Tech TV Series

COLLABORATE, INNOVATE, VALIDATE

CIS Top 20 #2 Inventory of Authorized and Unauthorized Software

Lisa Niles – CISSP, Chief Solution Architect

TECH TV SERIES

COLLABORATE, INNOVATE, VALIDATE

CIS Top 20 Critical Security Controls

- Introduction
- Many CISOs wonder where they should optimize processes and focus their resources to reduce security risk
- The CIS Critical Security Controls are 20 prioritized, vetted, and well supported security actions to assess and improve cyber security.
- Validating your security controls and processes against the CIS Top 20 can help secure your organization's assets, infrastructure, and information
- CSC strengthen your security posture: continuous, automated protection and monitoring
- "Offense must inform defense" approach to select and prioritize CSC

CIS Top 20 Critical Security Controls

- While the CSCs are broken down into 20 separate controls, the authors recognize that organizations need a place to start.
- The control sequence reflects their impact, from one to 20.
- Within each control, sub-levels provide further guidance so that every organization can experience "quick wins," gain "visibility and attribution" of assets in their infrastructure, and improve "configuration and hygiene" of assets to reduce exposure to threats.
- CSCs relevant to any organization, even if solely as a means to validate that existing efforts meet "due care" expectations for cybersecurity.

CIS Top 20 Critical Security Controls

- The Controls are specific guidelines that CISOs, CIOs, CTOs, systems administrators, and information security personnel can use to manage and measure the effectiveness of their defenses.
- They are designed to complement existing standards, frameworks, and compliance schemes by prioritizing the most critical threat and highest payoff defenses, while providing a common baseline for action against risks that we all face

CIS Top 20 Critical Security Controls

- The control areas in the CIS CSC focus on various technical aspects of information security
- Primary goal of supporting organizations in prioritizing their efforts in defending against today's most common and damaging attacks.
- Outside of the technical realm, a comprehensive security program should also take into account:
  - Numerous additional areas of security, including overall policy, organizational structure, personnel issues (e.g., background checks, etc.), and physical security.
- To help maintain focus, the controls in this document do not deal with these important, but non-technical, aspects of information security.
- Organizations should build a comprehensive approach in these other aspects of security as well

CIS Top 20 Critical Security Controls

- Because IT controls are just one aspect of being compliant, you may ask why **IT compliance** is such an important topic.
- The answer is, quite simply, that it's because the vast majority of business and government today is done through or with information technology.

CIS Top 20 Critical Security Controls

- Most IT compliance requirements start at the top with laws and regulations.
- They articulate the 'policies' governing their requirements.
- Policies, in turn, have their own operating requirements for compliance
- These organizations use standards as guidance for operational policies used to comply with the laws.
- Those same standards, combined with related methodologies, are the basis used by auditors to test policy controls and certify compliance.

CIS Top 20 Critical Security Controls

- Maintaining your perspective starts with understanding your organization's policy control objectives.
- This is a fancy way of saying, 'What are you trying to protect or control"
- Understand the types of controls that make up your compliance universe.
- Companies often focus only on controls for data security and overlook other key areas such as:
  - *Administrative controls:* policies, procedures, and processes associated with the control objectives.
  - *Physical and environmental controls:* the physical protection of electronic and non-electronic information or assets. Examples are door locks, camera monitoring, and fire suppression.
  - *Logical controls:* the control of access to specific networks and resources by an authorized user; generally managed by information technology.

CIS Top 20 Critical Security Controls

- **What is an IT security framework?**
  - An information security framework is a series of documented processes that are used to define policies and procedures around the implementation and ongoing management of information security controls in an enterprise environment.
  - These frameworks are basically a "blueprint" for building an information security program to manage risk and reduce vulnerabilities. Information security teams can utilize these frameworks to define and prioritize the tasks required to build security into an organization.
- NIST Cybersecurity Framework, NIST guidelines, and the ISO 27000 series or regulations such as PCI DSS, HIPAA, NERC CIP, FISMA

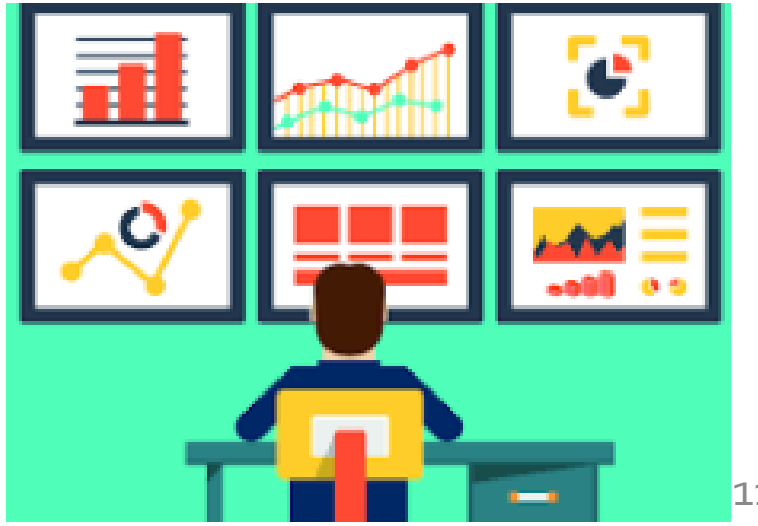
CIS Top 20 Critical Security Controls

CSC guiding principles:

- Defenses should focus on addressing the most common and damaging attacks
- Enterprise environments must ensure consistent controls across an enterprise to effectively negate attacks. (not 80%)
- Defenses should be automated where possible, and periodically or continuously measured using automated measurement techniques where feasible.

