Sponsored Whitepapers

To get your free vendor-sponsored whitepaper, visit https://www.sans.org/tools.php

Dell SecureWorks
Advantages of Managed Security Services vs. In-house SIEM
www.secureworks.com/criticalcontrols

nCircle
Solutions for Automating the Consensus Audit Guidelines Critical Security Controls
www.ncircle.com

FireEye
Advanced Targeted Attacks: How to Protect Against the Next Generation of Cyber Attacks
www2.fireeye.com/ATA

Qualys On Demand Security
Automating the 20 Critical Controls
www.qualys.com/SANS

Infogressive, Inc. Aggressive Information Security
Seeing 20/20: How the SANS 20 Critical Controls Provide Vision and Focus For Your Information Security Program
www.infogressive.com

Symantec
Beyond Continuous Monitoring: Threat Modeling for Real-time Response
www.symantec.com

invincea
Protect Your Organization From Its Largest Threat: Cyber Breach
www.invincea.com

tenable network security
Outcome-Based Security Monitoring in a Continuous Monitoring World
www.tenable.com

Lancope
Blocking Network-based Attacks with Lancope StealthWatch
www.lancope.com

Trend Micro
Continuous Monitoring in a Virtual Environment
www.trendmicro.com

McAfee An Intel Company
Achieve Situational Awareness
www.mcafee.com

tripwire
SANS Secure Configuration Management Demystified
www.tripwire.com

20 Critical Security Controls

POSTER

SPRING 2013 – 24TH EDITION

SANS

🟩 Indicates this provider is part of the SANS Analyst and/or WhatWorks program

Analyst Program

SANS What Works

2
Inventory of Authorized and Unauthorized Software

P PRIMARY:
Software Change Management, Vulnerability Management

S SECONDARY:
Application Whitelisting

SOLUTION = PROVIDER:

P Tivoli Endpoint Manager (BigFix) = IBM
P Vulnerability Management = Lumension
P System Center = Microsoft
P CCM (primary), IP360 = nCircle
P QualysGuard Policy Compliance Module = Qualys
P Corporate Software Inspector = Secunia
P Nessus, Security Center = Tenable
P Enterprise, Log Center = Tripwire
S Parity, Bit9 FileAdvisor = Bit9
S Bouncer = CoreTrace
S SolidCore = McAfee

1
Inventory of Authorized and Unauthorized Devices

P PRIMARY:
Discovery, Vulnerability Assessment

S SECONDARY:
Network Access Control

SOLUTION = PROVIDER:

P BSA Visibility = Insightix (McAfee)
P IPSonar = Lumeta
P CCM, IP360 = nCircle
P Nmap = Open Source
P QualysGuard = Qualys
P Nexpose = Rapid7
P CCS, RAS = Symantec
P Nessus, Security Center = Tenable
S Clear Pass = Aruba Networks
S Network Sentry = Bradford Networks
S Identity Services Engine (ISE) = Cisco
S CounterAct = ForeScout Technologies

20
Penetration Testing and Red Team Exercises

SOLUTION = PROVIDER:

CORE IMPACT Pro = Core Security
Penetration Testing, Incident Response Capabilities Testing = Dell SecureWorks
Immunity CANVAS = Immunity CANVAS
Penetration Testing = Infogressive
Metasploit Free and Pro = Rapid7
SAINT = SAINT
MySecurityScanner = Secure Ideas
Armitage / Cobalt Strike = Strategic Cyber LLC

19
Secure Network Engineering

SOLUTION = PROVIDER:

Firewall Analyzer & FireFlow = AlgoSec
FirePAC = Athena Security
CloudPassage = CloudPassage
SecurityManager = FireMon
Network Design Experts = Infogressive
StealthWatch = Lancope
Network Advisor = RedSeal
Network Compliance Auditor = Skybox Security
Network Configuration Manager = Solarwinds
Enterprise = Tripwire
Tufin Appliance = Tufin

18
Incident Response and Management

SOLUTION = PROVIDER:

FTK with Cerebrus = AccessData
CarBonBlack = CarbonBlack
UFED = Cellebrite
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
Mandiant Intelligent Response (MIR) = Mandiant

3
Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers

SOLUTION = PROVIDER:

