A Gentle, Caring Intro To Security

John Strand

Big Thanks!!

LEVEL UP

The MSP Security Training Challenge

Presented by

The Cyber Call

Mission: Raise the collective security posture across the channel.

Our challenge for ourselves: Help 500 MSPs get training in 30 Days.

The channel needs more security practitioners.

That's why we've teamed up with vendors across the channel who are passionate about security to make some of the industry's best training more accessible and affordable.

Our Sponsors

Each one of our sponsors has contributed funds to help secure the course discount and tuition assistance for those needing financial help. In addition, they each will be providing free seats in the course to help us hit our goal of providing the training to as many MSPs as possible.

blackpoint

ninja RMM

datto

CISCO

ConnectWise

HUNTRESS

pax8

SKOUT CYBERSECURITY

SOPHOS

THREATLOCKER

TruMethods A Kaseya COMPANY

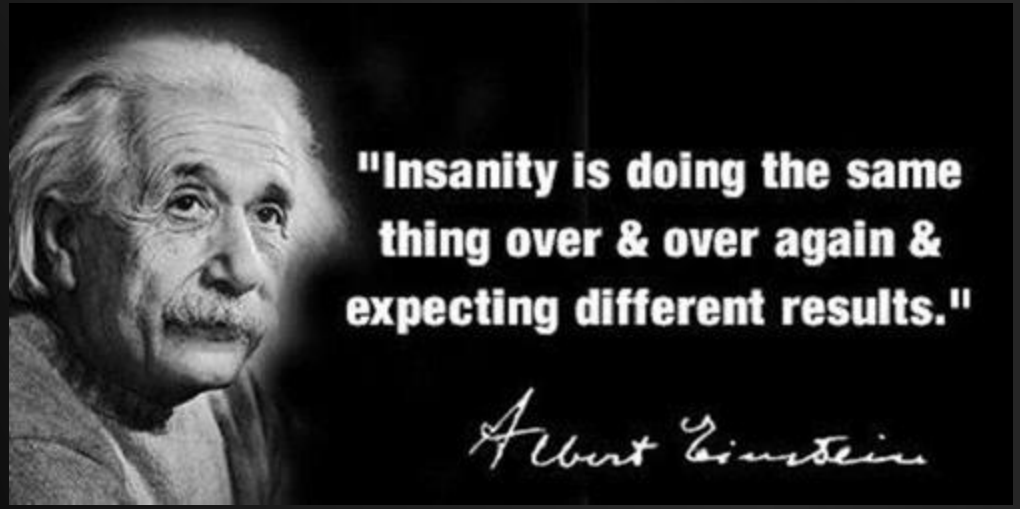
What Is This?

- This is meant to be a “bootstrap” security class
- We are going to cover what works to defend a network
- We are going to cover the things that BHIS loves/hates to see in a customer network
- We are going to cover 11 topics

What Works

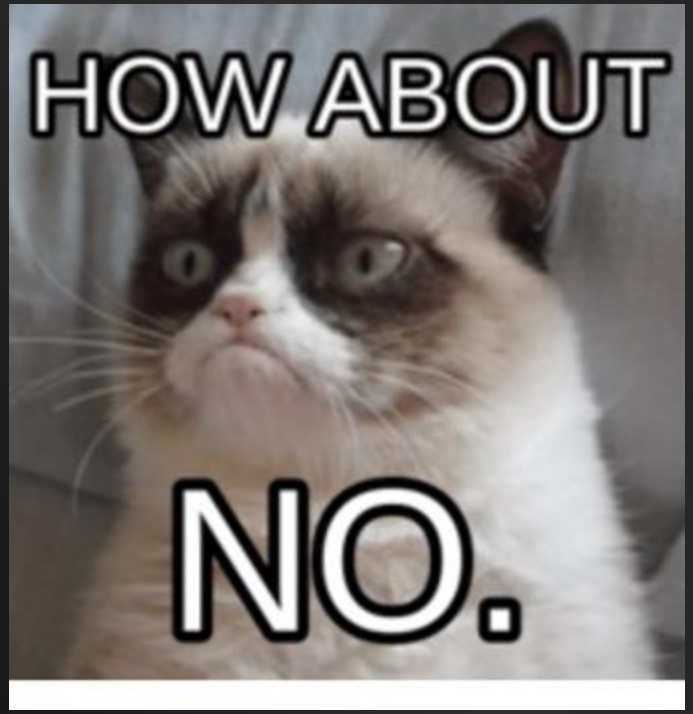
Key Tracking Indicators == Atomic Controls

- Mapping MITRE to Critical Controls we see trends:
  - Application Allow Listing
  - Password Controls
  - Egress Traffic Analysis
  - UEBA
  - Advanced Endpoint Protection
  - Logging
  - Host Firewalls
  - Internet Allow Listing
  - Vulnerability Management
  - Active Directory Hardening
  - Backup and Recovery



What We Are Not Covering

- Intro to Windows
- Intro to Linux
- Intro to TCP/IP
- Intro to Crypto
- Intro to Security Models
- The CBK
- NIST 800 series
- DLP
- Exploit of the day!



