RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: **STR-F01**

Cyber-Hygiene for All:
An Introduction to the CIS Controls

Phyllis Lee

Senior Director of CIS Controls
Center for Internet Security
Ø

Joshua M Franklin

Senior Cybersecurity Engineer
Center for Internet Security
@thejoshpit

Overview

- Introductions
- CIS Control Basics
- Implementation Groups
- Other Available Tools and Resources
- Feedback on the Controls
- Future Directions

Introductions

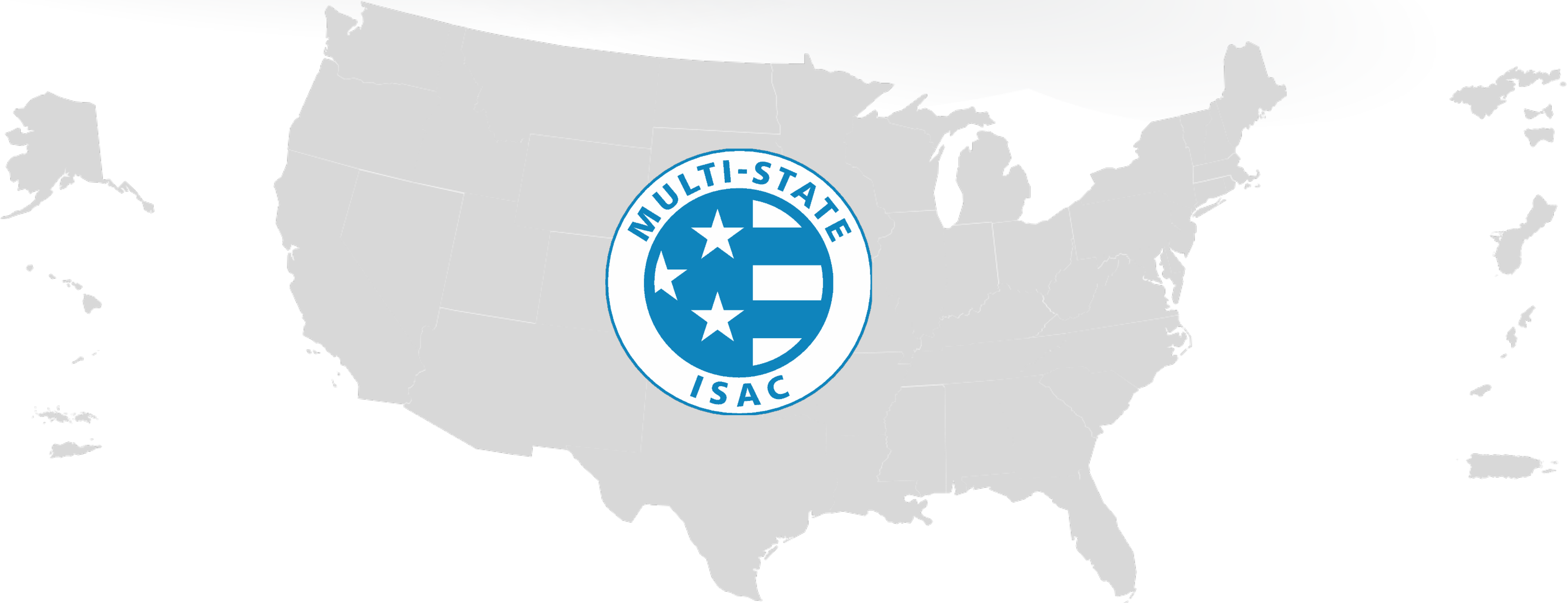
- Phyllis Lee
- 20 years in the US Federal Government
- Security Automation Lead for the Information Assurance Directorate (IAD) at the NSA
- Focus on virtualization and malware analysis

- Joshua M Franklin
- 10 years in the US Federal Government
  - 7 of those years at NIST
- Focus on telecommunications, mobile, and election security
- Cybersecurity standards (e.g., NIST, CIS, IEEE, OASIS, 3GPP)

CIS Introduction

- US-based forward-thinking, non-profit entity that harnesses the power of a global IT community
- Goal of safeguarding private & public organizations against cyber threats
- CIS Vision: Leading the global community to secure our connected world
- CIS Mission:
  - Identify, develop, validate, promote, and sustain best practice solutions for cyber defense
  - Build and lead communities to enable an environment of trust in cyberspace

MS-ISAC



The MS-ISAC has been designated by DHS as the key resource for cyber threat prevention, protection, response and recovery for the nation’s state, local, tribal, and territorial governments.