Deep Freeze = Faronics
Tivoli Endpoint Manager (BigFix) = IBM
Vulnerability Management = Lumension
System Center, Steady State = Microsoft
CCM, IP360 = nCircle
QualysGuard = Qualys
CSP = Symantec
Nessus, Security Center = Tenable
Enterprise = Tripwire
Configuration Manager = VMware

4
Continuous Vulnerability Assessment and Remediation

P PRIMARY:
Vulnerability Assessment

SOLUTION = PROVIDER:

P CORE IMPACT Pro = Core Security
P Vulnerability Management Services = Dell SecureWorks
P Retina = eEye Digital Security
P Vulnerability Management = Infogressive
P Vulnerability & Remediation Manager = McAfee
P IP360 = nCircle
P OpenVAS = Open Source
P QualysGuard (VM Module) = Qualys
P NexPose = Rapid7
P SAINT & SAINTmanager = SAINT
P CCS = Symantec
P Nessus, Security Center = Tenable

5
Malware Defense

P PRIMARY:
Endpoint Protection Platforms

S SECONDARY:
Application Whitelisting

SOLUTION = PROVIDER:

P vSentry = Bromium
P Enterprise, Security Pro = Invincea
P Adminstration Kit = Kaspersky
P ePolicy Orchestrator = McAfee
P Forefront, System Center = Microsoft
P Endoint Protection = Sophos
P SEP=Symantec
P Control Manager = Trend Micro
S Bit9 = Bit9
S Bouncer = CoreTrace
S SolidCore = McAfee

6
Application Software Security

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

SOLUTION = PROVIDER:

P Hailstorm Enterprise = Cenzic
P Checkmarx = Checkmarx
P Save = Coverity
P Managed Web App Firewall, Web Application Testing = Dell SecureWorks
P Fortify 360, Fortify on Demand, WebInspect = HP (Fortify)
P Ounce Labs Core, Appscan = IBM
P NTO Spider = NTObjectives
P QualysGuard WAS = Qualys
P Static/Dynamic = Veracode
P Sentinel = WhiteHat

7
Wireless Device Control

P PRIMARY:
Wireless LAN Intrusion Prevention System (WIPS)

SOLUTION = PROVIDER:

P WiFi Analyzer = AirMagnet (Fluke)
P WLS Manager = AirPatrol
P SpectraGuard = AirTight
P RF Protect = Aruba
P aWIPS, CleanAir = Cisco
P AirDefense = Motorola
P CCM = nCircle
P Nessus, Security Center = Tenable

8
Data Recovery Capability

SOLUTION = PROVIDER:

AccessData FTK and PRTK = AccessData
ElcomSoft EFDD, Bitlocker, TruCrypt = Elcom
Encase Enterprise Edition = Guidance Software
Mandiant Platform = Mandiant

9
Security Skills Assessment and Appropriate Training to Fill Gaps

SOLUTION = PROVIDER:

Assessment

Cyber Simulators (Netwars) and Skills Validation - SANS Institute
Cyber Skills Assessment - GIAC (SANS)

Skills Development

Dakota State University
Naval Postgraduate School
Northeastern
SANS Institute (50 Hands-on Immersion Courses)
SANS Technology Institute (STI) (Masters Degrees)
University of Tulsa
Security Awareness Training = SANS Institute
Virginia Tech

10
Secure Configurations for Firewalls, Routers, and Switches

P PRIMARY:
Network Policy Management (NPM)

SOLUTION = PROVIDER:

P Firewall Analyzer & FireFlow = AlgoSec
P FirePAC = Athena Security
P SecurityManager = FireMon
P Network Advisor = RedSeal
P Network Compliance Auditor = Skybox Security
P Network Configuration Manager = Solarwinds
P Enterprise = Tripwire
P Tufin Appliance = Tufin

11
Limitation and Control of Network Ports, Protocols, and Services

P PRIMARY:
Discovery, Vulnerability Assessment

S SECONDARY:
Application Firewall

SOLUTION = PROVIDER:

P BSA Visibility = Insightix (McAfee)
P IPSonar = Lumeta
P FoundScan = McAfee
P CCM, IP360 = nCircle
P QualysGuard = Qualys
P Nexpose = Rapid7
P CCS = Symantec
P Nessus, Security Center = Tenable
S 2200 = Checkpoint
S ASA Series and virtual ASA = Cisco
S SonicWall = Dell Sonicwall
S FortiGate = Fortinet
S SRX and vGW = Juniper
S PaloAlto NGFW = Palo Alto Networks

