

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.

	Going Beyond SIEM
	CIS Critical Security Controls – Accelerated & Simplified
	Securing the Enterprise – Enterprise-wide, Standards-based Continuous Monitoring of Automated Security Controls
	Maintaining Continuous Compliance – A New Best-Practice Approach
	The Ransomware Threat: A How-To Guide on Preparing for and Detecting an Attack Before It's Too Late
	Top 7 Security Controls to Prioritize
	Attack Your Attack Surface – How to Reduce Your Exposure to Cyber Attacks with an Attack Surface Visualization Solution
	2016 Internet Security Threat Report
	CIS Critical Security Controls: Technical Control Automation

SANS Monitoring and Measuring the CIS Critical Security Controls

P O S T E R

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



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 real-world threats.

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 (V6.0)	NIST Core Framework	Cybersecurity Framework (CSF) Core				
		Identify	Protect	Detect	Respond	Recover
1 Inventory of Authorized and Unauthorized Devices	ID.AM-1 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-1		IP			
4 Continuous Vulnerability Assessment & Remediation	ID.RA-1 PR.IP-12 DE.CM-8 RS.MI-3 ID.RA-2	RA		CM	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-1 DE.DP-1 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-1		PT			
8 Malware Defense	PR.PT-2 DE.CM-4 DE.CM-5		PT	CM		
9 Limitation & Control of Network Ports, Protocols, and Service	PR.AC-5 DE.AE-1		IP			
10 Data Recovery Capability	PR.IP-4					RP
11 Secure Configuration of Network Devices	PR.AC-5 PR.IP-1 PR.PT-4		IP			
12 Boundary Defense	PR.AC-3 PR.AC-5 PR.MA-2 DE.AE-1			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.AC-5 PR.DS-1 PR.DS-2 PR.PT-2 PR.PT-3		AC			
15 Wireless Access Control			AC			
16 Account Monitoring and Control	PR.IP-4		AC	CM		
17 Security Skills Assessment and Appropriate Training	PR.AT-1 PR.AT-3 PR.AT-4 PR.AT-5 PR.AT-2		AT			
18 Application Software Security	PR.AC-1 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

Defining Continuous Monitoring

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 risk-based 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

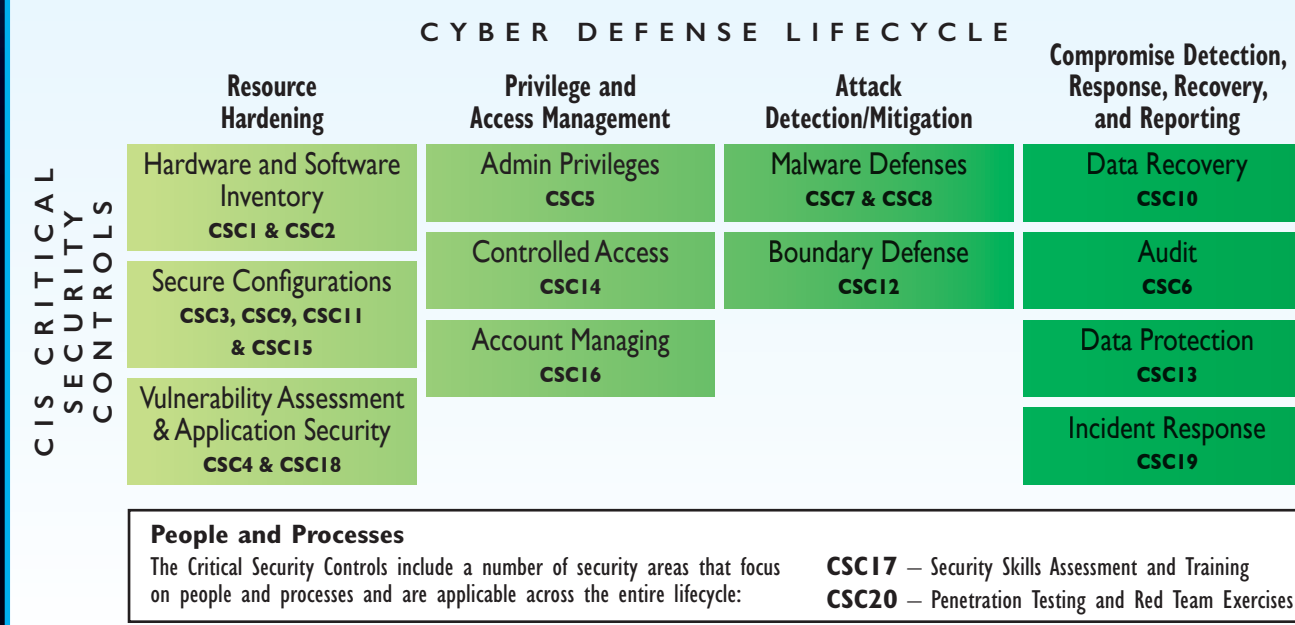
The CIS Critical Security Controls have proven to be an effective starting point for selecting key security metrics. A frequent question is "how frequently is continuous?" NIST 800-137 points to yet another complex document, SP 800-37 "Guide for Applying the Risk Management Framework to Federal Information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