The CIS Controls

- Globally recognized cybersecurity standard
- Over 228,000 downloads since CIS took the reigns
- 20 top-level controls followed by 171 sub-controls
- Prioritized set of actions that's designed to scale
- Provides a logical path to build a foundation and gradually improve your cybersecurity posture
- Version 7.1 released in April 2019
- Developed by cybersecurity experts - *like you*

Goals of the CIS Controls

- Concise
- Prioritized
- Attack-driven
- Measurable
- Defensible
- Consensus-based

7.1 Update

- Guiding principles for the 7.1 update:
  - Provide a new prioritization scheme (Implementation Groups)
  - Enhance the clarity and readability of the Controls
  - Refrain from modifying the spirit of any Controls
- Aimed as a way to:
  - Practice **basic cyber hygiene** with limited resources and expertise
  - Prioritize cybersecurity activities
  - Implement security best practices, regardless of resources
  - Ensure a standard duty of care

CIS Controls History

NSA/DoD Project

CSIS The Consensus Audit Guidelines (CSIS)

SANS "The SANS Top 20" (the SANS Institute)

CIS Critical Security Controls The Critical Security Controls (CCS/CIS)

CIS Controls®

The CIS Controls

V7.1

Basic

1 Inventory and Control of Hardware Assets

2 Inventory and Control of Software Assets

3 Continuous Vulnerability Management

4 Controlled Use of Administrative Privileges

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

6 Maintenance, Monitoring and Analysis of Audit Logs

Foundational

7 Email and Web Browser Protections

8 Malware Defenses

9 Limitation and Control of Network Ports, Protocols and Services

10 Data Recovery Capabilities

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

12 Boundary Defense

13 Data Protection

14 Controlled Access Based on the Need to Know

15 Wireless Access Control

16 Account Monitoring and Control

Organizational

17 Implement a Security Awareness and Training Program

18 Application Software Security

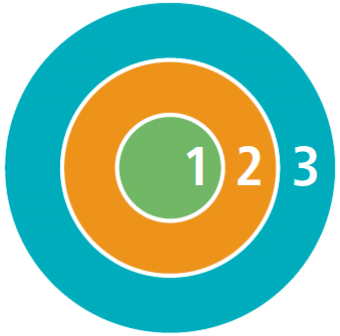
19 Incident Response and Management

20 Penetration Tests and Red Team Exercises

Staying Fresh with Basic Cyber Hygiene

- Comparing your organization against best practice helps you take stock of your cybersecurity health
  - Often nebulously defined as **basic cyber hygiene**
- Commonly used term but what does it mean?
- CIS defines Implementation Group 1 as *basic cyber hygiene*
  - 43 specific tasks to ensure your organization is performing the baseline

Implementation Groups



Implementation Group 3

A mature organization with significant resources and cybersecurity experience to allocate to Sub-Controls

Implementation Group 2

An organization with moderate resources and cybersecurity expertise to implement Sub-Controls

Implementation Group 1

An organization with limited resources and cybersecurity expertise available to implement Sub-Controls

V7.1

Definitions	1	2	3
Implementation Group 1 CIS Sub-Controls for small, commercial off-the-shelf or home office software environments where sensitivity of the data is low will typically fall under IG1. Remember, any IG1 steps should also be followed by organizations in IG2 and IG3.	●		
Implementation Group 2 CIS Sub-Controls focused on helping security teams manage sensitive client or company information fall under IG2. IG2 steps should also be followed by organizations in IG3.	●	●	
Implementation Group 3 CIS Sub-Controls that reduce the impact of zero-day attacks and targeted attacks from sophisticated adversaries typically fall into IG3. IG1 and IG2 organizations may be unable to implement all IG3 Sub-Controls.	●	●	●

What Group Are You?

