OVERVIEW

The Center for Internet Security (CIS) developed the Critical Security Controls for Effective Cyber Defense. The 20 controls are based on the latest information about common attacks and reflect the combined knowledge of commercial forensics experts, individual penetration testers and contributors from U.S. government agencies. IT security leaders use CIS Controls to quickly establish the protections providing the highest payoff in their organizations. They guide you through a series of 20 foundational and advanced cybersecurity actions, where the most common attacks can be eliminated.

BASIC 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/Software on Mobile Devices, Laptops, Workstations, Servers
6: Maintenance, Monitoring and Analysis of Audit Logs

FOUNDATIONAL Controls

7: Email and Web Browser Protections
8: Malware Defenses
9: Limitation and Control of Network Ports, Protocols, and Services
10: Control 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 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