Implementing CIS as an MSP

Right of Boom

https://www.cisecurity.org/controls/cis-controls-navigator/?version=8

What do you have?

- You probably have a lot of things in place now
- Backups, Endpoint Protection, Logs, Firewalls, etc.
- Find your gaps
- Then, map to CIS
- Sounds hard… Pretty easy with AuditScripts
- Set different price tiers

Tracking

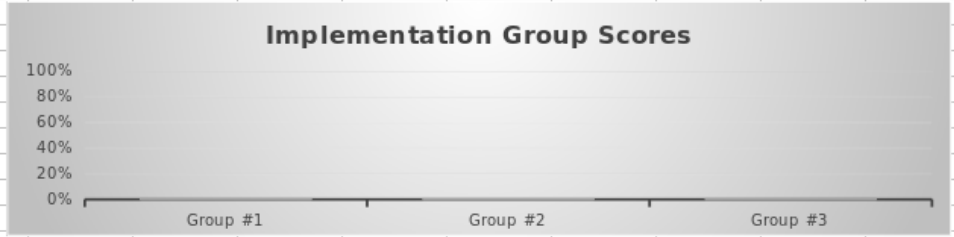
AuditScripts

CIS Controls Initial Assessment Tool (v8.0a)

enclave SECURITY

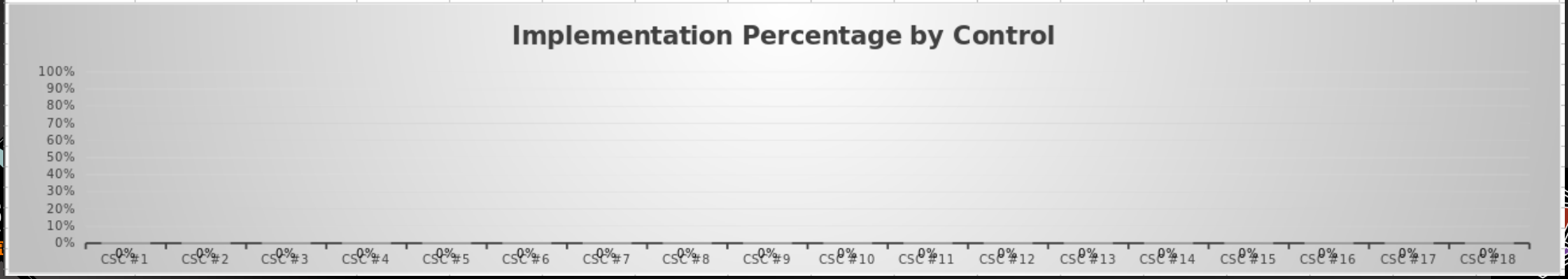
ATT&CK Activity	Preventive Capability	Detective Capability
Initial Access	Low	Low
Execution	Low	Low
Persistence	Low	Low
Privilege Escalation	Low	Low
Defense Evasion	Low	Low
Credential Access	Low	Low
Discovery	Low	Low
Lateral Movement	Low	Low
Collection	Low	Low
Command and Control	Low	Low
Exfiltration	Low	Low

Implementation Group Scores					
Group #1	0%	Group #2	0%	Group #3	0%



Maturity level:	Description:	Score:
Level One	Policies Complete	0.00
Level Two	Controls 1-5 Implemented	0.00
Level Three	All Controls Implemented	0.00
Level Four	All Controls Automated	0.00
Level Five	All Controls Reported	0.00
	Maturity Rating*:	0.00

*Rating is on a 0-5 scale.



BLACK HILLS Information Security CELEBRATING 10 YEARS •2008-2018•

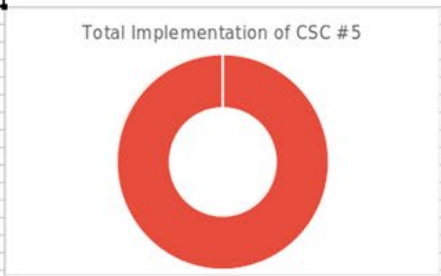
Backdoors & Breaches

Tracking

AuditScripts

CIS Control #5: Account Management

enclave SECURITY



Risk Addressed:	0%
Risk Accepted:	100%

ID	CIS Control Detail	NIST CSF	Implementation Groups	Sensor or Baseline	Policy Defined	Control Implemented	Control Automated or Technically Enforced	Control Reported to Business
5.1	Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.	Identify	1,2,3	Identity Management System	No Policy	Not Implemented	Not Applicable	Not Applicable
5.2	Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	Protect	1,2,3	Privileged Account Management System	No Policy	Not Implemented	Not Automated	Not Reported
5.3	Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported.	Respond	1,2,3	Identity Management System	No Policy	Not Implemented	Not Automated	Not Reported
5.4	Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.	Protect	1,2,3	Privileged Account Management System	No Policy	Not Implemented	Not Automated	Not Reported
5.5	Establish and maintain an inventory of service accounts. The inventory, at a minimum, must contain department owner, review date, and purpose. Perform service account reviews to validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.	Identify	2,3	Privileged Account Management System	No Policy	Not Implemented	Not Applicable	Not Applicable
5.6	Centralize account management through a directory or identity service.	Protect	2,3	Identity Management System	No Policy	Not Implemented	Not Automated	Not Reported