- That’s for you to decide
- Methodology for deciding your Implementation Group is provided based on the following:
  - Data sensitivity and criticality of services offered by the organization
  - Expected level of technical expertise exhibited by staff or on contract
  - Resources available and dedicated towards cybersecurity activities

Implementation Group 1 Topics

Procedural

- Maintaining an asset inventory
- Password management
- 1 offsite backup
- Network boundary inventory
- Incident response planning
- Isolating personal devices

Technical

- Automated patching
- Secure configuration
- Audit logging
- DNS filtering
- Dedicated admin workstations
- Account management

Other Tools to Help Along the Way

Supplementing the CIS Controls

Guides & Tools

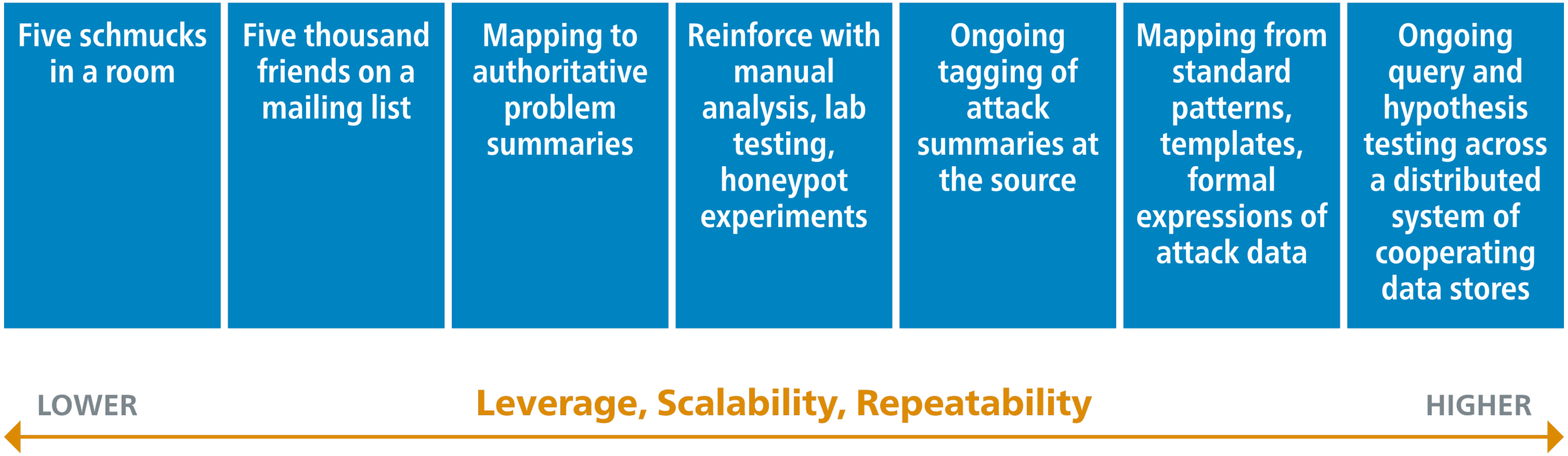
- CIS provides domain specific guidance for the CIS Controls
  - Cloud
  - Internet of Things (IoT)
  - Mobile
  - Industrial Control System (ICS)
- CIS provides a detailed Cyber Hygiene guide for Windows 10
- CIS provides an automated method to assess some CIS Controls on Windows 10 called the Controls Assessment Module

Mappings to Other Frameworks

- CIS is committed to interoperability with other industry frameworks
- CIS maps to a variety of security standards and frameworks
  - Available in a machine-readable format
- Available mappings:
  - NIST CSF
  - ISO 27000
  - NIST 800-53
  - NIST 800-171
- Upcoming:
  - HIPAA
  - PCI DSS
  - COBIT
  - MARS-E
- External:
  - Microsoft Azure Security Benchmark
  - NIST Online Informative Reference (OLIR)

Evolving a Cybersecurity Standard

Evolving the CIS Controls Selection Process



Five schmucks in a room

Five thousand friends on a mailing list

Mapping to authoritative problem summaries

Reinforce with manual analysis, lab testing, honeypot experiments

Ongoing tagging of attack summaries at the source

Mapping from standard patterns, templates, formal expressions of attack data

Ongoing query and hypothesis testing across a distributed system of cooperating data stores

LOWER **Leverage, Scalability, Repeatability** HIGHER

Community Attack Model Version 1

- CIS effort to analyze pertinent information relating to real-world attacks in the wild
- Goal: help enterprises make good choices about the most effective defensive actions they can take
- Released via Blackhat in 2016
- Leverages additional frameworks such as NIST CSF and Lockheed Martin Cyber Kill Chain
- Updating this model based on publicly available attack data

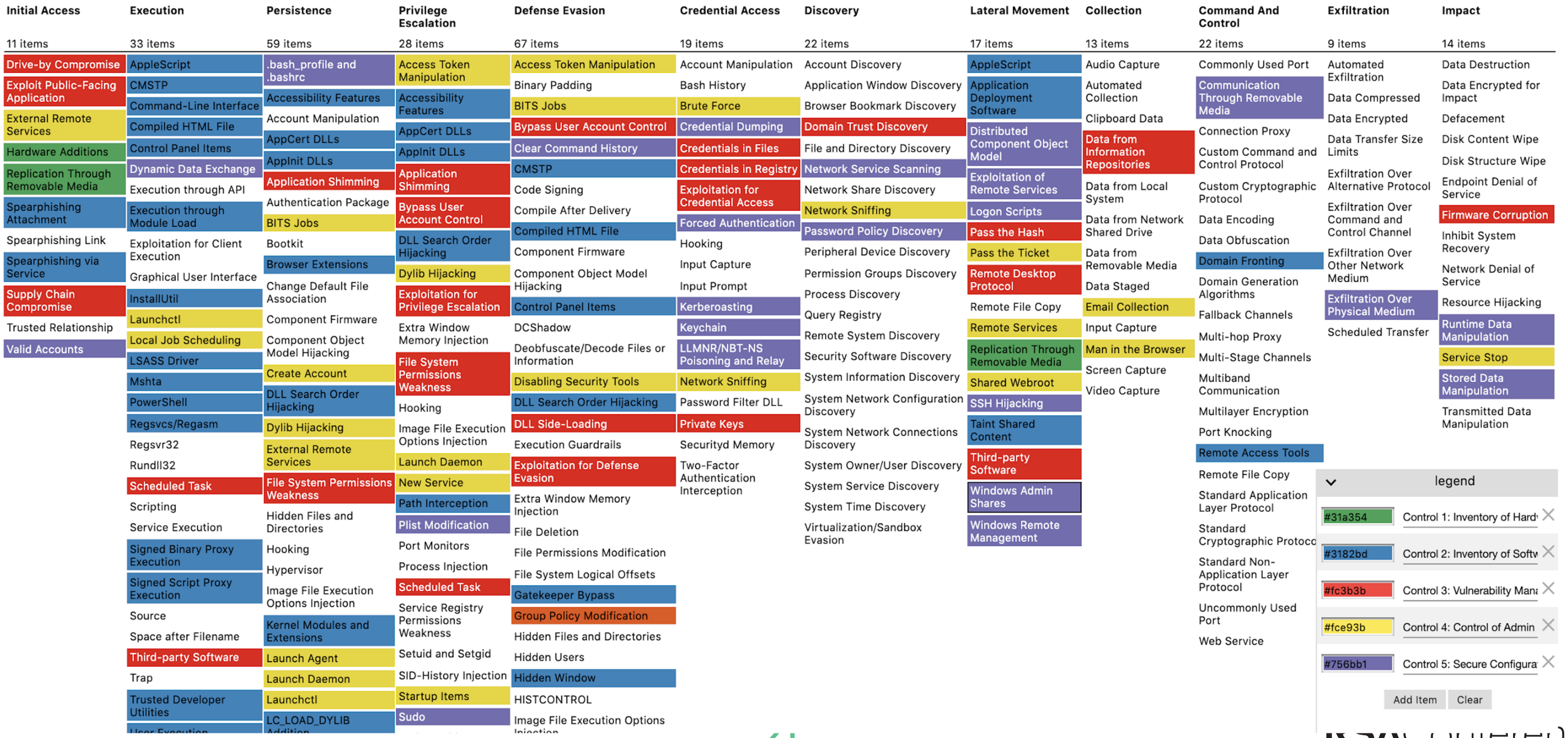
Community Defense Model

- Revamp and update the *Community Attack Model*
- Standard method of expression
- General methodology:
  - Analyze data sources
  - Identify key attack paths
  - Identify mitigations for key attacks
  - Map mitigations to CIS Controls
- Expected outputs:
  - Mapping of the CIS Controls to MITRE ATT&CK
  - Mappings of the CIS Controls to MITRE ATT&CK Mitigations
  - Data-backed attack patterns that the CIS Controls defend against

MITRE | ATT&CK®

Define What Attacks the CIS Controls Defend Against

- No other security standard or defensive framework does this



Initial Access

11 items

- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Replication Through Removable Media
- Spearphishing Attachment
- Spearphishing Link
- Spearphishing via Service
- Supply Chain Compromise
- Trusted Relationship
- Valid Accounts

Execution

33 items

- AppleScript
- CMSTP
- Command-Line Interface
- Compiled HTML File
- Control Panel Items
- Dynamic Data Exchange
- Execution through API
- Execution through Module Load
- Exploitation for Client Execution
- Graphical User Interface
- InstallUtil
- Launchctl
- Local Job Scheduling
- LSASS Driver
- Mshta
- PowerShell
- Regsvcs/Regasm
- Regsvr32
- Rundll32
- Scheduled Task
- Scripting
- Service Execution
- Signed Binary Proxy Execution
- Signed Script Proxy Execution
- Source
- Space after Filename
- Third-party Software
- Trap
- Trusted Developer Utilities
- User Execution

Persistence

59 items

- .bash_profile and .bashrc
- Accessibility Features
- Account Manipulation
- AppCert DLLs
- AppInit DLLs
- Application Shimming
- Authentication Package
- BITS Jobs
- Bootkit
- Browser Extensions
- Change Default File Association
- Component Firmware
- Component Object Model Hijacking
- Create Account
- DLL Search Order Hijacking
- Dylib Hijacking
- External Remote Services
- File System Permissions Weakness
- Hidden Files and Directories
- Hooking
- Hypervisor
- Image File Execution Options Injection
- Kernel Modules and Extensions
- Launch Agent
- Launch Daemon
- Launchctl
- LC_LOAD_DYLIB Addition

Privilege Escalation

28 items

- Access Token Manipulation
- Accessibility Features
- AppCert DLLs
- AppInit DLLs
- Application Shimming
- Bypass User Account Control
- DLL Search Order Hijacking
- Dylib Hijacking
- Exploitation for Privilege Escalation
- Extra Window Memory Injection
- File System Permissions Weakness
- Hooking
- Image File Execution Options Injection
- Launch Daemon
- New Service
- Path Interception
- Plist Modification
- Port Monitors
- Process Injection
- Scheduled Task
- Service Registry Permissions Weakness
- Setuid and Setgid
- SID-History Injection
- Startup Items
- Sudo

Defense Evasion

67 items

- Access Token Manipulation
- Binary Padding
- BITS Jobs
- Bypass User Account Control
- Clear Command History
- CMSTP
- Code Signing
- Compile After Delivery
- Compiled HTML File
- Component Firmware
- Component Object Model Hijacking
- Control Panel Items
- DCShadow
- Deobfuscate/Decode Files or Information
- Disabling Security Tools
- DLL Search Order Hijacking
- DLL Side-Loading
- Execution Guardrails
- Exploitation for Defense Evasion
- Extra Window Memory Injection
- File Deletion
- File Permissions Modification
- File System Logical Offsets
- Gatekeeper Bypass
- Group Policy Modification
- Hidden Files and Directories
- Hidden Users
- Hidden Window
- HISTCONTROL
- Image File Execution Options Injection

Credential Access

19 items

- Account Manipulation
- Bash History
- Brute Force
- Credential Dumping
- Credentials in Files
- Credentials in Registry
- Exploitation for Credential Access
- Forced Authentication
- Hooking
- Input Capture
- Input Prompt
- Kerberoasting
- Keychain
- LLMNR/NBT-NS Poisoning and Relay
- Network Sniffing
- Password Filter DLL
- Private Keys
- Securityd Memory
- Two-Factor Authentication Interception

Discovery

22 items

- Account Discovery
- Application Window Discovery
- Browser Bookmark Discovery
- Domain Trust Discovery
- File and Directory Discovery
- Network Service Scanning
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery
- Process Discovery
- Query Registry
- Remote System Discovery
- Security Software Discovery
- System Information Discovery
- System Network Configuration Discovery
- System Network Connections Discovery
- System Owner/User Discovery
- System Service Discovery
- System Time Discovery
- Virtualization/Sandbox Evasion

Lateral Movement

17 items

- AppleScript
- Application Deployment Software
- Distributed Component Object Model
- Exploitation of Remote Services
- Logon Scripts
- Pass the Hash
- Pass the Ticket
- Remote Desktop Protocol
- Remote File Copy
- Remote Services
- Replication Through Removable Media
- Shared Webroot
- SSH Hijacking
- Taint Shared Content
- Third-party Software
- Windows Admin Shares
- Windows Remote Management

Collection

13 items

- Audio Capture
- Automated Collection
- Clipboard Data
- Data from Information Repositories
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged
- Email Collection
- Input Capture
- Man in the Browser
- Screen Capture
- Video Capture

Command And Control

22 items

- Commonly Used Port
- Communication Through Removable Media
- Connection Proxy
- Custom Command and Control Protocol
- Custom Cryptographic Protocol
- Data Encoding
- Data Obfuscation
- Domain Fronting
- Domain Generation Algorithms
- Fallback Channels
- Multi-hop Proxy
- Multi-Stage Channels
- Multiband Communication
- Multilayer Encryption
- Port Knocking
- Remote Access Tools
- Remote File Copy
- Standard Application Layer Protocol
- Standard Cryptographic Protoco
- Standard Non-Application Layer Protocol
- Uncommonly Used Port
- Web Service

Exfiltration

9 items

- Automated Exfiltration
- Data Compressed
- Data Encrypted
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol
- Exfiltration Over Command and Control Channel
- Exfiltration Over Other Network Medium
- Exfiltration Over Physical Medium
- Scheduled Transfer

Impact

14 items

- Data Destruction
- Data Encrypted for Impact
- Defacement
- Disk Content Wipe
- Disk Structure Wipe
- Endpoint Denial of Service
- Firmware Corruption
- Inhibit System Recovery
- Network Denial of Service
- Resource Hijacking
- Runtime Data Manipulation
- Service Stop
- Stored Data Manipulation
- Transmitted Data Manipulation

legend

#31a354	Control 1: Inventory of Hard	✕
#3182bd	Control 2: Inventory of Softw	✕
#fc3b3b	Control 3: Vulnerability Mana	✕
#fce93b	Control 4: Control of Admin	✕
#756bb1	Control 5: Secure Configura	✕

Controls Assessment Specification

- Open specification allowing organizations to measure implementation of the CIS Controls
- CAS is focused on “what to measure” rather than “how to measure”
- Platform agnostic method allowing external tooling vendors to implement as best for their appropriate use cases

RSAConference2020

Feedback on the CIS Controls

What’s the community saying and doing?

State Adoption of the CIS Controls

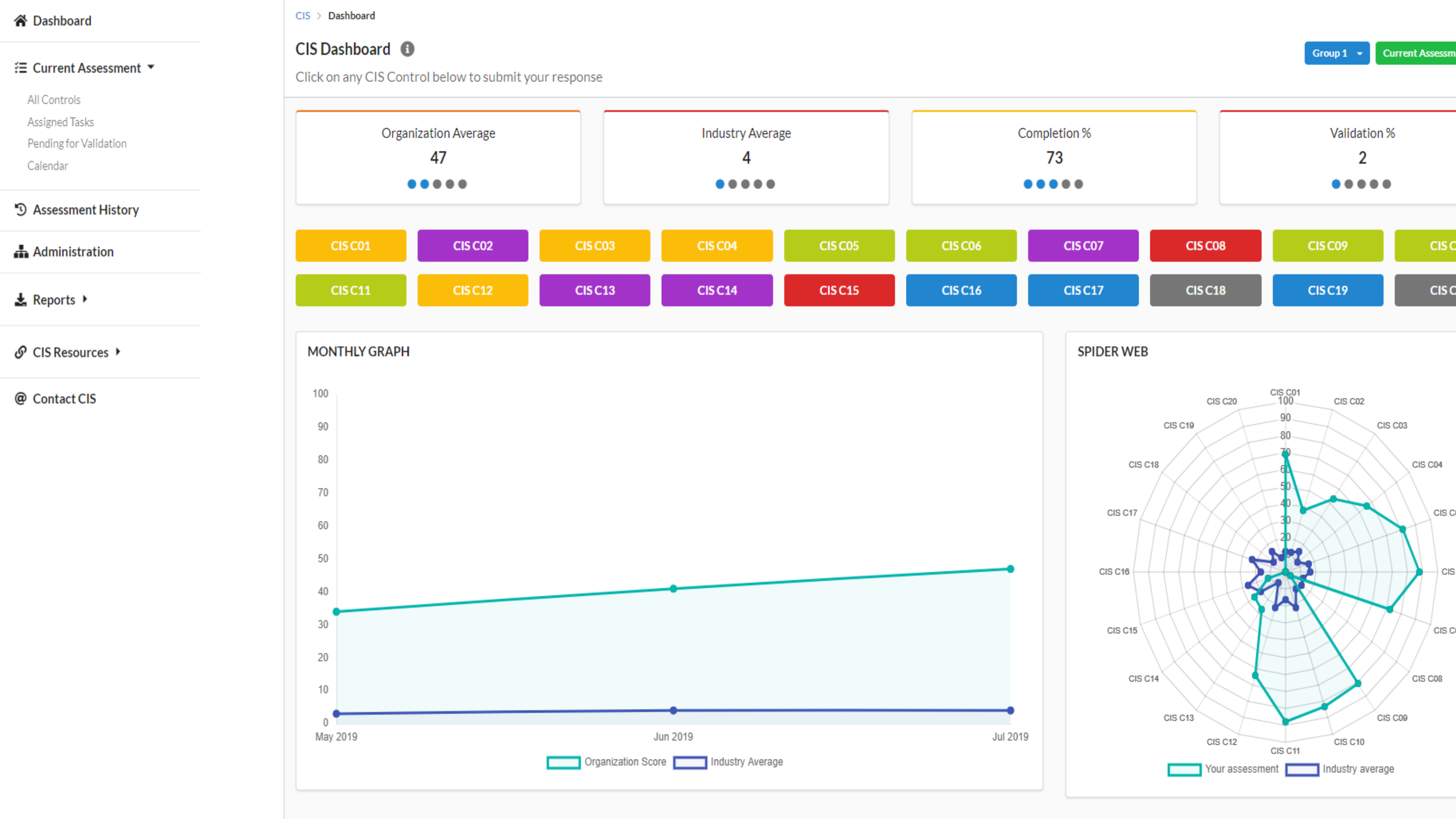
- States have adopted the CIS Controls in different ways
- **Nevada** defines the CIS Controls as a reasonable definition of security for state government agencies (NV S.B. 302)
- **Ohio** Data Protection Act provides legal protections for organizations voluntary implementing the CIS Controls or other defined frameworks
- **California** 2016 Data Breach Report warns that failing to implement the CIS Controls “constitutes a lack of reasonable security”
- **Idaho** Governor’s executive order requires executive branch agencies to implement the first 5 CIS Controls (EXECUTIVE ORDER NO. 2017-02)