Frequency (FedRAMP)	800-53 Control	CIS Critical Security Control
Continuous and Ongoing	Auditable Events	(6) Maintenance, Monitoring, Analysis of Logs
	Component Inventory	(1) Inventory of Devices
	Incident Reporting	(19) Incident Response and Management
Weekly	Vulnerability Scanning	(4) Continuous Vulnerability Assessment & Remediation
	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

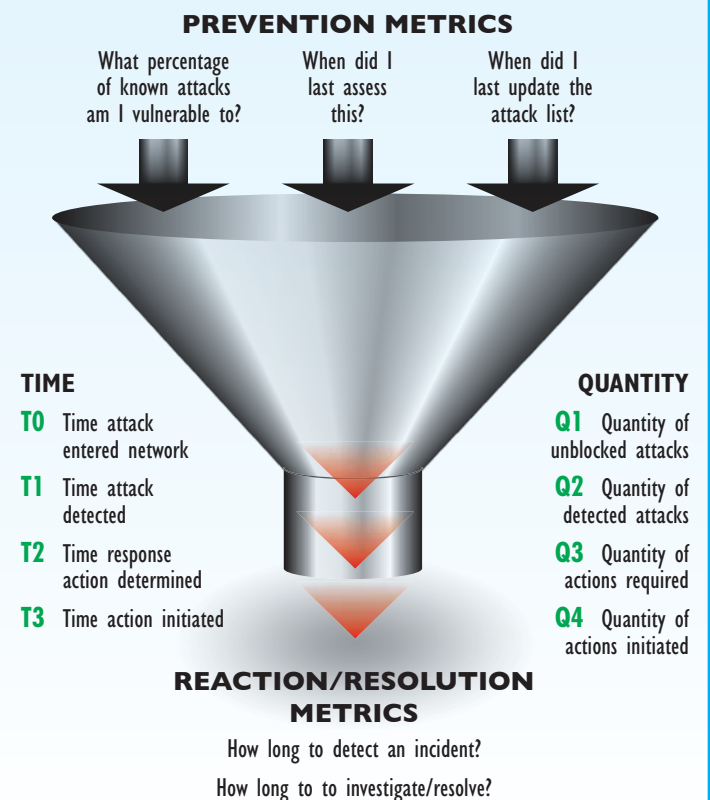
A simpler approach: The GSA Federal Risk and Authorization Program (FedRAMP) has established continuous monitoring guidelines for certifying and monitoring cloud services as being secure enough for unclassified use by federal government agencies. FedRAMP defines which security controls should be monitored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

Collecting Meaningful Security Data – Monitoring the Right Stuff

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.



The values you measure should include both quantity and time — how quickly you detect new misconfigurations, vulnerabilities, attacks, etc. is just as important as how many there are. Similarly, business damage is minimized (and often prevented) if intrusion detection and mitigation processes can move rapidly.



PROVEN SOLUTIONS TO

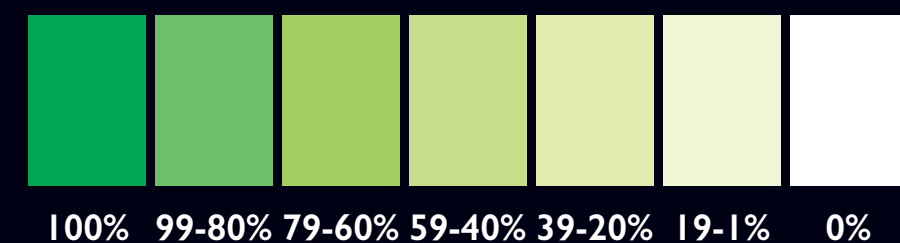
Monitor and Measure

THE CIS CRITICAL SECURITY CONTROLS

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



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:

- 1) 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.

SOLUTION PROVIDERS	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	TOT
Rapid7	1	1	2	1	2	2	2	1	2	0	1	2	2	1	1	2	1	2	1	2	2
Splunk	2	2	2	1	2	2	2	2	2	1	0	1	2	2	2	2	0	2	0	0	2
Tenable	2	2	2	2	2	2	2	2	2	0	2	2	2	1	2	2	0	2	0	0	2
IBM Big Fix	2	2	2	2	2	2	1	2	2	1	2	1	1	2	2	2	0	2	1	0	2
AlienVault	2	1	2	1	2	2	1	2	2	1	1	2	2	0	2	2	0	1	1	0	2
Skycure	1	2	2	1	1	2	1	2	1	0	0	1	1	0	2	0	0	2	1	2	2
IBM QRadar	2	1	1	0	2	2	2	2	2	0	1	1	2	2	2	2	0	1	0	0	2
Tripwire CCM	0	2	2	1	2	2	2	2	2	0	2	1	1	2	2	1	0	1	0	0	2
Imperva	1	1	2	0	2	2	0	0	1	0	0	2	2	2	0	2	0	2	0	0	2
Tripwire Enterprise	0	2	2	0	2	2	2	2	2	0	2	0	1	2	2	0	0	0	0	0	2
Beyond Security	1	1	2	2	1	2	2	1	2	0	2	0	0	0	2	0	0	2	0	2	2
Tripwire Connect/SI Hub	0	2	2	2	0	1	2	2	2	0	2	1	1	2	0	0	0	1	0	0	2
Tripwire Log Center	0	1	1	1	2	2	0	2	2	1	0	0	2	0	2	2	0	2	0	0	2
Belarc	2	2	2	2	1	0	2	2	2	0	0	0	0	0	2	2	0	0	0	0	2
Skybox Security	0	0	2	2	0	0	0	0	2	0	2	2	2	0	0	0	0	2	0	2	2
Cisco StealthWatch	1	0	1	0	1	0	0	2	0	0	1	2	0	0	2	0	2	2	2	2	2
EIQ Networks	0	1	2	0	0	2	0	2	2	0	2	0	0	0	0	2	0	0	0	0	2
Lumeta	2	0	1	2	0	0	0	1	2	0	2	2	2	0	2	0	0	2	0	0	2
Uplevel Security	2	2	0	0	0	1	2	2	0	0	0	2	2	0	2	2	0	0	1	0	2
Tripwire IP 360	0	2	2	2	0	2	2	1	2	0	1	0	0	0	2	0	0	2	0	0	2
Infoblox	2	0	0	2	0	1	2	1	0	0	1	0	2	0	0	0	0	0	0	0	2
Avecto	0	2	0	0	2	1	2	1	0	0	0	0	0	0	0	1	0	0	0	0	2
FireEye TAP	1	0	0	0	0	2	2	0	2	0	0	0	0	0	0	0	0	0	0	0	2
HexisCyber	0	0	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	2
Invincea	0	0	0	0	0	0	0	2	1	0	0	0	0	0	0	0	0	0	0	0	2
FireEye NX	0	0	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	2
FireEye IA	0	0	0	0	0	2	0	0	0	0	1	0	0	0	0	0	0	0	0	0	2
FireEye EX	1	0	0	0	0	0	2	0	0	0	0	0	2	0	0	0	0	0	0	0	2
FireEye ETP	1	0	0	0	0	0	2	0	0	0	0	0	2	0	0	0	0	0	0	0	2
FireEye HX	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	2
FireEye PX	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	2