12
Controlled Use of Administrative Privileges

SOLUTION = PROVIDER:

PowerBroker = BeyondTrust
PIM = Cyber-Ark
eDMZ = Dell
ArcSight ESM, ArcSight Identify View = HP
Security Manager = Intellitactics (Trustwave)
System Center, Active Directory = Microsoft
CCM = nCircle
sudo = Open Source
Access Auditor = Security Compliance Corporation (SCC)
CCS = Symantec
Enterprise, Log Center = Tripwire
Xsuite = Xceedium

20 CRITICAL SECURITY CONTROLS SOLUTION PROVIDERS

Solutions listed on this poster were selected and reviewed by SANS Institute faculty and John Pescatore, a 34-year security veteran, the last 13 years as a Gartner Analyst covering Cyber Security, recently joined SANS as Director of Emerging Security Trends.

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

16
Account Monitoring and Control

SOLUTION = PROVIDER:

Privileged Identity Management Suite = Cyber-Ark
Log Management = Dell SecureWorks
HyTrust = HyTrust
Security Manager = Intellitactics (Trustwave)
AD Reports = MaxPowerSoft
System Center = Microsoft
QualysGuard PC = Qualys
Enterprise Security Reporter = Quest
Enterprise, Log Center = Tripwire

17
Data Loss Prevention

SOLUTION = PROVIDER:

DLP Software Blade = Checkpoint
TrueDLP = Code Green
XPS = Fidelis
FortiGate = Fortinet
McAfee DLP = McAfee
Tablus DLP = RSA
DLP = Symantec
DLP = Trend Micro
Digital Guardian = Verdasys

15
Controlled Access Based on Need to Know

P PRIMARY:
Enterprise Access Management

SOLUTION = PROVIDER:

P IAM = Aveska
P AAS = Courion
P HyTrust = HyTrust
P IAG = IBM
P Active Directory = Microsoft
P Identity Analytics = Oracle
P Identity IQ = Sailpoint
P Access Auditor = Security Compliance Corporation (SCC)
P Enterprise, Log Center = Tripwire

14
Maintenance, Monitoring, and Analysis of Audit Logs

P PRIMARY:
Security Information and Event Managemnt (SIEM)

SOLUTION = PROVIDER:

P OSSIM = AlienVault
P CorreLog Enterprise Server = Correlog
P Security Monitoring, Log Management = Dell SecureWorks
P ArcSight ESM, Logger = HP (ArcSight)
P Q1 = IBM
P Event Correlation = Infogressive
P StealthWatch = Lancope
P Open Log Management = LogLogic
P SIEM 2.0 = LogRhythm
P Snare = Open Source
P Event Data Warehouse = SenSage
P Enterprise = Splunk
P Log Correlation Engine = Tenable
P Security Information Management = TriGeo
P Log Center = Tripwire

13
Boundary Defense

P PRIMARY:
Firewall

S SECONDARY:
Intrusion Prevention System

SOLUTION = PROVIDER:

P 2200 = Checkpoint
P ASA Series and virtual ASA = Cisco
P SonicWall = Dell Sonicwall
P FortiGate = Fortinet
P SRX and vGW = Juniper
P PaloAlto NGFW = Palo Alto Networks
S Firewall Management, Managed NGFW, Managed IDS/IPS, Managed UTM, Security Monitoring = Dell SecureWorks
S XPS = Fidelis
S Fireeye Malware Protection System = FireEye
S TippingPoint = HP
S Network IPS = IBM (ISS)
S StealthWatch = Lancope
S Network Security Platform = McAfee
Snort = Open Source
S Firepower = Sourcefire

20 Critical Security Controls

for Effective Cyber Defense

Effective Cybersecurity – Now.

The 20 Critical Controls are being prioritized for implementation by organizations that understand the evolving risk of cyber attack. Leading adopters include the ***U.S. National Security Agency***, the ***British Centre for the Protection of National Infrastructure***, and the ***U.S. Department of Homeland Security Federal Network Security Program***. Ten state governments as well as power generation and distribution companies and defense contractors are among the hundreds of organizations that have shifted from a compliance focus to a security focus by adopting the Critical Controls.

All of these entities changed over to the Critical Controls in answer to the key question: **"What needs to be done right now to protect my organization from known attacks?"** Adopting and operationalizing the Critical Controls allows organizations to easily document those security processes to demonstrate compliance.

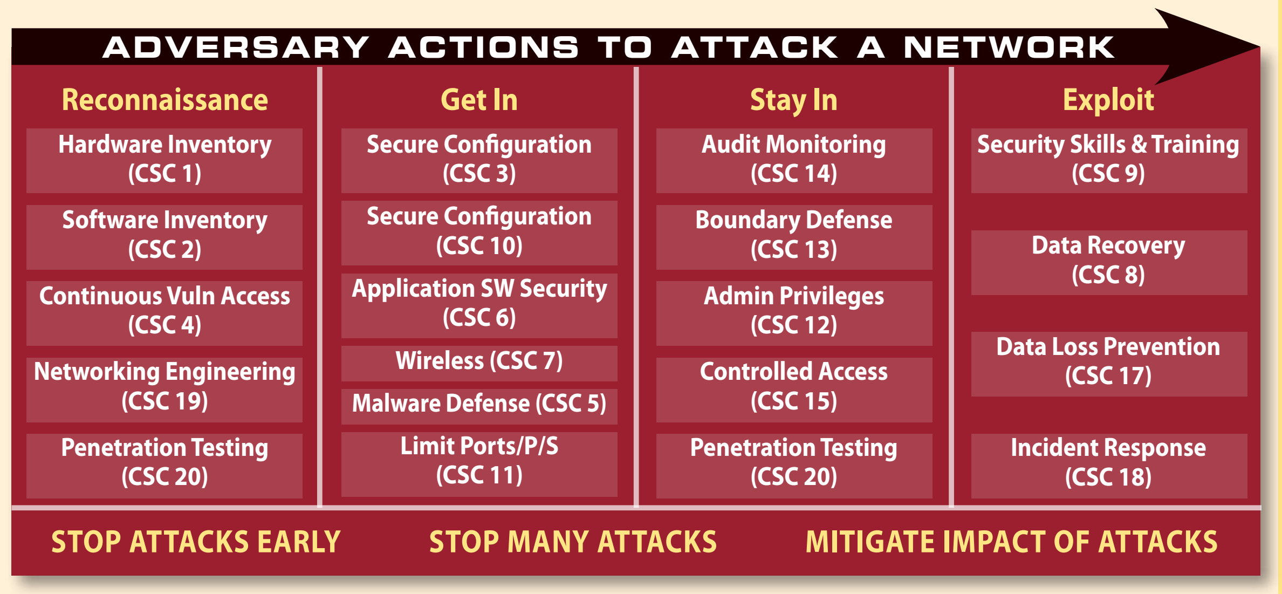
The Critical Controls reflect the consensus of major organizations with a deep understanding of how cyber attacks are carried out in the real world, why the attacks succeed, and what specific controls can stop them or mitigate their damage. Failure by management to implement the Critical Controls puts an organization's sensitive data or processes at great risk.

The Critical Controls are regularly updated by an international consortium headed by Tony Sager, who recently served as chief of the NSA's Vulnerability Analysis and Operations Group (which includes the NSA Red and Blue Teams and other top national cyber talent).

NSA's Attack Mitigation View Of The 20 Critical Controls

The National Security Agency categorized the 20 Critical Controls both by their attack mitigation impact and by their importance.

Categories of Attack Mitigation



ADVERSARY ACTIONS TO ATTACK A NETWORK

Reconnaissance	Get In	Stay In	Exploit
Hardware Inventory (CSC 1)	Secure Configuration (CSC 3)	Audit Monitoring (CSC 14)	Security Skills & Training (CSC 9)
Software Inventory (CSC 2)	Secure Configuration (CSC 10)	Boundary Defense (CSC 13)	Data Recovery (CSC 8)
Continuous Vuln Access (CSC 4)	Application SW Security (CSC 6)	Admin Privileges (CSC 12)	Data Loss Prevention (CSC 17)
Networking Engineering (CSC 19)	Wireless (CSC 7) Malware Defense (CSC 5)	Controlled Access (CSC 15)	
Penetration Testing (CSC 20)	Limit Ports/P/S (CSC 11)	Penetration Testing (CSC 20)	Incident Response (CSC 18)

STOP ATTACKS EARLY — STOP MANY ATTACKS — MITIGATE IMPACT OF ATTACKS

Ranking in Importance: In order for a Critical Control to be a priority, it must provide a direct defense against attacks. Controls that mitigate known attacks, a wide variety of attacks, attacks early in the compromise cycle, and the impact of a successful attack will have priority over other controls. Special consideration will be given to controls that help mitigate attacks that we haven't been discovered yet.

VERY HIGH These controls address operational conditions that are actively targeted and exploited by all threats.

HIGH These controls address known initial entry points for targeted attacks.

MEDIUM These controls reduce the attack surface, address known propagation techniques, and/or mitigate impact.

LOW These controls are about optimizing, validating, and/or effectively managing controls.

The Value of Automating the 20 Critical Controls

In order to effectively and efficiently combat advanced targeted threats, security controls need to be baked into repeatable organizational processes that use automation to support continuous monitoring, mitigation, and updates. Automating the Critical Controls provides daily, authoritative data on the readiness of computers to withstand attack as well as prioritized action lists for system administrators to maintain high levels of security.

At the U.S. State Department, the first federal agency to implement agency-wide automated security monitoring with unitary scoring, the risk score for eighty thousand computers across the Department dropped by nearly 90%, while scores for other agencies hardly changed at all (Chart 1 shows the State Department results). State's computers are safer because automation provides system administrators with unequivocal information on the most important security actions that need to be taken every day.

As importantly, when major new threats arose, the State Department was able to get 90% of its systems patched in 10 days (Chart 2), while other agencies, without automation, scoring, and system administration prioritization, got between 20% and 65% of their systems patched, and it took several months.

In another sign that agencies are stepping up investment in automation, the U.S. Department of Homeland Security recently announced a large procurement package to automate the first five of the Critical Controls across .gov networks with buying options for federal cloud initiatives and state and local governments.

Chart 1: 90% Risk Reduction In Less Than A Year *(U.S. State Department)*

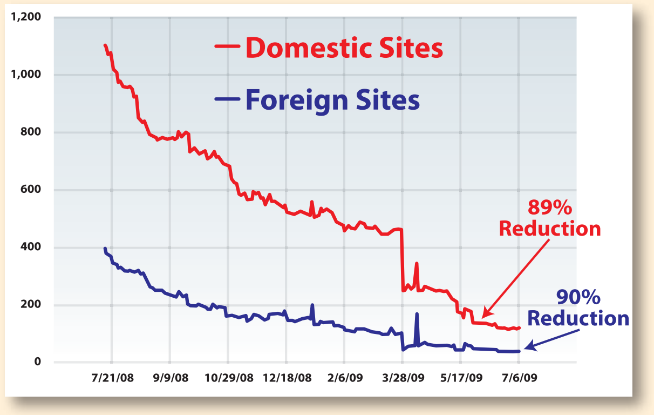
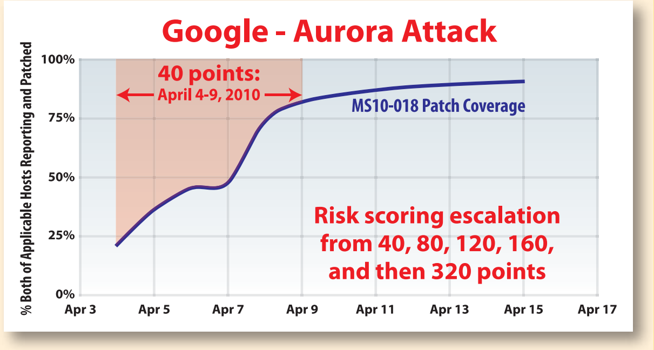


Chart 2: Threat-based mitigation: Giving the high priority fix a 40 point risk score gained rapid remediation to 80%; increasing it to 320 points pushed compliance to 90%. *(U.S. State Department)*



