Implementing the CIS critical security controls: Using university-sponsored solutions when possible and other solutions when necessary

Eric White

University of Wisconsin Survey Center

University of Wisconsin-Madison

IT Professionals Conference 2017

June 22, 2017

UWSC
UNIVERSITY of WISCONSIN
SURVEY CENTER

Two Questions

1. What tools does campus make available to help departments implement the CIS top 20 security controls?
2. How do current Survey Center security practices compare to the CIS top 20 controls?

Descriptive not Prescriptive

1. Identifying current tools, procedures, and policies that work for UWSC
2. Other tools and solutions may be a better fit for you

Survey Center Data and Device Security

Data

- Phone, mail, web, apps, focus groups, in-person surveys
- Tens of thousands of human subjects
- Millions of individual data points
- Data must be secured through the research lifecycle

Devices

- 250 devices
  - 125 Windows PCs & servers
  - 75 Windows laptops
  - 25 Android tablets
  - 25 phones (Android and iOS)

SANS / CIS Top 20 Security Controls

- Established in 2008
- Current version is 6.1
- Designed to give you most return on investment
  - Pareto Principle: 80% of the impact comes from 20% of the effort
- In 2013 per Australian Signals Directorate
  - 85% of cyber intrusions prevented by implementation of top 4 SANS controls[1]

[1] https://www.asd.gov.au/infosec/mitigationstrategies.htm

CIS Top 20 Critical Security Control 1

Inventory of Authorized and Unauthorized Devices

Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are identified and prevented from gaining access

Campus-sponsored tools

- AANTS, Nessus, Qualys, BigFix, AirWatch MDM pilot, Apple Device Enrollment Program (DEP) MDM

UWSC implementation

- AANTS, Qualys, Nessus, BigFix, AirWatch MDM, Lansweeper

CIS Top 20 Critical Security Control 2

Inventory of Authorized and Unauthorized Software

Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and unauthorized and unmanaged software is located and prevented from installation or execution.

Campus-sponsored tools

- BigFix, Qualys, Symantec Endpoint Protection whitelisting, Cisco AMP pilot, AirWatch, Apple DEP

UWSC implementation

- Qualys, Lansweeper, AirWatch, Cisco AMP

CIS Top 20 Critical Security Control 3

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

Establish, implement, and actively manage (track, report on, and correct) the security configuration of laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

Campus-sponsored tools

- CIS Benchmarks

UWSC implementation

- CIS Benchmarks, documenting exceptions

CIS Top 20 Critical Security Control 4

Continuous Vulnerability Assessment and Remediation

Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, and to remediate and minimize the window of opportunity for attackers.

Campus-sponsored tools

- Qualys, Nessus, BigFix, SSL Labs scans

UWSC implementation

- Qualys, Nessus, BigFix, Ninite, WSUS

CIS Top 20 Critical Security Control 5

Controlled Use of Administrative Privileges

Track, control, prevent, and correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.

Campus-sponsored tools

- Unknown / LAPS for domain-joined Windows PCs

UWSC implementation

- UWSC Policy, Lansweeper reports

CIS Top 20 Critical Security Control 6

Maintenance, Monitoring, and Analysis of Audit Logs

Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.

Campus-sponsored tools

- CIS benchmarks, QRadar SEM

UWSC implementation

- CIS benchmarks re. log collection and retention

CIS Top 20 Critical Security Control 7

Email and Web Browser Protections

Minimize the attack surface and the opportunities for attackers to manipulate human behavior through their interaction with web browsers and email systems.

Campus-sponsored tools

- Office 365

UWSC implementation

- Browser and application updates via BigFix and Ninite
- Training

CIS Top 20 Critical Security Control 8

Malware Defenses

Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action.

Campus-sponsored tools

- Symantec Endpoint Protection (SEP), Cisco AMP pilot, Palo Alto TRAPS pilot

UWSC implementation

- SEP, AMP pilot, Malwarebytes

CIS Top 20 Critical Security Control 9

Limitation and Control of Network Ports, Protocols, and Services

Manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.

Campus-sponsored tools

- AANTS, CIS benchmarks, Nessus, Qualys

UWSC implementation

- AANTS, CIS benchmarks, Nessus, Qualys

CIS Top 20 Critical Security Control 10

Data Recovery Capability

The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.

Campus-sponsored tools

- BuckyBackup, Cristi BMR

UWSC implementation

- BuckyBackup, Macrium

CIS Top 20 Critical Security Control 11

Secure Configurations for Network Devices such as Firewalls, Routers, and Switches

Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

Campus-sponsored tools

- Default configuration, AANTS, change management?

