CIS Critical Security Controls – Continuously Monitoring and Enforcing the Critical Security Controls

**CSC 19**
Incident Response and Recovery

- Proactively address vulnerabilities, prepare for an attack, and quickly respond to an incident.

- Implement an incident response plan that includes roles and responsibilities.

- Collect and store evidence, and ensure that all evidence is stored securely.

**CSC 18**
Application Software Security

- Manage the lifecycle of applications, including selection, testing, deployment, and maintenance.

- Ensure that all applications are properly configured and have the necessary security controls in place.

- Keep software up to date, and address vulnerabilities as soon as they are discovered.

**CSC 17**
Security Skills Assessment and Appropriate Training

- Identify skills gaps and provide training to fill those gaps.

- Ensure that all employees have the necessary skills to perform their roles securely.

- Conduct regular security awareness training for all employees.

**CSC 16**
Account Monitoring and Control

- Ensure that all accounts are properly authorized and have the necessary access privileges.

- Monitor accounts for unusual or suspicious activity.

- Implement strong password policies and regular account reviews.

**CSC 15**
Wireless Access Control

- Control access to wireless networks and ensure that only authorized devices can connect.

- Monitor wireless networks for unauthorized access.

- Implement strong encryption and authentication methods.

**CSC 14**
Controlled Access Based on the Need to Know

- Ensure that access to information is based on the need to know.

- Control access based on roles and responsibilities.

- Limit access to sensitive information.

**CSC 13**
Data Protection

- Protect sensitive data, including personal information and intellectual property.

- Ensure that data is encrypted and stored securely.

- Implement access controls to restrict access to sensitive data.

**CSC 12**
Boundary Defense

- Protect the boundary between trusted and untrusted networks.

- Implement strong network segmentation and firewalling.

- Monitor network traffic for signs of malicious activity.

**CSC 11**
Data Recovery Capability

- Ensure that data can be recovered in the event of a disaster.

- Implement backups and disaster recovery plans.

- Test disaster recovery plans regularly.

**CSC 10**
Limitation and Control of Network Ports, Protocols, and Services

- Limit access to network services, and ensure that only necessary services are available.

- Implement strong access controls and monitoring.

- Monitor networks for signs of malicious activity.

**CSC 9**
Controlled Use of Administrative Privileges

- Limit administrative privileges to only those who need them.

- Implement strong password policies.

- Monitor for unusual or suspicious activity.

**CSC 8**
Malware Defenses

- Prevent, detect, and remove malware.

- Monitor for signs of malware activity.

- Implement strong antivirus and anti-malware solutions.

**CSC 7**
Email and Web Browser Protections

- Prevent phishing and other attacks that use emails or web browsers.

- Implement strong anti-phishing and anti-malware solutions.

- Monitor for signs of malware activity.

**CSC 6**
Performance Monitoring and Analysis of Audit Logs

- Monitor system performance and logs for signs of malicious activity.

- Implement strong monitoring and logging solutions.

- Monitor for signs of malware activity.

**CSC 5**
Continuous Vulnerability Assessment and Remediation

- Regularly identify vulnerabilities and ensure that they are remediated.

- Implement strong vulnerability management solutions.

- Monitor for signs of malware activity.

**CSC 4**
Secure Configuration of Hardware Devices

- Ensure that hardware devices are properly configured for security.

- Implement strong configuration management solutions.

- Monitor for signs of malware activity.

**CSC 3**
Inventory of Authorized and Unmanaged Devices

- Identify and secure all devices on the network, including those that are not authorized.

- Monitor for signs of malware activity.

- Implement strong inventory management solutions.

**CSC 2**
Penetration Tests and Red Team Exercises

- Regularly test the network for vulnerabilities and identify potential attack vectors.

- Implement strong penetration testing solutions.

- Monitor for signs of malware activity.

**CSC 1**
Inventory of Devices

- Inventory all devices on the network, including those that are not authorized.

- Implement strong inventory management solutions.

- Monitor for signs of malware activity.

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

**SANS**
Products and Strategies for Continuously Monitoring and Improving the CIS Critical Security Controls

**DEFINING CONTINUOUS MONITORING**

Continuous monitoring involves monitoring systems and networks for signs of malicious activity, and responding to those signs in a timely manner.

- Real-time monitoring allows for immediate response to threats.

- Historical monitoring provides insights into past threats and can help identify trends.

- Predictive monitoring can help identify potential threats before they occur.

**MONITORING AND MEASURING THE CIS CRITICAL SECURITY CONTROLS**

- Use metrics to measure the effectiveness of your security controls.

- Monitor key performance indicators (KPIs) to identify areas for improvement.

- Implement a continuous monitoring framework to ensure that all systems are monitored.

**CIS Critical Security Controls**

- A comprehensive set of 18 core controls that provide a framework for implementing effective security practices.

- Each control is designed to address a specific security concern and helps organizations to improve their security posture.

- The controls cover a wide range of security areas, including access control, data protection, and network security.

**REFERENCES**


**ACKNOWLEDGMENTS**

- The authors would like to thank the following organizations for their support:

- The Center for Internet Security
- SANS Institute
- The National Institute of Standards and Technology (NIST)
- The Open Group
- The Cloud Security Alliance

**CONTACT INFORMATION**

- For more information, please visit the Center for Internet Security’s website at www.cisecurity.org.

- Contact us at info@cisecurity.org.

**COPYRIGHT NOTICE**

- © 2017 Center for Internet Security. All rights reserved.
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:

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.