



The Cybersecurity Workforce Gap

Read this report as the summary will be provided at a high level.

- https://csis-prod.s3.amazonaws.com/s3fs-public/publication/190129_Crumpler_Cybersecurity_FINAL.pdf

The Center for Strategic & International Studies (CSIS) 20 Critical Security Controls Initiative

- Offense Informs Defense
- Prioritization
- Metrics
- Continuous Monitoring
- Automation

Current List of Critical Security Controls

Basic CIS Controls

- | | | | |
|---|---|---|--|
| 1 | Inventory and Control of Hardware Assets | 2 | Inventory and Control of Software Assets |
| 3 | Continuous Vulnerability Management | 4 | Controlled Use of Administrative Privileges |
| 5 | Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers | 6 | Maintenance, Monitoring and Analysis of Audit Logs |

Foundational CIS Controls

- | | | | |
|----|---|----|---|
| 7 | Email and Web Browser Protections | 8 | Malware Defenses |
| 9 | Limitation and Control of Network Ports, Protocols and Services | 10 | Data Recovery Capabilities |
| 11 | Secure Configuration for Network Devices, such as Firewalls, Routers and Switches | 12 | Boundary Defense |
| 13 | Data Protection | 14 | Controlled Access Based on the Need to Know |
| 15 | Wireless Access Control | 16 | Account Monitoring and Control |

Organizational CIS Controls

- | | | | |
|----|---|----|--|
| 17 | Implement a Security Awareness and Training Program | 18 | Application Software Security |
| 19 | Incident Response and Management | 20 | Penetration Tests and Red Team Exercises |

NIST Security Content Automation Protocol (SCAP)

- Languages
- Reporting Formats
- Enumerations
- Measurement and Scoring Systems
- Integrity

Framework for Improving Critical Infrastructure Cyber security

- Describe their current cyber security posture.
- Describe their target state for cyber security.
- Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process.
- Assess progress toward the target state.
- Communicate among internal and external stakeholders about cyber security risk.

