| SOLUTION BRIEF

CIS Critical Security Controls & Tenable

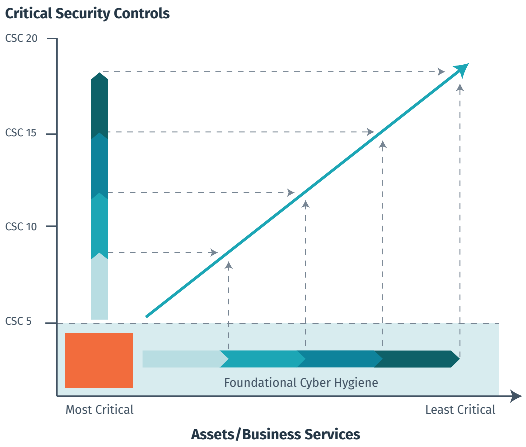
Streamline Critical Security Control Adoption

Organizations seeking to strengthen information security often adopt accepted policies, processes and procedures known to mitigate cyber attacks. These organizations frequently turn to the Center for Internet Security (CIS) Critical Security Controls (previously known as the SANS Top 20) for guidance. According to the CIS, which assumed responsibility for the controls in 2015, the "Critical Security Controls (CSCs) are 20 prioritized, well-vetted and supported security actions that organizations can take to assess and improve their current security state."

Challenges of Critical Security Control Conformance

Implementing any security framework involves education & training, resource, technical and other challenges. You should apply project management disciplines to manage the undertaking. The four specific challenges discussed below map to the CIS' critical tenets of an effective cyber defense system.

Prioritization: It isn't realistic to implement all 20 CSCs concurrently. You must first implement the controls that will provide the greatest risk reduction and protection against the most dangerous threats. You will need a reasonable plan to roll out the most important controls without straining IT resources that are already stretched thin. You can start by identifying your high risk assets and business services. They are likely to be the same ones subject to compliance requirements, such as systems containing PII. The CIS has designated CSC1 through CSC5 controls as essential *Foundational Cyber Hygiene* controls, and you should implement these controls for the asset or service identified as highest risk. As the diagram below shows, you can progress upward and to the right, taking the next step appropriate to your situation. It may be to apply Foundational Cyber Hygiene to the next priority asset or to implement additional CSC controls for the most critical asset.



Starting with the Foundational Cyber Hygiene controls for the Most Critical Business Service, you can Progress to Additional Controls and/or Services

Metrics: You must identify metrics to assess if the controls are operating effectively and to efficiently communicate status to various stakeholders.

Continuous Monitoring: Extended networks are highly dynamic so you cannot rely on periodic snapshots. You need continuous monitoring to collect real-time data across your systems, with the contextual analysis to prioritize your actions. This enables you to continuously adapt your security program to better protect and enable the business.

SecurityCenter Continuous View® Security CIS Critical Security Control Capabilities

- **Conformance Assessment** - Automate the assessment of most Critical Security Controls to determine what is in place and operating effectively
- **Continuous Monitoring** - benefit from both active and passive monitoring to ensure all stakeholders have near real-time visibility into your security posture
- **Complete Coverage** - Gain continuous visibility across your IT networks and industrial control systems, including physical and virtual infrastructure, cloud, and mobile environments
- **Assurance and Reports** - Use customizable CSC reports, dashboards and Assurance Report Cards to evaluate and communicate security status

Automation: Given limited resources and the huge volume of data generated from continuous monitoring, manual validation of adherence to the CSCs is nearly impossible, and at best would only provide limited visibility. You must automate the controls and associated metrics.

Automate Effective Conformance

Tenable SecurityCenter Continuous View (SecurityCenter CV™) enables you to measure, visualize and effectively communicate adherence to most of the CSCs security controls by automating their operation and assessment to ensure they are in place and operating effectively.

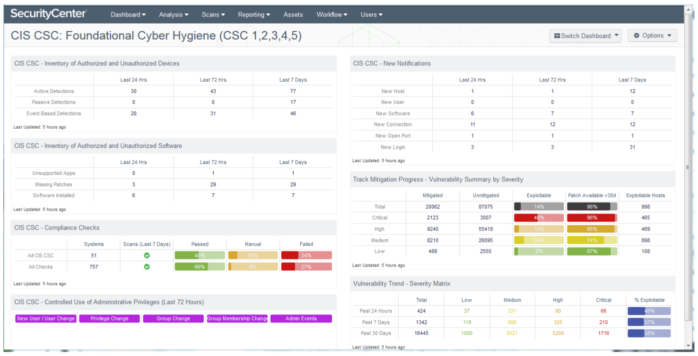
SecurityCenter CV will fit your specific needs. It delivers broad and continuous coverage across your entire environment, including physical, cloud, virtualized and mobile systems used in IT and industrial control networks. Dynamic asset lists let you logically segment, manage and report on the status of specific systems, such as those used for processing PII or for processing payment card data. Intelligent connectors to your existing security products audit configurations and analyze events to identify control weaknesses.

Communicate Security Status

Executives, auditors and business partners are scrutinizing security now more than ever. You must provide them with the information they need, when they need it, without spending your time manually analyzing and summarizing data.

SecurityCenter CV provides fully customizable reports, dashboards and Assurance Report Cards (ARCs) specific to the CSCs – all out-of-the box. You can use them "as-is" or quickly and easily tailor them to meet your specific security and business needs. For example, you can tailor dashboards for specific assets or business systems.

