



Interested in learning more
about cyber security training?

SANS Institute InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Back to Basics: Focus on the First Six CIS Critical Security Controls

Post-breach investigations reveal that the majority of security incidents occur because well-known security controls and practices were not implemented or were not working as organizations had assumed. This paper explores how Version 7.0 of the Center for Internet Security (CIS) Critical Security Controls addresses the current threat landscape, emerging technologies and tools, and changing mission and business requirements around security.

Copyright SANS Institute
Author Retains Full Rights

Back to Basics: Focus on the First Six CIS Critical Security Controls

Written by **John Pescatore**
Updated by **Barbara Filkins**

April 2018

Sponsored by:
Tripwire

Introduction

Year after year, investigations performed after breaches and other security incidents reveal that the majority of security incidents occur because well-known security controls and practices were not implemented or were not working as organizations had assumed. And the major problem in cyber security remains a lack of defined and repeatable processes for selecting, implementing and monitoring the security controls that are most effective against real-world threats.

The Center for Internet Security (CIS) Critical Security Controls¹ has proven to be a valuable, effective framework for addressing this problem. First, the Controls are informed by real-world attacks and effective defenses, creating a prioritized set of actions that organizations can take to assess and improve their current security state. Second, the Controls are not static, with each new release harnessing the experience of a global community to ensure that the Controls remain well-vetted and supported.

The Version 7.0 update addresses the current threat landscape, emerging technologies and tools, and changing mission and business requirements around security. For these reasons, SANS elected to update this white paper.

Figure 1 (on the next page) lists the Controls in the CIS latest version, Version 7.0.

¹ www.cisecurity.org/critical-controls.cfm



Ongoing Community Effort

In 2008, the Information Assurance Directorate (IAD) of the National Security Agency was tasked with performing penetration testing and “red team” exercises against government and critical infrastructure systems. Although many of those systems had been audited and were considered compliant with existing requirements, the IAD teams regularly succeeded in compromising supposedly well-protected government systems. The reason? Security resources were being diluted by compliance mandates. Because auditors equally weighted all security requirements, security teams did the same. Not all risks are equal, nor should the Controls be equally weighted. NSA IAD began an effort to address that problem, starting with a few key concepts:

- **Offense should inform defense.** Security controls should be chosen because they have been proven effective in real-world use against real-world attacks.
- **Prioritize “must do” over “good to do.”** Security resources are not infinite; prioritize security controls and auditor attention in order of “bang for the buck.”
- **Enlist community participation.** Involve red teams, defenders and security managers from across government and industry to periodically update the list and priority as threats and security processes evolve.

The initial effort produced what was known as the “Consensus Audit Guidelines,” published by the Center for Strategic and International Studies. The approach proved successful at NSA, and to reach the broader security community, the effort transitioned to the SANS Institute and became known as the SANS Top 20 Critical Security Controls. In 2015, stewardship of the process was moved to the Center for Internet Security, which led the community effort to update the Controls and produce Version 6.0.

Focus on the First Six

Version 7.0 of the Critical Security Controls recommends the first six Critical Controls as the highest priority and considered as among the very first set of activities to be accomplished. CIS refers to these Controls as “Cyber Hygiene”—the basic things that you must do to create a strong foundation for your defense.”²

“The [CIS Controls] identify a minimum level of information security that all organizations that collect or maintain personal information should meet.”

Kamala D. Harris, Attorney General, California Department of Justice³

Basic CIS Controls

1. Inventory and Control of Hardware
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Assessment and Remediation
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs

Foundational CIS Controls

7. Email and Web Browser Protection
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols and Services
10. Data Recovery Capabilities
11. Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control

Organizational CIS Controls

17. Implement a Security Awareness and Training Program
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

Figure 1. Critical Security Controls Defined by the CIS

² <https://learn.cisecurity.org/20-controls-download>, CIS Controls V7, p. 5

³ <https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf>

The CIS Critical Security Controls are an example of the Pareto Principle at work: 80 percent of the impact comes from 20 percent of the effort. Adoption of the first six CIS Critical Security Controls have proven to deliver a highly effective and efficient level of defense for a number of organizations against the majority of real-world attacks and provide the necessary foundation for dealing with more advanced attacks.

In Version 7.0, the first six Controls essentially focus on the basics to prevent disruptive attacks, including configuration management, vulnerability assessment and continuous monitoring to know when a new critical vulnerability surfaces or an asset becomes exposed. See Table 2 on the next page.