UWSC implementation

- Change management for firewall rules using departmental ticketing system

CIS Top 20 Critical Security Control 12

Boundary Defense

Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.

Campus-sponsored tools

- Co-managed firewalls, WiscVPN, Symantec Network Protection module (IPS), continuous monitoring

UWSC implementation

- Co-managed firewalls, WiscVPN, Symantec Network Protection module (IPS)

CIS Top 20 Critical Security Control 13

Data Protection

The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.

Campus-sponsored tools

- Identity Finder, BitLocker, G Suite, Box

UWSC implementation

- Identify Finder, G Suite, Box, AxCrypt, McAfee Endpoint Encryption

CIS Top 20 Critical Security Control 14

Controlled Access Based on the Need to Know

The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.

Campus-sponsored tools

- Unknown

UWSC implementation

- NTFSReports tool, combination of OUs, NTFS rights, and policy

CIS Top 20 Critical Security Control 15

Wireless Access Control

The processes and tools used to track, control, prevent, and correct the security use of wireless local area networks (LANS), access points, and wireless client systems.

Campus-sponsored tools

- Nessus, Qualys, CIS benchmarks, BigFix, AirWatch, Apple DEP, UWNet

UWSC implementation

- Nessus, Qualys, CIS benchmarks, BigFix, AirWatch, UWNet

CIS Top 20 Critical Security Control 16

Account Monitoring and Control

Actively manage the life cycle of system and application accounts – their creation, use, dormancy, deletion – in order to minimize opportunities for attackers to leverage them.

Campus-sponsored tools

- NetID expiration policy

UWSC implementation

- Work with business office re. start and end dates
- Application-specific account management should be added to this workflow

CIS Top 20 Critical Security Control 17

Security Skills Assessment and Appropriate Training to Fill Gaps

For all functional roles in the organization (prioritizing those mission-critical to the business and its security), identify the specific knowledge, skills, and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs.

Campus-sponsored tools

- Ad hoc IT security training & awareness opportunities

UWSC implementation

- Ad hoc IT security training & awareness opportunities

CIS Top 20 Critical Security Control 18

Application Software Security

Manage the security life cycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses.

Campus-sponsored tools

- Qualys, Nessus, BigFix, Watchfire Web Application Vulnerability Scan

UWSC implementation

- Qualys, Nessus, BigFix, Watchfire, ad hoc training, internal code review, best practices information sharing

CIS Top 20 Critical Security Control 19

Incident Response and Management

Protect the organization’s information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker’s presence, and restoring the integrity of the network and systems.

Campus-sponsored tools

- Unknown

UWSC implementation

- Log creation and retention, disaster recovery preparation and planning

CIS Top 20 Critical Security Control 20

Penetration Tests and Red Team Exercises

Test the overall strength of an organization’s defenses (the technology, the processes, and the people) by simulating the objectives and actions of an attacker.

Campus-sponsored tools

- Phishing simulations

UWSC implementation

- Nothing

Original Questions

Q1: What tools does campus make available to help departments implement the CIS top 20 security controls?

A: Many tools available, addressing a majority of the controls in the CIS top 20.

Q2: How do current Survey Center security practices compare to the CIS top 20 controls?

A: Many controls in place. Identified some small gaps, but overall it’s a fairly positive assessment.

Final Score

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
🟩	🟩	🟩	🟩	🟨	🟩	🟩	🟩	🟩	🟩	🟨	🟩	🟩	🟨	🟩	🟨	🟩	🟩	🟨	🟩
✓	✓	✓	✓		✓	✓	✓	✓	✓		✓	✓		✓		✓	✓		
+	+		+	+		+	+		+	+		+	+		+	+	+	+	

Key

🟩 = campus-sponsored solution available

🟨 = campus-sponsored solution unclear or not applicable

✓ = UWSC uses campus-sponsored solution

+ = UWSC uses non-campus-sponsored solution

Thanks

Thanks to Steve Bochte and everyone at UWSC.

For more information or questions please contact Eric White (ewhite@ssc.wisc.edu).

Further Reading

1. CIS Controls: https://www.cisecurity.org/controls/
2. Back to Basics: Focus on the First Six CIS Critical Security Controls: http://go.wisc.edu/nrku0p
3. ASD Top 4 report: http://go.wisc.edu/5lmz5y
4. Mobile Security Companion: http://go.wisc.edu/gs2f21