Solution Provider Poster Sponsors

Through their sponsorship, the technology providers below helped bring this poster to the SANS community. Sponsorship had no connection with the rankings of product measurement capabilities.



Monitoring and Measuring the CIS Critical **Security Controls**

Products and Strategies for Continuously Monitoring and Improving Your Implementation of the CIS Critical Security Controls

THE CENTER FOR INTERNET SECURITY (CIS) CRITICAL SECURITY CONTROLS V6.0

CSC 19

Incident Response and Management

Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight).

CSC 20

Penetration Tests and Red Team Exercises

Test the overall strength of an Actively manage (inventory, track, and organization's defenses (technology, correct) all hardware devices on the processes, and people) by simulating the network so that only authorized devices are given access, and unauthorized and objectives and actions of an attacker. unmanaged devices are identified and

CSC I

prevented from gaining access.

Inventory of Authorized and Inventory of Authorized and **Unauthorized Devices Unauthorized Software**

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

CSC 2

CSC 3

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

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

CSC 4

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

CSC 5

Controlled Use of **Administrative Privileges** Track, control, prevent, and correct the use, assignment, and configuration of administrative privileges on computers,

networks, and applications.

CSC 6

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

CSC 7 **Email and Web Browser Protections**

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

CSC 8

Malware Defenses

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

CSC 9

CSC 10

Data Recovery

Capability

Properly back up critical

information with a proven

methodology for timely

recovery.

Limitation and Control of Network Ports. **Protocols, and Services**

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

The CIS Critical Security Controls Are the **Core of the NIST Cybersecurity Framework**

In February 2015, the President issued Executive Order (EO) 13636, Improving Critical Infrastructure Cybersecurity, directing National Institute of Standards and Technology (NIST) to develop a voluntary framework based on existing standards. This has become known as the NIST Cybersecurity Framework or CSF. At the time this poster was produced (Summer 2016) Version 1.0 was the latest version, but NIST has announced that revisions based on community comments would be released in 2017.

Like all frameworks, the NIST CSF does not specify any priority of security controls or recommend sequences of actions. That is where the Critical Security Controls shine — they map directly to the CSF core requirements and provide a realistic and community-driven risk management approach for making sure your security program will be both effective and efficient against

The chart below maps the Center for Internet Security (CIS) Critical Security Controls (Version 6.0) into the most relevant NIST CSF (Version 1.0) Core Functions and Categories. If you are using the NIST CSF, the mapping (thanks to James Tarala) lets you use the Critical Security Controls to prioritize measuring and monitoring the most important core NIST Framework elements.

CIS Critical Security Controls		Cybersecurity Framework (CSF) Core				
(V6.0)	NIST Core Framework	Identify	Protect	Detect	Respond	Recover
I Inventory of Authorized and Unauthorized Devices	ID.AM-I ID.AM-3 ID.AM-4 PR.DS-3	AM				
2 Inventory of Authorized and Unauthorized Software	ID.AM-2 PR.DS-6	AM				
3 Secure Configuration of End-User Devices	PR.IP-I		IP			
4 Continuous Vulnerability Assessment & Remediation	ID.RA-I PR.IP-12 DE.CM-8 RS.MI-3 ID.RA-2	RA		СМ	MI	
5 Controlled Use of Administrative Privileges	PR.AC-4 PR.AT-2 PR.MA-2 PR.PT-3		AC			
6 Maintenance, Monitoring, and Analysis of Audit Logs	PR.PT-I DE.DP-I DE.DP-3 DE.DP-5 DE.AE-3 DE.DP-2 DE.DP-4			AE	AN	
7 Email and Web Browser Protections	PR.IP-I		PT			
8 Malware Defense	PR.PT-2 DE.CM-4 DE.CM-5		PT	СМ		
9 Limitation & Control of Network Ports, Protocols, and Service	PR.AC-5 DE.AE-I		IP			
10 Data Recovery Capability	PR.IP-4					RP
II Secure Configuration of Network Devices	PR.AC-5 PR.IP-I PR.PT-4		IP			
12 Boundary Defense	PR.AC-3 PR.AC-5 PR.MA-2 DE.AE-I			DP		
13 Data Protection	PR.AC-5 PR.DS-2 PR.DS-5 PR.PT-2		DS			
14 Controlled Access Based on Need to Know	PR.AC-4 PR.DS-I PR.PT-2 PR.AC-5 PR.DS-2 PR.PT-3		AC			
15 Wireless Access Control			AC			
16 Account Monitoring and Control	PR.IP-4		AC	СМ		
17 Security Skills Assessment and Appropriate Training	PR.AT-I PR.AT-3 PR.AT-4 PR.AT-5 PR.AT-2		AT			
18 Application Software Security	PR.AC-I PR.AC-4 PR.PT-3		IP			
19 Incident Response and Management	PR.IP-10 DE.CM-1-7 RS.AN-1-4 RC.RP-1 DE.AE-2 RS.RP-1 RS.MI-1-2 RC.IM-1-2 DE.AE-4 RS.CO-1-5 RS.IM-1-2 RC.CO-1-3 DE.AE-5			AE	RP	
20 Penetration Tests and Red Team Exercises					IM	IM

CSC 18

Application Software Security Manage the security lifecycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses.

CSC 17

Security Skills Assessment and Appropriate Training to Fill Gaps

Identify the specific knowledge, skills, and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify and remediate gaps, through policy, organizational planning, training, and awareness programs for all functional roles in the organization.

CSC 16 Account Monitoring

Actively manage the lifecycle of system and application accounts — their creation, use, dormancy, deletion — in order to minimize opportunities for

attackers to leverage them.

and Control

CSC 15

Wireless Access Control

Track, control, prevent, and correct the security use of wireless local area networks (LANS), access points, and wireless client systems.

CSC 14

Controlled Access Based on the Need to Know

Track, control, prevent, correct, and 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.

CSC 13

Data Protection Prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.

CSC 12

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

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

Establish, implement, and actively manage (track, report on, and 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.

CIS Critical Security Control

Defining Continuous Monitoring

Frequency (FedRAMP) 800-53 Control

National Institute of Standards and Technology (NIST) 800-137 is the U.S. government's guide to "Information Security Continuous Monitoring for Federal Information Systems and Organizations." It defines continuous monitoring as:

"...ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions....The terms 'continuous' and 'ongoing' in this context mean that security controls and organizational risks are assessed and analyzed at a frequency sufficient to support riskbased security decisions to adequately protect organization information. Data collection, no matter how frequent, is performed at discrete intervals."

The SANS simplified version of this is to:

- Establish and measure meaningful security metrics
- Monitor those metrics frequently enough to minimize incident impact
- Take action rapidly, efficiently and effectively to improve overall security

The CIS Critical Security Controls have proven to be an effective starting point for selecting key security metrics. A frequent question is "how frequently is continuous?" NIST 800-137 points to yet another complex document, SP 800-37 "Guide for Applying the Risk Management Framework to Federal Information Systems" for a risk-based methodology for making this decision. But there is an easier way.

Continuous and Ongoing	Auditable Events	(6) Maintenance, Monitoring, Analysis of Logs
	Component Inventory	(I) Inventory of Devices
	Incident Reporting	(19) Incident Response and Management
	Vulnerability Scanning	(4) Continuous Vulnerability Assessment & Remediation
Weekly	Audit Review, Report	(6) Maintenance, Monitoring, Analysis of Logs
Monthly	Vulnerability Scanning	(4) Continuous Vulnerability Assessment & Remediation
	Securing State Monitoring	(6) Maintenance, Monitoring, Analysis of Logs
	Flaw Remediation	(3) Secure Configurations
	Software/Info Integrity	(2) Software Inventory
	Least Functionality	(9) Limitation & Control of Network Ports, Services

A simpler approach: The GSA Federal Risk and Authorization Program (FedRAMP) has established continuous monitoring guidelines for certifying and monitoring cloud services as being secure enough for unclassified use by federal government agencies. FedRAMP defines which security controls should be monitored monthly, weekly, or on an ongoing basis (as frequently as possible, or driven by changes.)

Collecting Meaningful Security Data – Monitoring the Right Stuff

can move rapidly.

Security monitoring has no value on its own unless it leads to meaningful action to prevent or reduce damage from cyber attacks. More prevention, faster detection, and more accurate response require measuring different CIS Critical Security Controls to reduce vulnerabilities, detect and mitigate attacks, and optimize incident response and restoration. SANS has mapped the Critical Controls across the CyberDefense lifecycle.

		CYBER DEFEN	Compromise Detection,	
	Resource Hardening	Privilege and Access Management	Attack Detection/Mitigation	Response, Recovery, and Reporting
CIS CRITICAL SECURITY CONTROLS	Hardware and Software Inventory	Admin Privileges csc5	Malware Defenses csc7 & csc8	Data Recovery csc10
	Secure Configurations csc3, csc9, csc11 & csc15	Controlled Access csc14	Boundary Defense csc12	Audit csc6
		Account Managing csc16		Data Protection csc13
	Vulnerability Assessment & Application Security CSC4 & CSC18			Incident Response csc19

People and Processes The Critical Security Controls include a number of security areas that focus CSC17 — Security Skills Assessment and Training on people and processes and are applicable across the entire lifecycle: **CSC20** — Penetration Testing and Red Team Exercises

The values you measure When did I When did I should include both What percentage last update the quantity and time am I vulnerable to? this? attack list? how quickly you detect new misconfigurations vulnerabilites, attacks, etc. is just as important as how many there are. Similarly, business damage is minimized Q1 Quantity of (and often prevented) intrusion detection and Q2 Quantity of mitigation processes Q3 Quantity of T3 Time action initiated Q4 Quantity of REACTION/RESOLUTION

> **METRICS** How long to detect an incident? How long to to investigate/resolve?

Monitor and Measure the cis critical security controls

SANS surveyed industry vendors in March 2016, using the Center for Internet Security (CIS) document "A Measurement Companion to the CIS Critical Security Controls (Version 6)" dated October 2015 as the baseline. The "heat map" shaded areas represent totalling the number of measurements a vendor said YES to and divided by the total number of measurements listed for that Critical Control. SANS did not independently test the products. Products change frequently, and the information represented on this poster is current as of May 2016. Check with the vendors to get the latest information.

Product Matrix Heat Map Key



100% 99-80% 79-60% 59-40% 39-20% 19-1% 0%

How to use this chart:

There are two factors to keep in mind when evaluating products for monitoring and measuring your implementation of the CIS Critical Security Controls:

- No single product measures all sub-controls defined in the CIS Critical Security Controls.
- 2) Your gap assessment probably found that you are already using some security (or IT operations) products to measure some of the Controls.

Driven by your gap assessment and implementation plan, decide which CIS Critical Security Controls require enhanced measuring and monitoring capabilities.

Use the Proven Solutions Heat Map to select those products that cover all or most of your needs and then evaluate and compare those products to best meet the security demands of your business or mission.

