SANS

Critical Security Controls

POSTER

FALL 2014 – 31ST EDITION

CRITICAL SECURITY CONTROLS
SOLUTION PROVIDERS

and

CRITICAL SECURITY CONTROLS
FOR EFFECTIVE CYBER DEFENSE

THE CRITICAL SECURITY CONTROLS SOLUTION PROVIDERS

1 INVENTORY OF AUTHORIZED AND UNAUTHORIZED DEVICES

P **PRIMARY:**
Discovery, Vulnerability Assessment

S **SECONDARY:**
Network Access Control

SOLUTION = PROVIDER:

- P AVDS = Beyond Security
- P Retina = Beyond Trust
- P Fusion VM = Critical Watch
- P McAfee Vulnerability Manager = Intel Security/McAfee
- P IPSonar = Lumeta
- P NMAP, Open VAS = Open Source
- P QualysGuard = Qualys
- P Nexpose = Rapid7
- P Altiris Asset Management Suite, CCS = Symantec
- P Nessus, PVS = Tenable
- P Tripwire IP360, Tripwire Enterprise and Tripwire CCM = Tripwire
- S ClearPass = Aruba
- S Network Sentry = Bradford Networks
- S Identity Services Engine = Cisco
- S CounterACT = ForeScout

2 INVENTORY OF AUTHORIZED AND UNAUTHORIZED SOFTWARE

P **PRIMARY:**
Software Change Management, Vulnerability Management

S **SECONDARY:**
Application Whitelisting, Virtual Container

SOLUTION = PROVIDER:

- P Retina = Beyond Trust
- P Endpoint Manager = IBM
- P Patch and Remediation = Lumension
- P System Center = Microsoft
- P QualysGuard = Qualys
- P Corporate Software Inspector = Secunia
- P Altiris Client Management Suite = Symantec
- P Nessus, PVS = Tenable
- P Tripwire IP360, Tripwire Enterprise and Tripwire CCM = Tripwire
- S Privilege Guard = Avecto
- S Security Platform = Bit9
- S vSentry = Bromium
- S Trusteer Apex = IBM
- S McAfee Application Control = Intel Security/McAfee
- S FreeSpace Enterprise = Invincea
- S Application Control = Lumension
- S Integrity = Signacert
- S Application Control = Viewfinity

3 SECURE CONFIGURATIONS FOR HARDWARE AND SOFTWARE ON LAPTOPS, WORKSTATIONS, AND SERVERS

P **PRIMARY:**
Vulnerability Assessment

S **SECONDARY:**
Patch Management, Secure Remote Access

SOLUTION = PROVIDER:

- P Retina = BeyondTrust
- P Endpoint Manager = IBM
- P McAfee Vulnerability Manager/McAfee Policy Auditor = Intel Security/McAfee
- P Patch and Remediation = Lumension
- P System Center = Microsoft
- P QualysGuard = Qualys
- P Altiris ITMS, CCS = Symantec
- P Nessus, PVS = Tenable
- P Tripwire IP360, Tripwire Enterprise and Tripwire CCM = Tripwire
- P vCenter Configuration Manager = VMWare
- S Connected Access = Axeda
- S Enterprise = SecureLink
- S Xsuite = Xceedium

4 CONTINUOUS VULNERABILITY ASSESSMENT AND REMEDIATION

P **PRIMARY:**
Vulnerability Assessment

SOLUTION = PROVIDER:

- P AVDS = Beyond Security
- P Retina = Beyond Trust
- P Fusion VM = Critical Watch
- P Endpoint Manager = IBM
- P McAfee Vulnerability Manager = Intel Security/McAfee
- P IPSonar = Lumeta
- P NMAP, Open VAS = Open Source
- P QualysGuard = Qualys
- P Nexpose, Metasploit = Rapid7
- P Altiris ITMS, CCS = Symantec
- P Nessus, PVS = Tenable
- P Tripwire IP360, Tripwire Log Center = Tripwire

5 MALWARE DEFENSE

P **PRIMARY:**
Endpoint Protection Platforms

S **SECONDARY:**
Network-Based Protection

SOLUTION = PROVIDER:

- P McAfee Endpoint Protection = Intel Security/McAfee
- P Endpoint Security for Business = Kaspersky
- P Complete Security Suite = Sophos
- P SEP = Symantec
- P Enterprise Security for Endpoints = Trend Micro
- S FailSafe = Damballa
- S FireEye Network Threat Prevention Platform = FireEye
- S Network IPS = IBM
- S Advanced Threat Defense = Intel Security/McAfee
- S StealthWatch = Lancope
- S Firepower = Sourcefire
- S Deep Discovery = Trend Micro

6 APPLICATION SOFTWARE SECURITY

P **PRIMARY:**
Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST)

S **SECONDARY:**
Web Application Firewalls

SOLUTION = PROVIDER:

- P HackAlert CodeSecure = Armorize (ProofPoint)
- P Cenzic Enterprise = Cenzic (Trustwave)
- P CX Suite = Checkmarx
- P Code Advisor = Coverity (Synopsis)
- P HP Fortify 360, HP Fortify on Demand, HP WebInspect = HP (Fortify)
- P Appscan = IBM
- P Insight = Klocwork (RogueWave Software)
- P NTO Spider = NTObjectives
- P Agnitio, W3AF, Wapiti = Open Source
- P QualysGuard WAS = Qualys
- P CLM = Sonatype
- P Static/Dynamic = Veracode
- P Sentinel = WhiteHat
- S Kona = Akamai
- S Web App Firewall = Barracuda
- S Netscaler = Citrix
- S CloudFlare Pro, Business, Enterprise = Cloudflare
- S Managed Web App Firewall, Web Application Testing = Dell SecureWorks
- S Application Security Manager = F5
- S SecureSphere, Incapsula = Imperva
- S Mod Security, IronBee = Open Source
- S QualysGuard WAF = Qualys
- S AppWall = Radware
- S StingRay Application Firewall = Riverbed
- S WAF Cloud Proxy = Sucuri
- S Web Application Firewall = Trustwave

7 WIRELESS ACCESS CONTROL

P **PRIMARY:**
Wireless LAN Intrusion Prevention System (WIPS)

S **SECONDARY:**
Network Access Control

SOLUTION = PROVIDER:

- P HiveOS = Aerohive
- P WiFi Analyzer = AirMagnet (Fluke)
- P Zone Defense = AirPatrol (Sysorex)
- P WIPS = AirTight
- P RF Protect = Aruba
- P aWIPS = Cisco
- P AirDefense = Motorola
- P Nessus, Security Center = Tenable
- P Tripwire CCM = Tripwire
- S ClearPass = Aruba
- S Network Sentry = Bradford Networks
- S Identity Services Engine = Cisco
- S CounterACT = ForeScout

8 DATA RECOVERY CAPABILITY

SOLUTION = PROVIDER:

- AccessData FTK and PRTK = AccessData
- PowerBroker Recovery for Active Directory = BeyondTrust
- ElcomSoft EFDD — Bitlocker, TruCrypt = Elcom
- Encase Enterprise Edition = Guidance Software
- Tivoli Storage Manager = IBM
- NBU = Symantec

9 SECURITY SKILLS ASSESSMENT AND APPROPRIATE TRAINING TO FILL GAPS

P **PRIMARY:**
Assessment

S **SECONDARY:**
Skills Development/Degrees

SOLUTION = PROVIDER:

- P Cyber Skills Assessment = GIAC (SANS)
- P Cyber Simulators (Netwars) and Skills Validation = SANS Institute
- S GIAC Critical Controls Certification = GIAC (SANS)
- S 50 Hands-on Immersion Courses = SANS Institute
- S Degree Programs = SANS Technology Institute
- S Degree Programs = University of Tulsa
- S Degree Programs = Virginia Tech
- S Degree Programs = Dakota State University
- S Degree Programs = Naval Postgraduate School

10 SECURE CONFIGURATIONS FOR FIREWALLS, ROUTERS, AND SWITCHES

SOLUTION = PROVIDER:

- Firewall Analyzer & FireFlow = AlgoSec
- SecurityManager = FireMon
- Network Configuration Manager = IBM
- Platform = RedSeal
- Firewall Assurance = Skybox Security
- Firewall Security Manager = Solarwinds
- Tripwire Enterprise = Tripwire
- Security Policy Orchestration Solution = Tuffin

The blue box indicates this provider is part of the WhatWorks program or a sponsor of this poster

SANS WHAT WORKS

11 LIMITATION AND CONTROL OF NETWORK PORTS, PROTOCOLS, AND SERVICES

P **PRIMARY:**
Discovery, Vulnerability Assessment

S **SECONDARY:**
Application Firewall

SOLUTION = PROVIDER:

- P AVDS = Beyond Security
- P Retina = Beyond Trust
- P Fusion VM = Critical Watch
- P McAfee Vulnerability Manager = Intel Security/McAfee
- P IPSonar = Lumeta
- P NMAP, Open VAS = Open Source
- P QualysGuard = Qualys
- P Altiris Asset Management Suite, CCS = Symantec
- P Nexpose = Rapid7
- P Nessus, PVS = Tenable
- P Tripwire IP360, Tripwire Enterprise and Tripwire CCM = Tripwire
- S ASA Series and Virtual ASA = Cisco
- S SonicWall = Dell Sonicwall
- S FortiGate = Fortinet
- S McAfee Next Generation Firewall = Intel Security/McAfee
- S SRX, Netscreen, Firefly = Juniper
- S PaloAlto NGFW = Palo Alto Networks

12 CONTROLLED USE OF ADMINISTRATIVE PRIVILEGES

SOLUTION = PROVIDER:

- Privilege Guard = Avecto
- PowerBroker = BeyondTrust
- SuperSU = Chainfire
- Privileged Account Security Solution = Cyber-Ark
- Privileged Password Manager = Dell
- Security Privileged identity Manager = IBM
- System Center, Active Directory = Microsoft
- sudo = Open Source
- Access Auditor = Security Compliance Corporation (SCC)
- CCS = Symantec
- Privilege Management = Viewfinity
- Xsuite = Xceedium

13 BOUNDARY DEFENSE

P **PRIMARY:**
Firewall

S **SECONDARY:**
Intrusion Prevention System

SOLUTION = PROVIDER:

- P 2200 = Check Point
- P ASA Series and Virtual ASA = Cisco
- P SonicWall = Dell Sonicwall
- P FortiGate = Fortinet
- P McAfee Next Generation Firewall = Intel Security/McAfee
- P SRX, Netscreen, Firefly = Juniper
- P PaloAlto NGFW = Palo Alto Networks
- S XPS = Fidelis
- S FireEye Network Threat Prevention Platform = FireEye
- S HP Tipping Point NGFW = HP
- S Network IPS = IBM
- S McAfee Network Security Platform = Intel Security/McAfee
- S StealthWatch = Lancope
- S Snort, Suricata = Open Source
- S Firepower = Sourcefire (Cisco)

14 MAINTENANCE, MONITORING, AND ANALYSIS OF AUDIT LOGS

SOLUTION = PROVIDER:

- SIEM = AccelOps
- Unified Security Management = AlienVault
- CorreLog Security Correlation Server = CorreLog
- Security Monitoring, Log Management = Dell SecureWorks
- SecureVUE = EIQ Networks
- Enterprise = EventTracker
- ArcSight ESM, Logger = HP
- QRadar = IBM
- Event Correlation = Infogressive
- McAfee Enterprise Security Manager = Intel Security/McAfee
- StealthWatch = Lancope
- Security Intelligence Platform = LogRhythm
- Hawkeye AP = KeyW
- Snare, OSSIM = Open Source
- Log and Event Manager = SolarWinds
- Splunk App for Enterprise Security = Splunk
- Security Center = Tenable
- LogLogic = TIBCO
- Tripwire Log Center = Tripwire

15 CONTROLLED ACCESS BASED ON NEED TO KNOW

SOLUTION = PROVIDER:

- Access Assurance Suite = Courion
- Appliance = HyTrust
- Access Manager for Web = IBM
- Active Directory = Microsoft
- Access Goverance Suite = Novell
- Identity Governance Suite = Oracle
- Aveksa = RSA
- Identity IQ = Sailpoint
- Access Auditor = Security Compliance Corporation (SCC)

16 ACCOUNT MONITORING AND CONTROL

SOLUTION = PROVIDER:

- Access Assurance Suite = Courion
- Enterprise Reporter = Dell
- Appliance = HyTrust
- Security Identity Manager = IBM
- AD Reports = MaxPowerSoft
- Active Directory = Microsoft
- Access Management Suite = Novell
- Identity Governance Suite = Oracle
- Aveska = RSA
- Identity IQ = Sailpoint
- Access Auditor = Security Compliance Corporation (SCC)

17 DATA PROTECTION

P **PRIMARY:**
DLP

S **SECONDARY:**
Encryption

SOLUTION = PROVIDER:

- P DLP Software Blade = Check Point
- P TrueDLP = Code Green
- P XPS = Fidelis
- P FortiGate = Fortinet
- P McAfee Total Protection for DLP = Intel Security/McAfee
- P DLP = RSA
- P DLP = Symantec
- P DLP and SecureCloud = Trend Micro
- P Digital Guardian = Verdasys
- S Full Disk Encryption = Check Point
- S Cloud Lock for Salesforce = CloudLock
- S McAfee Total Protection for DLP = Intel Security/McAfee
- S BitLocker = Microsoft
- S Data Protection Manager = RSA
- S Storage Secure = Safenet
- S Encryption Manager Services = Symantec
- S Safend Data Protection Suite = Wave
- S SecureDoc = WinMagic

18 INCIDENT RESPONSE AND MANAGEMENT

SOLUTION = PROVIDER:

- ResolutionOne™ Platform = AccessData
- CarbonBlack = Bit9
- UFED = Cellebrite
- Security Module = Co3 Systems
- CorreLog Enterprise Server = CorreLog
- CyberSponse = CyberSponse
- Essential Series, Incident Response Services, Security Monitoring = Dell SecureWorks
- F-Response Enterprise = F-Response
- EnCase Cybersecurity = Guidance Software
- Incident Response & Forensics = Infogressive
- StealthWatch = Lancope
- Smart Response = LogRhythm
- Mandiant Intelligent Response (MIR) = Mandiant

19 SECURE NETWORK ENGINEERING

SOLUTION = PROVIDER:

- Firewall Analyzer & FireFlow = AlgoSec
- Halo Platform = CloudPassage
- SecurityManager = FireMon
- Platform = RedSeal
- Firewall Assurance = Skybox Security
- Firewall Security Manager = Solarwinds
- Tripwire Enterprise = Tripwire
- Security Policy Orchestration Solution = Tuffin

20 PENETRATION TESTING AND RED TEAM EXERCISES

SOLUTION = PROVIDER:

- Core Impact = Core Security
- Penetration Testing Services = Dell SecureWorks
- Penetration Testing Services = Infogressive
- CANVAS = Immunity
- Mobisec = Open Source
- Pwn Pad/Plug/Appliance = Pwnie Express
- Metasploit = Rapid7
- SAINT 8 Security Suite = SAINT
- MySecurityScanner = Secure Ideas
- Armitage / Cobalt Strike = Strategic Cyber LLC

Solutions listed on this poster were selected and reviewed by SANS Institute faculty, other members of the SANS Community and John Pescatore, SANS Director of Emerging Security Trends.

For an ongoing discussion of these, please visit the Solutions Directory at sans.org/critical-security-controls/vendor-solutions

Critical Security Controls

for Effective Cyber Defense

Effective Cybersecurity – Now

The Critical Security Controls for Effective Cyber Defense (**the Controls**) are a recommended set of actions for cyber defense that provide **specific and actionable ways to stop today's most pervasive and dangerous attacks.** They are developed, refined, validated, and supported by a large volunteer community of security experts under the stewardship of the Council on CyberSecurity (www.counciloncybersecurity.org). Contributors, adopters, and supporters are found around the world, and represent every type of role, experience, and mission or business. State and local governments, power generation and distribution, transportation, academic institutions, financial services, Federal government, defense contractors, and many more – are among the hundreds of organizations that have **shifted from a compliance focus to a security focus** by adopting the Critical Security Controls. All of these entities changed over to the Controls in answer to the key question: "What needs to be done right now to protect my organization from advanced and targeted attacks?"

The Controls do not attempt to replace comprehensive frameworks, (e.g., NIST SP 800-53, ISO 27001, the NIST Cyber Security Framework) but rather **prioritize and focus** on a smaller number of actionable controls with high-payoff, aiming for a "must do first" philosophy. Since the Controls are derived from the most common attack patterns and vetted across a very broad community of government and industry security practitioners, with very strong consensus on the resulting set of controls, they serve as the **basis for immediate high-value action**. An enterprise can use the Controls to rapidly define the starting point to assess and improve their defenses, direct their scarce resources on actions with immediate and high-value payoff, and then focus their attention and resources on additional risk issues that are unique to their mission or business. An underlying theme of the Controls is support for large-scale, standards-based security automation for the management of cyber defenses.

The Controls illustrate the kind of large-scale, public-private, voluntary cooperation needed to improve individual and collective security in cyberspace. Too often in cybersecurity, it seems the "bad guys" are better organized and collaborate more closely than the "good guys." The Controls provide a means to turn that around.

Mapping the Controls Across the Cyber Defense Lifecycle

The Critical Controls provide high value across different stages of the typical "Prevent/Detect/Respond" cybersecurity lifecycle. SANS has created a mapping allocating the Controls across four phases:

CYBER DEFENSE LIFECYCLE

CRITICAL SECURITY CONTROLS

Resource Hardening	Privilege and Access Management	Attack Detection/Mitigation	Compromise Detection, Response, Recovery, and Reporting
Hardware and Software Inventory CSC1 & CSC2	Admin Privileges CSC12	Malware Defenses CSC5	Data Recovery CSC8
Secure Configurations CSC3, CSC7, CSC10 & CSC11	Controlled Access CSC15	Boundary Defense CSC13	Audit CSC14
Vulnerability Assessment & Application Security CSC4 & CSC6	Account Managing CSC16		Data Protection CSC17
			Incident Response CSC18

People and Processes

The Critical Security Controls includes a number of security areas which focus on people and processes and are applicable across the entire lifecycle:

CSC9 – Security Skills Assessment and Training

CSC19 – Secure Network Engineering

CSC20 – Penetration Testing and Red Team Exercises

The Department of Homeland Security Continuous Diagnostics and Mitigation program has multiple phases of security product and services offerings across cybersecurity. The Critical Controls map directly against those CDM phases:

CDM CAPABILITY FAMILIES

CRITICAL SECURITY CONTROLS

Manage Assets	Manage Accounts for People and Services	Manage Events	Manage Security Lifecycle
Hardware Inventory CSC1	Security Skills CSC9	Data Recovery CSC8	Security Engineering CSC19
Software Inventory & Malware Defenses CSC2 & CSC5	Admin Privileges CSC12	Audit CSC14	Red Team/Pen Testing CSC20
Vulnerability Assessment & Application Security CSC4 & CSC6	Controlled Access CSC15	Incident Response CSC18	
Wireless Access Control CSC7	Account Monitoring CSC16		
Secure Configurations CSC3 & CSC10			
Boundary Defense & Ports, Protocols, and Service CSC13 & CSC11			
Data Protection CSC17			

CDM is being deployed in three phases:

Phase 1 (yellow): Hardware, Software, Configuration Settings, and Vulnerability Management

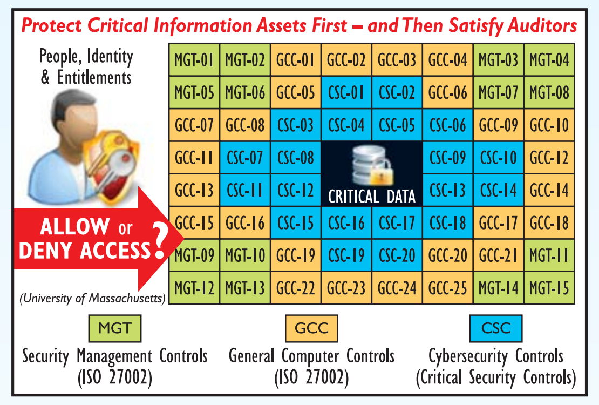
Phase 2 (orange): Managing Trust, Security-Related Behavior, Credentials and Authentication, Privileges and Accounts, and Filter-Based Boundaries

Phase 3 (red): Managing Physical and Virtual (Encryption) Boundaries, Incident Planning, Incident Response, Suspicious Pattern Detection, Enterprise Planning and Policy, Quality Management, and Risk Management.

The Value of Using the Critical Security Controls to Focus on Protecting Critical Information Assets

The Critical Security Controls are not intended to replace any of the major security frameworks, such as ISO 27001, the NIST Cybersecurity Framework, the Payment Card Industry Data Security Standards, etc. In the real world, auditors will still perform audits across those complex, exhaustive frameworks. However, adopting the Controls allows you to convince your management and those auditors that you have focused on the most important security processes first in both your current and planned efforts – which is what risk management is all about.

Protect Critical Information Assets First – and Then Satisfy Auditors


People, Identity & Entitlements
ALLOW or DENY ACCESS?
(University of Massachusetts)

MGT-01	MGT-02	GCC-01	GCC-02	GCC-03	GCC-04	MGT-03	MGT-04
MGT-05	MGT-06	GCC-05	CSC-01	CSC-02	GCC-06	MGT-07	MGT-08
GCC-07	GCC-08	CSC-03	CSC-04	CSC-05	CSC-06	GCC-09	GCC-10
GCC-11	CSC-07	CSC-08	CRITICAL DATA		CSC-09	CSC-10	GCC-12
GCC-13	CSC-11	CSC-12			CSC-13	CSC-14	GCC-14
GCC-15	GCC-16	CSC-15	CSC-16	CSC-17	CSC-18	GCC-17	GCC-18
MGT-09	MGT-10	GCC-19	CSC-19	CSC-20	GCC-20	GCC-21	MGT-11
MGT-12	MGT-13	GCC-22	GCC-23	GCC-24	GCC-25	MGT-14	MGT-15

MGT	GCC	CSC
Security Management Controls (ISO 27002)	General Computer Controls (ISO 27002)	Cybersecurity Controls (Critical Security Controls)

Larry Wilson was hired by the University of Massachusetts in 2009 as the UMASS President's Office Information Security Lead. His primary role was to develop a University-wide Information Security Policy and Written Information Security Program (WISP). He formed an information security controls team with representatives from all five campuses (Amherst, Dartmouth, Lowell, Worcester, and Boston).

The controls team established a standards-based program consisting of management, administrative/operational and technical controls. Management and administrative/operational security controls (also called General Computer Controls) are based on ISO 27001 / 27002. The technical security controls are based on Critical Security Controls implemented as the "inner core" to protect "Critical Information Assets." This has allowed UMASS to increase the maturity of their security controls to actively mitigate advanced threats, resulting in both fewer incidents and faster response to incidents that do occur.

UMASS implemented the Critical Controls with an initial focus of protecting critical resources and information assets but under an architecture that supported scalability and integration to pave the way for broader deployment. The controls team also advised the internal audit department and executive management on the importance of this approach. In May, 2014, Larry helped organize a week-long training event where 68 individuals representing 32 local colleges and universities received in depth training on the Critical Security Controls.

CRITICAL SECURITY CONTROL	DESCRIPTION	MAPPINGS TO THE CRITICAL SECURITY CONTROLS (V5.0A)								
		NIST CORE FRAMEWORK	PCI DSS 3.0	ISO 27002: 2013	DHS CDM PROGRAM	AUSTRALIAN TOP 35	GCHQ 10 STEPS	UK CYBER ESSENTIALS	UK ICO PROTECTING DATA	NIST 800-53 REV4*
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 found and prevented from gaining access.	ID.AM-1 ID.AM-3 PR.DS-3	2.4	A.8.1.1 A.9.1.2 A.13.1.1	Configuration Settings Management	1 14 17			Inappropriate locations for processing data	CA-7 SC-17 CM-8 SI-4 IA-3: PM-5 SA-4
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 that unauthorized and unmanaged software is found and prevented from installation or execution.	ID.AM-2 PR.DS-6		A.12.5.1 A.12.6.2	Hardware Asset Management Software Asset Management				Decommissioning of software or services	CA-7 CM-10 SC-34 CM-2 CM-11 SI-4 CM-8 SA-4 PM-5 SC-18
3 Secure Configurations for Hardware and Software	Establish, implement, and actively manage (track, report on, 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.	PR.IP-1	2.2 2.3 6.2 11.5	A.14.2.4 A.14.2.8 A.18.2.3	Configuration Settings Management	2-5 21	Secure Configuration	Secure Configuration Patch Management	Inappropriate locations for processing data	CA-7 CM-6 CM-11 SC-14 CM-2 CM-7 MA-4 SC-34 CM-3 CM-8 RA-5 SI-2 CM-5 CM-9 SA-4 SI-4
4 Continuous Vulnerability Assessment and Remediation	Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.	ID.RA-1 DE.CM-8 ID.RA-2 RS.MI-3 PR.IP-12	6.1 6.2 11.2	A.12.6.1 A.14.2.8	Vulnerability Management	2-3		Patch Management	Software Updates	CA-2 SC-34 CA-7 SI-4 RA-5 SI-7
5 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.	PR.PT-2 DE.CM-4 DE.CM-5	5.1 - 5.4	A.8.3.1 A.12.2.1 A.13.2.3		7 26 17 30 22	Removable Media Controls Malware Protection	Malware Protection		CA-7 SI-3 SC-39 SI-4 SC-44 SI-8
6 Application Software Security	Manage the security lifecycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses.	PR.DS-7	6.3 6.5 - 6.7	A.9.4.5 A.12.1.4 A.14.2.1 A.14.2.6 - A.14.2.8	Vulnerability Management	24			SQL Injection	SA-13 SA-20 SI-11 SA-15 SA-21 SI-15 SA-16 SC-39 SI-16 SA-17 SI-10
7 Wireless Access Control	The processes and tools used to track/control/prevent/correct the security use of wireless local area networks (LANS), access points, and wireless client systems.		4.3 11.1	A.10.1.1 A.12.4.1 A.12.7.1			Monitoring Network Security			AC-18 CA-7 SC-17 AC-19 CM-2 SC-40 CA-3 IA-3 SI-4 SC-8
8 Data Recovery Capability	The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.	PR.IP-4	4.3 9.5 - 9.7	A.10.1.1 A.12.3.1						CP-9 CP-10 MP-4
9 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.	PR.AT-1 PR.AT-4 PR.AT-2 PR.AT-5 PR.AT-3	12.6	A.7.2.2	Security-Related Behavior Management	28	User Education & Awareness			AT-1 AT-4 PM-13 AT-2 SA-11 PM-14 AT-3 SA-16 PM-16
10 Secure Configurations for Network Devices	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.	PR.AC-5 PR.IP-1 PR.PT-4	1.1 - 1.2 2.2 6.2	A.9.1.2 A.13.1.1 A.13.1.3	Configuration Settings Management Boundary Protection	2 3 10	Secure Configuration Network Security	Boundary firewalls and internet gateways Secure Configuration Patch Management	Software Updates Inappropriate locations for processing data	AC-4 CM-2 CM-8 CA-3 CM-3 MA-4 CA-7 CM-5 SC-24 CA-9 CM-6 SI-4
11 Limitation and Control of Network Ports	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.	PR.AC-5 DE.AE-1	1.4	A.9.1.2 A.13.1.1 A.13.1.2 A.14.1.2	Boundary Protection	2 13 3 27 12	Network Security		Decommissioning of software or services Unnecessary Services	AC-4 CM-6 SC-22 CA-7 CM-8 SC-41 CA-9 SC-20 SI-4 CM-2 SC-21
12 Controlled Use of Administrative Privileges	The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.	PR.AC-4 PR.MA-2 PR.AT-2 PR.PT-3	2.1 7.1 - 7.3 8.1 - 8.3 8.7	A.9.1.1 A.9.2.2 - A.9.2.6 A.9.3.1 A.9.4.1 - A.9.4.4		4 11 9 25	Monitoring	Access Control	Configuration of SSL and TLS Default Credentials	AC-2 AC-19 IA-4 AC-6 CA-7 IA-5 AC-17 IA-2 SI-4
13 Boundary Defense	Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.	PR.AC-3 PR.MA-2 PR.AC-5 DE.AE-1	1.1 - 1.3 8.3 10.8 11.4	A.9.1.2 A.13.1.1 A.12.4.1 A.13.1.3 A.12.7.1 A.13.2.3	Boundary Protection	10-11 18-20 23 32-34	Home and Mobile Working Monitoring Network Security	Boundary firewalls and internet gateways	Configuration of SSL and TLS Inappropriate locations for processing data	AC-4 CA-7 SC-7 AC-17 CA-9 SC-8 AC-20 CM-2 SI-4 CA-3 SA-9
14 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.	PR.PT-1 DE.DP-3 DE.AE-3 DE.DP-4 DE.DP-1 DE.DP-5 DE.DP-2	10.1 - 10.7	A.12.4.1 - A.12.4.4 A.12.7.1	Generic Audit Monitoring	15-16 35	Monitoring			AC-23 AU-5 AU-9 AU-13 SI-4 AU-2 AU-6 AU-10 AU-14 AU-3 AU-7 AU-11 CA-7 AU-4 AU-8 AU-12 IA-10
15 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.	PR.AC-4 PR.DS-2 PR.AC-5 PR.PT-2 PR.DS-1 PR.PT-3	1.3 - 1.4 4.3 7.1 - 7.3 8.7	A.8.3.1 A.9.1.1 A.10.1.1	Access Control Management Privileges	26	Managing User Privileges Network Security	Access Control	Inappropriate locations for processing data	AC-1: AC-6 RA-2 AC-2: AC-24 SC-16 AC-3 CA-7 SI-4 MP-3
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.	PR.AC-1 PR.AC-4 PR.PT-3	7.1 - 7.3 8.7 - 8.8	A.9.1.1 A.9.2.1 - A.9.2.6 A.9.3.1 A.9.4.1 - A.9.4.3 A.11.2.8	Credentials and Authentication Management	25	Managing User Privileges	Access Control	Configuration of SSL and TLS	AC-2 AC-12 SC-17 AC-3 CA-7 SC-23 AC-7 IA-5 SI-4 AC-11 IA-10
17 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.	PR.AC-5 PR.DS-5 PR.DS-2 PR.PT-2	3.6 4.1 - 4.3	A.8.3.1 A.10.1.1 - A.10.1.2 A.13.2.3 A.18.1.5		26	Removable Media Controls			AC-3 CA-9 SC-8 SI-4 AC-4 IR-9: SC-28: AC-23 MP-5 SC-31 CA-7 SA-18 SC-41
18 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.	PR.IP-10 RS.RP-1 RC.RP-1 DE.AE-2 RS.CO-1-5 RC.IM-1-2 DE.AE-4 RS.AN-1-4 RC.CO-1-3 DE.AE-5 RS.MI-1-2 DE.CM-1-7 RS.IM-1-2	12.10	A.6.1.3 A.7.2.1 A.16.1.2 A.16.1.4 - A.16.1.7	Plan for Events Respond to Events		Incident Management			IR-1 IR-4 IR-7 IR-2 IR-5 IR-8 IR-3 IR-6 IR-10
19 Secure Network Engineering	Make security an inherent attribute of the enterprise by specifying, designing, and building-in features that allow high confidence systems operations while denying or minimizing opportunities for attackers.	PR.AC-5		A.13.1.3 A.14.2.5		10	Network Security		Inappropriate locations for processing data	AC-4 SA-8 SC-22 CA-3 SC-20 SC-32 CA-9 SC-21 SC-37
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.		11.3	A.14.2.8 A.18.2.1 A.18.2.3						CA-2 CA-8 PM-6 CA-5 RA-6 PM-14 CA-6 SI-6

***NIST 800-53 LISTINGS**

A-3: Device Identification and Authentication
A-5: Authenticator Management
AC-1: Access Control Policy and Procedures
AC-2: Account Management
AC-3: Access Enforcement
AC-4: Information Flow Enforcement
AC-6: Least Privilege
AC-7: Unsuccessful Logon Attempts
AC-11: Session Lock
AC-12: Session Termination
AC-17: Remote Access
AC-18: Wireless Access
AC-19: Access Control for Mobile Devices
AC-20: Use of External Information Systems
AC-23: Data Mining Protection
AC-24: Access Control Decisions
AT-1: Security Awareness and Training Policy and Procedures
AT-2: Security Awareness Training
AT-3: Role-Based Security Training
AT-4: Security Training Records
AU-2: Audit Events
AU-3: Content of Audit Records
AU-4: Audit Storage Capacity
AU-5: Response to Audit Processing Failures
AU-6: Audit Review, Analysis, and Reporting
AU-7: Audit Reduction and Report Generation
AU-8: Time Stamps
AU-9: Protection of Audit Information
AU-10: Non-repudiation
AU-11: Audit Record Retention
AU-12: Audit Generation
AU-13: Monitoring for Information Disclosure
AU-14: Session Audit
CA-2: Security Assessments
CA-3: System Interconnections
CA-5: Plan of Action and Milestones
CA-6: Security Authorization
CA-7: Continuous Monitoring
CA-8: Penetration Testing
CA-9: Internal System Connections
CM-2: Baseline Configuration
CM-3: Configuration Change Control
CM-5: Access Restrictions for Change
CM-6: Configuration Settings
CM-7: Least Functionality
CM-8: Information System Component Inventory
CM-9: Configuration Management Plan
CM-10: Software Usage Restrictions
CM-11: User-Installed Software
CP-9: Information System Backup
CP-10: Information System Recovery and Reconstitution
IA-2: Identification and Authentication (Organizational Users)
IA-4: Identifier Management
IA-10: Adaptive Identification and Authentication
IR-1: Incident Response Policy and Procedures
IR-2: Incident Response Training
IR-3: Incident Response Testing
IR-4: Incident Handling
IR-5: Incident Monitoring
IR-6: Incident Reporting
IR-7: Incident Response Assistance
IR-8: Incident Response Plan
IR-9: Information Spillage Response
IR-10: Integrated Information Security Analysis Team
ISC-23: Session Authenticity
ISC-40: Wireless Link Protection
MA-4: Nonlocal Maintenance
MP-3: Media Marking
MP-4: Media Storage
MP-5: Media Transport
PM-5: Information System Inventory
PM-6: Information Security Measures of Performance
PM-13: Information Security Workforce
PM-14: Testing, Training, & Monitoring
PM-16: Threat Awareness Program
RA-5: Vulnerability Scanning
RA-2: Security Categorization
RA-6: Technical Surveillance Countermeasures Survey
SA-4: Acquisition Process
SA-8: Security Engineering Principles
SA-9: External Information System Services
SA-11: Developer Security Testing and Evaluation
SA-13: Trustworthiness
SA-15: Development Process, Standards, and Tools
SA-16: Developer-Provided Training
SA-17: Developer Security Architecture and Design
SA-18: Tamper Resistance and Detection
SA-20: Customized Development of Critical Components
SA-21: Developer Screening
SC-7: Boundary Protection
SC-8: Transmission Confidentiality and Integrity
SC-17: Public Key Infrastructure Certificates
SC-18: Mobile Code
SC-15: Collaborative Computing Devices
SC-16: Transmission of Security Attributes
SC-20: Secure Name /Address Resolution Service (Authoritative Source)
SC-21: Secure Name /Address Resolution Service (Recursive or Caching Resolver)
SC-22: Architecture and Provisioning for Name/ Address Resolution Service
SC-24: Fail in Known State
SC-28: Protection of Information at Rest
SC-31: Covert Channel Analysis
SC-32: Information System Partitioning
SC-34: Non-Modifiable Executable Programs
SC-37: Out-of-Band Channels
SC-39: Process Isolation
SC-41: Port and I/O Device Access
SC-44: Detonation Chambers
SI-2: Flaw Remediation
SI-3: Malicious Code Protection
SI-4: Information System Monitoring
SI-6: Security Function Verification
SI-7: Software, Firmware, and Information Integrity
SI-8: Spam Protection
SI-10: Information Input Validation
SI-11: Error Handling
SI-15: Information Output Filtering
SI-16: Memory Protection

Thanks to James Tarala for his awesome effort mapping the Critical Controls across these and other frameworks.

Support for Implementing the Controls is a Click Away

Here are some additional resources for effective planning and implementation of the Critical Controls:

1) **The Council on CyberSecurity** is an independent, non-profit organization dedicated to the establishment and sustainment of best practices in cybersecurity, including the Critical Security Controls. The Council website hosts the current version of the Controls, numerous working aids (including current versions of the mappings above), presentations, and other materials to support the Critical Security Controls community. counciloncybersecurity.org

2) Updates and in-depth explanations of the **Controls** posted at sans.org/critical-security-controls

3) **The SANS Solutions Directory** (sans.org/critical-security-controls/vendor-solutions) posts case studies of organizations that have successfully implemented the Controls and seen immediate benefits. These "What Works" reports provide real-world evidence that you should look at before buying any product.

4) **Courses** on planning and implementing the Critical Controls include:
- **Two-day courses:** sans.org/course/critical-security-controls-planning-implementing-auditing
- **Six-day in-depth courses:** sans.org/course/implementing-auditing-critical-security-controls

5) **Summits** where managers from user organizations and strategists from vendor companies share lessons learned and plan for future improvements: sans.org/summit

SANS
Fall 2014

Council on CyberSecurity
Le Conseil de la CyberCécurité

Selling Management on Adopting the Critical Security Controls

Gaining widespread adoption of the Critical Security Controls has been a bottoms-up movement, and getting buy-in from senior management early has enabled adopters to accelerate real security progress. Jane Holl Lute, the President and Chief Executive Officer of the Council has spent the past year talking with policymakers and CEOs to get the value of the Controls across and has some recommendations on how to sell the concept to management. Jane should know – she was formerly the Deputy Secretary and chief operating officer for the Department of Homeland Security (DHS). Before that she spent six years as Assistant Secretary-General of the United Nations (UN) coordinating efforts on behalf of the Secretary General to build sustainable peace in countries emerging from violent conflict.

Jane's "elevator pitch" to corporate and government leaders:

Every senior company executive and Board director should know that four or five steps of basic cybersecurity hygiene prevent 80-90% of all known attacks. Where does your business stand on basic cyber hygiene? Give your organization this simple "smell test."

Ask your business, IT, and security managers the following questions to see where your enterprise stands:

1. Do we know what is connected to our systems and networks?
2. Do we know what's running (or trying to run) on our systems and networks?
3. Are we limiting and managing the number of people who have the administrative privileges to change, bypass, or override the security settings on our systems and networks?
4. Do we have in place continuous processes backed by security technologies that would allow us to prevent most breaches, rapidly detect all that do succeed and minimize damage to our business and our customers?
5. Can you demonstrate all this to me, to our Board, and to our shareholders and customers today?

If they can't say yes to all these questions, you may still be compliant with regulations but your company's data and customers are not safe. If you don't ask these questions, your customers and shareholders will – or will be soon, because we are spreading the word!

Give your corporate management the plan for how to say yes to those five questions!

Getting Started: Ask and Answer Key Questions

- **What am I trying to protect?** Create a prioritized list of business- or mission-critical processes and inventory the information and computing assets that map to those processes. This information will be crucial for baselining your current capabilities against the Critical Controls.
- **What are my gaps?** For each business- or mission critical asset, compare existing security controls against the Critical Controls, indicating the subcontrols that the existing controls already meet and those they do not meet.
- **What are my priorities?** Based on your identified gaps and specific business risks and concerns, take immediate tactical steps to implement the five quick wins and develop a strategic plan to implement beyond the first five.
- **Where can I automate?** As you plan implementation of the Controls, focus on opportunities to create security processes that can be integrated and automated using tools that relieve skilled security and administrative staff of grunt work and continuous monitoring processes. The Controls were specifically created to enable automation. The goal is to more rapidly and efficiently deliver accurate, timely, and actionable information to the system administrators and others who can take proactive steps to deter threats.
- **How can my vendor partners help?** Some vendor solutions significantly improve and automate implementation of the Critical Controls, especially in terms of continuous monitoring and mitigation. Contact your current vendors to see how they can support your implementation of the Critical Controls and compare their capabilities with other vendor products with user validation at sans.org/critical-security-controls/vendor-solutions.
- **Where can I learn more?** See the list of resources at the bottom of this poster.

Four Basic Principles That Are Driving the Adoption of the Controls

The Critical Security Controls have always been more than just another list of things to do. They are created, used, and supported by a grass-roots community representing every part of the cyber ecosystem, banding together to help each other identify and implement the most effective defenses. And rather than being driven by mandate, they have tried to stay true to a number of basic principles that guide their evolution and sustainment.

Prioritize

- Offense Informs Defense: Controls are selected based on specific knowledge of adversarial behavior and how to stop it.
- Focus: Avoid adding "good things to do."

Implement

- Action today is more valuable than elegance or completeness tomorrow.
- Provide specific, practical steps on how to implement Controls.
- Help enterprises that are just starting adoption, as well as those that are mature in their adoption.

Sustain

- Create and support a community of contributors, advocates, adopters, solution vendors, teachers, consultants, auditors, etc.
- Create an ecosystem of working aides, use-cases, tools, references, interest groups, mappings, etc.
- Identify and take on barriers as a community.

Align

- Create and demonstrate "peaceful co-existence" with existing governance, regulatory, process, management schemes, frameworks, and structures.
- Recognize that the Controls exist in a context that is different for each enterprise. Make value judgments about priority as a community, but also allow for local, community, or more informed risk judgments.

Mobilizing the Community for Action: The Council on CyberSecurity

The Council on CyberSecurity is an independent, expert, not-for-profit organization with a global scope committed to improving the security of an open Internet. The Council is committed to the ongoing development and widespread adoption of the Critical Security Controls, to elevating the competencies of the cybersecurity workforce, and to the development of policies that lead to measurable improvements in our ability to operate safely, securely and reliably in cyberspace. A moment now exists in which everyone has begun to feel the urgent need to act. The Council was formed to seize this moment and drive change – specifically, to accelerate the widespread availability and adoption of effective cybersecurity measures, practice and policy.

Based in the Washington, D.C. area, the Council has assumed the responsibilities associated with leading the volunteer collaboration credited with identifying and developing the Critical Security Controls. In addition, the Council is home to the U.S. Cyber Challenge that works with the cybersecurity community to bring accessible, compelling programs that motivate students and professionals to pursue education, development and career opportunities in cybersecurity. For more information, visit the website at CouncilonCyberSecurity.org.