1. INVENTORY OF AUTHORIZED AND UNAUTHORIZED DEVICES

- PRIMARY: Altiris Asset Management Suite, CCS = Symantec
- SECONDARY: Tripwire IP360, Tripwire Enterprise and Network Sentry = Bradford Networks
- APPLICATION: Tripwire Enterprise and Tripwire IP360, Tripwire Enterprise and Network Sentry = Bradford Networks

2. INVENTORY OF AUTHORIZED AND UNAUTHORIZED SOFTWARE

- PRIMARY: Altiris Asset Management Suite, CCS = Symantec
- SECONDARY: Tripwire ITMS, CCS = Symantec
- SOLUTION PROVIDER: Altiris Asset Management Suite, CCS = Symantec
- APPLICATION: Altiris ITMS, CCS = Symantec

3. SECURE CONFIGURATIONS FOR HARDWARE AND SOFTWARE ON LAPTOPS, WORKSTATIONS, AND SERVERS

- PRIMARY: Tripwire Enterprise and Tripwire IP360, Tripwire Enterprise and Network Sentry = Bradford Networks
- SECONDARY: SonicWall = Dell Sonicwall
- SOLUTION PROVIDER: SonicWall = Dell Sonicwall
- APPLICATION: SonicWall = Dell Sonicwall

4. CONTINUOUS VULNERABILITY ASSESSMENT AND REHABILITATION

- PRIMARY: LogRhythm SIEM
- SECONDARY: Splunk App for Enterprise Security = Splunk
- SOLUTION PROVIDER: Splunk App for Enterprise Security = Splunk
- APPLICATION: Splunk App for Enterprise Security = Splunk

5. MALWARE DEFENSE

- PRIMARY: LogRhythm SIEM
- SECONDARY: Splunk App for Enterprise Security = Splunk
- SOLUTION PROVIDER: Splunk App for Enterprise Security = Splunk
- APPLICATION: Splunk App for Enterprise Security = Splunk

6. APPLICATION SOFTWARE SECURITY

- PRIMARY: LogRhythm SIEM
- SECONDARY: Splunk App for Enterprise Security = Splunk
- SOLUTION PROVIDER: Splunk App for Enterprise Security = Splunk
- APPLICATION: Splunk App for Enterprise Security = Splunk

7. WIRELESS ACCESS CONTROL

- PRIMARY: Wireless LAN Admin Security (WLAS) = Tuffin
- SECONDARY: Wireless LAN Admin Security (WLAS) = Tuffin
- SOLUTION PROVIDER: Wireless LAN Admin Security (WLAS) = Tuffin
- APPLICATION: Wireless LAN Admin Security (WLAS) = Tuffin

8. DATA RECOVERY CAPABILITY

- PRIMARY: LogRhythm SIEM
- SECONDARY: Splunk App for Enterprise Security = Splunk
- SOLUTION PROVIDER: Splunk App for Enterprise Security = Splunk
- APPLICATION: Splunk App for Enterprise Security = Splunk

9. SECURITY SKILLS ASSESSMENT AND APPROPRIATE TRAINING TO FILL GAPS

- PRIMARY: LogRhythm SIEM
- SECONDARY: Splunk App for Enterprise Security = Splunk
- SOLUTION PROVIDER: Splunk App for Enterprise Security = Splunk
- APPLICATION: Splunk App for Enterprise Security = Splunk

10. SECURITY TASKS DEFINED AS CSR OR CSRIS FOR EACH SECURITY control

- PRIMARY: LogRhythm SIEM
- SECONDARY: Splunk App for Enterprise Security = Splunk
- SOLUTION PROVIDER: Splunk App for Enterprise Security = Splunk
- APPLICATION: Splunk App for Enterprise Security = Splunk

11. LIMITATION AND CONTROL OF NETWORK PORTS, PROTUlOS, AND SERVICES

- PRIMARY: LogRhythm SIEM
- SECONDARY: Splunk App for Enterprise Security = Splunk
- SOLUTION PROVIDER: Splunk App for Enterprise Security = Splunk
- APPLICATION: Splunk App for Enterprise Security = Splunk

12. SECURE CONFIGURATIONS FOR FIREWALLS, ROUTERS AND SWITCHES

- PRIMARY: LogRhythm SIEM
- SECONDARY: Splunk App for Enterprise Security = Splunk
- SOLUTION PROVIDER: Splunk App for Enterprise Security = Splunk
- APPLICATION: Splunk App for Enterprise Security = Splunk

13. BOUNDARY DEFENSE

- PRIMARY: LogRhythm SIEM
- SECONDARY: Splunk App for Enterprise Security = Splunk
- SOLUTION PROVIDER: Splunk App for Enterprise Security = Splunk
- APPLICATION: Splunk App for Enterprise Security = Splunk

