Interested in learning more about security?

SANS Institute InfoSec Reading Room

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

Rather than a lack of choices in security solutions, a major problem in cyber security is an inability to implement mature processes - many organizations lack a defined and repeatable process for selecting, implementing and monitoring the security controls that are most effective against real-world threats. This paper explores how the Center for Internet Security (CIS) Critical Security Controls has proven to be an effective framework for addressing that problem.

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

A SANS Spotlight Whitepaper

Written by John Pescatore

January 2017

Sponsored by
Tripwire

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.

Rather than a lack of choices in security solutions, the major problem in cyber security is a lack of a defined and repeatable process for selecting, implementing and monitoring the security controls that are most effective against real-world threats. The Center for Internet Security (CIS) Critical Security Controls[1] has proven to be an effective framework for addressing that problem. Figure 1 lists the Controls in the CSC's latest version, version 6.1.

Figure 1. Top 20 Critical Security Controls Defined by the CIS

[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.

Main Changes in 6.0 Update

In October 2015, the Version 6.0 update from the community effort resulted in some changes to CIS Controls rankings, including:

- "Controlled Use of Administrative Privileges" was increased in priority, moving from Control #12 to Control #5, recognizing the high number of attacks that were taking advantage of overprivileged accounts.
- Control #19: "Secure Network Engineering" was deleted, as the key concepts of segmentation were covered in other areas.
- A new Control #7: "Email and Web Browser Protections" was added, based on the high percentage of incidents caused by threats initiated by phishing attacks.
- Subcontrols were grouped into one of three families: System, Network or Application, to aid in deployment planning and to clarify mapping to frameworks such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

Latest Version: 6.1

Version 6.1 of the Critical Security Controls, updated in August 2016, still recommends the first four Critical Controls as the highest priority. Accurate inventory and vulnerability knowledge of hardware, software and configurations remain the basic fundamental needs for effective and efficient cyber security.

Focus on the First Six

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. That truism also applies to the Controls themselves. In 2013, the Australian Signals Directorate reported preventing at least 85 percent of targeted cyber intrusions through proper implementation of the first four Controls (know your devices and apps, secure configurations and continuous monitoring/assessment).[2]

[2] www.asd.gov.au/infosec/mitigationstrategies.htm

In today's version, 6.1, 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 1.

Implementations of the first six CIS Critical Security Controls have proven to deliver a highly effective and efficient level of defense against the majority of real-world attacks and provide the necessary foundation for dealing with more advanced attacks.

Table 1. 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 of Authorized and Unauthorized Devices** **CIS Control #2: Inventory of Authorized and Unauthorized Software**	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.
Define Secure Configuration Baselines	**CIS Control #3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers**	With an accurate inventory in place, the next step is evaluating 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.
Continuously Monitor Vulnerability of Resources	**CIS Control #4: Continuous Vulnerability Assessment and Remediation**	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 #5: 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.
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.

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.

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

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.[3]

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

Common Success Patterns

The Australian Signals Directorate,[4] the Center for Internet Security[5] and the SANS WhatWorks program,[6] 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.

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.[7] "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] www.asd.gov.au/infosec/mitigationstrategies.htm

[5] Practical Guidance for Implementing the Critical Security Controls (V6): https://www.cisecurity.org/critical-controls/documents/Controls Practical Guidance for Web v4.pdf

[6] www.sans.org/vendor/whatworks

[7] The CIS-CAT Benchmark Assessment Tool: https://benchmarks.cisecurity.org/downloads/audit-tools/

4. **Extend to the "Next Big Thing" à la Cloud, Internet of Things, 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.

About the Author

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.

Sponsor

SANS would like to thank this paper's sponsor:

Last Updated: June 27th, 2017

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS London July 2017	London, GB	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, JP	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Los Angeles - Long Beach 2017	Long Beach, CAUS	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS ICS & Energy-Houston 2017	Houston, TXUS	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, SG	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, DE	Jul 10, 2017 - Jul 15, 2017	Live Event
SANSFIRE 2017	Washington, DCUS	Jul 22, 2017 - Jul 29, 2017	Live Event
Security Awareness Summit & Training 2017	Nashville, TNUS	Jul 31, 2017 - Aug 09, 2017	Live Event
SANS San Antonio 2017	San Antonio, TXUS	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Hyderabad 2017	Hyderabad, IN	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, CZ	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MAUS	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS New York City 2017	New York City, NYUS	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UTUS	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VAUS	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Chicago 2017	Chicago, ILUS	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Adelaide 2017	Adelaide, AU	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS San Francisco Fall 2017	San Francisco, CAUS	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FLUS	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Network Security 2017	Las Vegas, NVUS	Sep 10, 2017 - Sep 17, 2017	Live Event
SANS Dublin 2017	Dublin, IE	Sep 11, 2017 - Sep 16, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, DK	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, GB	Sep 25, 2017 - Sep 30, 2017	Live Event
Rocky Mountain Fall 2017	Denver, COUS	Sep 25, 2017 - Sep 30, 2017	Live Event
Data Breach Summit & Training	Chicago, ILUS	Sep 25, 2017 - Oct 02, 2017	Live Event
SANS SEC504 at Cyber Security Week 2017	The Hague, NL	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MDUS	Sep 25, 2017 - Sep 30, 2017	Live Event
SEC564:Red Team Ops	OnlineCAUS	Jun 29, 2017 - Jun 30, 2017	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced