The 20 Critical Controls

1 - **Inventory of Authorised and Unauthorised 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 found and prevented from gaining access.

2 - **Inventory of Authorised and Unauthorised Software**

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

3 - **Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers**

Establish, implement, and actively manage (track, report on, 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.

4 - **Continuous Vulnerability Assessment and Remediation**

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

5 - **Malware Defences**

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.

6 - **Application Software Security**

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

7 - **Wireless Access Control**

The processes and tools used to track/control/prevent/correct the security use of wireless local area networks (LANS), access points, and wireless client systems.

8 - **Data Recovery Capability**

The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.

9 - **Security Skills Assessment and Appropriate Training to Fill Gaps**

For all functional roles in the organization (prioritizing those mission-critical to the business and its security), identify the specific knowledge, skills, and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs.

10 - **Secure Configurations for Network Devices such as Firewalls, Routers and Switches**

Establish, implement, and actively manage (track, report on, 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.

11 - **Limitation and Control of Network Ports, Protocols and Services**

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

12 - **Controlled Use of Administrative Privileges**

The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.

13 - **Boundary Defence**

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

14 - **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.

15 - **Control Access Based on the Need to Know**

The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, and 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.

16 - **Account Monitoring and Control**

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

17 - **Data Protection**

The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.

18 - **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) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems..

19 - **Secure Network Engineering**

Make security an inherent attribute of the enterprise by specifying, designing, and building-in features that allow high confidence systems operations while denying or minimizing opportunities for attackers.

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

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