14. MAINTENANCE, MONITORING, AND ANALYSIS OF AUDIT LOGS

- PRIMARY: LogRhythm SIEM
- SECONDARY: Splunk App for Enterprise Security = Splunk
- SOLUTION PROVIDER: Splunk App for Enterprise Security = Splunk
- APPLICATION: Splunk App for Enterprise Security = Splunk

15. CONTROLE LED USE OF ADMINISTRATIVE PRIVILEGES

- PRIMARY: LogRhythm SIEM
- SECONDARY: Splunk App for Enterprise Security = Splunk
- SOLUTION PROVIDER: Splunk App for Enterprise Security = Splunk
- APPLICATION: Splunk App for Enterprise Security = Splunk

16. ACCOUNT MONITORING AND CONTROL

- PRIMARY: LogRhythm SIEM
- SECONDARY: Splunk App for Enterprise Security = Splunk
- SOLUTION PROVIDER: Splunk App for Enterprise Security = Splunk
- APPLICATION: Splunk App for Enterprise Security = Splunk

17. DATA PROTECTION

- PRIMARY: LogRhythm SIEM
- SECONDARY: Splunk App for Enterprise Security = Splunk
- SOLUTION PROVIDER: Splunk App for Enterprise Security = Splunk
- APPLICATION: Splunk App for Enterprise Security = Splunk

18. INCIDENT RESPONSE AND HANLGEMENT

- PRIMARY: LogRhythm SIEM
- SECONDARY: Splunk App for Enterprise Security = Splunk
- SOLUTION PROVIDER: Splunk App for Enterprise Security = Splunk
- APPLICATION: Splunk App for Enterprise Security = Splunk

19. SECURE NETWORK ENGINEERING

- PRIMARY: LogRhythm SIEM
- SECONDARY: Splunk App for Enterprise Security = Splunk
- SOLUTION PROVIDER: Splunk App for Enterprise Security = Splunk
- APPLICATION: Splunk App for Enterprise Security = Splunk

20. PENETRATION TESTING AND RED TEAM EXERCISES

- PRIMARY: LogRhythm SIEM
- SECONDARY: Splunk App for Enterprise Security = Splunk
- SOLUTION PROVIDER: Splunk App for Enterprise Security = Splunk
- APPLICATION: Splunk App for Enterprise Security = Splunk

SANS Critical Security Controls

Critical Security Controls

SOLUTION PROVIDERS

for Effective Cyber Defense
The Value of Using the Critical Security Controls to Focus on Processing Critical Information Assets

The Critical Security Controls (CSCs) are a set of 20 safeguards that organizations can use to protect their information and systems. The CSCs are intended to help organizations mitigate cyber threats and protect their assets. The CSCs are divided into five categories: Access Control, Asset Management, Auditing, Architecture and Design, and Configuration Management.

CSC 1: Access Control
- Identify and authenticate users
- Authorize users
- Monitor changes

CSC 2: Asset Management
- Identify and classify assets
- Secure inventory
- Control access

CSC 3: Auditing
- Collect and maintain audit trails
- Assess and monitor
- Review and report

CSC 4: Architecture and Design
- Design for security
- Protect the system
- Design for privacy

CSC 5: Configuration Management
- Manage software and hardware
- Secure configurations
- Patch management

CSC 6: Incident Response
- Identify and contain
detect and communicate
- Mitigate and recover

CSC 7: Monitoring and Analysis
- Detect and analyze
- Monitor and respond
- Review and report

CSC 8: Security Controls Overview
- Ensure security controls are implemented
- Implement controls
- Review and report

CSC 9: Security Control Implementation
- Develop and implement
- Monitor and maintain
- Review and report

CSC 10: Security Control Management
- Maintain security controls
- Monitor and maintain
- Review and report

CSC 11: Security Control Assessment
- Assess security controls
- Monitor and maintain
- Review and report

CSC 12: Security Control Approval
- Approve security controls
- Monitor and maintain
- Review and report

CSC 13: Security Control Attestation
- Attest to security controls
- Monitor and maintain
- Review and report

CSC 14: Security Control Monitoring
- Monitor security controls
- Monitor and maintain
- Review and report

CSC 15: Security Control Reporting
- Report security controls
- Monitor and maintain
- Review and report

CSC 16: Security Control Analysis
- Analyze security controls
- Monitor and maintain
- Review and report

CSC 17: Security Control Administration
- Administer security controls
- Monitor and maintain
- Review and report

CSC 18: Security Control Management
- Manage security controls
- Monitor and maintain
- Review and report

CSC 19: Security Control Approval
- Approve security controls
- Monitor and maintain
- Review and report

CSC 20: Security Control Attestation
- Attest to security controls
- Monitor and maintain
- Review and report

The Value of the Critical Security Controls is to help organizations improve their cybersecurity posture. By implementing the Critical Security Controls, organizations can reduce the risk of cyber attacks and better protect their assets. The Critical Security Controls are a framework that can be used to assess and improve an organization's cybersecurity posture.