SANS @ Night

To download and follow along with this presentation, you can retrieve it from:

https://mjhedu.github.io/SANSMpls2019/

HTML

PDF

The QR Code 2D Symbols are links to GitHub; promise, I wouldn't prank you in a classroom.

SANS @ Night

Boring Solutions

Tuesday, 13 August 2019
7:15pm - 8:15pm

Matthew J. Harmon
GSEC, GCIH, GCIA, CISSP
@mjharmon

Stick around after for

Infosec Rock Star: Accelerate Your Career By Building FIVE Critical Professional Skills

with

Ted Demopoulos

8:15pm - 9:15pm

@teddemop

Matthew J. Harmon

Hello everyone, my name is Matthew J. Harmon. I was recently asked by a friend of mine "Why do you teach? What is this teaching thing?" as I had mentioned that I am studying towards my Master of Education and Advanced Teaching.

In response, I gave my stump answer of "I love seeing the lightbulb turn on above my students as they grasp a new concept" and "it's a backup in case everything goes pear shaped" *(I do love pears)* followed by how one of my students explained to me that my teaching method forced them to learn complex concepts quickly

Chloe Anthony Wofford "Toni" Morrison

However, it goes deeper than that and few people put the power of Education better than Toni Morrison, who recently passed away, on **August 5th, 2019 at the age of 88, after a lifetime of achievements -** she said: "I tell my students, 'When you get these jobs that you have been so brilliantly trained for, just remember that your real job is that if you are free, you need to free somebody else.' If you have some power, then your job is to empower somebody else."

Receiving the Presidential Medal of Freedom

What are we going to cover tonight?

Most organizations are using the "shovel money at the security problem" approach. Tonight we'll discuss alternatives.

To start, if you can rebuild I.T., do it.

Before we talk about some Boring Solutions that can improve your security posture, I do have one not-boring thing that I think people need to hear. Everything reaches a point where it is more costly to address the maintenance debt in a high friction environment, then it is to burn it all to the ground and rebuild. So, if you have the opportunity (and of course management and peer buy-in) to burn it all to the ground and rebuild programmatically - **PLAN IT, TEST IT, DO IT!**

20 Critical Security Controls

(these are the first 10 we'll talk about today)

CSC 1: Inventory and Control of Hardware Assets
CSC 2: Inventory and Control of Software Assets
CSC 3: Continuous Vulnerability Management
CSC 4: Controlled Use of Administrative Privileges
CSC 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
CSC 6: Maintenance, Monitoring and Analysis of Audit Logs
CSC 7: Email and Web Browser Protections
CSC 8: Malware Defenses
CSC 9: Limitation and Control of Network Ports, Protocols, and Services
CSC 10: Data Recovery Capabilities

CIS Controls™

http://www.cisecurity.org/controls/

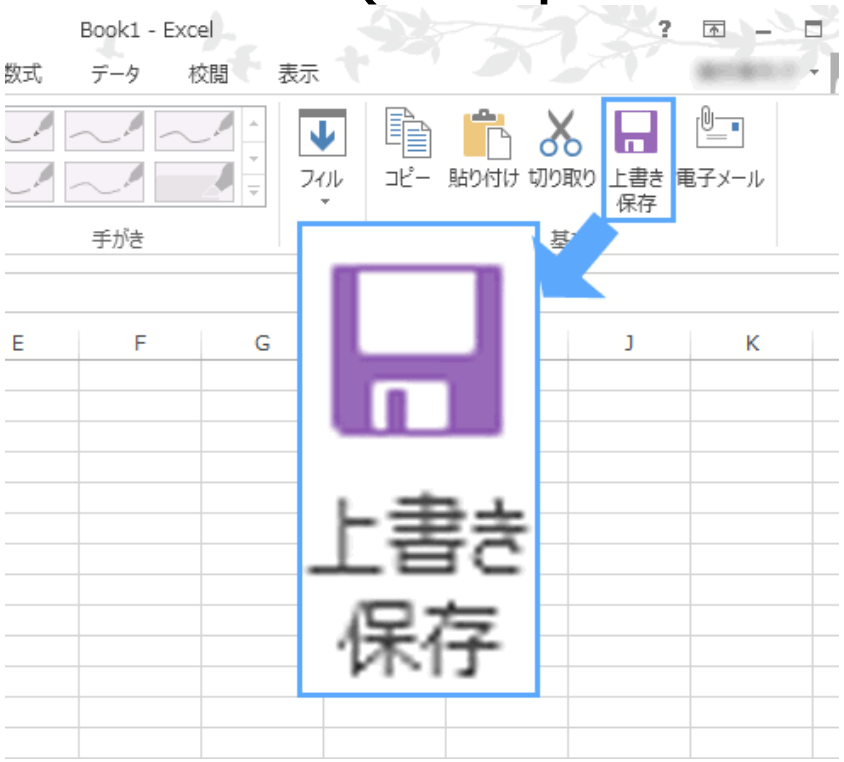
V7

BUT HOW!?

HOW DO WE DO IT!?

Perspective

Why is the "Save" button on MS Excel represented by the picture of vending machine? (with purchased drink at the bottom)



Nobi Hayashi 林信行 @nobi on Twitter

Turn the control into a question.

CSC 1: Inventory and Control of Hardware Assets

Rephrasing this control it easily becomes
"What things are under my control?"

What things are under my control?

CSC 1: Inventory and Control of Hardware Assets

Inventory and Control of Hardware Assets **Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.**	
Utilize an Active Discovery Tool	Utilize an active discovery tool to identify devices connected to the organization's network and update the hardware asset inventory.
Use a Passive Asset Discovery Tool	Utilize a passive discovery tool to identify devices connected to the organization's network and automatically update the organization's hardware asset inventory.
Use DHCP Logging to Update Asset Inventory	Use Dynamic Host Configuration Protocol (DHCP) logging on all DHCP servers or IP address management tools to update the organization's hardware asset inventory.
Maintain Detailed Asset Inventory	Maintain an accurate and up-to-date inventory of all technology assets with the potential to store or process information. This inventory shall include all hardware assets, whether connected to the organization's network or not.
Maintain Asset Inventory Information	Ensure that the hardware asset inventory records the network address, hardware address, machine name, data asset owner, and department for each asset and whether the hardware asset has been approved to connect to the network.
Address Unauthorized Assets	Ensure that unauthorized assets are either removed from the network, quarantined, or the inventory is updated in a timely manner.
Deploy Port Level Access Control	Utilize port level access control, following 802.1x standards, to control which devices can authenticate to the network. The authentication system shall be tied into the hardware asset inventory data to ensure only authorized devices can connect to the network.
Utilize Client Certificates to Authenticate Hardware Assets	Use client certificates to authenticate hardware assets connecting to the organization's trusted network.

http://www.cisecurity.org/controls/

What things are under my control?

CSC 1: Inventory and Control of Hardware Assets

Automate an inventory audit of everything on the network under your control, in AWS, Azure, any VPS provider and run it weekly.

Get the purchasing department on board to routinely give you a couple of years of hardware purchased and match it against your inventory.

Those tiny EC2 instances, Raspberry Pi's and employee phones which are connected to the company WiFi? Enumerate each one of these into a source of truth repository that you and others can reference.

What things are under my control?

CSC 1: Inventory and Control of Hardware Assets

Start simple, request a CSV export from your purchasing vendor and an internal list from your purchasing department. Match those records up against what you gather from in the ARP tables on your WiFi access points and network switches.

Configuration management tools such as Ansible and SaltStack have integrated NAPALM (Network Automation and Programmability Abstraction Layer with Multivendor support) to gather facts. They can return to you some well-formatted JSON output ready to be compared to your records.

What things are under my control?

CSC 1: Inventory and Control of Hardware Assets

More aggressively, you can analyze your local network with tools such as Nmap with Wireshark or tcpdump running. After that, piece together your spreadsheets based on a device serial number and MAC address.

Alternatively, you can run a passive discovery tool, such as tcpdump running on a SPAN or mirror port on a switch feeding into the Passive Network Audit Framework (PNAF). This tool unites others such as p0f and prads and a wide range of other tools.

Let's do it again.

CSC 2: Inventory and Control of Software Assets

"What is running on those things?"

What software is running on those things?

CSC 2: Inventory and Control of Software Assets

Inventory and Control of Software Assets **Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.**	
Maintain Inventory of Authorized Software	Maintain an up-to-date list of all authorized software that is required in the enterprise for any business purpose on any business system.
Ensure Software is Supported by Vendor	Ensure that only software applications or operating systems currently supported and receiving vendor updates are added to the organization's authorized software inventory. Unsupported software should be tagged as unsupported in the inventory system.
Utilize Software Inventory Tools	Utilize software inventory tools throughout the organization to automate the documentation of all software on business systems.
Track Software Inventory Information	The software inventory system should track the name, version, publisher, and install date for all software, including operating systems authorized by the organization.
Integrate Software and Hardware Asset Inventories	The software inventory system should be tied into the hardware asset inventory so all devices and associated software are tracked from a single location.
Address unapproved software	Ensure that unauthorized software is either removed or the inventory is updated in a timely manner
Utilize Application Whitelisting	Utilize application whitelisting technology on all assets to ensure that only authorized software executes and all unauthorized software is blocked from executing on assets.
Physically or Logically Segregate High Risk Applications	Physically or logically segregated systems should be used to isolate and run software that is required for business operations but incurs higher risk for the organization.

http://www.cisecurity.org/controls/

What software is running on those things?

CSC 2: Inventory and Control of Software Assets

Windows:

```
# Search registry for program based on Uninstaller records
Create-Item $tmpFile
$loc = Get-ChildItem HKLM:\Software\Microsoft\Windows\CurrentVersion\Uninstall
$names = $loc |foreach-object {Get-ItemProperty $_.PsPath}
foreach ($name in $names)
{
    IF(-Not [string]::IsNullOrEmpty($name.DisplayName)) {
        $line = $name.DisplayName+$separator+$name.DisplayVersion+
$separator+$name.InstallDate
        Write-Host $line
        Add-Content $tmpFile "$line`n"
    }
}
```

Credit Arivan Bastos

What software is running on those things?

CSC 2: Inventory and Control of Software Assets

OpenBSD

```
$ pkg_info
```

MacOS X

```
$ system_profiler SPApplicationsDataType
$ lsappinfo
```

Alpine

```
$ apk info
```

Debian

```
$ dpkg --get-selections
$ apt list –installed
```

RedHat/CentOS

```
$ yum list installed
$ rpm -qa
```

Gentoo

```
$ equery list “*”
$ cat /var/lib/portage/world
```

Are those things exploitable?

CSC 3: Continuous Vulnerability Management

Continuous Vulnerability Management **Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.**	
Run Automated Vulnerability Scanning Tools	Utilize an up-to-date Security Content Automation Protocol (SCAP) compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.
Perform Authenticated Vulnerability Scanning	Perform authenticated vulnerability scanning with agents running locally on each system or with remote scanners that are configured with elevated rights on the system being tested.
Protect Dedicated Assessment Accounts	Use a dedicated account for authenticated vulnerability scans, which should not be used for any other administrative activities and should be tied to specific machines at specific IP addresses.
Deploy Automated Operating System Patch Management Tools	Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.
Deploy Automated Software Patch Management Tools	Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.
Compare Back-to-Back Vulnerability Scans	Regularly compare the results from consecutive vulnerability scans to verify that vulnerabilities have been remediated in a timely manner.
Utilize a Risk-Rating Process	Utilize a risk-rating process to prioritize the remediation of discovered vulnerabilities.

http://www.cisecurity.org/controls/

Who *really* needs admin rights?

CSC 4: Controlled Use of Administrative Privileges

Controlled Use of Administrative Privileges **The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.**	
Maintain Inventory of Administrative Accounts	Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.
Change Default Passwords	Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts.
Ensure the Use of Dedicated Administrative Accounts	Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.
Use Unique Passwords	Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.
Use Multi-Factor Authentication for All Administrative Access	Use multi-factor authentication and encrypted channels for all administrative account access.
Use Dedicated Workstations For All	Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading e-mail, composing documents, or browsing the Internet.
Limit Access to Script Tools	**Limit access to scripting tools (such as Microsoft® PowerShell and Python) to only administrative or development users with the need to access those capabilities.**
Log and Alert on Unsuccessful Administrative Account Login	Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.

http://www.cisecurity.org/controls/

Limit access to Script Tools

CSC 4: Controlled Use of Administrative Privileges

Binary	Functions	Type
Atbroker.exe	Execute	Binaries
Bash.exe	Execute, AWL bypass	Binaries
Bitsadmin.exe	Alternate data streams, Download, Copy, Execute	Binaries
Certutil.exe	Download, Alternate data streams, Encode, Decode	Binaries
Cmd.exe	Alternate data streams	Binaries
Cmdkey.exe	Credentials	Binaries
Cmstp.exe	Execute, AWL bypass	Binaries
Control.exe	Alternate data streams	Binaries
Csc.exe	Compile	Binaries
Cscript.exe	Alternate data streams	Binaries
Dfsvc.exe	AWL bypass	Binaries
Diskshadow.exe	Dump, Execute	Binaries
Dnscmd.exe	Execute	Binaries

Credit to LOLBAS Living Off The Land Binaries And Scripts - (LOLBins and LOLScripts)

How is this thing configured?

