SANS' Critical Security Controls

CSC 1 **Inventory of Authorized and Unauthorized Devices**

Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are identified and prevented from gaining access.

CSC 2 **Inventory of Authorized and Unauthorized Software**

Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and unauthorized and unmanaged software is located and prevented from installation or execution.

CSC 3 **Secure Configurations for Hardware and Software**

Establish, implement, and actively manage (track, report on, and correct) the security configuration of laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

CSC 4 **Continuous Vulnerability Assessment and Remediation**

Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, and to remediate and minimize the window of opportunity for attackers.

CSC 5 **Controlled Use of Administrative Privileges**

Track, control, prevent, and correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.

CSC 6 **Maintenance, Monitoring, and Analysis of Audit Logs**

Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.

CSC 7 **Email and Web Browser Protections**

Minimize the attack surface and the opportunities for attackers to manipulate human behavior through their interaction with web browsers and email systems.

CSC 8 **Malware Defenses**

Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action.

CSC 9 **Limitation and Control of Network Ports**

Manage (track, control, and correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.

CSC 10 **Data Recovery Capability**

Properly back up critical information with a proven methodology for timely recovery.

Credit: https://www.sans.org/media/critical-security-controls/critical-controls-poster-2016.pdf

CSC 11 **Secure Configurations for Network Devices**

Establish, implement, and actively manage (track, report on, and correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

CSC 12 **Boundary Defense**

Detect, prevent, and correct the flow of information-transferring networks of different trust levels with a focus on security-damaging data.

CSC 13 **Data Protection**

Prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.

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

Track, control, prevent, correct, and secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.

CSC 15 **Wireless Access Control**

Track, control, prevent, and correct the security use of wireless local area networks (LANS), access points, and wireless client systems.

CSC 16 **Account Monitoring and Control**

Actively manage the lifecycle of system and application accounts – their creation, use, dormancy, deletion – in order to minimize opportunities for attackers to leverage them.

CSC 17 **Security Skills Assessment and Appropriate Training to Fill Gaps**

Identify the specific knowledge, skills, and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify and remediate gaps, through policy, organizational planning, training, and awareness programs for all functional roles in the organization.

CSC 18 **Application Software Security**

Manage the security lifecycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses.

CSC 19 **Incident Response and Management**

Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight).

CSC 20 **Penetration Tests and Red Team Exercises**

Test the overall strength of an organization's defenses (technology, processes, and people) by simulating the objectives and actions of an attacker.

Credit: https://www.sans.org/media/critical-security-controls/critical-controls-poster-2016.pdf