20 Critical Security Controls			National Security Agency Assessment of the 20 Critical Controls			
	Critical Security Control	Critical Security Control Description	Tier	Attack Mitigation	Dependencies	Technical Maturity
1	Inventory of Authorized and Unauthorized Devices	**Reduce the ability of attackers to find and exploit unauthorized and unprotected systems:** Use active monitoring and configuration management to maintain an up-to-date inventory of devices connected to the enterprise network, including servers, workstations, laptops, and remote devices.	1	Very High	Foundational	High
2	Inventory of Authorized and Unauthorized Software	**Identify vulnerable or malicious software to mitigate or root out attacks:** Devise a list of authorized software for each type of system, and deploy tools to track software installed (including type, version, and patches) and monitor for unauthorized or unnecessary software.	1	Very High	Foundational	High
3	Secure Configurations for Hardware & Software on Laptops, Workstations, and Servers	**Prevent attackers from exploiting services and settings that allow easy access through networks and browsers:** Build a secure image that is used for all new systems deployed to the enterprise, host these standard images on secure storage servers, regularly validate and update these configurations, and track system images in a configuration management system.	1a	Very High	Capability	High
4	Continuous Vulnerability Assessment and Remediation	**Proactively identify and repair software vulnerabilities reported by security researchers or vendors:** Regularly run automated vulnerability scanning tools against all systems and quickly remediate any vulnerabilities, with critical problems fixed within 48 hours.	1a	Very High	Capability	High
5	Malware Defenses	**Block malicious code from tampering with system settings or contents, capturing sensitive data, or spreading:** Use automated anti-virus and anti-spyware software to continuously monitor and protect workstations, servers, and mobile devices. Automatically update such anti-malware tools on all machines on a daily basis. Prevent network devices from using auto-run programs to access removable media.	1a	High/ Medium	Capability	High/ Medium
6	Application Software Security	**Neutralize vulnerabilities in web-based and other application software:** Carefully test internally developed and third-party application software for security flaws, including coding errors and malware. Deploy web application firewalls that inspect all traffic, and explicitly check for errors in all user input (including by size and data type).	2	High	Capability	Medium
7	Wireless Device Control	**Protect the security perimeter against unauthorized wireless access:** Allow wireless devices to connect to the network only if they match an authorized configuration and security profile and have a documented owner and defined business need. Ensure that all wireless access points are manageable using enterprise management tools. Configure scanning tools to detect wireless access points.	2	High	Capability	Medium
8	Data Recovery Capability	**Minimize the damage from an attack:** Implement a trustworthy plan for removing all traces of an attack. Automatically back up all information required to fully restore each system, including the operating system, application software, and data. Back up all systems at least weekly; back up sensitive systems more often. Regularly test the restoration process.	2	Medium	Capability	Medium
9	Security Skills Assessment and Appropriate Training to Fill Gaps	**Find knowledge gaps, and fill them with exercises and training:** Develop a security skills assessment program, map training against the skills required for each job, and use the results to allocate resources effectively to improve security practices.	2	Medium	Capability	Medium
10	Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	**Preclude electronic holes from forming at connection points with the Internet, other organizations, and internal network segments:** Compare firewall, router, and switch configurations against standards for each type of network device. Ensure that any deviations from the standard configurations are documented and approved and that any temporary deviations are undone when the business need abates.	3	High/ Medium	Capability/ Dependent	Medium/ Low
11	Limitation and Control of Network Ports, Protocols, and Services	**Allow remote access only to legitimate users and services:** Apply host-based firewalls and port-filtering and -scanning tools to block traffic that is not explicitly allowed. Properly configure web servers, mail servers, file and print services, and domain name system (DNS) servers to limit remote access. Disable automatic installation of unnecessary software components. Move servers inside the firewall unless remote access is required for business purposes.	3	High/ Medium	Capability/ Dependent	Medium/ Low
12	Controlled Use of Administrative Privileges	**Protect and validate administrative accounts on desktops, laptops, and servers to prevent two common types of attack:** (1) enticing users to open a malicious e-mail, attachment, or file, or to visit a malicious website; and (2) cracking an administrative password and thereby gaining access to a target machine. Use robust passwords that follow Federal Desktop Core Configuation (FDCC) standards.	4	High/ Medium	Dependent	Medium
13	Boundary Defense	**Control the flow of traffic through network borders, and police content by looking for attacks and evidence of compromised machines:** Establish multilayered boundary defenses by relying on firewalls, proxies, demilitarized zone (DMZ) perimeter networks, and other network-based tools. Filter inbound and outbound traffic, including through business partner networks ("extranets").	4	High/ Medium	Dependent	Medium/ Low
14	Maintenance, Monitoring, and Analysis of Security Audit Logs	**Use detailed logs to identify and uncover the details of an attack, including the location, malicious software deployed, and activity on victim machines:** Generate standardized logs for each hardware device and the software installed on it, including date, time stamp, source addresses, destination addresses, and other information about each packet and/or transaction. Store logs on dedicated servers, and run biweekly reports to identify and document anomalies.	4	Medium	Dependent	Medium
15	Controlled Access Based on the Need to Know	**Prevent attackers from gaining access to highly sensitive data:** Carefully identify and separate critical data from information that is readily available to internal network users. Establish a multilevel data classification scheme based on the impact of any data exposure, and ensure that only authenticated users have access to nonpublic data and files.	4	Medium	Dependent	Medium/ Low
16	Account Monitoring and Control	**Keep attackers from impersonating legitimate users:** Review all system accounts and disable any that are not associated with a business process and owner. Immediately revoke system access for terminated employees or contractors. Disable dormant accounts and encrypt and isolate any files associated with such accounts. Use robust passwords that conform to FDCC standards.	4	Medium	Dependent	Medium/ Low
17	Data Loss Prevention	**Stop unauthorized transfer of sensitive data through network attacks and physical theft:** Scrutinize the movement of data across network boundaries, both electronically and physically, to minimize the exposure to attackers. Monitor people, processes, and systems, using a centralized management framework.	5	Medium/ Low	Dependent	Low
18	Incident Response Management	**Protect the organization's reputation, as well as its information:** Develop an incident response plan with clearly delineated roles and responsibilities 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.	5	Medium	Dependent	Low
19	Secure Network Engineering	**Keep poor network design from enabling attackers:** Use a robust, secure network engineering process to prevent security controls from being circumvented. Deploy a network architecture with at least three tiers: DMZ, middleware, private network. Allow rapid deployment of new access controls to quickly deflect attacks.	6	Low	Indirect	Low
20	Penetration Tests and Red Team Exercises	**Use simulated attacks to improve organizational readiness:** Conduct regular internal and external penetration tests that mimic an attack to identify vulnerabilities and gauge the potential damage. Use periodic red team exercises—all-out attempts to gain access to critical data and systems to test existing defenses and response capabilities.	6	Low	Indirect	Low

