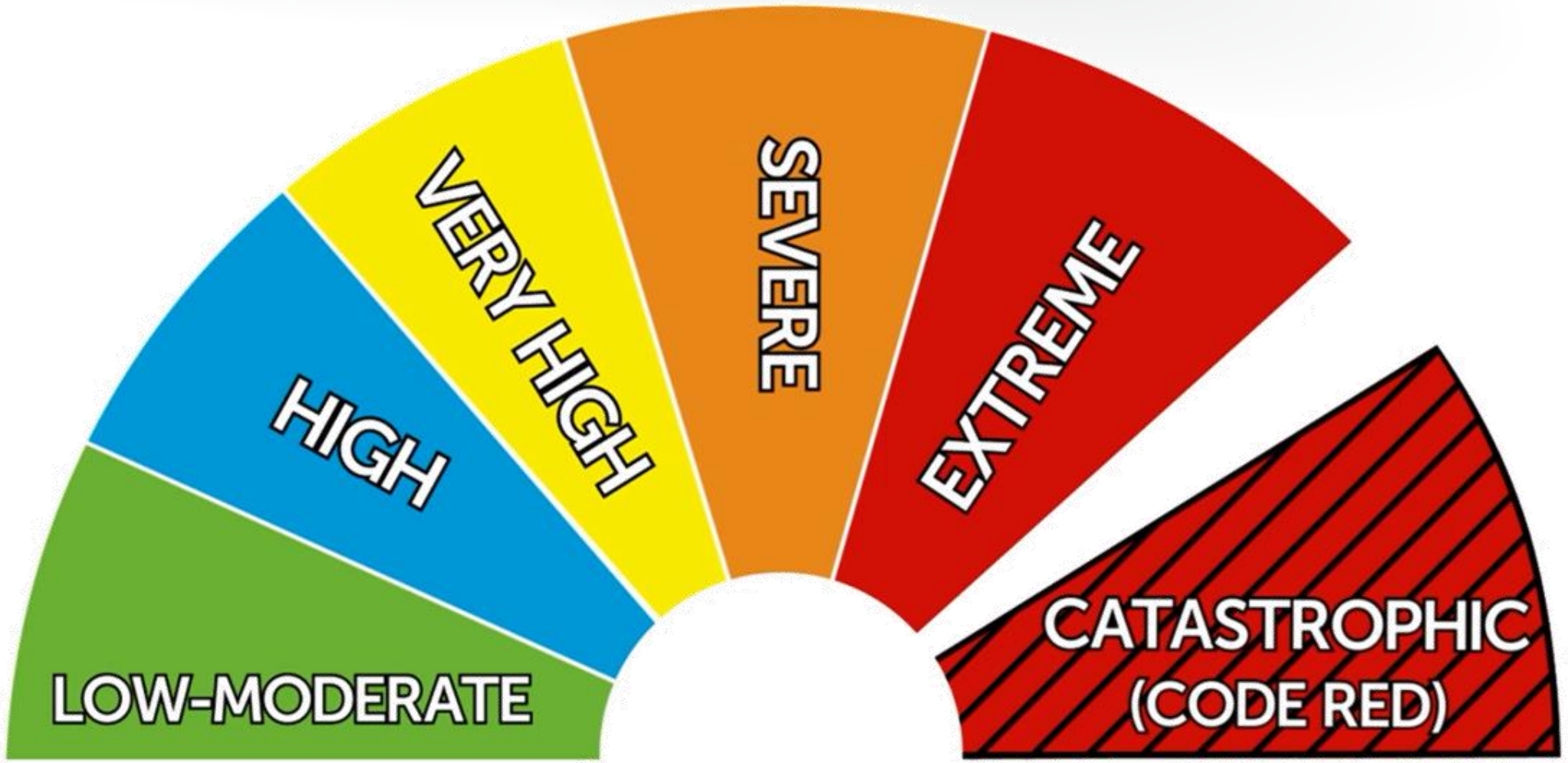


Risk correlation?
Cumulative risk?
Linear vs Interconnected Risks

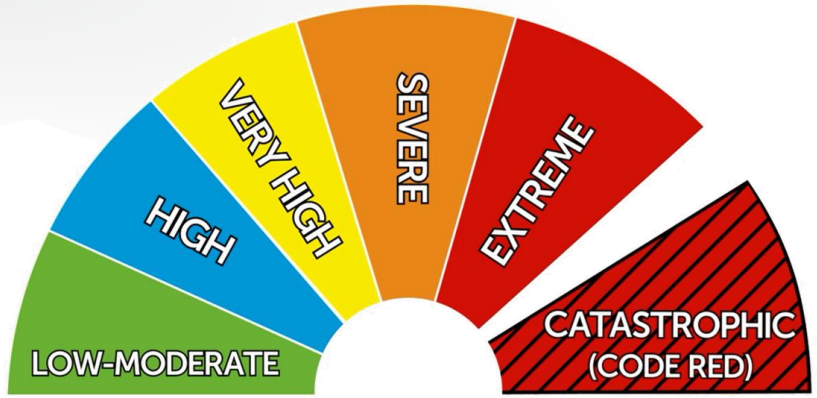
Full Stack Security

- Problems
  - Gateway Controls that allow malware inbound (email)
  - Gateway Controls that allow alternative paths for malware (email → web)
  - OS Controls that don't block execution (failed whitelisting)
  - End Point Controls that don't stop sleeper malware (appref.ms)
  - End Point Controls that don't stop malware!
  - Enterprise Controls that don't detect changes to OS's (Config Mgt)
- Testing
  - Various scenarios to test breadth and depth of above
- Improvements
  - As needed to defeat the attacks. This is the crux of the SOE/Golden Image philosophy

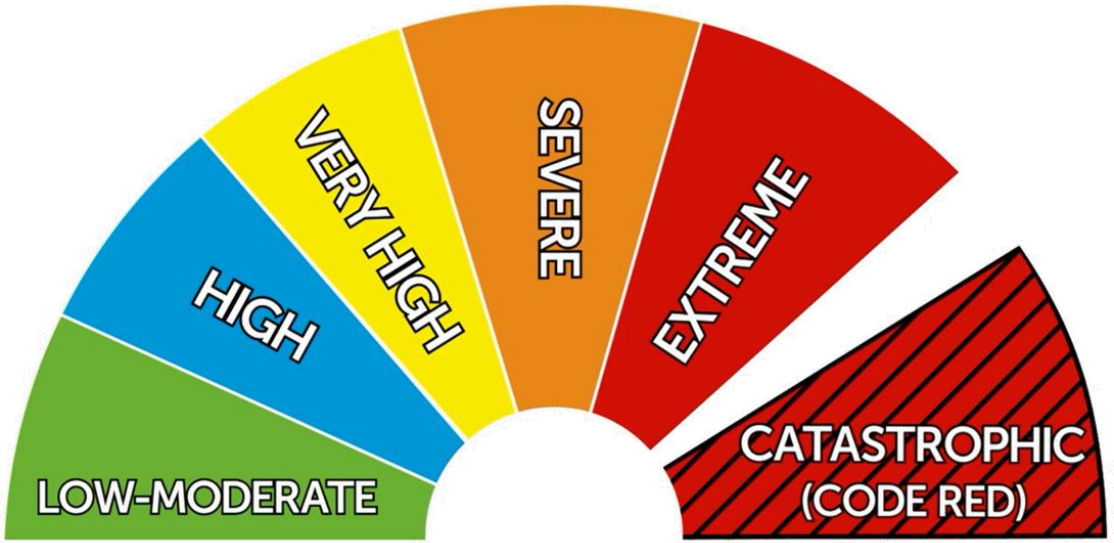
Catastrophe Scale



Catastrophe Scale



- One isolated user affected
- One user infected, but issue is propagating over the network
- Loss of Integrity of Workstation Fleet, but operational
- Total loss of control of Workstation Fleet, not operational (encrypted, ransom)
- [sort of like Corona Virus situation now…..]


LOW-MODERATE
HIGH
VERY HIGH
SEVERE
EXTREME
CATASTROPHIC
(CODE RED)


EXCUSE ME
WHILE I TAKE A SIP
FROM THIS BIG CUP OF
I TOLD
YOU SO

SUMMARY

- Understand your Supply Chain Risks (S/W and Services)
- Incorporate Static & Dynamic Tests – Upfront & Ongoing
- Validation of Effectiveness of Hardening
- Validation of Effectiveness of End Point Control
- Fault Condition Injection
- Introduce Continuous Monitoring/Validation (across wide attributes)
- Incorporate into Vuln Mgt Program

Apply What You Have Learned Today

- Next week you should:
  - Identify where your SOE/Rollout Security Strategy is
    - Already rolled out? Not too late.
      - Gap assessment of the coverage of the testing vs what we learned today
    - Planning a rollout?
      - Consider the assessments from all the angles.
    - Budgeting?
      - Look at the Catastrophe scale and determine your risk appetite?
    - 3rd Parties
      - Identify the extent to which you rely on 3rd Parties to secure your deployments

Apply What You Have Learned Today

- In the first three months following this presentation you should:
  - Develop & Execute Assessment Plan (all the methods described here)
  - Understand the relationship between configuration (static) and actual operation (dynamic)
  - Build resilience into your OS's at all the layers
  - Automate hardening validation & Implement Continuous Monitoring to identify Configuration Drift

Apply What You Have Learned Today

- Within six months you should:
  - Improve the overall security of the OS and the ecosystem
  - Manage 3rd party risk
  - Implement Continuous Monitoring to identify sleeper malware
  - Run Time Security Testing: Enter Purple Teaming, SOC, NOC, Validation
- Beyond:
  - Automate Testing to demonstrate current state without the need to conduct intensive manual tests

Questions

A CyberCX company

Cyber Security + Customer Experience

Murray Goldschmidt
Chief Operating Officer
murrayg@senseofsecurity.com.au
Office: +61 2 9290 4444
Mob: +61 422 978 311