## The Critical Security Controls

### Solution Providers

#### Critical Security Controls

**Primary:**
- Selenium
- Security Controls
- Security Monitoring
- Security Posture
- Security Policy
- Security Tools
- Security Training
- Security Vendor

**Secondary:**
- Security Management
- Security Operations
- Security Risk
- Security Testing
- Security Vulnerability

**Provider:**
- Security, Risk, and Compliance
- Security, Risk, and Technology
- Security, Risk, and Vulnerability
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
- Security, Risk, and Workforce
Critical Security Controls for Effective Cyber Defense

The Critical Security Controls (CSCs) are a set of recommended actions that organizations can take to improve their cybersecurity posture. The CSCs are based on best practices from the Department of Homeland Security (DHS) and other cybersecurity experts. These controls are designed to help organizations protect against advanced threats and reduce the risk of successful cyber attacks.

1. Inventory of Authorized and Unauthorized Software
2. Inventory of Authorized and Unauthorized Software
3. Secure Configurations for Hardware and Software
4. Continuous Vulnerability Assessment andRemediation
5. Malware Defenses
6. Application Security Software
7. Wireless Access Control
8. Data Recovery Capability
9. Security Skills Assessment and Appropriate Training to Fill Gaps
10. Secure Configurations for Network Devices
11. Limitation and Control of Network Ports
12. Controlled Use of Administrative Privileges
13. Boundary Defense
14. Maintenance, Monitoring, and Analysis of Audit Logs
15. Controlled Access Based on the Need to Know
16. Account Monitoring andControl
17. Data Protection
18. Incident Response and Management
19. Secure Network Engineering
20. Penetration Tests andRed Team Exercises

These controls are designed to help organizations improve their cybersecurity posture and reduce the risk of successful cyber attacks. By implementing these controls, organizations can better protect their systems and data from advanced and targeted attacks.

SANS Institute

The SANS Institute is a nonprofit global cybersecurity research and education organization. SANS offers a wide range of cybersecurity training and certification programs, as well as research and analysis on the latest threats and trends in the cybersecurity field. SANS is dedicated to providing the best possible cybersecurity education and training to help organizations protect themselves against cyber threats.

The Value of the Critical Security Controls

The Critical Security Controls (CSCs) are a set of recommended actions that organizations can take to improve their cybersecurity posture. The CSCs are based on best practices from the Department of Homeland Security (DHS) and other cybersecurity experts. These controls are designed to help organizations protect against advanced threats and reduce the risk of successful cyber attacks.

1. Inventory of Authorized and Unauthorized Software
2. Inventory of Authorized and Unauthorized Software
3. Secure Configurations for Hardware and Software
4. Continuous Vulnerability Assessment andRemediation
5. Malware Defenses
6. Application Security Software
7. Wireless Access Control
8. Data Recovery Capability
9. Security Skills Assessment and Appropriate Training to Fill Gaps
10. Secure Configurations for Network Devices
11. Limitation and Control of Network Ports
12. Controlled Use of Administrative Privileges
13. Boundary Defense
14. Maintenance, Monitoring, and Analysis of Audit Logs
15. Controlled Access Based on the Need to Know
16. Account Monitoring andControl
17. Data Protection
18. Incident Response and Management
19. Secure Network Engineering
20. Penetration Tests andRed Team Exercises

These controls are designed to help organizations improve their cybersecurity posture and reduce the risk of successful cyber attacks. By implementing these controls, organizations can better protect their systems and data from advanced and targeted attacks.

SANS Institute