By implementing CIS Controls 1–6 as continuous and evolving processes, organizations can reduce risk while adapting to both changing threats and changing business demands. These should be implemented in every organization for essential cyber defense readiness. Without this foundation, it is impossible to effectively or efficiently implement the higher-level Controls.

Basic Hygiene

CIS Controls 1–6 focus on the fundamentals of securing the infrastructure and monitoring it regularly for changes. The Critical Security Controls guidance recommends monitoring assets at least weekly, yet only 37 percent of respondents to the SANS 2016 Continuous Monitoring survey conduct scanning at least once per week. Of those who were monitoring regularly, 48 percent cited improved visibility into their infrastructures as a result of their programs.⁵

Main Changes in 7.0 Update

In March 2018, the Version 7.0 update from the community effort resulted in the following major changes to the CIS Controls:

- Identify types of CIS Controls, separating them into three distinct categories:
 - Basic (CIS Controls 1–6): Key controls that should be implemented in every organization for essential cyber defense readiness
 - Foundational (CIS Controls 7–16): Technical best practices that provide clear security benefits and are a smart move for any organization to implement
 - Organizational (CIS Controls 17–20): Controls focused on people and processes involved in cybersecurity
- Structural changes and wording changes to make the Controls easier to measure, monitor, and implement—specifically, several subcontrols were restated so there is one “ask” or one requirement per subcontrol.
- Renaming and reordering of the top six controls as illustrated in Table 1:

Table 1. Comparison of CIS Controls 1–6 from Version 6 to Version 7

Control #	CIS Controls V6	CIS Controls V7
1	Inventory of Authorized and Unauthorized Devices	Inventory and Control of Hardware Assets
2	Inventory of Authorized and Unauthorized Software	Inventory and Control of Software Assets
3	Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	Continuous Vulnerability Management
4		Controlled Use of Administrative Privileges
5	Continuous Vulnerability Assessment and Remediation	Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6	Controlled Use of Administrative Privileges	Maintenance, Monitoring, and Analysis of Audit Logs
	Maintenance, Monitoring, and Analysis of Audit Logs	Maintenance, Monitoring and Analysis of Audit Logs

“Start by taking care of the basics: Build a solid cybersecurity foundation by implementing the [CIS Controls], especially application white-listing, standard secure configurations, reduction of administrative privileges, and a quick patching process.”

Zurich Insurance Group, Switzerland⁴

⁴ <https://www.cisecurity.org/testimonials>

⁵ “Reducing Attack Surface: SANS’ Second Survey on Continuous Monitoring Programs,” pg. 1, Table 1, “Continuous Monitoring Report Card” www.sans.org/reading-room/whitepapers/analyst/reducing-attack-surface-sans'-second-survey-continuous-monitoring-programs-37417

Common Success Patterns

The Australian Signals Directorate,⁶ the Center for Internet Security⁷ and the SANS WhatWorks program,⁸ as well as other case studies at organizations that have successfully implemented Controls 1–6, provide some lessons learned for success in implementing the CIS Controls, including:

1. Use Common Processes/Shared Tools Across IT Operations and Security.

In most organizations, IT operations is responsible for configuration management, while the security team is responsible for vulnerability assessment. Privilege management is often a shared responsibility, and both IT operations and security have requirements for continuous monitoring. When security and IT operations teams work together to emphasize the use of common processes, data standards and shared (or at least integrated) tools, costs can be reduced and responsiveness increased.

2. Minimize Business Disruption.

Through the years, most of the resistance to standard configurations and limited administrator privileges has come from users complaining about restrictions or slow responses to requests that have an impact on business operations. The inventory of software applications should be driven by business needs, and “fast-track” mechanisms should be supported to enable rapid deployment of new applications with appropriate security monitoring to reduce risk. Business security beta testers can be recruited for small-scale tests of new security Controls before widespread rollouts.