Mapping

AuditScripts — CIS Controls Master Mappings Tool (v7.1c) — enclave SECURITY

Critical Security Control	NIST 800-53 rev4	NIST CSF v1.0	NIST CSF v1.1	NIST 800-82 rev2
Critical Security Control #10: Data Recovery Capabilities	CP-9: Information System Backup CP-10: Information System Recovery and Reconstitution MP-4: Media Storage	PR.IP-4	PR.IP-4	6.2.16 6.2.17
Critical Security Control #11: Secure Configuration for Network Devices, such as Firewalls, Routers and Switches	AC-4: Information Flow Enforcement CA-3: System Interconnections CA-7: Continuous Monitoring CA-9: Internal System Connections CM-2: Baseline Configuration CM-3: Configuration Change Control CM-5: Access Restrictions for Change CM-6: Configuration Settings CM-8: Information System Component Inventory MA-4: Nonlocal Maintenance SC-24: Fail in Known State SI-4: Information System Monitoring	PR.AC-5 PR.IP-1 PR.PT-4	PR.AC-5 PR.IP-1 PR.PT-4	5.15 6.2.7
Critical Security Control #12: Boundary Defense	AC-4: Information Flow Enforcement AC-17: Remote Access AC-20: Use of External Information Systems CA-3: System Interconnections CA-7: Continuous Monitoring CA-9: Internal System Connections CM-2: Baseline Configuration SA-9: External Information System Services SC-7: Boundary Protection SC-8: Transmission Confidentiality and Integrity SI-4: Information System Monitoring	PR.AC-3 PR.AC-5 PR.MA-2 DE.AE-1	PR.AC-3 PR.AC-5 PR.MA-2 DE.AE-1	5.1 - 5.11
Critical Security Control #13: Data Protection	AC-3: Access Enforcement AC-4: Information Flow Enforcement AC-23: Data Mining Protection CA-7: Continuous Monitoring CA-9: Internal System Connections IR-9: Information Spillage Response MP-5: Media Transport SA-18: Tamper Resistance and Detection SC-8: Transmission Confidentiality and Integrity SC-28: Protection of Information at Rest SC-31: Covert Channel Analysis SC-41: Port and I/O Device Access SI-4: Information System Monitoring	PR.AC-5 PR.DS-2 PR.DS-5 PR.PT-2	PR.AC-5 PR.DS-2 PR.DS-5 PR.PT-2	
Critical Security Control #14: Controlled Access Based on the Need to Know	AC-1: Access Control Policy and Procedures AC-2: Account Management AC-3: Access Enforcement AC-6: Least Privilege AC-24: Access Control Decisions CA-7: Continuous Monitoring	PR.AC-4 PR.AC-5 PR.DS-1 PR.DS-2	PR.AC-4 PR.AC-5 PR.DS-1 PR.DS-2	5.1 5.4 5.5

Compliance and the Critical Controls

Why We Are Covering What We Are Covering

- We started tracking vulnerabilities in our pentests
- Over 650+ per year
- We started tracking what would have stopped us
- This is a class based on what works
- Kind of took a bit of unlearning
- We are also tying this to MITRE
- Because everything has to tie to MITRE
- By Law….

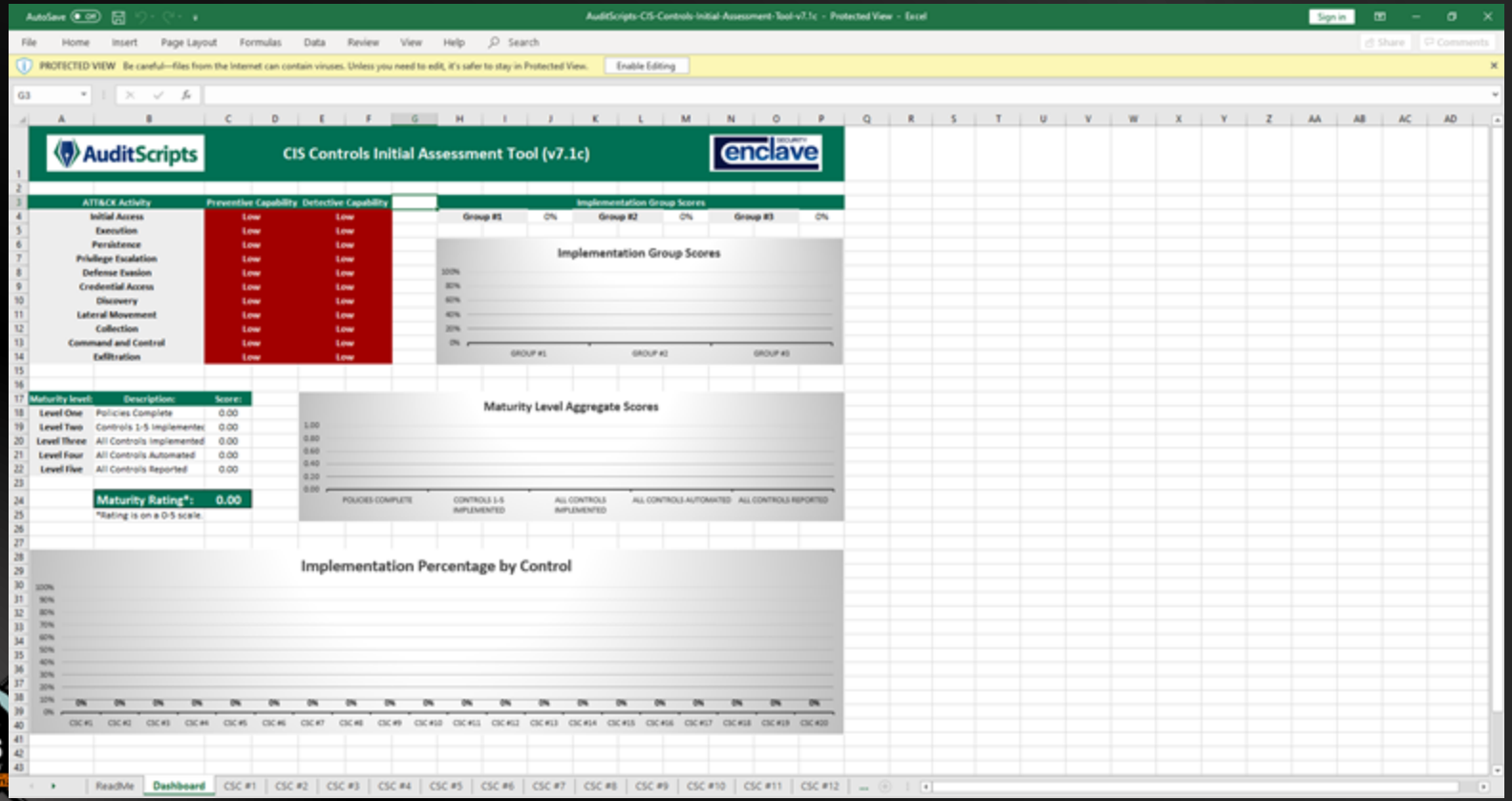
Compliance Issues

- Far too many frameworks
- Overlapping and conflicting recommendations
- Recommendations get out of date quickly
- NIST Greenbook
- PCI Min Password length
- Meeting the Minimum

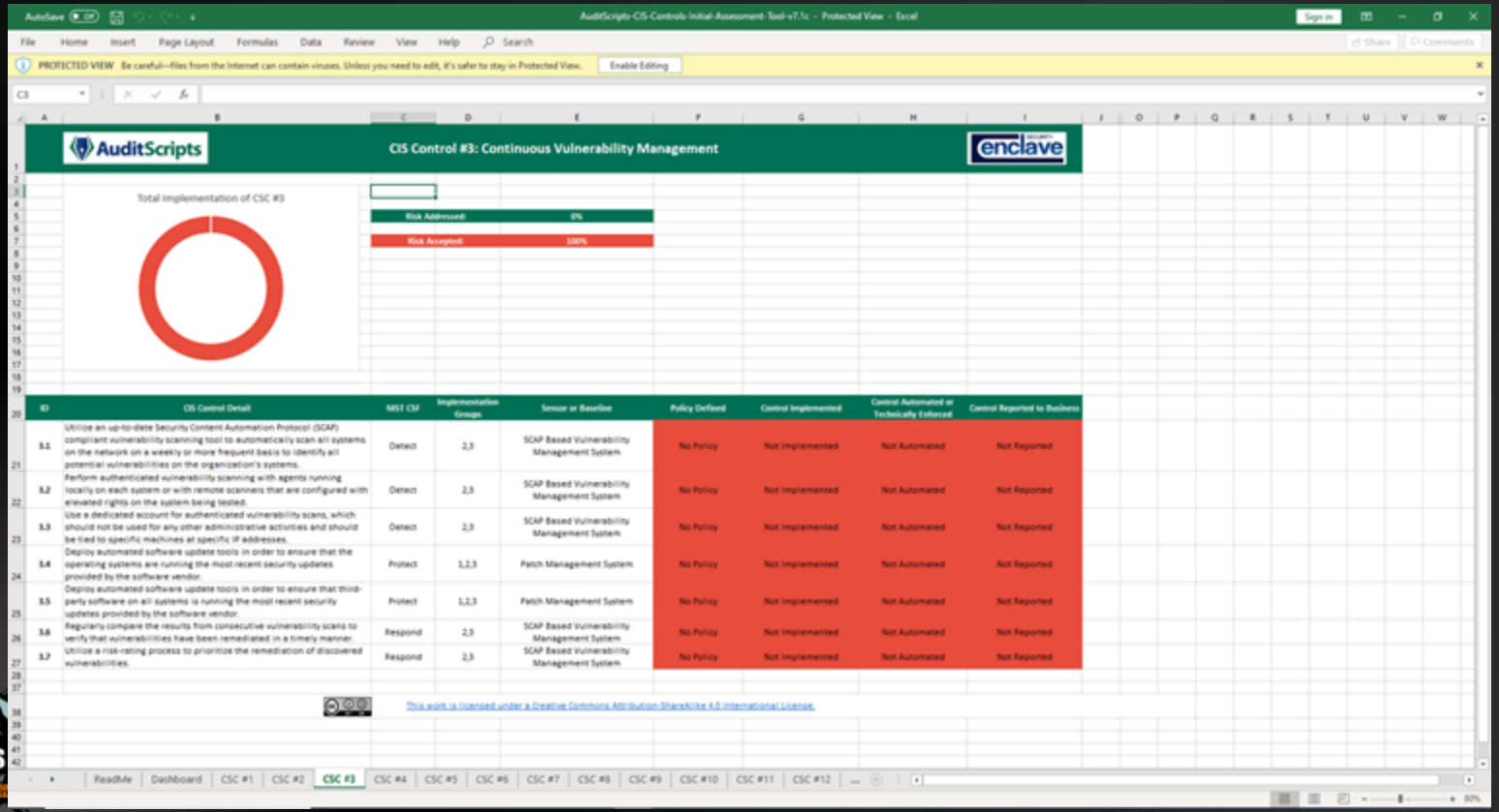
AuditScripts Spreadsheets

- Create a smaller framework set
- Create a framework based on actual attacks and things that matter
- Create a cross-reference to other frameworks
- Differing levels of compliance
- Dynamic Meant to be updated regularly
- History and Future
- Heavy lifting by James and Kellie Tarala
- https://www.auditscripts.com/free-resources/critical-security-controls/

AuditScripts Spreadsheets



AuditScripts Spreadsheets



ID	CIS Control Detail	NIST CSF	Implementation Groups	Sensor or Baseline	Policy Defined	Control Implemented	Control Automated or Technically Enforced	Control Reported to Business
3.1	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.	Detect	2,3	SCAP Based Vulnerability Management System	No Policy	Not Implemented	Not Automated	Not Reported
3.2	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.	Detect	2,3	SCAP Based Vulnerability Management System	No Policy	Not Implemented	Not Automated	Not Reported
3.3	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.	Detect	2,3	SCAP Based Vulnerability Management System	No Policy	Not Implemented	Not Automated	Not Reported
3.4	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.	Protect	1,2,3	Patch Management System	No Policy	Not Implemented	Not Automated	Not Reported
3.5	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.	Protect	1,2,3	Patch Management System	No Policy	Not Implemented	Not Automated	Not Reported
3.6	Regularly compare the results from consecutive vulnerability scans to verify that vulnerabilities have been remediated in a timely manner.	Respond	2,3	SCAP Based Vulnerability Management System	No Policy	Not Implemented	Not Automated	Not Reported
3.7	Utilize a risk-rating process to prioritize the remediation of discovered vulnerabilities.	Respond	2,3	SCAP Based Vulnerability Management System	No Policy	Not Implemented	Not Automated	Not Reported

BLACK HILLS Information Security

AuditScripts Spreadsheets

AuditScripts-CIS-Controls-Master-Mappings-v7.1c - Protected View - Excel

PROTECTED VIEW Be careful—files from the Internet can contain viruses. Unless you need to edit, it's safer to stay in Protected View. Enable Editing

AuditScripts | CIS Controls Master Mappings Tool (v7.1c) | enclave

Critical Security Control	NIST 800-53 rev4	NIST CSF v1.0	NIST CSF v1.1	NIST 800-82 rev2	NIST SMB Guide	DHS CDM Program	ISO 2700
Critical Security Control #1: Inventory of Authorized and Unauthorized Devices	CA-7: Continuous Monitoring CM-8: Information System Component Inventory IA-3: Device Identification and Authentication SA-4: Acquisition Process SC-17: Public Key Infrastructure Certificates SI-4: Information System Monitoring PM-5: Information System Inventory	ID.AM-1 ID.AM-3 ID.AM-4 PR.DS-3	ID.AM-1 ID.AM-3 ID.AM-4 PR.DS-3	6.2.16 6.2.17	4.0d	HWAM: Hardware Asset Management	A.8.1 A.9.1 A.15.1
Critical Security Control #2: Inventory of Authorized and Unauthorized Software	CA-7: Continuous Monitoring CM-2: Baseline Configuration CM-8: Information System Component Inventory CM-10: Software Usage Restrictions CM-11: User-Installed Software SA-4: Acquisition Process SC-18: Mobile Code SC-34: Non-Modifiable Executable Programs SI-4: Information System Monitoring PM-5: Information System Inventory	ID.AM-2 PR.DS-6	ID.AM-2 PR.DS-6	6.2.16 6.2.17		HWAM: Hardware Asset Management SWAM: Software Asset Management	A.12.5 A.12.6
Critical Security Control #3: Continuous Vulnerability Assessment and Remediation	CA-2: Security Assessments CA-7: Continuous Monitoring RA-5: Vulnerability Scanning SC-34: Non-Modifiable Executable Programs SI-4: Information System Monitoring SI-7: Software, Firmware, and Information Integrity	ID.RA-1 ID.RA-2 PR.IP-12 DE.CM-8 RS.MI-3	ID.RA-1 ID.RA-2 PR.IP-12 DE.CM-8 RS.AN-5 RS.MI-3	6.2.16 6.2.17	3.2c	VUL: Vulnerability Management	A.12.6 A.14.2
Critical Security Control #4: Controlled Use of Administrative Privileges	AC-2: Account Management AC-6: Least Privilege AC-17: Remote Access AC-19: Access Control for Mobile Devices CA-7: Continuous Monitoring IA-2: Identification and Authentication (Organizational Users) IA-4: Identifier Management IA-5: Authenticator Management SI-4: Information System Monitoring	PR.AC-4 PR.AT-2 PR.MA-2 PR.PT-3	PR.AC-4 PR.AT-2 PR.MA-2 PR.PT-3	5.15 6.2.7 6.2.16 6.2.17			A.9.1 A.9.2.2 - A A.9.3 A.9.4.1 - A
Critical Security Control #5: Secure Configurations for Hardware and Software	CA-7: Continuous Monitoring CM-2: Baseline Configuration CM-3: Configuration Change Control CM-5: Access Restrictions for Change CM-6: Configuration Settings CM-7: Least Functionality CM-8: Information System Component Inventory CM-9: Configuration Management Plan CM-11: User-Installed Software MA-4: Nonlocal Maintenance RA-5: Vulnerability Scanning SA-4: Acquisition Process SC-15: Collaborative Computing Devices SC-34: Non-Modifiable Executable Programs SI-2: Flaw Remediation	PR.IP-1	PR.IP-1	6.2.16 6.2.17		CSM: Configuration Settings Management	A.14.2 A.14.3 A.18.2

Summary | NIST 800-53 rev4 | NIST CSF 1.1 | NIST CSF 1.0 | NIST 800-82 rev2 | NIST SMB Guide | DHS CDM Program | ISO 27002-2013 | ISO 27002-2005 | IEC 62443-3-3-2013 | NIST 800-171 | NSA MNT

Ready

BLACK HILLS Information Security
ETERNAL FOR 10 YEARS
•2008-2018•

To the Future!

AuditScripts

Security Control Category Coverage Analysis (v1.0g)

Security Control Category	Common Control Count	CIS Control (v7.1) Count	NIST CSF (v1.1) Count	NIST CSF (v1.0) Count	ISO 27002:2013 Count	NIST 800-171 Count	NIST Privacy (v1.0)
Security Program Governance	60	17%	32%	30%	25%	8%	28%
Auditing and Reporting	53	15%	15%	6%	21%	8%	11%
Security Program Operations	38	21%	95%	95%	87%	34%	45%
Asset Inventory and Control	18	94%	17%	17%	22%	22%	22%
System Protection	55	76%	20%	20%	7%	38%	11%
System Monitoring	23	65%	30%	30%	22%	57%	30%
Identity and Access Management	51	41%	25%	22%	43%	67%	37%
Network Device Protection	7	71%	14%	0%	0%	0%	0%
Boundary Protection	35	63%	11%	11%	6%	29%	6%
Internal Network Protection	16	94%	19%	19%	25%	25%	19%
Secure Software Development	18	44%	17%	11%	72%	0%	17%
Data Privacy	15	0%	0%	0%	0%	7%	107%

To the Future!

AuditScripts

Common Control Library (v1.0g)

Control Reference ID #	Control Description	CIS Control (v7.1)	NIST CSF (v1.1)	NIST CSF (v1.0)	ISO 27002:2013	NIST 800-171	NIST Privacy (v1.0)	Australian DSD35	CMMC (v1)
GOV-01	Create an information assurance charter that articulates the organization's commitment to data protection and its goals towards the confidentiality, integrity and availability of data.		ID.BE-3 PR.DS-4 PR.PT-5	ID.BE-3 PR.DS-4	A.12.1.3 A.17.2.1		ID.BE-P2 PR.DS-P4		
GOV-02	Establish the authority of a committee to define the organization's information assurance program strategy and administer the program.								
GOV-03	Define the key stakeholders that will serve as members of the organization's information Assurance program committee.								
GOV-04	Establish that an senior executive leadership representative with authority will always be a member of this organization's committee.								
GOV-05	Define additional leadership roles and responsibilities for the organization's information security program and committee.								
GOV-06	Ensure that the organization's information security program committee is composed of key stakeholders from a cross-section of the organization, not simply technology workforce members.		ID.RM-1	ID.RM-1					
GOV-07	Ensure that the organization's information assurance program charter defines the organization's approach to addressing cyber security risk.		ID.RM-1 ID.RM-2 ID.RM-3 ID.GV-4 ID.RA-4	ID.RM-1 ID.RM-2 ID.RM-3 ID.GV-4 ID.RA-4			ID.DE-P1 GV.PO-P6 GV.RM-P1 GV.RM-P2 GV.RM-P3		
GOV-08	Ensure that the organization's information assurance program charter defines the specific regulatory requirements, contractual requirements, and standards that the organization's assurance program shall achieve.		ID.BE-2 ID.GV-3 ID.RM-3	ID.BE-2 ID.GV-3 ID.RM-3	A.18.1.1 A.18.1.2		GV.PO-P5		

To the Future!

AuditScripts

Security Control System Coverage Analysis (v1.0g)

Governance and Operations Controls	Common Control Count	CIS Control (v7.1) Count	NIST CSF (v1.1) Count	NIST CSF (v1.0) Count	ISO 27002:2013 Count	NIST 800-171 Count	NIST Privacy (v1.0)
Technical Infrastructure Controls	**Common Control Count**	**CIS Control (v7.1) Count**	**NIST CSF (v1.1) Count**	**NIST CSF (v1.0) Count**	**ISO 27002:2013 Count**	**NIST 800-171 Count**	**NIST Privacy (v1.0)**
Asset Inventory and Discovery System	6	5	2	2	2	0	4
Software Inventory and Discovery System	6	6	1	1	0	0	0
Application Control System	6	6	0	0	2	4	0
Patch Management System	3	2	0	0	0	0	0
Vulnerability Management System	9	10	5	5	0	3	2
Configuration Management System	21	14	2	2	0	6	2
Endpoint Protection System	12	8	2	2	2	5	0
Removable Media Protection System	5	3	1	1	1	6	1
Backup and Recovery System	5	5	1	1	1	1	1
Log Management System	20	14	6	6	5	13	5
File Integrity Management System	3	1	1	1	0	0	2
Identity Management System	16	10	3	1	9	13	2
Data Inventory System	12	3	4	4	3	3	9
Access Management System	10	2	5	5	9	11	6
Privileged Account Management System	13	6	1	1	1	7	2
Network Device Management System	7	5	1	0	0	0	0
Boundary Filtering System	11	11	2	2	0	3	1
Remote Access System	11	1	2	2	1	7	1
Web Filtering System	8	7	0	0	0	0	0
Email Filtering System	5	3	0	0	1	0	0
Network Segmentation and Control System	8	9	3	3	4	1	3
Wireless Access System	8	6	0	0	0	3	0

MITRE and The Critical Controls

MITRE | ATT&CK

Matrices | Tactics | Techniques | Mitigations | Groups | Software | Resources | Blog | Contribute | Search

The sub-techniques beta is now live! Read the release blog post for more info.

MATRICES

- PRE-ATT&CK
- Enterprise
  - Windows
  - macOS
  - Linux
  - Cloud
- Mobile
- ICS

Home > Matrices > Enterprise

Launch the ATT&CK® Navigator

Enterprise Matrix

Below are the tactics and technique representing the MITRE ATT&CK® Matrix for Enterprise. The Matrix contains information for the following platforms: Windows, macOS, Linux, AWS, GCP, Azure, Azure AD, Office 365, SaaS.

Last Modified: 2019-10-09 18:48:31.906000

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Application Access Token	Bash History	Application Window Discovery	Application Access Token	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Application Deployment Software	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	BITS Jobs	Cloud Instance Metadata API	Cloud Service Dashboard	Component Object Model and Distributed COM	Data from Cloud Storage Object	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Component Object Model and Distributed COM	AppInit DLLs	Application Shimming	Bypass User Account Control	Credential Dumping	Cloud Service Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Spearphishing Attachment	Control Panel Items	Application Shimming	Bypass User Account Control	Clear Command History	Credentials from Web Browsers	Domain Trust Discovery	Internal Spearphishing	Data from Local System	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Spearphishing Link	Dynamic Data Exchange	Authentication Package	DLL Search Order Hijacking	CMSTP	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Network Shared Drive	Data Obfuscation	Exfiltration Over Other Network Medium	Endpoint Denial of Service
Spearphishing via Service	Execution through API	BITS Jobs	Dylib Hijacking	Code Signing	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Removable Media	Domain Fronting	Exfiltration Over Physical Medium	Firmware Corruption

AuditScripts-CIS-C...xlsx | AuditScripts-CIS-C...xlsx | AuditScripts-CIS-C...xlsx | Show all

MITRE and The Critical Controls

AuditScripts MITRE ATTACK to CIS Controls Mapping – v7.1a.xlsx

Open with

AuditScripts &CK Enterprise Techniques Mapped to the CIS Controls (v7.1a)

Category	ID	Technique Title	Technique Description	Johns call
Initial Access	T1189	Drive-by Compromise	A drive-by compromise is when an adversary gains access to a system through a user visiting a website over the normal course of browsing. With this technique, the user's web browser is targeted for exploitation. This can happen in several ways, but there are a few main components:	CSC(17.0) CSC(8.0)
Initial Access	T1190	Exploit Public-Facing Application	The use of software, data, or commands to take advantage of a weakness in an Internet-facing computer system or program in order to cause unintended or unanticipated behavior. The weakness in the system can be a bug, a glitch, or a design vulnerability. These applications are often websites, but can include databases (like SQL), standard services (like SMB or SSH), and any other applications with Internet accessible open sockets, such as web servers and related services. Depending on the flaw being exploited this may include Exploitation for Defense Evasion.	CSC(3.0) CSC(18.0)
Initial Access	T1200	Hardware Additions	Computer accessories, computers, or networking hardware may be introduced into a system as a vector to gain execution. While public references of usage by APT groups are scarce, many penetration testers leverage hardware additions for initial access. Commercial and open source products are leveraged with capabilities such as passive network tapping, man-in-the-middle encryption breaking, Keystroke Injection, Kernel memory reading via DMA, adding new wireless access to an existing network, and others.	CSC(2.0)
Initial Access	T1091	Replication Through Removable Media	Adversaries may move onto systems, possibly those on disconnected or air-gapped networks, by copying malware to removable media and taking advantage of Autorun features when the media is inserted into a system and executes. In the case of Lateral Movement, this may occur through modification of executable files stored on removable media or by copying malware and renaming it to look like a legitimate file to trick users into executing it on a separate system. In the case of Initial Access, this may occur through manual manipulation of the media, modification of systems used to initially format the media, or modification to the media's firmware itself.	CSC(8.8)
Initial Access	T1193	Spearphishing Attachment	Spearphishing attachment is a specific variant of spearphishing. Spearphishing attachment is different from other forms of spearphishing in that it employs the use of malware attached to an email. All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this scenario, adversaries attach a file to the spearphishing email and usually rely upon User Execution to gain execution.	CSC(7.0) CSC(8.8)
Initial Access	T1192	Spearphishing Link	Spearphishing with a link is a specific variant of spearphishing. It is different from other forms of spearphishing in that it employs the use of links to download malware contained in email, instead of attaching malicious files to the email itself, to avoid defenses that may inspect email attachments.	CSC(7.0) CSC(8.8)
Initial Access	T1194	Spearphishing via Service	Spearphishing via service is a specific variant of spearphishing. It is different from other forms of spearphishing in that it employs the use of third party services rather than directly via enterprise email channels.	CSC(7.0) CSC(8.8)
Initial Access	T1195	Supply Chain Compromise	Supply chain compromise is the manipulation of products or product delivery mechanisms prior to receipt by a final consumer for the purpose of data or system compromise. Supply chain compromise can take place at any stage of the supply chain including:	CSC(18.0)
Initial Access	T1199	Trusted Relationship	Adversaries may breach or otherwise leverage organizations who have access to intended victims. Access through trusted third party relationship exploits an existing connection that may not be protected or receives less scrutiny than standard mechanisms of gaining access to a network.	CSC(9.4)
Initial Access	T1078	Valid Accounts	Adversaries may steal the credentials of a specific user or service account using Credential Access techniques or capture credentials earlier in their reconnaissance process through social engineering for means of gaining Initial Access.	CSC(6.0)
Execution	T1155	AppleScript	macOS and OS X applications send AppleEvent messages to each other for interprocess communications (IPC). These messages can be easily scripted with AppleScript for local or remote IPC. Osascript executes AppleScript and any other Open Scripting Architecture (OSA) language scripts. A list of OSA languages installed on a system can be found by using the osalang program.	CSC(5.0) CSC(8.8)

BLACK HILLS Information Security
Celebrating 10 Years
2008-2018