Support for Implementing the Controls is a Click Away

Here are some additional resources for effective planning and implementation of the 20 Critical Controls:

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

2) The SANS "Solutions" (**www.sans.org/critical-security-controls/vendor-solutions**) posts case studies of organizations that have used various tools to implement and operationalize the Controls. Many vendors claim to automate the Critical Controls, but the case studies provide real-world evidence that you should look at for before buying any product.

3) Courses on planning and implementing the 20 Critical Controls include:
2-day courses: www.sans.org/course/20-critical-security-controls-planning-implementing-auditing
6-day in-depth courses: www.sans.org/course/implementing-auditing-twenty-critical-security-controls

4) Summits in London and Washington where managers from user organizations and strategists from vendor companies share lessons learned and plan for future improvements: **www.sans.org/event/critical-security-controls-international-summit**

5) The Consortium for Cybersecurity Action, a virtual community of more than 100 agencies, companies, and individuals that supports ongoing updates to the Critical Controls, provides information on use cases, working aids, mappings, and other tools to help others adopt and implement the Controls. **www.cyberaction.org**

SANS
Spring 2013

CPNI Centre for the Protection of National Infrastructure

Homeland Security

Getting Started Part I: Implement the First Five Quick Wins

The Critical Controls represent the biggest bang for the buck to protect your organization against real security threats. Within Critical Controls 2-4 are five "quick wins." These are subcontrols that have the most immediate impact on preventing the advanced targeted attacks that have penetrated existing controls and compromised critical systems at thousands of organizations. The five quick wins are:

1. **Application white listing (in CSC2)**
2. **Using common, secure configurations (in CSC3)**
3. **Patch application software within 48 hours (in CSC4)**
4. **Patch systems software within 48 hours (CSC4)**
5. **Reduce the number of users with administrative privileges (in CSC3 and CSC12)**

Getting Started Part II: When Planning Implementation of the Other Critical Controls, 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 www.sans.org/critical-security-controls/vendor-solutions.
- **Where can I learn more?** See the list of resources at the bottom of this poster.

Seven Reasons Why Top Managers Are Supporting Security Professionals Who Implement the 20 Critical Controls

1) The Contributors

A virtual community of more than 100 of the most trusted government agencies, private companies, and top-rated experts ensure that the Critical Controls are continuously and thoroughly updated to combat all threats on the horizon. This means that every organization that implements the Critical Controls has the direct benefit of a world of expertise that could not be purchased at any cost.