CSC 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers **Establish, implement, and actively manage (track, report on, correct) the security configuration of mobile devices, laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.**	
Establish Secure Configurations	Maintain documented security configuration standards for all authorized operating systems and software.
Maintain Secure Images	Maintain secure images or templates for all systems in the enterprise based on the organization's approved configuration standards. Any new system deployment or existing system that becomes compromised should be imaged using one of those images or templates.
Securely Store Master Images	Store the master images and templates on securely configured servers, validated with integrity monitoring tools, to ensure that only authorized changes to the images are possible.
Deploy System Configuration Management Tools	Deploy system configuration management tools that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals.
Implement Automated Configuration Monitoring Systems	Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.

http://www.cisecurity.org/controls/

What is this thing doing?

CSC 6: Maintenance, Monitoring and Analysis of Audit Logs

Maintenance, Monitoring and Analysis of Audit Logs **Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.**	
Utilize Three Synchronized Time Sources	Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.
Activate Audit Logging	Ensure that local logging has been enabled on all systems and networking devices.
Enable Detailed Logging	Enable system logging to include detailed information such as a event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.
Ensure Adequate Storage for Logs	Ensure that all systems that store logs have adequate storage space for the logs generated.
Central Log Management	Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.
Deploy SIEM or Log Analytic Tools	Deploy Security Information and Event Management (SIEM) or log analytic tool for log correlation and analysis.
Regularly Review Logs	On a regular basis, review logs to identify anomalies or abnormal events.
Regularly Tune SIEM	On a regular basis, tune your SIEM system to better identify actionable events and decrease event noise.

http://www.cisecurity.org/controls/

Defending against direct download damage

CSC 7: Email and Web Browser Protections

Email and Web Browser Protections **Minimize the attack surface and the opportunities for attackers to manipulate human behavior though their interaction with web browsers and email systems.**	
Ensure Use of Only Fully Supported Browsers and Email Clients	Ensure that only fully supported web browsers and email clients are allowed to execute in the organization, ideally only using the latest version of the browsers and email clients provided by the vendor.
Disable Unnecessary or Unauthorized Browser or Email Client Plugins	Uninstall or disable any unauthorized browser or email client plugins or add-on applications.
Limit Use of Scripting Languages in Web Browsers and Email Clients	Ensure that only authorized scripting languages are able to run in all web browsers and email clients.
Maintain and Enforce Network-Based URL Filters	Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.
Subscribe to URL-Categorization Service	Subscribe to URL-categorization services to ensure that they are up-to-date with the most recent website category definitions available. Uncategorized sites shall be blocked by default.
Log All URL requester	Log all URL requests from each of the organization's systems, whether on-site or a mobile device, in order to identify potentially malicious activity and assist incident handlers with identifying potentially compromised systems.
Use of DNS Filtering Services	Use Domain Name System (DNS) filtering services to help block access to known malicious domains.
Implement DMARC and Enable Receiver-Side Verification	To lower the chance of spoofed or modified emails from valid domains, implement Domain-based Message Authentication, Reporting and Conformance (DMARC) policy and verification, starting by implementing the Sender Policy Framework (SPF) and the DomainKeys Identified Mail(DKIM) standards.

http://www.cisecurity.org/controls/

Defending against badness

CSC 8: Malware Defenses

Malware Defenses **Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action.**	
Utilize Centrally Managed Anti-malware Software	Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.
Ensure Anti-Malware Software and Signatures Are Updated	Ensure that the organization's anti-malware software updates its scanning engine and signature database on a regular basis.
Enable Operating System Anti-Exploitation Features/Deploy Anti-Exploit Technologies	Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.
Configure Anti-Malware Scanning of Removable Devices	Configure devices so that they automatically conduct an anti-malware scan of removable media when inserted or connected.
Configure Devices to Not Auto-Run Content	Configure devices to not auto-run content from removable media.
Enable DNS Query Logging	Enable Domain Name System (DNS) query logging to detect hostname lookups for known malicious domains.
Enable Command-Line Audit Logging	Enable command-line audit logging for command shells, such as Microsoft PowerShell and Bash.

http://www.cisecurity.org/controls/

What is the profile of running services?