Tenable reports, dashboards and ARCs demonstrate adherence with best practice security controls to external business partners and large customers that may have the right to audit your security program.



CIS CSC: Foundational Cyber Hygiene (CSC 1,2,3,4,5)

CIS CSC - Inventory of Authorized and Unauthorized Devices

	Last 24 Hrs	Last 72 Hrs	Last 7 Days
Active Detections	30	43	77
Passive Detections	0	0	17
Event Based Detections	28	31	46

Last Updated: 5 hours ago

CIS CSC - Inventory of Authorized and Unauthorized Software

	Last 24 Hrs	Last 72 Hrs	Last 7 Days
Unsupported Apps	0	1	1
Missing Patches	3	29	29
Software Installed	6	7	7

Last Updated: 5 hours ago

CIS CSC - Compliance Checks

	Systems	Scans (Last 7 Days)	Passed	Manual	Failed
All CIS CSC	51	✓	48%	18%	34%
All Checks	757	✓	66%	6%	27%

Last Updated: 5 hours ago

CIS CSC - Controlled Use of Administrative Privileges (Last 72 Hours)

New User / User Change | Privilege Change | Group Change | Group Membership Change | Admin Events

CIS CSC - New Notifications

	Last 24 Hrs	Last 72 Hrs	Last 7 Days
New Host	1	1	12
New User	0	0	0
New Software	6	7	7
New Connection	11	12	12
New Open Port	1	1	1
New Login	3	3	31

Last Updated: 5 hours ago

Track Mitigation Progress - Vulnerability Summary by Severity

	Mitigated	Unmitigated	Exploitable	Patch Available >30d	Exploitable Hosts
Total	20062	87075	14%	86%	998
Critical	2123	3007	48%	96%	465
High	9240	55418	10%	95%	469
Medium	8210	26095	20%	74%	898
Low	489	2555	8%	87%	108

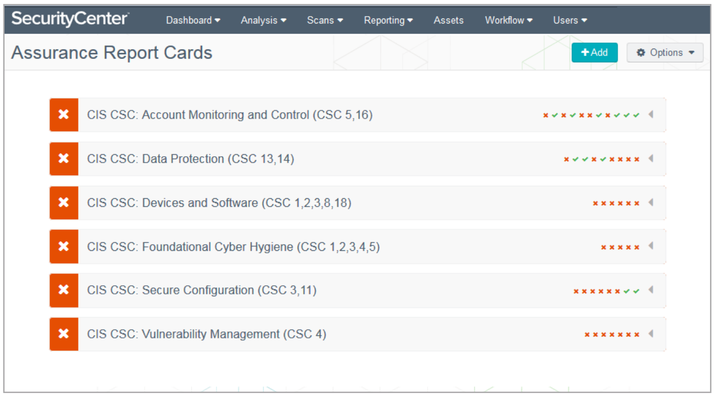
Last Updated: 5 hours ago

Vulnerability Trend - Severity Matrix

	Total	Low	Medium	High	Critical	% Exploitable
Past 24 Hours	424	37	231	90	66	40%
Past 7 Days	1342	119	688	325	210	37%
Past 30 Days	16445	1000	8521	5208	1716	38%

Last Updated: 5 hours ago

Interactive dashboards consolidate information that you can quickly drill into Assurance Report Cards present security status at a high level for a non-technical audience



Assurance Report Cards

- ✗ CIS CSC: Account Monitoring and Control (CSC 5,16) ✗✓✗✓✗✗✓✗✓✓✓
- ✗ CIS CSC: Data Protection (CSC 13,14) ✗✓✓✗✓✗✗✗✗
- ✗ CIS CSC: Devices and Software (CSC 1,2,3,8,18) ✗✗✗✗✗✗
- ✗ CIS CSC: Foundational Cyber Hygiene (CSC 1,2,3,4,5) ✗✗✗✗✗
- ✗ CIS CSC: Secure Configuration (CSC 3,11) ✗✗✗✗✗✗✓✓
- ✗ CIS CSC: Vulnerability Management (CSC 4) ✗✗✗✗✗✗✗

ARCs complement the Tenable comprehensive data collection approach, which uses a combination of active scanning, agent scanning, intelligent connectors to your third-party systems, passive listening and host data monitoring to assess the protection status of your complete infrastructure. Together, these capabilities provide you the ability to:

- Measure, visualize and effectively communicate the technical security controls that help you manage risk
- Communicate security status to business partners and other external stakeholders
- Understand the context you need to prioritize remediation

About Tenable

Tenable Network Security transforms security technology for the business needs of tomorrow through comprehensive solutions that provide continuous visibility and critical context, enabling decisive actions to protect your organization. Tenable eliminates blind spots, prioritizes threats, and reduces exposure and loss. With more than one million users and more than 20,000 enterprise customers worldwide, organizations trust Tenable for proven security innovation. Tenable's customers range from Fortune Global 500 companies, to the U.S. Department of Defense, to mid-sized and small businesses in all sectors, including finance, government, healthcare, higher education, retail and energy. Transform security with Tenable, the creators of Nessus and leaders in continuous monitoring, by visiting tenable.com.

tenable™

For More Information: Please visit tenable.com
Contact Us: Please email us at sales@tenable.com or visit tenable.com/contact