Known at the Consortium for Cybersecurity Action (CCA), the community includes the National Security Agency, the Department of Homeland Security, U.K. Centre for the Protection of National Infrastructure, Mandiant, Qualys, Symantec, McAfee, nCircle, and CoreImpact. The CCA is led by the Tony Sager, recently retired chief of the NSA's Vulnerability Analysis, and draws on the expertise of such renowned specialists as Ed Skoudis, Dr. Eric Cole, Dr. Johannes Ullrich, and John Pescatore.

The collective experience of these organizations and individuals spans every dimension of the business, including threat, vulnerability, technology, risk management, and cyber defense. This knowledge is then translated into action: what are the most important Controls your enterprise needs to adopt right now to stop the attacks we see every day? How can your enterprise implement the Controls in a cost-effective, manageable, and automated way?

2) Keeping the Focus on High-Priority Security Actions

Compliance regimes contain literally thousands of security requirements that are all treated equally. What has been lacking is a consensus method of prioritizing the highest payback areas to focus on first. The Critical Controls are driven by an "Offense Informs Defense" philosophy that uses specific knowledge of actual attacks to set risk-based priority for effective defense. They don't attempt to solve every security problem, but instead focus on the steps to ward off known attacks. This gives top managers confidence that they are focusing their resources on the highest-value and most cost-effective defensive strategy. Demonstration of compliance then becomes largely a reporting effort.

3) Successes

The Critical Controls reduced risk by more than 90% at the U.S. State Department when they were automated in a continuous monitoring and mitigation program.

4) The Adopters

The Critical Controls have been adopted by hundreds of enterprises across many nations and spanning every sector, including government, finance, energy, academia, defense, consulting, construction, health care, and transportation. The U.S. Department of Homeland Security has adopted the Controls and put in place contracts to help federal, state, and local agencies acquire the technology to implement them. The U.K.'s Center for the Protection of National Infrastructure (CPNI) selected the Critical Controls as a national baseline of high-priority information security measures and controls.

5) The Controls Are Supported by Tools

The Controls were specifically chosen for effectiveness against real threats and with an eye toward off-the-shelf automation and continuous management of security. Dozens of tool vendors have become part of the Consortium for Cybersecurity Action, bringing their expertise to improve the Controls. Many more have chosen to support the Controls with their products and services. Vendors have posted white papers with success stories of how their customers have implemented and operationalized the Controls, and with more general descriptions of how their products map to the Controls. Enterprises are also making use of numerous freeware and open source options.

6) The Controls Map to Existing Security Frameworks

The Critical Controls complement existing frameworks and compliance regimes by bringing community consensus to a small number of high-priority, actionable steps that provide the most security value in terms of stopping attacks. They map well into existing frameworks and are a logical starting point for compliance with larger, more comprehensive frameworks. With their focus on measurement and automation, the Controls are particularly supportive of the movement toward continuous monitoring and a more dynamic view of cyber-defense.

7) The Controls Provide a Manageable Roadmap to Improve Security

Many adopters of the Critical Controls tell the same story: the Controls have provided the "aha" moment to demonstrate to CEOs and agency heads the value of investing in security improvement. Initial gap assessment of how your enterprise's security matches up against the Controls provides the baseline. Quick wins demonstrate that the Controls bring immediate results. An implementation roadmap is developed and agreed to by senior management. Progress against the roadmap (using timelines, stoplight charts, etc.) then becomes the reporting mechanism to track progress, identify resource issues, and support decision-making. This approach keeps the focus away from the technology and the thousands of action items, and squarely on management and progress of implementation.

A Support Network for All: The Consortium for Cybersecurity Action

The Consortium for Cybersecurity Action (CCA) is a virtual community of more than 100 agencies, companies, and individuals that leads the development and evolution of the Critical Controls. The CCA is also creating the support ecosystem of use cases, working aids, mappings, and tools to help others adopt and implement the Critical Controls. And it sponsors Special Action Group volunteers who take on specific topics (e.g., how to apply the Controls to a specific critical sector) and create products and ideas to share with the entire community.

Individual or enterprise, you can become a part of this international movement at no cost, and with no specific time obligation. Bring your experience to the areas that match your expertise, interests, and mission. The CCA brings together people and institutions to improve the Controls, learn from the experiences of others, and find and break down common barriers to more effective cyber defense. To learn more about the CCA, go to **www.cyberaction.org**.