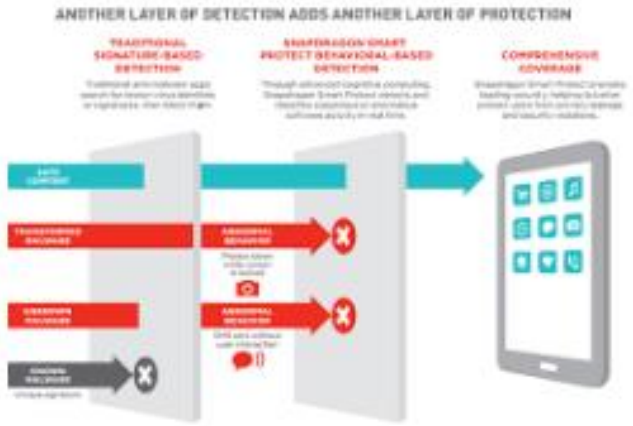
CIS Top 20 Critical Security Controls

- **The five critical tenets of an effective cyber defense system as reflected in the CIS Critical Security Controls are:**
  - Offense informs defense
  - Prioritization
  - Metrics
  - Continuous diagnostics and mitigation
  - Automation



CIS Top 20 Critical Security Controls

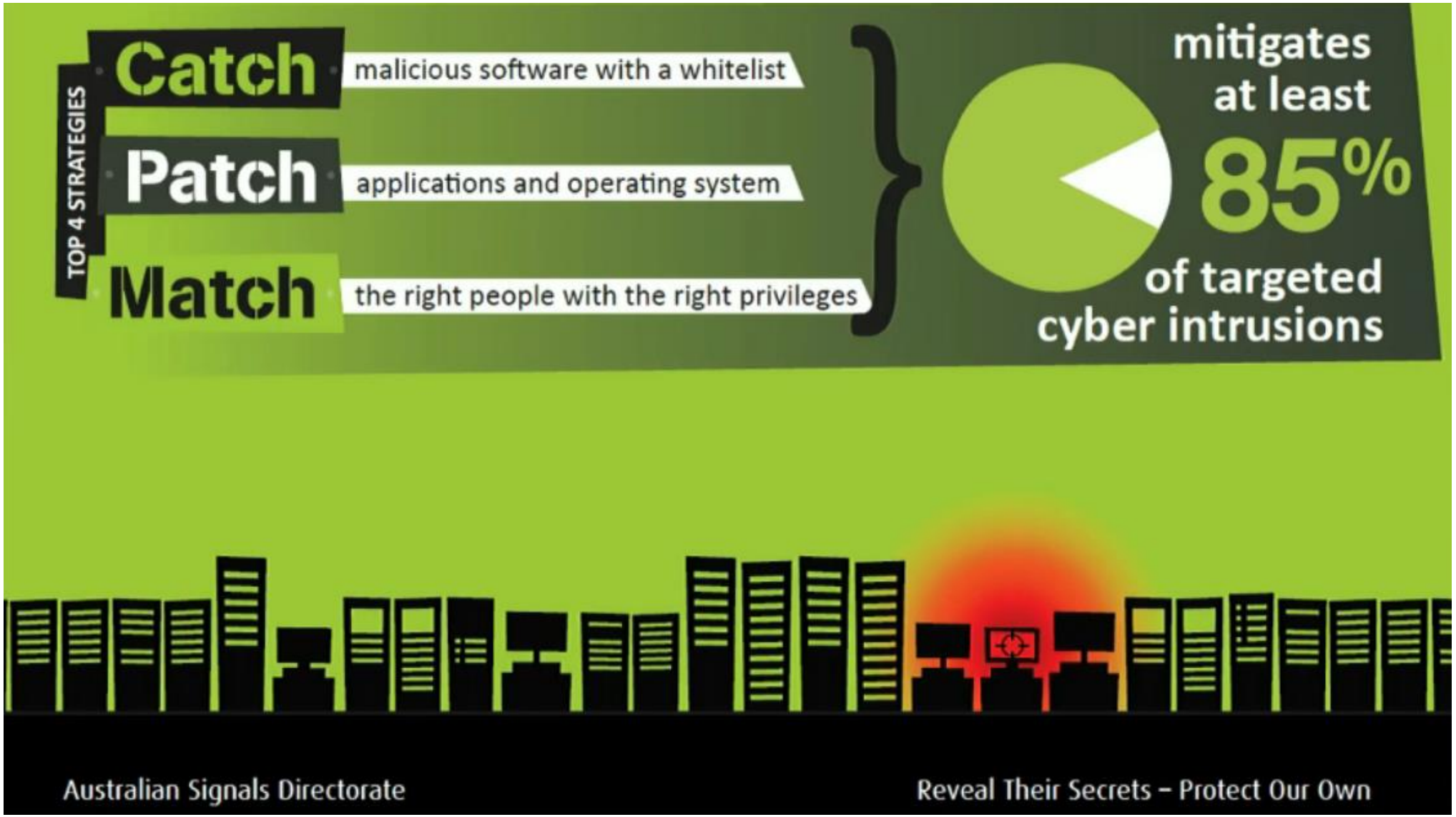
- Prevent, detect, remediate, report
- Rinse and repeat



CIS Top 20 Critical Security Controls

- Getting Started: Key Questions
  - What am I trying to protect?
  - Where are my gaps?
  - What are my priorities?
  - Where can I automate?
  - How can my vendor partners help?

CIS Top 20 Critical Security Controls



CIS Top 20 Critical Security Controls

Basic Security Hygiene (Back to the Basics!)

- Know what you have (Inventory HW &SW)
- Limit what you don't NEED (EOL, Services, Networks, Rights)
- Update your software
- Secure Default Configurations
- Employ Process Controls
- Secure Web Apps

CIS Top 20 Critical Security Controls

General Guidance for Implementing the Controls:

- Carefully plan.
- Organizational structure for program's success.
- Establish a "Governance, Risk, and Compliance (GRC)" program.
- Assigning program managers

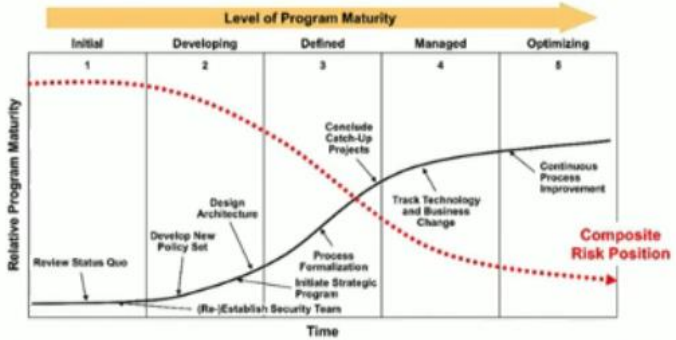
TECH TV SERIES

COLLABORATE, INNOVATE, VALIDATE

CIS Top 20 Critical Security Controls

Defining a Strong Security Team/Program

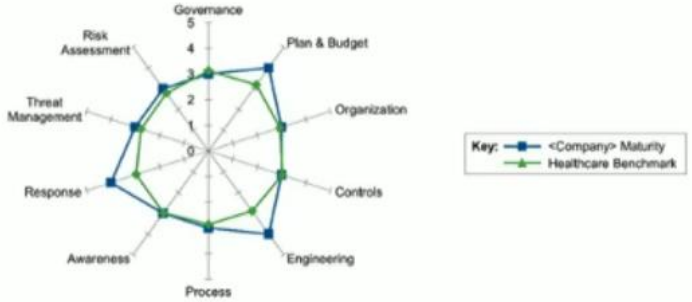
Cybersecurity Program Maturity



Example

Gartner

Current State of the Security Program



Example

Gartner

- Mature = Effective and efficient
- Key indicators:
  - Basic security hygiene
  - Security Operations Center processes and tools
  - "Business Security Analysts"
  - Integration into procurement, M&A, supply chain decisions
  - Cross-industry participation

TECH TV SERIES

COLLABORATE, INNOVATE, VALIDATE

CIS Top 20 Critical Security Controls

CIS Controls

First 5 CIS Controls
Eliminate the vast majority of your organization's vulnerabilities

Secure Your Organization

All 20 CIS Controls
Secure your entire organization against today's most pervasive threats

1: Inventory of Authorized and Unauthorized Devices
2: Inventory of Authorized and Unauthorized Software
3: Secure Configurations for Hardware and Software
4: Continuous Vulnerability Assessment and Remediation
5: Controlled Use of Administrative Privileges
6: Maintenance, Monitoring, and Analysis of Audit Logs
7: Email and Web Browser Protections
8: Malware Defenses
9: Limitation and Control of Network Ports
10: Data Recovery Capability
11: Secure Configurations for Network Devices
12: Boundary Defense
13: Data Protection
14: Controlled Access Based on the Need to Know
15: Wireless Access Control
16: Account Monitoring and Control
17: Security Skills Assessment and Appropriate Training to Fill Gaps
18: Application Software Security
19: Incident Response and Management
20: Penetration Tests and Red Team Exercises

CIS SecureSuite™ Membership

Become a member

CIS Top 20 Critical Security Controls

- **Control #2**
- Inventory of Authorized and Unauthorized Software
- Key Principle Control:
  - Control #2 focuses on knowing all software that is installed on servers and workstations & devices throughout your organization

CIS Top 20 Critical Security Controls

Securing: IoT Security

- Explosion of varying types of IoT endpoints creates a **broad attack surface**
- IoT security-related technology disruptions can be broken down into the following:
  - Asset discovery, profiling and tracking
  - Authentication
  - Network-based protection
  - Secure software development
  - Visibility through monitoring, detection and response
- The **integration** of these IoT security technologies with traditional IT and operational technology (OT) security infrastructures and practices **remains a challenge**
- Latest disruptive trends and developments:
  - IoT endpoint threats

Securing:
IoT Security

CIS Top 20 Critical Security Controls

How to Get Started

Step 1. Gap Assessment.

Step 2. Implementation Roadmap

Step 3. Implement the First Phase of Controls

Step 4. Integrate Controls into Operations

Step 5. Report and Manage Progress

CIS Top 20 Critical Security Controls

- Successful implementation of the Controls will require many organizations to shift their mindset on security and how they approach IT operations and defense.
- No longer can employees be allowed to install software at random or travel with sensitive data in their pockets.
- A BIG change in mindset on this control CSC#2 inventory of software deals with the change in mindset with allowing the "Local admin" credentials on devices.

CIS Top 20 Critical Security Controls

- **Why is CIS Control 2 critical?**
- An organization without the ability to inventory and control its computers' installed programs makes its systems more vulnerable to attack.
- The vast majority of attacks are leveraging vulnerabilities in software.
- Self contained .exe viruses are old school.
- In order to combat this potential threat, an organization should scan a network and identify known or responding hosts and applications to help prioritize patching, removal, blocking, quarantine, alerting

TECH TV SERIES

COLLABORATE, INNOVATE, VALIDATE

CIS Top 20 Critical Security Controls

Inventory of Authorized and Unauthorized Software	2.1	Devise a list of authorized software and version that is required in the enterprise for each type of system, including servers, workstations, and laptops of various kinds and uses. This list should be monitored by file integrity checking tools to validate that the authorized software has not been modified.	Protect	Software Whitelisting System
Inventory of Authorized and Unauthorized Software	2.2	Deploy application whitelisting technology that allows systems to run software only if it is included on the whitelist and Protects execution of all other software on the system. The whitelist may be very extensive (as is available from commercial whitelist vendors), so that users are not inconvenienced when using common software. Or, for some special-purpose systems (which require only a small number of programs to achieve their needed business functionality), the whitelist may be quite narrow.	Protect	Software Whitelisting System
Inventory of Authorized and Unauthorized Software	2.3	Deploy software inventory tools throughout the organization covering each of the operating system types in use, including servers, workstations, and laptops. The software inventory system should track the version of the underlying operating system as well as the applications installed on it. The software inventory systems must be tied into the hardware asset inventory so all devices and associated software are tracked from a single location.	Identify	Software Application Inventory
Inventory of Authorized and Unauthorized Software	2.4	Virtual machines and/or air-gapped systems should be used to isolate and run applications that are required for business operations but based on higher risk should not be installed within a networked environment.	Protect	OS Virtualization System
		Establish standard secure configurations of your operating systems and		

TECH TV SERIES

COLLABORATE, INNOVATE, VALIDATE

CIS Top 20 Critical Security Controls

Sub-Control	Description	Control	Security Technology Controls
2.1	File Integrity monitoring	This list should be monitored by file integrity checking tools to validate that the authorized software has not been modified.	Tenable, Qualys, Rapid 7, Tripwire, Solarwinds, LogRhythm, Alienvault
2.2	Whitelisting	Deploy application whitelisting technology that allows systems to run software only if it is included on the whitelist and prevents execution of all other software	Windows (app locker, config manager, Policy PAK) Tenable, Qualys, Rapid 7, Alienvault
2.3	Inventory of Authorized Software	Perform regular scanning for unauthorized software. A change-control process should also be implemented to control any changes or installation of (executable files, DLLs, other libraries, etc.) are found	Tenable, Qualys, Rapid7
2.4	Inventory of Authorized Software	Virtual Machines should be isolated/air gapped	Vmware NSX firewalls, Virtual Box, Comodo

TECH TV SERIES

COLLABORATE, INNOVATE, VALIDATE

CIS Top 20 Critical Security Controls

CSC 2.1 Requirement: Inventory of Authorized and Unauthorized Software
CSC 2.1 Procedure: Software Inventory
The organization:
1. Departments will document and clearly define what authorized and unauthorized software are in their respective areas. 2. Departments will update the Assets inventory reports and auditors of inventory software. 3. Departments will spot check devices monthly to ensure that they are authorized
Metrics:
1. The IT department will maintain a list of whitelist & blacklisted software 2. The IT department spot check each department every 6-months

CIS Top 20 Critical Security Controls

- **CSC 2 Procedures and Tools**

- The Control requires both technical and procedural actions;
  - In order to combat this potential threat, an organization should scan a network and identify known or responding applications
  - Commercial software and Free inventory tools are widely available.
  - The best tools provide an inventory check of hundreds of common applications, pulling information about the patch level of each installed program.
  - This ensures that it is the latest version and that it leverages standardized application names, like those found in the Common Platform Enumeration (CPE) specification

CIS Top 20 Critical Security Controls

- How to start..
  - Automated asset/application inventory discovery tool
  - Create a list of authorized software/version (IoT)
  - File integrity checking tools to validate that the authorized software has not been modified.
  - Application whitelisting that allows systems to run software only if it is included on the whitelist and prevents execution of all other software on the system.
  - Vulnerability prevention tools to protect against Zeroday and unpatchables
  - Segmentation-- IoT and other "unpatchables"

CIS Top 20 Critical Security Controls

- 2-1 - *Deploy application whitelisting technology*
- **Free Tools**
  - RunAsSPC - While not an application whitelist, it can allow users to run applications which require elevation
- **Commercial Tools**
  - If you have Enterprise Edition of Windows, you can use Software Restriction Policies with AppLocker.
  - If you have Windows 8, You can use application whitelisting for child accounts.
  - PowerBroker - Powerful tool to escalate privileges and take care of pesky UNC. Solution for Windows and Linux.
  - PolicyPak - Integrates with Group Policy
  - Dell Authority Management Suite - Centralized, secure and consistent desktop management software for Windows environments.
  - Avecto - Offers Privilege Management, Application Control, and Sandboxing
  - Centrify Server Suite - Windows and Linux application and Privilege control.

CIS Top 20 Critical Security Controls

- 2-2 - *Devise a list of authorized software and version that is required in the enterprise for each type of system, including servers, workstations, and laptops of various kinds and uses. This list should be monitored by file integrity checking tools to validate that the authorized software has not been modified.*
- This item goes hand-in-hand with control 2-1. Your whitelist of software will be your list of authorized software.
- **Free Tools**
  - Spiceworks - Scans for software (Inventory > Software) but not for whitelisting or application control. Can be configured to alert you if it detects potentially unwanted software.
  - AlienVault OSSIM - Can monitor file system changes and alert you when something is accessed, changed, or tampered with.
- **Commercial Tools**
  - AlienVault USM - Commercial version of OSSIM, provides persistent logging for SIEM.
  - Tripwire - Develop secure system baselines and monitor changes to file systems.

CIS Top 20 Critical Security Controls

- 2-3 - *Perform regular scanning for unauthorized software and generate alerts when it is discovered on a system. A strict change-control process should also be implemented to control any changes or installation of software to any systems on the network.*
- **Free Tools**
  - May be able to leverage existing tools (AV, etc)
- **Commercial Software**
  - Nessus - This dashboard tracks assets that have unauthorized software installed on them. It also lists the most common types of software, services and the frequency of software installations.

CIS Top 20 Critical Security Controls

- 2-4 - *Deploy software inventory tools throughout the organization covering each of the operating system types in use, including servers, workstations, and laptops. The software inventory system should track the version of the underlying operating system as well as the applications installed on it. Furthermore, the tool should record not only the type of software installed on each system, but also its version number and patch level.*
- **Free Tools**
  - Spiceworks - does this pretty well.
- **Commercial Tools**
  - LAN Sweeper - Audit and find software, but also centrally deploy software.

CIS Top 20 Critical Security Controls

- 2-5 - *The software inventory systems must be integrated with the hardware asset inventory so that all devices and associated software are tracked from a single location.*
  - Many of the tools listed above can do this.
- 2-6 - *Dangerous file types (e.g., .exe, .zip, .msi) should be closely monitored and/or blocked.*
  - Many of the tools listed above can do this.

CIS Top 20 Critical Security Controls

- *2-7 - Virtual machines and/or air-gapped systems should be used to isolate and run applications that are required for business operations but based on higher risk should not be installed within a networked environment.*
- **Free Tools**
  - VirtualBox
  - Comodo Internet Security - Allows you to run applications within a virtual desktop and sandbox environment. How to configure.
  - Comodo Dragon - Chrome based browser, has a virtual sandbox mode.
  - Comodo Ice Dragon - Firefox based browser, has a virtual sandbox mode.

CIS Top 20 Critical Security Controls

- 2-8 - *Configure client workstations with non-persistent, virtualized operating environments that can be quickly and easily restored to a trusted snapshot on a periodic basis.*
- This control specifically states "virtual environments". While we cannot all jump to VDI, nor see the need to, these are alternatives that I believe can meet the core requirements of the control
- **Free Tools**
  - FOG - while not exactly what the control specifies, it can offer a clean slate in the need of a restore. Centralized server, based on PXE booting.
- **Commercial Tools**
  - ShadowProtect - Backup software that has the ability to revert to previous snapshots/save points across any hardware/VM platform.
  - DeepFreeze - protects endpoints by Freezing a snapshot of a workstation's desired configuration and settings set by the IT Admin. With an instant reboot, any unwelcome or unwanted changes are removed from the system, restoring it to its pristine frozen state.

CIS Top 20 Critical Security Controls

- 2-9 - *Deploy software that only provides signed software ID tags. A software identification tag is an XML file that is installed alongside software and uniquely identifies the software, providing data for software inventory and asset management.*
- **Tools**
  - Windows, Apple, Symantec

CIS Top 20 Critical Security Controls

- **CSC 2 Procedures and Tools**
- Start with an initial assessment from these tools to begin the process of realizing what software is installed and leverage them
  - Free or low-cost
    - Spiceworks
    - PDQ Inventory
    - Microsoft Intune
  - Enterprise
    - McAfee, Trend Micro, Symantec Endpoint Security
    - Microsoft System Center Configuration Manager (SCCM)
    - Tenable.io, Rapid7 Nexpose/InsightVM, Qualys

CIS Top 20 Critical Security Controls

- More tools:
- WMIC – Windows Management Instrumentation Command-line lists software on given systems (Command line Kung Fu blog)

- Psexec tool from Microsoft can perform software inventory that do not use standard Windows installer
  - @echo off
  - Psexec dir *.exe>%computername%_ExeFound.txt
  - Attack.mitre.org Great site to see, use published attack vectors for validation testing

Application Whitelisting Techniques

- Probably already available in your environment
  - Software Restriction Policies
  - Microsoft AppLocker Policies
  - AppArmor/SeLinux
- Endpoint Security Products
  - Symantec, Trend, Carbon Black, etc.

CIS Top 20 Critical Security Controls

- Now for some Enterprise type solutions..

SecurityCenter | Dashboard | Analysis | Scans | Reporting | Assets | Workflow | Users

CIS CSC: Foundational Cyber Hygiene (CSC 1,2,3,4,5)

Switch Dashboard | Options

CSC - Inventory of Authorized and Unauthorized Devices

	Last 24 Hrs	Last 72 Hrs	Last 7 Days
Active Detections	12	49	87
Passive Detections	5	7	20
Event Based Detections	73	88	103

Last Updated: Less than a minute ago

CSC - Inventory of Authorized and Unauthorized Software

	Last 24 Hrs	Last 72 Hrs	Last 7 Days
Unsupported Apps	0	0	3
Missing Patches	1	5	12
Software Installed	7	7	7

Last Updated: Less than a minute ago

CSC - Compliance Checks

	Systems	Scans (Last 7 Days)	Passed	Manual	Failed
All CIS CSC	50	✔	46%	18%	33%
All Checks	790	✔	66%	6%	28%

Last Updated: Less than a minute ago

CSC - Controlled Use of Administrative Privileges (Last 72 Hours)

New User / User Change | Privilege Change | Group Change | Group Membership Change | Admin Events

Last Updated: Less than a minute ago

CSC - New Notifications

	Last 24 Hrs	Last 72 Hrs	Last 7 Days
New Host	2	2	19
New User	0	0	0
New Software	7	7	7
New Connection	10	11	11
New Open Port	1	1	1
New Login	12	23	39

Last Updated: Less than a minute ago

Track Mitigation Progress - Vulnerability Summary by Severity

	Mitigated	Unmitigated	Exploitable	Patch Available >30d	Exploitable Hosts
Total	20075	85772	13%	80%	659
Critical	2170	2910	47%	90%	448
High	5060	55485	9%	98%	445
Medium	8027	25164	20%	78%	762
Low	195	2213	8%	88%	99

Last Updated: Less than a minute ago

Vulnerability Trend - Severity Matrix

	Total	Low	Medium	High	Critical	% Exploitable
Past 24 Hours	287	17	85	158	29	40%
Past 7 Days	1770	119	914	526	211	40%
Past 30 Days	3355	231	1738	1051	335	40%

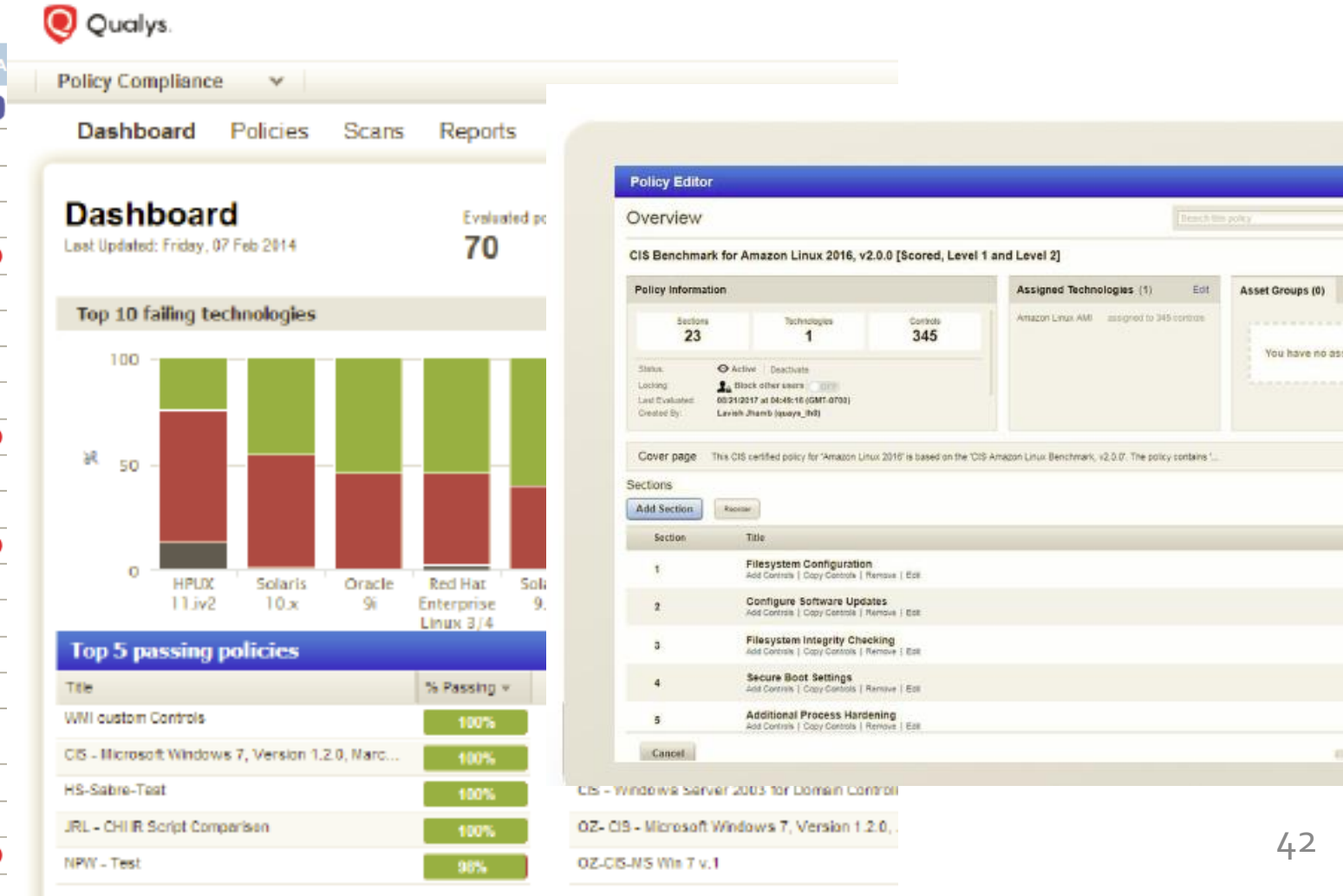
Last Updated: Less than a minute ago

CIS Top 20 Critical Security Controls

CIS Top 20 Critical Security Controls

- Now for a for a few Enterprise packages:

CSC #	CRITICAL SECURITY CONTROL	QUA					
		AI	SYN	VM	PC	TP	CM
CSC #1	Inventory of Authorized and Unauthorized Devices	✓	✓	✓	✓		
CSC #2	Inventory of Authorized and Unauthorized Software	✓	✓	✓	✓		
CSC #3	Secure Configurations for Hardware and Software				✓		
CSC #4	Continuous Vulnerability Assessment & Remediation			✓		✓	✓
CSC #5	Controlled Use of Administrative Privileges				✓		
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			✓	✓		✓
CSC #10	Data Recovery Capability				✓		
CSC #11	Secure Configurations for Network Devices			✓	✓		
CSC #12	Boundary Defense			✓	✓	✓	✓
CSC #13	Data Protection				✓		
CSC #14	Controlled Access Based on the Need to Know	✓			✓		
CSC #15	Wireless Access Control			✓	✓		
CSC #16	Account Monitoring and Control				✓		
CSC #17	Security Skills Assessment and Appropriate Training to Fill Gaps						
CSC #18	Application Software Security	✓	✓		✓		
CSC #19	Incident Response and Management				✓		
CSC #20	Penetration Tests and Red Team Exercises			✓		✓	✓



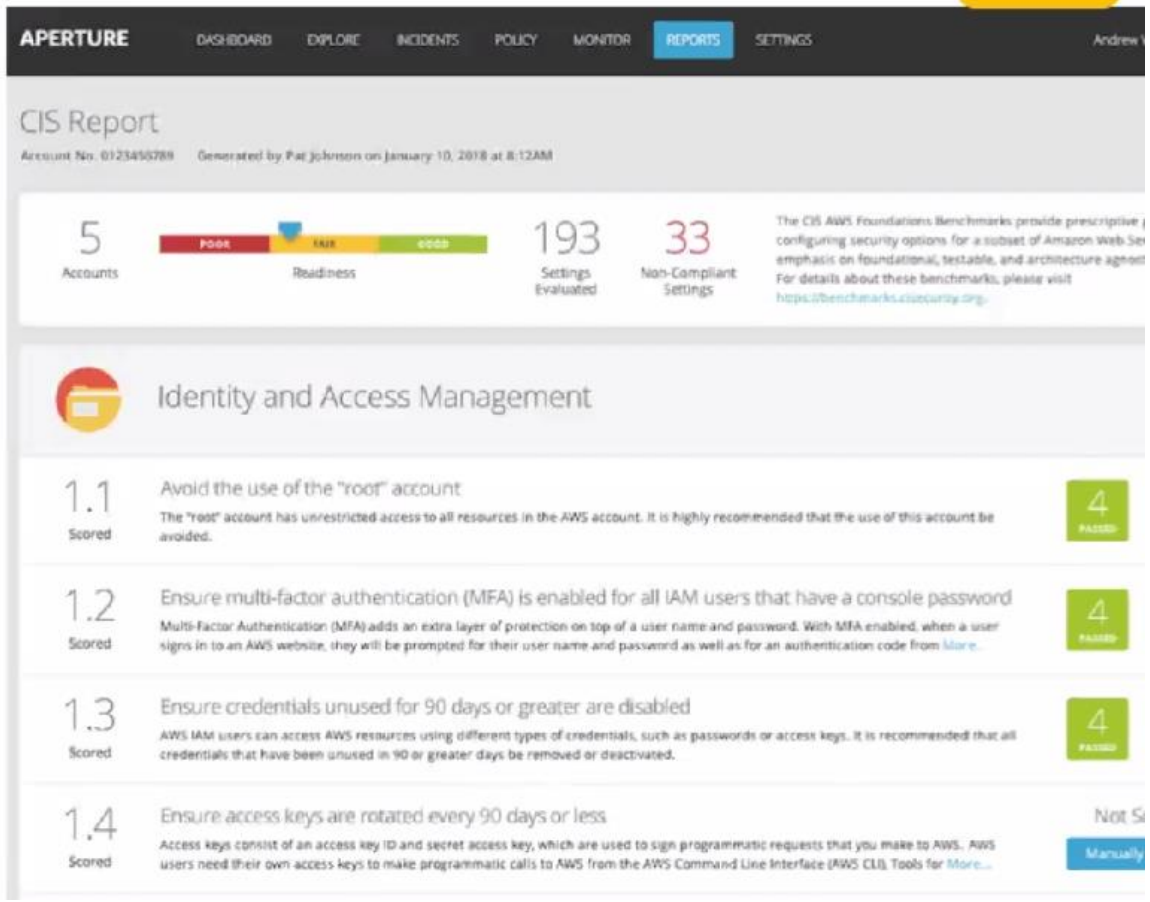
CIS Top 20 Critical Security Controls

- Even AWS is recommending the CIS

COMPLIANCE REPORTING FOR AWS

NEW

- Actively report on security compliance of cloud accounts
  - Evaluates 50+ security best practices for AWS
  - On-demand report generation from the console
  - Designed for the CIO/CISO and compliance teams
  - Interactive dashboard for SecOps & SOC team



TECH TV SERIES

COLLABORATE, INNOVATE, VALIDATE

CIS Top 20 Critical Security Controls

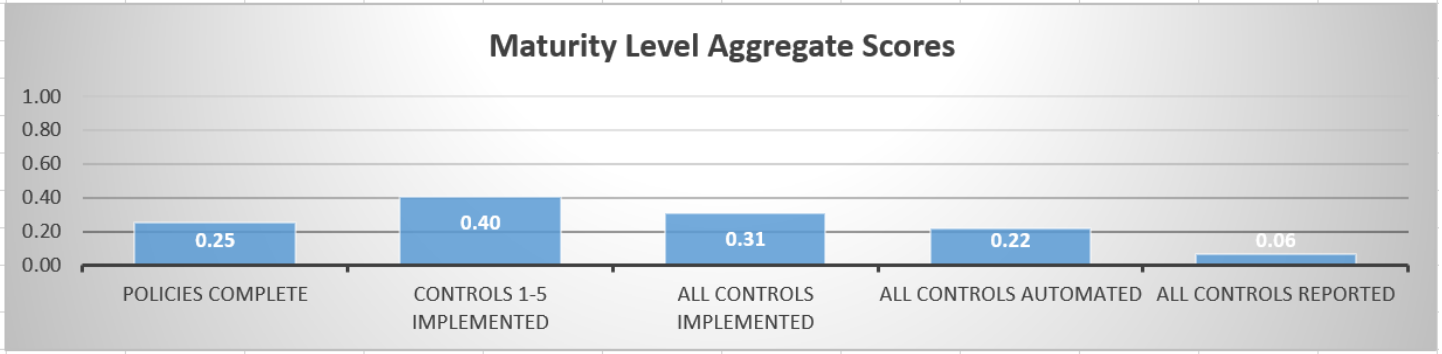
AuditScripts

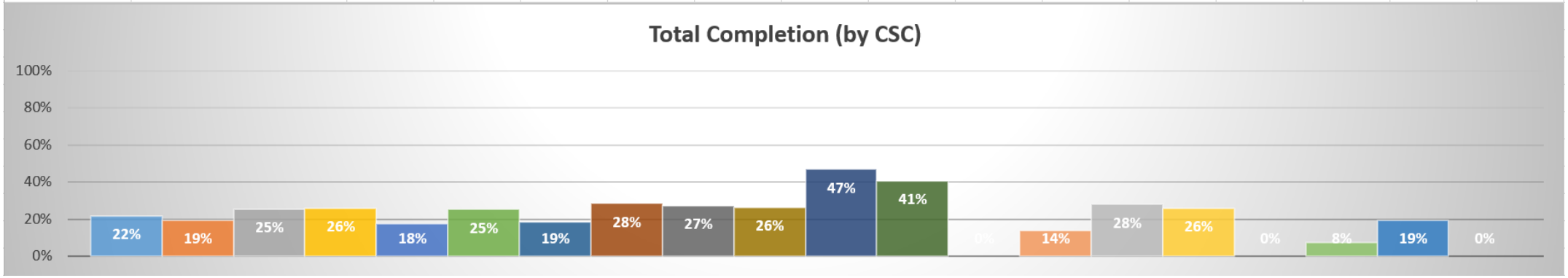
Critical Security Controls Initial Assessment Tool (v6.0a)

SECURITY enclave

Maturity level:	Desription:	Score:
Level One	Policies Complete	0.25
Level Two	Controls 1-5 Implemented	0.40
Level Three	All Controls Implemented	0.31
Level Four	All Controls Automated	0.22
Level Five	All Controls Reported	0.06
	Maturity Rating*:	**1.239**

*Rating is on a 0-5 scale.





TECH TV SERIES

COLLABORATE, INNOVATE, VALIDATE

CIS Top 20 Critical Security Controls

Tools
- Printable version
- Permanent link

Follow @MITREattack

Last 5 Pages Viewed
- Adversarial Tactics, Techniques & Common Knowledge

ATT&CK Matrix for Enterprise

The full ATT&CK Matrix below includes techniques spanning Windows, Mac, and Linux platforms and can be used to navigate through the threat models.

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Command-Line Interface	Automated Collection	Data Compressed	Communication Through Removable Media
AppCert DLLs	AppCert DLLs	Bypass User Account Control	Brute Force	File and Directory Discovery	Distributed Component Object Model	Dynamic Data Exchange	Browser Extensions	Data Encrypted	Connection Proxy
AppInit DLLs	AppInit DLLs	Clear Command History	Credential Dumping	Network Service Scanning	Exploitation of Vulnerability	Execution through API	Clipboard Data	Data Transfer Size Limits	Custom Command and Control Protocol
Application Shimming	Application Shimming	Code Signing	Credentials in Files	Network Share Discovery	Logon Scripts	Execution through Module Load	Data Staged	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Authentication Package	Bypass User Account Control	Component Firmware	Exploitation of Vulnerability	Peripheral Device Discovery	Pass the Hash	Graphical User Interface	Data from Local System	Exfiltration Over Command and Control Channel	Data Encoding
Bootkit	DLL Search Order Hijacking	Component Object Model Hijacking	Forced Authentication	Permission Groups Discovery	Pass the Ticket	InstallUtil	Data from Network Shared Drive	Exfiltration Over Other Network Medium	Data Obfuscation

TECH TV SERIES

COLLABORATE, INNOVATE, VALIDATE

CIS Top 20 Critical Security Controls

#	CIS Critical Security Controls	Customer solution?	Budgeted 2018?	Reviewed solutions?	SynerComm Solutions
1	Inventory of Authorized and Unauthorized Devices				Tenable, Qualys, Infoblox, Forescout
2	Inventory of Authorized and Unauthorized Software				Tenable, Qualys, Infoblox, Carbonblack
3	Secure Configuration of end-user devices				Tenable, Rapid7
4	Continious Vulnerability & remediation				Qualys, Tenable, Rapid7
5	Controlled Use of Administrative priviledges				Centrify, CyberArk, BeyondTrust, Okta
6	Maintenance, Monitoring and Analysis of Audit Logs				SolarWinds, Log Rhythum
7	Email and Web Browser Protection				Barracuda, Proofpoint, zScaler, Fireeye (Web - Palo, Checkpoint, Forcepoint)
8	Malware Defense				Bitdefender, carbonblack, PaloAlto TRAPS, Sophos, TrendMicro
9	Limitation & Control of network Ports, protocols, and Service				PaloAlto, Juniper, Checkpoint, Fortinet
10	Data Recovery Capability				Barracuda
11	Secure Configuration of Network Devices				SynerComm Config Assurance, A&A, Firemon, RedSeal, Tenable, Rapid7
12	Boundry Defense				PaloAlto, Juniper, Checkpoint, Fortinet
13	Data Protection				Rapid7, tenable, Imperva, Infoblox, PaloAlto
14	Controlled Access Based on Need to Know				Centrify , OKTA
15	Wireless Access Control				Aerohive with 802.1x & WIPS/FW
16	Account Monitoring and Control				Centrify, Beyond Trust, OKTA,
17	Security Skills Assessment and Appropriate Training				A&A training
18	Application Software Security				Rapid7, Splunk
19	Incident Response and Management				Rapid7, redseal, A&A
20	Penetration Tests and Red Team Exercises				A&A

CIS Top 20 Critical Security Controls

- Center for Internet Security (CIS): https://www.cisecurity.org/
- NIST Cyber Security Framework (CSF): http://www.nist.gov/cyberframework/
- CIS Critical Security Controls (CSC): https://www.cisecurity.org/critical-controls.cfm
- Auditscripts resources (provided by James Tarala, CSC Editor): https://www.auditscripts.com/free-resources/critical-security-controls/
- CSF planning spreadsheet: http://www.tenable.com/whitepapers/nist-csf-implementation-planning-tool

CIS Top 20 Critical Security Controls

- CISsecurity.org JOIN!!

TECH TV SERIES

COLLABORATE, INNOVATE, VALIDATE

CIS Top 20 Critical Security Controls

The SANS Best of Awards are not driven by vendors, but by the people actually using these products. The Awards are an extension of the SANS WhatWorks Program which creates awareness of security programs and solutions that are actually being used to stop bad guys and improve security. The 2016 winners can be found below.

The Best of 2016 Award winners and Honorable Mentions

Vulnerability Assessment

Winner:
Tenable Nessus

Honorable Mention:
Rapid7
Qualys

Next Generation Firewall

Winner:
Palo Alto Networks PA Series

Honorable Mention:
CheckPoint Software
Fortinet

Advanced Threat Detection

Winner:
FireEye Intrusion NX

Honorable Mention:
Snort
Cisco

End Point Protection

Winner:
Cylance Protect

Honorable Mention:
Symantec
Trend Micro

Application Security

Winner:
Qualys WAS

Honorable Mention:
Rapid7
Checkmarx (tie)
Veracode (tie)

SIEM

Winner:
LogRhythm Security Intelligence Platform

Honorable Mention:
Splunk
IBM

Threat Intelligence

Winner:
Crowdstrike Falcon Intelligence

Honorable Mention:
FireEye Threat Intelligence
Cisco ThreatGrid

Endpoint Detection/Response

Winner:
Carbon Black Platform

Honorable Mention:
Palo Alto Network Traps
CounterTack Sentinel

TECH TV SERIES

COLLABORATE, INNOVATE, VALIDATE

CIS Top 20 Critical Security Controls

Thank you for Attending.

Hope you can join us for the Complete CIS Top 20 CSC