Feedback

- Where do I start?
  - Many organizations get very bogged down in Control 1
- What isn’t **[my_favorite_technology]** reflected within the Controls?
- Where is my guidance for performing a risk assessment?
- Why don’t the Controls tell me what specific policies to use?

CIS Security Assessment Tool (CSAT)

- Web application allowing security professionals to track the implementation of the CIS Controls
  - At the Sub-Control level
  - Recent inclusion of CIS Implementation Groups
- Essentially a GRC tool designed to ease implementation of the CIS Controls
- Allows users to compare their scores against others in their industry



CIS Dashboard

Click on any CIS Control below to submit your response

Organization Average
47

Industry Average
4

Completion %
73

Validation %
2

Top 10 Sub-Control Scores

Rank	Sub-Control #	Sub-Control Title	Average	IG
1	8.2	Ensure Anti-Malware Software and Signatures Are Updated	81.42	1
2	8.1	Utilize Centrally Managed Anti-Malware Software	80.00	2
3	15.7	Leverage the Advanced Encryption Standard (AES) to Encrypt Wireless Data	79.69	1
4	15.10	Create Separate WiFi Network for Untrusted Devices	78.53	1
5	15.1	Maintain an Inventory of Authorized Wireless Access Points	76.75	2
6	10.1	Ensure Regular Automated Backups	76.12	1
7	4.2	Change Default Passwords	75.35	1
8	7.9	Block Unnecessary File Types	69.80	2
9	10.2	Perform Complete System Backups	69.67	1
10	16.11	Lock Workstation Sessions After Inactivity	69.10	1

Bottom 10 Sub-Control Scores

Rank	Sub-Control #	Sub-Control Title	Average	IG
171	20.5	Create a Test Bed for Elements Not Typically Tested in Production	12.50	2
170	14.5	Utilize an Active Discovery Tool to Identify Sensitive Data	13.78	3
169	4.6	Use Dedicated Workstations For All Administrative Tasks	14.92	3
168	14.7	Enforce Access Control to Data Through Automated Tools	15.05	3
167	20.3	Perform Periodic Red Team Exercises	15.33	3
166	15.9	Disable Wireless Peripheral Access to Devices	15.84	2
165	2.9	Implement Application Whitelisting of Scripts	15.99	3
164	2.8	Implement Application Whitelisting of Libraries	16.13	3
163	5.5	Implement Automated Configuration Monitoring Systems	16.88	2
162	11.6	Use Dedicated Workstations for All Network Administrative Tasks	17.59	2

Future of the Controls

- Looking to release version 8 of the CIS Controls in 2021
- Primary tasks: *simplification, decrease of cost and time to implement the Controls*
- Integrate the Community Defense Model into the CIS Controls
- Integrate CSAT data into the CIS Controls
- Will also be reflective of cloud technologies
- New approach to identity, authentication, and authorization

Apply What You've Learned Today

- Next week you should:
  - Review Implementation Group 1
  - Verify your organization is implementing **basic cyber hygiene**
- In the first three months following this presentation you should:
  - Assess whether your organization is Implementation Group 1, 2, or 3
  - Develop a plan for prioritize CIS Sub-Controls in your Implementation Group
- Within six months you should:
  - Review other free CIS resources such as Mobile, Cloud, and IoT Guides
  - Consider assessing your organization's via CSAT

Conclusions

- CIS provides free tools and guidance for all organizations:
  - https://www.cisecurity.org
- Share your cybersecurity expertise, join a community:
  - Visit https://workbench.cisecurity.org to participate
- The CIS Community Defense Model releasing soon
- Download CIS Controls v7.1
  - Fun web application to view, filter, and relate the Controls