Table 2. First Six CIS Controls: High Impact, Immediate Benefits

Category	Control Title(s)	Why It's So Important
Know What You Are Protecting	CIS Control #1: Inventory and Control of Hardware Assets CIS Control #2: Inventory and Control of Software Assets	The first two Controls require rigor in knowing what endpoints must be protected and what software is running on those endpoints. Although many IT organizations have some version of a Configuration Management Database, invariably security teams find devices and software that are either not visible to or not managed by IT operations.
Continuously Monitor Vulnerability of Resources	CIS Control #3: Continuous Vulnerability Management	After the baseline is known and endpoints are configured securely, those configurations must be monitored for changes that introduce vulnerabilities or the availability of patches or upgrades needed to maintain security.
Limit and Monitor Administrative Privileges	CIS Control #4: Controlled Use of Administrative Privileges	Having addressed the basic vulnerabilities of the hardware and software resources, the vulnerabilities of user accounts must be minimized. Maintaining the least privilege to support “need to share” while maintaining “need to know” can keep malicious software from successfully executing if it does get installed.
Define Secure Configuration Baselines	CIS Control #5: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers	With an accurate inventory and the ability to continuously monitor assets, the next step is to establish, implement and actively manage the configuration of endpoints against configuration standards, such as the CIS benchmarks, the United States Department of Defense (DoD) Security Technical Implementation Guide (STIG) and so forth.
Continuous Monitoring/Situational Awareness	CIS Control #6: Maintenance, Monitoring and Analysis of Audit Logs	Nothing stands still: IT installs new software, threats develop new attacks, organizations and priorities change. Situational awareness is key for security teams to focus on deploying resources in the most effective and efficient areas to meet business security needs.

The concepts underlying CIS Controls 1–6 represent well-known, basic security hygiene.

⁶ www.asd.gov.au/infosec/mitigationstrategies.htm

⁷ <https://www.cisecurity.org/cis-ram-puts-the-cis-controls-into-action>

⁸ www.sans.org/vendor/whatworks

- 3. Demonstrate Real Risk Reduction.** CEOs and boards of directors are aware of the need for basic organizational competency in areas such as manufacturing, customer service and finances before advanced business challenges can be attacked. The Critical Security Controls can be sold as being as effective for security as ISO9000 and the generally accepted accounting principles (GAAP) are in other disciplines, and their value can be demonstrated by tracking metrics that directly connect to business risk reduction.⁹ “Mean time to detect an incident” and “mean time to restore operations” are two key metrics that improve significantly when the first six Critical Security Controls are implemented correctly.
- 4. Extend to the “Next Big Thing” à la cloud, IoT, etc.** The “choose your own IT” trend is not going away, as business users continue to demand the ability to use new devices and cloud services both internally and when delivering services to customers. Security teams defining architectures, processes and Controls selections must avoid tunnel vision on standard Windows PCs and Windows/Linux servers, and include standards, interfaces and other mechanisms to work across a wide variety of consumer-driven hardware and software.
- 5. Combine Skilled Staff with “Force Multipliers.”** Although there is a lot of publicity around staffing shortfalls in cyber security, the most successful organizations don’t generally have the largest staffs. Training security staff in the Critical Security Controls and related technologies—combined with the use of security tools that automate routine tasks—is a common characteristic of effective, efficient and successful cyber security programs.

Summary

Press coverage focuses on advanced targeted threats and zero-day attacks, but most of the damage caused by cyber security incidents is enabled by security programs that have been unable to implement mature processes. The CIS Critical Security Controls has been successful in providing a framework for addressing those deficiencies and delivering basic foundational levels of security. In particular, the first six of the Critical Security Controls provide a proven jump-start to rapidly reducing the risk of business impact due to real-world cyber security attacks.

⁹ The CIS-CAT Benchmark Assessment Tool: <https://benchmarks.cisecurity.org/downloads/audit-tools>

About the Authoring Team

John Pescatore joined SANS as director of emerging technologies in January 2013 after more than 13 years as lead security analyst for Gartner, 11 years with GTE, and service with both the National Security Agency, where he designed secure voice systems, and the U.S. Secret Service, where he developed secure communications and voice systems “and the occasional ballistic armor installation.” John has testified before Congress about cyber security, was named one of the 15 most-influential people in security in 2008 and remains an NSA-certified cryptologic engineer.

Barbara Filkins, a senior SANS analyst, holds several SANS certifications, including the GSEC, GCIH, GCPM, GLEG and GICSP, the CISSP, and an MS in information security management from the SANS Technology Institute. She has done extensive work in system procurement, vendor selection and vendor negotiations as a systems engineering and infrastructure design consultant. Barbara focuses on issues related to automation—privacy, identity theft and exposure to fraud, plus the legal aspects of enforcing information security in today’s mobile and cloud environments, particularly in the health and human services industry, with clients ranging from federal agencies to municipalities and commercial businesses.

