Tech TV Series

COLLABORATE, INNOVATE, VALIDATE

CIS Top 20 #3 Secure Configuration of Hardware and Software

Lisa Niles – CISSP, Chief Solution Architect

TECH TV SERIES

COLLABORATE, INNOVATE, VALIDATE

CIS Top 20 Critical Security Controls

- Critical Governance and the CIS Critical Security Controls

CIS Top 20 Critical Security Controls

- How the CIS Critical Security Controls can help?

CIS Top 20 Critical Security Controls

- Sample:
- Governance item #1: *Manage the known cyber vulnerabilities of your information and make sure the necessary security policies are in place to manage the risk.*
  - *At a minimum, you should be able to identify and manage the large volume of known flaws and vulnerabilities found in information technology and processes. The flowing CIS Critical Security Controls are the primary means to establish a baseline of responsible practices that can be measured, managed and reported.*
  - *CSC3: Secure Configurations of Hardware and Software*
  - *CSC#4: Continuous Vulnerability Assessment and Remediation*

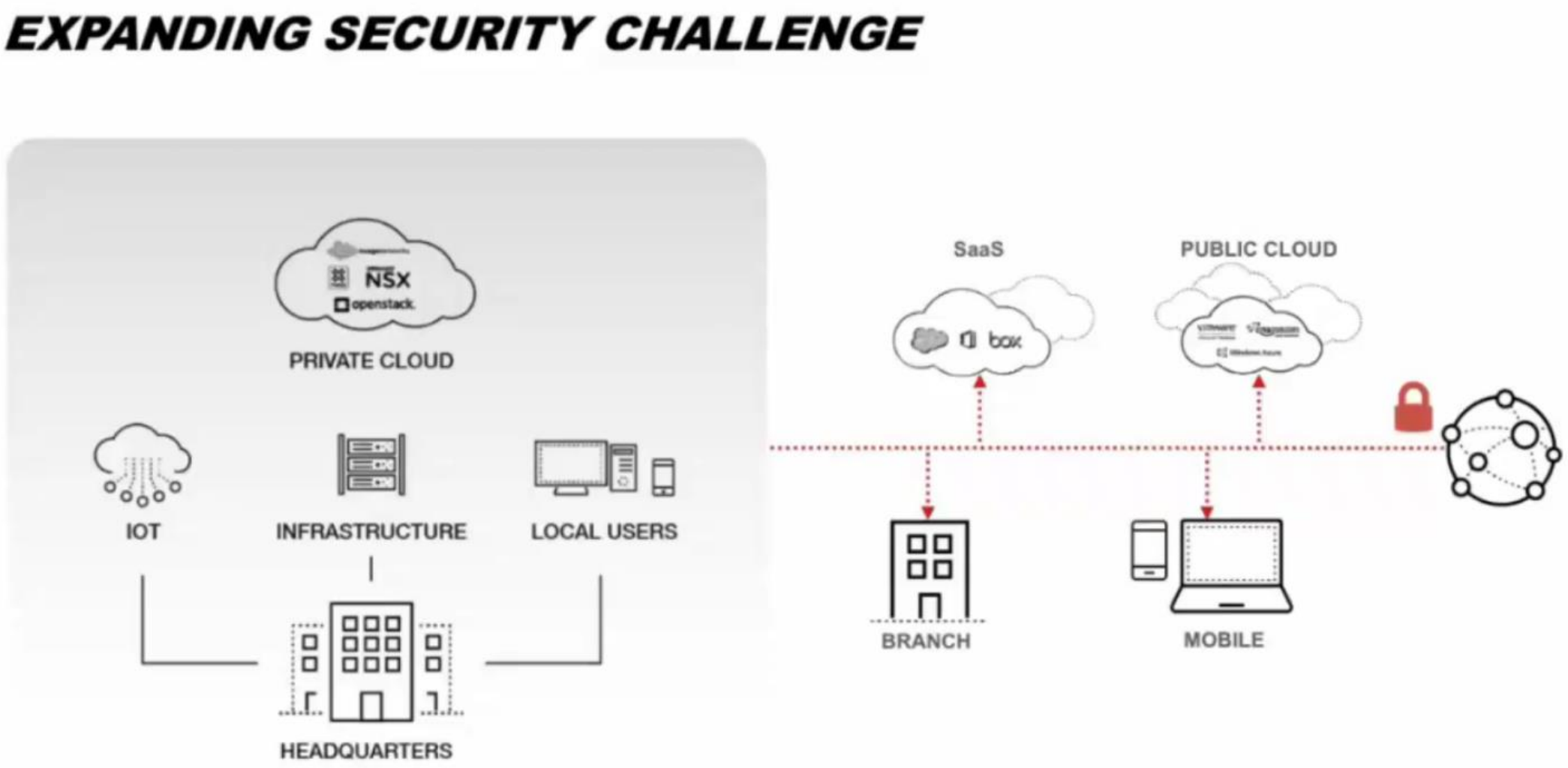
CIS Top 20 Critical Security Controls

- CIS CSC focus on various technical aspects of information security
- Outside of the technical realm, a comprehensive security program should also take into account:
  - Numerous additional areas of security
    - Policies
    - Procedures
    - Process
    - Organizational structure
    - Physical security.

CIS Top 20 Critical Security Controls

- What am I trying to protect?
- Where are my gaps?
- What are my priorities?
- Where can I automate?

CIS Top 20 Critical Security Controls



CIS Top 20 Critical Security Controls

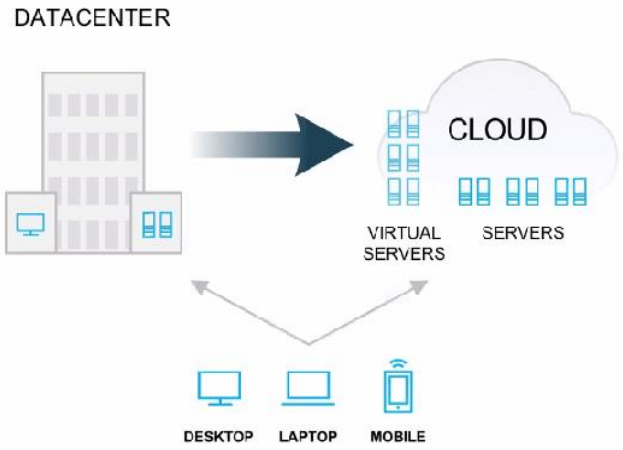
Confluence of Macro Trends Creating Visibility Challenges

Growth of Devices and Platform Diversity

- 28Bn IP-based devices by 2020

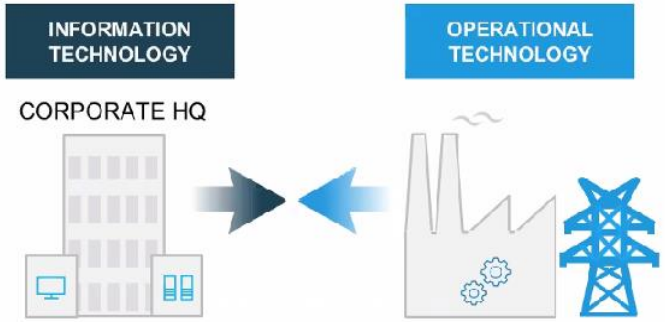
- Innumerable device-specific operating systems (OS)
- Cannot get agents onto new devices
- Cannot write agent-based software for every OS

Cloud Adoption Creates New Challenges



- Multiple Device Locations and Access Points
- Heterogeneous Environment with Multiple Vendors
- De-centralized Management

IT and OT Convergence



- INDUSTRIAL CONTROL SYSTEMS
- CRITICAL INFRASTRUCTURE

- OT networks are no longer physically separated
- Threats moving between cyber and physical dimensions
- Assets are highly vulnerable and rarely can be patched

CIS Top 20 Critical Security Controls

Implementing the Controls:

- Carefully plan
- Organizational structure
- "Governance, Risk, and Compliance (GRC)" program.
- Program managers

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

TECH TV SERIES

COLLABORATE, INNOVATE, VALIDATE

CIS Top 20 Critical Security Controls

Who are you?	Who owns your device?	What type of device?	Where/how are you connecting?	What is the device hygiene?
• Employee • Partner • Contractor • Guest	• Corporate • BYOD • Rogue	• Windows, Mac • iOS, Android • VM • Non-user devices, IoT	• Switch/ • Port/PoE • Wireless/Controller • VPN • IP, MAC • VLAN	• Configuration • Software • Services • Patches • Security Agent

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 #3**
- Secure Configuration of Hardware and Software
- Key Principle Control:
  - Establish, implement, and actively manage (track, report on, correct) the security configuration of laptops, servers, workstations, mobile devices using rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

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

Why is CIS Control 3 critical?

- CSC #3 is all about preventing exposure due to misconfiguration.

Most Breaches are Preventable

97% of breaches are avoidable through standard controls*

- No **visibility** of the environment
- Lack of **actionable intelligence**
- **Disjointed** security tools and data
- Lack of cross-functional **expertise**

Organizations don't understand their attack surface

*According to Verizon Data Breach Investigation Report

TECH TV SERIES

COLLABORATE, INNOVATE, VALIDATE

CIS Top 20 Critical Security Controls

System	3.1	Establish standard secure configurations of your operating systems and software applications. Standardized images should represent hardened versions of the underlying operating system and the applications installed on the system. These images should be validated and refreshed on a regular basis to update their security configuration in light of recent vulnerabilities and attack vectors.
System	3.2	Follow strict configuration management, building a secure image that is used to build all new systems that are deployed in the enterprise. Any existing system that becomes compromised should be re-imaged with the secure build. Regular updates or exceptions to this image should be integrated into the organization's change management processes. Images should be created for workstations, servers, and other system types used by the organization.
System	3.3	Store the master images on securely configured servers, validated with integrity checking tools capable of continuous inspection, and change management to ensure that only authorized changes to the images are possible. Alternatively, these master images can be stored in offline machines, air-gapped from the production network, with images copied via secure media to move them between the image storage servers and the production network.
System	3.4	Perform all remote administration of servers, workstation, network devices, and similar equipment over secure channels. Protocols such as telnet, VNC, RDP, or others that do not actively support strong encryption should only be used if they are performed over a secondary encryption channel, such as SSL, TLS or IPSEC.
System	3.5	Use file integrity checking tools to ensure that critical system files (including sensitive system and application executables, libraries, and configurations) have not been altered. The reporting system should: have the ability to account for routine and expected changes; highlight and alert on unusual or unexpected alterations; show the history of configuration changes over time and identify who made the change (including the original logged-in account in the event of a user ID switch, such as with the su or sudo command). These integrity checks should identify suspicious system alterations such as: owner and permissions changes to files or directories; the use of alternate data streams which could be used to hide malicious activities; and the introduction of extra files into key system areas (which could indicate malicious payloads left by attackers or additional files inappropriately added during batch distribution processes).
System	3.6	Implement and test an automated configuration monitoring system that verifies all remotely testable secure configuration elements, and alerts when unauthorized changes occur. This includes detecting new listening ports, new administrative users, changes to group and local policy objects (where applicable), and new services running on a system. Whenever possible use tools compliant with the Security Content Automation Protocol (SCAP) in order to streamline reporting and integration.
System	3.7	Deploy system configuration management tools, such as Active Directory Group Policy Objects for Microsoft Windows systems or Puppet for UNIX systems that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals. They should be capable of triggering redeployment of configuration settings on a scheduled, manual, or event-driven basis.

TECH TV SERIES

COLLABORATE, INNOVATE, VALIDATE

CIS Top 20 Critical Security Controls

CSC 3.1 Establish standard secure configurations of your operating systems and software applications. Standardized images should represent hardened versions of the underlying operating system and the applications installed on the system. These images should be validated and refreshed on a regular basis to update their security configuration in light of recent vulnerabilities and attack vectors.
CSC 3.1 Procedure: Standardize configuration of operating system.
The organization:
1. IT department to build hardened OS configuration data base. 2. IT department will update hardened configurations as high risk vulnerabilities are identified. 3. IT department will push confirmation updates out to active devices
Metrics:
1. The IT department will maintain a list hardened configurations 2. The IT department will audit configurations monthly.

CIS Top 20 Critical Security Controls

- **CSC 3 Procedures and Tools**
- Start with publicly developed, vetted, supported benchmarks, security guides or checklists:
  - CISecurity.org
  - NIST (checklists.nist.gov)
  - DISA STIG's
- Many tools available to measure (agent or agentless)

CIS Top 20 Critical Security Controls

- How to start..
  - Automated discovery tool (MBSA) for Windows
  - Use you CSC #1 & #2 inventories
    - Network devices (Firewalls, switches, routers, wifi)
  - Create system baselines (CISecurity.org)

TECH TV SERIES

COLLABORATE, INNOVATE, VALIDATE

CIS Top 20 Critical Security Controls

Skybox - Access Analyzer

Access Query

Source

Scope: 0.0.0.0 / 0 - Internet

Destination

Scope: 10.170.27.0 / 24 - Finance

Services & Applications: Any

Filter By

Advanced

Analyze

Analysis Results

Show: Blocked Destinations

Group By: Network

Locations & Networks [256 IPs; Any protocol]

FinanceServers (10.170.27.0 / 24) [256 IPs; Any protocol]

10.170.27.0-10.170.27.255 [256 IPs; Any protocol]

Any Internet Protocol

Routes

View

Current Map

Route Map

Show Route Map

Default Settings

Detail Level: Display all blocking rules

Show Routing Rules

Access Route

From Internet (cloud) To FinanceServers (10.170.27.0/24)

(maximal number of routes (1) is reached)

#	Step	Inbound Access Rules	Outbou Access Rules
	Source: Internet (cloud) Source IP range(s) 200.160.3.1-200.160.3.1 Sending To IP range(s): 192.170.27.11-192.170.27.11 Sending to service(s): 80/TCP		
1.	main_FW (16.0.0.1)	1 (ACCESS) - Deny	17 (ACCES - Allow
2.	Main Router (192.169.1.2)		
3.	Core Router (192.170.8.4)		
4.	finance FW (192.170.1.65)	6 (ACCESS) - Deny	
5.	Finance Router (192.170.1.82)		
6.	BigIP Load Balancer (192.170.27.254)	9 (ACCESS) - Translate Destination IP: 192.170.27.11 => 10.170.27.11	
	[Blocked] Destination:		

Cloud

Azure

Azure - Test

Azure - Prod

AWS

AWS-Customers

AWS-Prod

AWS-Dev

US

Los Angeles

New York

Europe

London

NSX

Paris

Branches

Lab

Access Query

TECH TV SERIES

COLLABORATE, INNOVATE, VALIDATE

CIS Top 20 Critical Security Controls

Skybox - Network Assurance

File Edit View Tools Section Help

Address: Network Assurance ▸ Access Policies ▸ Public Access Policies (89%) ▸ NIST 800-41 Policy (88%) ▸ NIST Internal Access (81%) ▸ NIST-Internal to DMZ (17%)

Network Assurance

- Network Assurance
  - Access Policies
    - Public Access Policies (89%)
      - NIST 800-41 Policy (88%)
        - NIST External Access (94%)
        - NIST Partner Access (95%)
        - NIST DMZ Access (99%)
        - NIST Internal Access (81%)
          - NIST-Internal to External (67%)
          - NIST-Internal to Partner (72%)
          - NIST-Internal to DMZ (17%)
            - Block ICMP Replying Messages (17%)
            - Block Login Services (17%)
            - Block Miscellaneous (17%)
            - Block RPC and NFS (17%)
            - Block Small Services (17%)
            - Block Trojan and Worm Ports (17%)
            - Block X-Windows (17%)
            - Limited Access - non-specified services- (50 Dest IPs) (17%)
            - Limited Access - Services(10 ports) (17%)
          - NIST-Internal to Internal (97%)
      - NIST 800-41 & Application Policy (89%)
      - PCI DSS V3.1 Policy
      - NSX Access Queries
    - Private Access Policies [skybox view]
    - Access Policy Violations
    - Zones
  - Configuration Policies
  - All Network Devices
  - Analyses

Firewall Assurance | Network Assurance | Tickets | Reports | Model

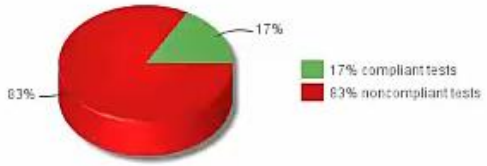
NIST-Internal to DMZ (17%)

Access Policy Section | Access Checks | Violations | All Access Tests | Violating Rules | Exceptions

NIST-Internal to DMZ - 17% Compliance

6 Violating Rules (6 M)

Analyzed: 11/14/16 11:09 PM



	Info	Low	Medium	High	Critical	Overall
Compliant Tests	0	0	9	0	0	9
Noncompliant Tests	0	0	45	0	0	45
Overall	0	0	54	0	0	54

Block ICMP Replying Messages	ICMP replying messages between Internal Servers zone and DMZ zone should be blocked. According to NIST publication 800-41, ICMP replying messages (e.g. Echo Reply) should not be allowed between network zones of different security levels. ICMP replying messages can be used as part of a network reconnaissance, which is the basis for cyber attacks.	17% Compliance
Block Login Services	Login services between Internal Servers zone and DMZ zone should be blocked. According to NIST publication 800-41, login services (e.g. Telnet, SSH) should not be allowed between network zones of different security levels. Login services enable remote administration, and should be allowed from trusted sources only.	17% Compliance
Block Miscellaneous	Miscellaneous services between Internal Servers zone and DMZ zone should be blocked. According to NIST publication 800-41, this group of services should not be allowed between network zones of different security levels, as these services are known to have a large number of vulnerabilities.	17% Compliance
Block RPC and NFS	RPC and NFS services between Internal Servers zone and DMZ zone should be blocked. According to NIST publication 800-41, RPC and NFS services should not be allowed between network zones of different security levels, as these services are known to have a large number of vulnerabilities.	17% Compliance
Block Small Services	Small services between Internal Servers zone and DMZ zone should be blocked. According to NIST publication 800-41, Small Services group should not be allowed between network zones of different security levels, as they are known to have a large number of vulnerabilities.	17% Compliance
Block Trojan and Worm Ports	Trojan and Worm ports between Internal Servers zone and DMZ zone should be blocked. This group of ports is known to be used by worms and Trojans; according to NIST publication 800-41, it should be blocked.	17% Compliance
Block X-Windows	X-Windows services between Internal Servers zone and DMZ zone should be blocked. According to NIST publication 800-41, the X-Windows service should not be allowed between network zones of different security levels. X-Windows service enables remote administration, and should be allowed from trusted sources only.	17% Compliance
Limited Access - non-specified services		17% Compliance
Limited Access - Services	Access between Internal Servers zone and DMZ zone should not exceed the limit of 10 destination ports. According to network design best practices, it is	17%

No running tasks | User Name: skyboxview | Server: 192.168.20.105:8443

CIS Top 20 Critical Security Controls

- 3-1 *Establish and ensure the use of standard secure configurations of your operating systems.*
- **Free Tools**
- DISA STIGs - DoD recommended secure systems baselines including phones, applications, OSes, network devices, etc…
- MBSA - assessing missing security updates and less-secure security settings within Microsoft Windows
- Cisecurity.org Baselines, hardening guides and templates.
- **Commercial Tools**
- Qualys - Policy Compliance – automatic tech control assessment across network ***Also available for cloud resources
- skybox - Policy Compliance, firewall audit, network map andmodeling

CIS Top 20 Critical Security Controls

- *3-2 Follow strict configuration management, building a secure image that is used to build all new systems that are deployed in the enterprise.*
- **Free Tools**
- Cisecurity.org Baselines, hardening guides and templates.
- FOG - Free and Open Source imaging from a central server based on Linux.
- **Commercial Tools**
- Deep Freeze - Build a clean image, revert to it easily with a reboot.
- ManageEngine OS Deployer

CIS Top 20 Critical Security Controls

- *3-3 Store the master images on securely configured servers, validated with integrity checking tools capable of continuous inspection, and change management to ensure that only authorized changes to the images are possible.*
- **Free Tools**
- FOG - Free and Open Source imaging from a central server based on Linux.
- **Commercial Tools**
- Deep Freeze - Build a clean image, revert to it easily with a reboot.
- ManageEngine OS Deployer-OS Deployer automates the disk imaging and deployment process
- Avecto - Offers Privilege Management, Application Control, and Sandboxing

CIS Top 20 Critical Security Controls

- *3-4 Do all remote administration of servers, workstation, network devices, and similar equipment over secure channels.*
- This is referring to protocols, such as RDP, SSH, etc…
- **Free Tools**
- MRemoteNG - All-in-one for remote access. does NOT support encrypted VNC.
- UltraVNC - Offers a server and client which can provide encrypted VNC
- **Commercial Tools**
- RealVNC - Feature rich VNC server/client
- RemoteDesktopManager - Feature rich RDP client
- Centrify - Secure and manage super user, service, and application accounts on servers and network devices, both on-premises and in the cloud.

CIS Top 20 Critical Security Controls

- *3-5 Utilize file integrity checking tools to ensure that critical system files (including sensitive system and application executables, libraries, and configurations) have not been altered…*
- This is basically referring to a HIDS.
- **Free Tools**
- AlienVault OSSIM - HIDS, SEIM, Inventory, Service Monitor, and more.
- OSSEC - used in OSSIM, it is just the HIDS portion.
- OpenHIDS - Windows only
- **Commercial Tools**
- Tripwire - heterogeneous server monitoring across Windows, Linux, Solaris, AIX and HP-UX platforms.

CIS Top 20 Critical Security Controls

- *3-6 Implement and test an automated configuration monitoring system that measures all secure configuration elements that can be measured through remote testing using features such as those included with tools compliant with Security Content Automation Protocol (SCAP), and alerts when unauthorized changes occur.*
- **Free Tools**
- AlienVault OSSIM - HIDS, SEIM, Inventory, Service Monitor, and more.
- OSSEC - used in OSSIM, it is just the HIDS portion.
- OpenHIDS - Windows only
- SCM – Microsoft's Security Compliance manager
- nmap –Security Scanner, Port Scanner, & Network Exploration Tool.
- **Commercial Tools**
- ForeScout - **see** devices, **control** them and **orchestrate** system-wide wired and wireless campus, data center, cloud and operational technology deployments without agents.
- Qualys – Unparalleled visibility and control of all your assets
- Skybox – as mentioned earlier

CIS Top 20 Critical Security Controls

- *3-7 Deploy system configuration management tools, such as Active Directory Group Policy Objects for Microsoft Windows systems or Puppet for UNIX systems that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals.*
- **Free Tools**
- Salt - Meant for deploying change management to ANY scale. Great for cloud deployments with OpenStack.
- Puppet - GPMC for Linux. Kind of.
- **Commercial Tools**
- Chef - The Chef client is installed on each server, virtual machine, container, or networking device you manage. The client periodically polls Chef server latest policy and state of your network. If anything on the node is out of date, the client brings it up to date.
- Ansible - Deploy apps. Manage systems. Centrally managed.

CIS Top 20 Critical Security Controls

Security camera

Windows PC

NOTIFY

- Open trouble ticket
- Send email notification
- SNMP Traps
- Start application
- Run script to install application
- Auditable end-user acknowledgement
- HTTP browser hijack
- Trigger endpoint management system

COMPLY

- Deploy a virtual firewall
- Reassign the device to a VLAN
- Update access lists
- DNS hijack (captive portal)
- Move device to a guest network

RESTRICT

- Move device to quarantine VLAN
- Block access with 802.1x
- Alter login credentials to block access
- Block access with device authentication
- Turn off switch port (802.1X, SNMP)
- Wi-Fi port block
- Terminate applications
- Disable peripheral device

TECH TV SERIES

COLLABORATE, INNOVATE, VALIDATE

CIS Top 20 Critical Security Controls

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	3	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	✓	48%	18%	33%
All Checks	750	✓	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%	90%	659
Critical	2170	2910	47%	90%	448
High	9060	55485	9%	96%	445
Medium	8027	25164	20%	79%	762
Low	195	2213	8%	89%	99

Last Updated: Less than a minute ago

Vulnerability Trend - Severity Matrix

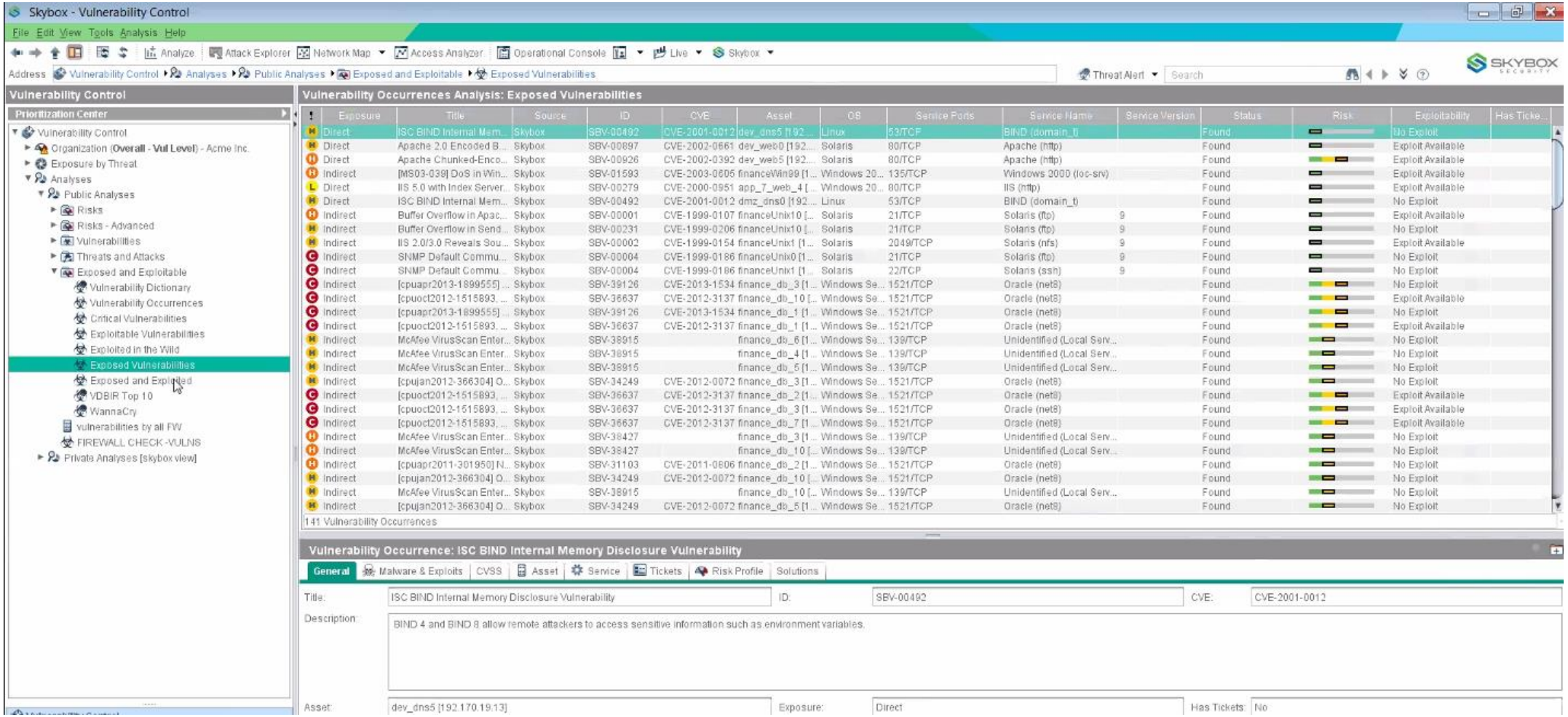
	Total	Low	Medium	High	Critical	% Exploitable
Past 24 Hours	287	17	85	156	29	49%
Past 7 Days	1770	119	914	526	211	40%
Past 30 Days	3355	231	1738	1051	335	40%

Last Updated: Less than a minute ago

TECH TV SERIES

COLLABORATE, INNOVATE, VALIDATE

CIS Top 20 Critical Security Controls



TECH TV SERIES

COLLABORATE, INNOVATE, VALIDATE

CIS Top 20 Critical Security Controls

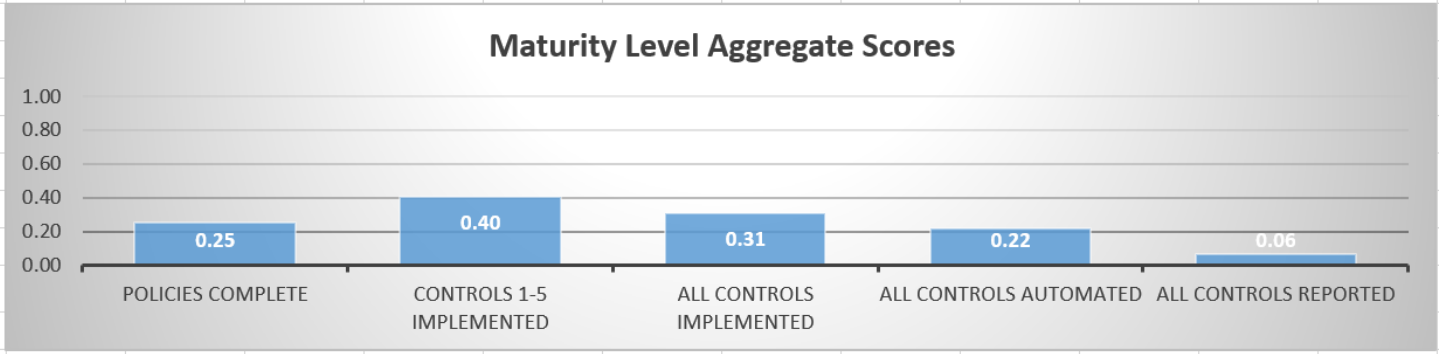
AuditScripts

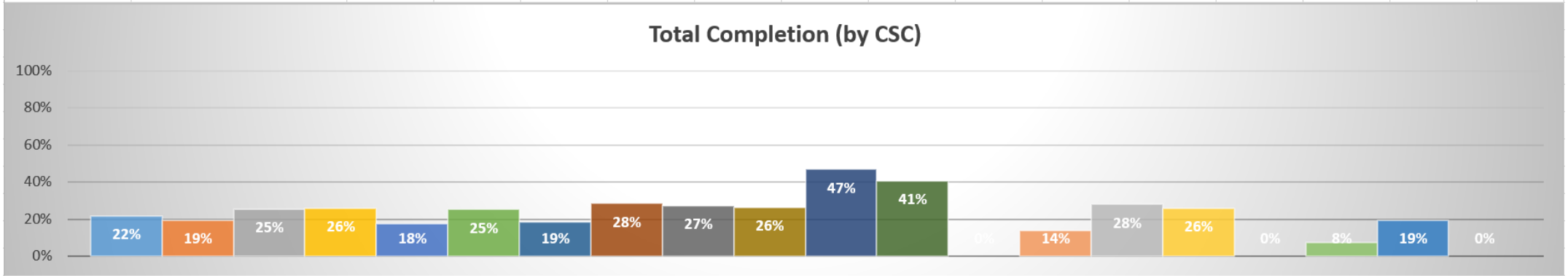
Critical Security Controls Initial Assessment Tool (v6.0a)

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.





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/
- STIG https://iase.disa.mil/stigs/Pages/index.aspx

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

Tuesday March 6th

CIC CSC #4 – Continuous Vulnerability & Remediation