CSC 9: Limitation and Control of Network Ports, Protocols, and Services

Limitation and Control of Network Ports, Protocols, and Services **Manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.**	
Associate Active Ports, Services, and Protocols to Asset Inventory	Associate active ports, services, and protocols to the hardware assets in the asset inventory.
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.
Perform Regular Automated Port Scans	Perform automated port scans on a regular basis against all systems and alert if unauthorized ports are detected on a system.
Apply Host-Based Firewalls or Port-Filtering	Apply host-based firewalls or port-filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.
Implement Application Firewalls	Place application firewalls in front of any critical servers to verify and validate the traffic going to the server. Any unauthorized traffic should be blocked and logged.

http://www.cisecurity.org/controls/

Turn the control into a question.

CSC 9: Limitation and Control of Network Ports, Protocols, and Services

If we just turn off all of the ports, it is secure - no one can access it - right?

No... no no no no…

If I know the common source and destination IPs and ports for this service I can filter accordingly and detect anomalies

That's a BINGO! YES!

How can we quickly recover?

CSC 10: Data Recovery Capabilities

Data Recovery Capabilities **The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.**	
Ensure Regular Automated BackUps	Ensure that all system data is automatically backed up on a regular basis.
Perform Complete System Backups	Ensure that all of the organization's key systems are backed up as a complete system, through processes such as imaging, to enable the quick recovery of an entire system.
Test Data on Backup Media	
Protect Backups	Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services.
Ensure All Backups Have at Least One Offline Backup Destination	Ensure that all backups have at least one offline (i.e., not accessible via a network connection) backup destination.

http://www.cisecurity.org/controls/

What Boring Solutions we discussed today.

Focused on Implementing Critical Security Controls 1-10

We started with knowing what is in our environment, progressed to discover what it is installed, how it is configured, and what it is doing.

We then looked at the unique challenges of protecting email and browsers, we explored malware defenses, profiling the data flow and ports used by systems, and looked at recovery methods.

Events

Cyber Security Summit

October 28-30, 2019

https://cybersecuritysummit.org/

Thank you!

mjh@itys.net

https://mjhedu.github.io/

Sources, References & Credits

i) Good Omens: The Nice and Accurate Prophecies of Agnes Nutter, Witch (1990)

ii) QR Codes by Terry Burton's Barcode Writer in Pure PostScript project

   i) https://bwipp.terryburton.co.uk/

iii) Toni Morrison

   i) https://www.tonimorrisonfilm.com/

iv) Center for Internet Security

   i) This work is licensed under a Creative Commons Attribution-Non Commercial-No Derivatives 4.0 International Public License (the link can be found at https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode

   ii) To further clarify the Creative Commons license related to the CIS Controls™ content, you are authorized to copy and redistribute the content as a framework for use by you, within your organization and outside of your organization for non-commercial purposes only, provided that (i) appropriate credit is given to CIS, and (ii) a link to the license is provided. Additionally, if you remix, transform or build upon the CIS Controls, you may not distribute the modified materials. Users of the CIS Controls framework are also required to refer to (http://www.cisecurity.org/controls/) when referring to the CIS Controls in order to ensure that users are employing the most up-to-date guidance. Commercial use of the CIS Controls is subject to the prior approval of CIS® (Center for Internet Security, Inc.).

v) Nobi Hayashi 林信行 @nobi on Twitter

Sources, References & Credits

vi) Disaster Girl

- i) David Roth's daughter Zoe (January 2004)

vii) Springfield Tire Fire

- i) From "The Simpsons" owned by 20th Century Fox (Walt Disney Company), created by Matt Groening, originally from The Tracey Ullman Show.

viii) Ansible Network Automation with NAPALM

- i) https://github.com/napalm-automation/napalm-ansible

ix) SaltStack

- i) https://www.saltstack.com/

x) NAPALM

- i) https://github.com/napalm-automation/napalm

xi) p0f

- i) https://github.com/skord/p0f

xii) PRADS

- i) https://gamelinux.github.io/prads/
- ii) https://github.com/gamelinux/prads