Sponsor

SANS would like to thank this paper’s sponsor:





Upcoming SANS Training

[Click here to view a list of all SANS Courses](#)

SANS Copenhagen August 2018	Copenhagen, DK	Aug 27, 2018 - Sep 01, 2018	Live Event
SANS SEC504 @ Bangalore 2018	Bangalore, IN	Aug 27, 2018 - Sep 01, 2018	Live Event
SANS Tokyo Autumn 2018	Tokyo, JP	Sep 03, 2018 - Sep 15, 2018	Live Event
SANS Amsterdam September 2018	Amsterdam, NL	Sep 03, 2018 - Sep 08, 2018	Live Event
SANS Wellington 2018	Wellington, NZ	Sep 03, 2018 - Sep 08, 2018	Live Event
SANS MGT516 Beta One 2018	Arlington, VAUS	Sep 04, 2018 - Sep 08, 2018	Live Event
SANS Tampa-Clearwater 2018	Tampa, FLUS	Sep 04, 2018 - Sep 09, 2018	Live Event
Threat Hunting & Incident Response Summit & Training 2018	New Orleans, LAUS	Sep 06, 2018 - Sep 13, 2018	Live Event
SANS Baltimore Fall 2018	Baltimore, MDUS	Sep 08, 2018 - Sep 15, 2018	Live Event
SANS Alaska Summit & Training 2018	Anchorage, AKUS	Sep 10, 2018 - Sep 15, 2018	Live Event
SANS Munich September 2018	Munich, DE	Sep 16, 2018 - Sep 22, 2018	Live Event
SANS London September 2018	London, GB	Sep 17, 2018 - Sep 22, 2018	Live Event
SANS Network Security 2018	Las Vegas, NVUS	Sep 23, 2018 - Sep 30, 2018	Live Event
SANS DFIR Prague Summit & Training 2018	Prague, CZ	Oct 01, 2018 - Oct 07, 2018	Live Event
Oil & Gas Cybersecurity Summit & Training 2018	Houston, TXUS	Oct 01, 2018 - Oct 06, 2018	Live Event
SANS Brussels October 2018	Brussels, BE	Oct 08, 2018 - Oct 13, 2018	Live Event
SANS Amsterdam October 2018	Amsterdam, NL	Oct 08, 2018 - Oct 13, 2018	Live Event
SANS Riyadh October 2018	Riyadh, SA	Oct 13, 2018 - Oct 18, 2018	Live Event
SANS Northern VA Fall- Tysons 2018	Tysons, VAUS	Oct 13, 2018 - Oct 20, 2018	Live Event
SANS October Singapore 2018	Singapore, SG	Oct 15, 2018 - Oct 27, 2018	Live Event
SANS London October 2018	London, GB	Oct 15, 2018 - Oct 20, 2018	Live Event
SANS Denver 2018	Denver, COUS	Oct 15, 2018 - Oct 20, 2018	Live Event
SANS Seattle Fall 2018	Seattle, WAUS	Oct 15, 2018 - Oct 20, 2018	Live Event
Secure DevOps Summit & Training 2018	Denver, COUS	Oct 22, 2018 - Oct 29, 2018	Live Event
SANS Houston 2018	Houston, TXUS	Oct 29, 2018 - Nov 03, 2018	Live Event
SANS Gulf Region 2018	Dubai, AE	Nov 03, 2018 - Nov 15, 2018	Live Event
SANS Sydney 2018	Sydney, AU	Nov 05, 2018 - Nov 17, 2018	Live Event
SANS Dallas Fall 2018	Dallas, TXUS	Nov 05, 2018 - Nov 10, 2018	Live Event
SANS London November 2018	London, GB	Nov 05, 2018 - Nov 10, 2018	Live Event
SANS DFIRCON Miami 2018	Miami, FLUS	Nov 05, 2018 - Nov 10, 2018	Live Event
Pen Test HackFest Summit & Training 2018	Bethesda, MDUS	Nov 12, 2018 - Nov 19, 2018	Live Event
SANS Osaka 2018	Osaka, JP	Nov 12, 2018 - Nov 17, 2018	Live Event
SANS San Francisco Summer 2018	OnlineCAUS	Aug 26, 2018 - Aug 31, 2018	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced