**Name: Lakshmi Likitha Malemarpuram**

**Reg no: 21BCE8963**

**Email:** [**likitha.21bce8963@vitapstudent.ac.in**](mailto:likitha.21bce8963@vitapstudent.ac.in)

**DATE: 30-08-2023**

**DAY: WEDNESDAY**

**TASK 5: Information about CIS Top 20**

**UNDERSTANDING THE CIS POLICIES**

**1: Inventory and Control of Hardware Assets**

* Control 1 helps the CIS to actively manage (inventory, track, and

correct) 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.

* “Attackers, who can be located anywhere in the world, are

continuously scanning the address space of target organizations,

waiting for new and possibly unprotected systems to be attached

to the network. They are particularly interested in devices which

come and go off of the enterprise’s network such as laptops or

Bring-Your-Own-Device (BYOD) which might be out of

synchronization with security updates or might already be  
compromised.

* Attacks can take advantage of new hardware that is installed on  
  the network one evening but not configured and patched with  
  appropriate security updates until the following day. Even devices  
  that are not visible from the Internet can be used by attackers who  
  have already gained internal access and are hunting for internal  
  pivot points or victims.
* Additional systems that connect to the enterprise’s network (e.g.,  
  demonstration systems, temporary test systems, guest networks)  
  should also be managed carefully and/or isolated in order to  
  prevent adversarial access from affecting the security of  
  enterprise operations.”

**2: Inventory and Control of Software Assets**

• The focus of this control is to actively manage (inventory, track,  
and correct) software installed on systems within the organization.  
A fundamental aspect of risk management is discovering risk by  
tracking software present on information systems.  
• Ensuring only authorized software is used by the organization will  
increase the effectiveness of risk management efforts. Being able  
to quickly identify unauthorized and unmanaged software can  
prevent security breaches and increase the productivity of users.  
The CIS states this control is critical:  
• “Attackers continuously scan target organizations looking for  
vulnerable versions of software that can be remotely exploited.  
Some attackers also distribute hostile web pages, document files,  
media files, and other content via their own web pages or  
otherwise trustworthy third-party sites.  
• When unsuspecting victims access this content with a vulnerable  
browser or other client-side program, attackers compromise their  
machines, often installing backdoor programs and bots that give  
the attacker long-term control of the system.

• Some sophisticated attackers may use zero-day exploits, which  
take advantage of previously unknown vulnerabilities for which  
no patch has yet been released by the software vendor.  
• Without proper knowledge or control of the software deployed in  
an organization, defenders cannot properly secure their assets.

**3.Continuous Vulnerability Management**

• The Center for Internet Security (CIS) provides Critical Security  
Controls to help organizations improve cybersecurity.  
• Control 7 addresses continuous vulnerability management (this  
topic was previously covered under CIS Control 3).  
• Continuous vulnerability management is the process of  
identifying, prioritizing, documenting and remediating weak  
points in an IT environment.  
• Vulnerability management must be continual because sensitive  
data is growing at an unprecedented rate and attacks are  
increasing in both frequency and sophistication.  
• This control outlines 7 best practices that can help organizations  
minimize risks to their critical IT resources.

**4: Controlled Use of Administrative Privileges**

• The focus of this control is to ensure that all users with  
administrative level access use a dedicated or secondary account  
for any elevated activity.  
• This administrator account should not be used for any other  
purpose, and should not be used for email, web-browsing, or  
similar activity.  
The CIS states this Control is critical:  
• “The misuse of administrative privileges is a primary method for  
attackers to spread inside a target enterprise. Two very common  
attacker techniques take advantage of uncontrolled administrative  
privileges.

• In the first, a workstation user running as a privileged user is  
fooled into opening a malicious email attachment, downloading  
and opening a file from a malicious website, or simply surfing to  
a website hosting attacker content that can automatically exploit  
browsers.  
• The file or exploit contains executable code that runs on the  
victim’s machine either automatically or by tricking the user into  
executing the attacker’s content.  
• If the victim user’s account has administrative privileges, the  
attacker can take over the victim’s machine completely and install  
keystroke loggers, sniffers, and remote control software to find  
administrative passwords and other sensitive data.  
• Similar attacks occur with email. An administrator inadvertently  
opens an email that contains an infected attachment and this is  
used to obtain a pivot point within the network that is used to  
attack other systems.

**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.  
• Organizations must establish a baseline security configuration,  
implement a configuration management and change control  
process, and actively be able to report on the security  
configuration of all endpoint devices such as:  
Mobile devices  
Laptops  
Servers  
Workstations  
The CIS states this Control is critical:

“As delivered by manufacturers and resellers, the default  
configurations for operating systems and applications are normally  
geared towards ease-of-deployment and ease-of-use – not security.  
Basic controls, open services and ports, default accounts or  
passwords, older (vulnerable) protocols, and pre-installation of  
unneeded software can be exploitable in their default state.  
Developing configuration settings with good security properties is a  
complex task beyond the ability of individual users, requiring  
analysis of potentially hundreds or thousands of options in order to  
make good choices (the Procedures and Tools section below provides  
resources for secure configurations). Even if a strong initial  
configuration is developed and installed, it must be continually  
managed to avoid security “decay” as software is updated or  
patched, new security vulnerabilities are reported, and  
configurations are “tweaked” to allow the installation of new  
software or support new operational requirements. If not, attackers  
will find opportunities to exploit both network accessible services  
and client software.”  
• The journey of implementing the CIS Controls continues with the  
Secure Configuration for Hardware and Software on Mobile  
Devices, Laptops, Workstations, and Servers.  
Organizations are directed to develop strong, secure baseline  
configurations for each deployed software system. Organizations are  
also directed to maintain documented security configuration  
standards for all authorized operating systems and software.

**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.  
The CIS states this Control is critical:

“Deficiencies in security logging and analysis allow attackers to hide  
their location, malicious software, and activities on victim machines.  
Even if the victims know that their systems have been compromised,  
without protected and complete logging records they are blind to the  
details of the attack and to subsequent actions taken by the attackers.  
Without solid audit logs, an attack may go unnoticed indefinitely and  
the particular damages done may be irreversible. Sometimes logging  
records are the only evidence of a successful attack. Many  
organizations keep audit records for compliance purposes, but  
attackers rely on the fact that such organizations rarely look at the  
audit logs, and they do not know that their systems have been  
compromised.  
• Because of poor or nonexistent log analysis processes, attackers  
sometimes control victim machines for months or years without  
anyone in the target organization knowing, even though the  
evidence of the attack has been recorded in unexamined log  
files.”  
• The journey of implementing the CIS Controls continues with the  
Maintenance, Monitoring and Analysis of Audit Logs.  
Organizations are directed to ensure that local logging has been  
enabled on all systems and networking devices.  
• The specific sub-controls that are part of Implementation

**7: Email and Web Browser Protections**

• The Center for Internet Security (CIS) publishes Critical  
Security Controls that help organization improve cybersecurity.  
CIS Control 9 covers protections for email and web browsers.  
• Attackers target email and web browsers with several types of  
attacks. Some of the most popular are social  
engineering attacks, such as phishing.  
• Social engineering attempts to manipulate people into exposing  
sensitive data, providing access to restricted systems or spreading  
malware.

• Techniques include attaching a file containing ransomware to an  
email that purports to be from a reputable source, or including a  
link that appears to be for a legitimate websites but actually points  
to a malicious site that enables the hacker to collect valuable  
information, such as the user’s account credentials.  
• Certain features of email clients can leave them particularly  
vulnerable, and successful attacks can enable hackers to breach  
your network and compromise your systems, applications and  
data.

**8: Malware Defenses**

• The internet can be a dangerous place, whether you're a big  
organization or just an everyday user. And, while digital  
technologies open up to new possibilities, cybercriminals are  
getting smarter and smarter in taking advantage of them.  
• According to the CrowdStrike 2022 Global Threat Report, there  
were 82% more ransomware-related data leaks last year. At the  
same time, State-backed Iranian hackers were recently found  
guilty of spying on users via fake VPN apps. Phishing campaigns,  
like the recent one targeting shoppers this Black Friday, are  
often the simpler way to strike.  
• What all these attacks have in common is malicious software  
managing to elude the security infrastructure of one or more  
devices to inflict harm on their users. That's what, in technical  
jargon, is known as malware.  
• You might be inclined to think that just downloading one of  
the best antivirus apps is everything you need to secure your  
information. However, to truly protect your device from being  
infected, the truth is less straightforward. As malware can be so  
varied, your protection plan needs to be diversified too.  
• The best defense against malware doesn't lie on a mere  
combination of security software, either. You must know your

enemy before defeating it. Knowledge and precautions are the  
first weapons necessary to fight back!

**9: Limitation and Control of Network Ports,  
Protocols, and Services**

• The focus of this control is to 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.  
• A common denominator is that attackers will always search for,  
and attempt to exploit, accessible and vulnerable network  
services. The most common attacks are generally against hosts  
such as web servers, mail servers, file and printer servers, etc.  
The CIS states this Control is critical:  
“Attackers search for remotely accessible network services that are  
vulnerable to exploitation. Common examples include poorly  
configured web servers, mail servers, file and print services, and  
DNS servers installed by default on a variety of different device  
types, often without a business need for the given service. Many  
software packages automatically install services and turn them on as  
part of the installation of the main software package without  
informing a user or administrator that the services have been  
enabled. Attackers scan for such services and attempt to exploit these  
services, often attempting to exploit default user IDs and passwords  
or widely available exploitation code.”

**10: data recovery**

• Enterprise data recovery is the process of restoring lost,  
corrupted, accidentally deleted, or otherwise inaccessible data to  
its server, computer, mobile device, or storage device (or to a new  
device if the original device no longer works).  
• Typically, the data is restored from a backup copy that is stored in  
another location. The more recent the backup copy, the more

completely the data can be recovered in the event of loss or  
damage.  
• For any business, successful data recovery—data recovery that  
prevents a greater-than-tolerable loss of data or discontinuity of  
business due to loss of data—requires the business to have  
a backup and restore plan that meets specific data recovery  
objectives, usually as part of a larger disaster recovery plan.

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

• The focus of this control is to 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.  
The CIS states this Control is critical:  
“As delivered from manufacturers and resellers, the default  
configurations for network infrastructure devices are geared for  
ease-of-deployment and ease-of-use – not security. Open services  
and ports, default accounts (including service accounts) or  
passwords, support for older (vulnerable) protocols, pre-installation  
of unneeded software; all can be exploitable in their default state.  
The management of the secure configurations for networking devices  
is not a one-time event, but a process that involves regularly re-  
evaluating not only the configuration items but also the allowed  
traffic flows. Attackers take advantage of network devices becoming  
less securely configured over time as users demand exceptions for  
specific business needs. Sometimes the exceptions are deployed and  
then left undone when they are no longer applicable to the business  
needs. In some cases, the security risk of the exception is neither  
properly analyzed nor measured against the associated business  
need and can change over time.

**12: Boundary Defense**

• Boundary defense is control 12 of the CIS Critical  
Controls and is part of the network family. There are ten  
subsections to this control that cover your DMZ, firewalls  
and proxies, IDS/IPS, NetFlow, and remote access.  
• Boundary defense is typically an organization’s first line  
of protection against outside threats. Today, many  
attackers focus on exploiting systems that they can reach  
across the internet; they are  
• constantly probing perimeters for vulnerabilities and information  
needed to build their attack plan.

**13: Data Protection**

• Data protection is the process of protecting sensitive information  
from damage, loss, or corruption.  
• As the amount of data being created and stored has increased at  
an unprecedented rate, making data protection increasingly  
important. In addition, business operations increasingly depend  
on data, and even a short period of downtime or a small amount  
of data loss can have major consequences on a business.  
• The implications of a data breach or data loss incident can bring  
organizations to their knees. Failure to protect data can cause  
financial losses, loss of reputation and customer trust, and legal  
liability, considering most organizations today are subject to  
some data privacy standard or regulation.  
• Data protection is one of the key challenges of digital  
transformation in organizations of all sizes.

**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.

The CIS states this Control is critical:  
“Encrypting data provides a level of assurance that even if data is  
compromised, it is impractical to access the plaintext without  
significant resources; however, controls should also be put in place  
to mitigate the threat of data exfiltration in the first place. Many  
attacks occurred across the network, while others involved physical  
theft of laptops and other equipment holding sensitive information.  
Yet, in many cases, the victims were not aware that the sensitive data  
were leaving their systems because they were not monitoring data  
outflows. The movement of data across network boundaries both  
electronically and physically must be carefully scrutinized to  
minimize its exposure to attackers.

**15 Wireless Access Control**

• Experience the seamless convenience and enhanced security  
offered by wireless access control systems. At Monarch, we  
specialize in providing cutting-edge solutions for businesses  
seeking advanced access control.  
• With wireless technology, you can say goodbye to traditional  
wiring limitations and embrace the flexibility and scalability that  
wireless systems offer. Our team of security experts is here to  
help you navigate the world of wireless access control, ensuring  
your premises are protected with the latest innovations.  
• Connect with us today to explore how wireless access control can  
revolutionize your security infrastructure.

**16: Account Monitoring and Control**

• Everybody wants the latest and greatest next-gen product  
to get rid of the APTs and h4x0r$ hiding within their  
networks.  
• But what if I told you…  
You don’t need all those bells and whistles to have a great  
security program? Specifically, by following CIS Critical

• Control 16: Account Monitoring and Control, which  
focuses on processes to manage the lifecycle (creation,  
use, dormancy, and deletion) of system and application  
accounts, you can do much good by practicing one of the  
most

**17: implement security awareness training**

• Find the right time to voice out your ideas and concerns about  
your company’s network security to your senior management.  
Explain why security awareness training is essential in today’s  
world and its benefits.  
• Tailor the pitch and sharpen your message by blending in the  
organisational goals or values. Once the company leaders see how  
your initiative fits into the big picture, they’ll be more willing to  
devote resources to it. Take reference from our article, and learn  
how to persuade the senior management in order to get a budget.  
• Getting support with a top-down approach can help you quickly  
acquire needed material and resources. It will also empower you  
to get authority and credibility to increase the likelihood for  
employees to adopt the training.

**18: Application Software Security**

• Application security is the process of making apps more secure by  
finding, fixing, and enhancing the security of apps. Much of this  
happens during the development phase, but it includes tools and  
methods to protect apps once they are deployed.  
• This is becoming more important as hackers increasingly target  
applications with their attacks.  
• Application security is getting a lot of attention. Hundreds of tools  
are available to secure various elements of your applications  
portfolio, from locking down coding changes to assessing  
inadvertent coding threats, evaluating encryption options and  
auditing permissions and access rights.

• There are specialized tools for mobile apps, for network-based  
apps, and for firewalls designed especially for web applications.

**19: Incident Response Management**

• Incident response management is a systematic strategy that  
allows an organization to address cybersecurity incidents and  
security breaches. The goal of incident response is to identify  
real security incidents, get the situation under control, limit the  
damage caused by an attacker, and reduce the time and costs of  
recovery.  
• Incident response management typically includes formal  
documentation describing incident response procedures. These  
procedures should cover the entire incident response process,  
including preparation, detection, analysis, containment, and  
post-incident cleanup. By following these procedures,  
organizations can limit damage, prevent further losses, and  
comply with applicable compliance regulations.

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

• Follow recommendations from Azure Security Center on  
performing vulnerability assessments on your Azure virtual  
machines, container images, and SQL servers.  
• Use a third-party solution for performing vulnerability  
assessments on network devices and web applications. When  
conducting remote scans, do not use a single, perpetual,  
administrative account. Consider implementing JIT provisioning  
methodology for the scan account. Credentials for the scan  
account should be protected, monitored, and used only for  
vulnerability scanning.