1)Inventory and control of hardware assets

It helps the CIS to actively manage all hardware devices on the network.This ensures only authorized devices are given access and unauthorized and unmanaged devices are found and prevented from gaining access.

2**)Inventory and control of hardware assets**

The focus of this control is to actively manage software installed on systems within the organization.A fundamental aspect of risk management is discovering risk by tracking software present on information systems.

3)Continuous Vulnerability Management:

It is a automated processes that support real-time visibility of vulnerability and risk across an organization's entire network.

4)Continuous use of administrative privileges

This allow a user to perform certain function on a system or network, such as installing software and changing configuration settings.has more control over a computer or network system.

5)Secure Configuration for Hardware and Software on Mobile Devices,Laptops,Workstations and servers

The focus of this control is to maintain documented security configuration standards for all authorized operating systems and software.Organization must establish a baseline security configuration,implement a configuration management and change control process, and actively be able to report on the security configurations of all endpoints**.**

6)Maintenance,Monitoring and Analysis of Audit Logs

The focus of this control is to collect,manage, and analyze audit logs of events that could help detect,understand or recover from an attack.

7)Email and web Browser Protections

The focus is to control is to minimize the attack surface and the opportunities for attackers to manipulate human behavior through their interaction with web browsers and email systems

8)Malware Defenses

To prevent or control the installation,spread,and execution of malicious applications,codemor scripts on enterprise assets.

9)Limitations and control of Network Ports,protocols,and services

The focus of this control is to manage the ongoing operational use of ports,protocols ,and services on networked devices in order to minimize windows of vulnerability available to attackers.

10)Data recovery Capability

This addresses the importance of backing-up system data and properly protecting those back-ups.By doing so,you ensure the ability of your organization to recover lost or tampered-with data.Every minute your network is down is productivity lost.

11)Secure Configuration for Network Devices,such as Firewalls,Routers and Switches

The focus of this control is to establish,implement and actively manage 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.

12)Boundary Defense

The focus of this control is to ensure that the entry points into the network are clearly defined and monitored.Network boundaries in today’s environment do not have a clear edge, and are typically no longer defined as a single ingress point protected by a firewall and edge routers of the past.Today,the network perimeter extends well beyond this gateway into the organization, and encompasses the cloud when using AWS,ASURE,or other services.A network edge is also the reach of a wireless network radio signal and the VPN endpoints with more users working at home. THis CISO must have a clear understanding of each network edge and the risks associated with each edge.

13)Data Protection

Tenable is committed to protecting the confidentially,integrity and availability of all of your data.Tenable Vulnerability Management data is encrypted in transit and stored using modern ciphers and methods recommended by security industry and standards organizations.

14)Controlled Access Based on the Need to Know

The focus of this control is to ensure users are only allowed access to information they are authorized or needed to perform job duties. There are several layers to this complex problem, beginning with network segmentation, and growing to data classification and Data Loss Prevention (DLP) products.

15)Wireless Access Control

The focus of this control is to ensure wireless access is configured to track and control access, prevent unauthorized access. If misconfigurations are found, the settings should be corrected. Wireless access has become a common and natural part of a majority of organizations network infrastructure.

16)Account Monitoring and Control

The focus of this control is to ensure that all accounts are managed in a fashion that promotes clean account hygiene. This misuse or neglect of account maintenance can lead to system compromise.

17)Implement a Security Awareness and Training Program

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.

18)Application software Security

As an organization grows, custom applications are often developed to help with business workflow or other services which are offered to customers. These applications expose the organization to risk. Additionally, if the data stored is customer data, the customers may also be exposed. There are several tools in the market to help with Application Software Security.

19)Incident response and Management

A big part of a mature information security program is the Incidence Response (IR) program. The organization will grow into this practice as the size of the organization increases. However, the need for such a team remains constant. Many security incidents happen because a company is unaware of the asset or risk to the asset. The first and arguably most important step in vulnerability management is discovering assets, as risk can’t be assessed, if the asset is unknown.

20)Penetration Tests and Red Team Exercises

As a final testament to a good security program, the CIS Control 20 recommends the organization test all the security controls. These exercises are very beneficial to training and security awareness. Many times well intended measures can be exploited. For example, a really strict password policy can result in users taping passwords to their keyboard. A great technical control, thwarted by a forgetful user and an observant adversary. Many times developers find protocols they find useful, and never realize there is an inherent security flaw But in both cases, all credential exchanges are in clear text, allowing passwords and other information to be captured easily. Many chat programs use a form of HTTP and not HTTPS, again data is exchanged in the clear. With wireless technologies, many times with a simple wireless receiver, anyone can monitor the full exchanges of information. Penetration tests and red team exercises help to bring this information to the forefront of the security conversation.