Implementing Cyber Security through Open Source in a Big Enterprise

AT

Nuclear Power Corporation Of India Limited

(A Government Of India Enterprise)

TARAPUR ATOMIC POWER STATION 3&4

A Project Report on

Cyber security in a Big Enterprise

SUBMITTED BY:

RITIKA KUMARI

Under the Guidance of

Mr. Rakesh Rao
IT Head TAPS(3&4)

NUCLEAR POWER CORPORATION OF INDIA LIMITED

TARAPUR ATOMIC POWER STATION 3&4

CERTIFICATE

This is to certify that **Ms. RITIKA KUMARI** of Fr. Conceicao Rodrigues Institute of Technology, Vashi has successfully completed her vocational training entitled "**Implementing cyber security through open source in a big enterprise**" in our organisation **"Tarapur Atomic Power Station 3&4**".

The duration of the training was from **1st June 2023 to 30th June 2023**.

During this period of the project, she worked with full dedication and her behaviour was satisfactory. According to organisation policy, we cannot provide the project code.

On behalf of "Tarapur Atomic Power Station 3 & 4", we wish her best of luck for her future.

Mr. Rakesh Rao
IT Head(TAPS 3&4)

Acknowledgement

Any successful endeavour requires an opportunity, an opening and proper direction. Such an opportunity was provided to me by Nuclear Power Corporation of India Limited (NPCIL) by approbation in Tarapur Atomic Power Project (TAPP) 3 & 4, Tarapur, an unit of NPCIL.

I am really grateful to **Ms. Shibanee Saraf Manager(HR)** for accepting my training request and allowing access to TAPP 3 & 4 facilities. In TAPP 3&4, I was provided with constant encouragement and inputs related to my work. The work, culture and willingness of all officials and staff that helped me in my way were truly amazing.

The environment and resources made available enabled me to put in my best efforts and complete the project in time, while giving me insights as to how an industry, plant and office work.

I would like to thank **Mr. Rakesh Rao (IT Head)** for giving me time in his busy schedule. He also provided me with the most congenial and conductive environment and his unrelenting support and also let me use his official premises for training related purposes.

Also I would like to thank **Mr. Jatin Shrivastava (Technical officer)** and **Mr. Wiquar Ahmad (Technical Officer)** and all the staff of IT Department for providing all the practical help I needed during my training and being ready always for help.

I also thank all the employees of the TAPP 3 & 4 who helped in my training directly or indirectly and it is because of them, I completed my project successfully.

Lastly I would like to thank my friends and teachers of my College, who encouraged me, supported me morally and guided me to put in my best.

Index

Chapter 1

Introduction

Company Profile:-

Nuclear Power is the fifth-largest source of generating electricity in India after coal, gas, wind power, and hydroelectricity. At present, India has 22 operational nuclear reactors with an installed capacity of about 6,780 MW. The nuclear energy programme in India was launched around the time of independence under the leadership of Homi J. Bhabha.

Nuclear Power Plants in India 2022- Operational

Power Plant	Location	Operator	Type	Total Capacity (MW)
Kaiga	Karnataka	NPCIL	IPHWR-220	880
Kakrapar	Gujarat	NPCIL	IPHWR-220 IPHWR-700	1,140
Kudankulam	Tamil Nadu	NPCIL	VVER-1000	2,000
Madras (Kalpakkam)	Tamil Nadu	NPCIL	IPHWR-220	440
Narora	Uttar Pradesh	NPCIL	IPHWR-220	440
Rajasthan	Rajasthan	NPCIL	CANDU IPHWR-220	1,180
Tarapur	Maharashtra	NPCIL	BWR IPHWR-540	1,400
			Total	7,480

Nuclear Power Plants in India 2022- Under Construction

Power Plant	Location	Operator	Type	Total Capacity (MW)
Chennai (Kalpakkam)	Tamil Nadu	BHAVINI	PFBR	500
Kakrapar Unit 4	Gujarat	NPCIL	IPHWR-700	700
Gorakhpur	Haryana	NPCIL	IPHWR-700	1,400
Rajasthan Unit 7 & 8	Rajasthan	NPCIL	IPHWR-700	1,400
Kudankulam Unit 3,4,5 & 6	Tamil Nadu	NPCIL	VVER-1000	4,000
			Total	8,000

Nuclear Power Plants in India 2022- Planned Projects

Power Plant	Location	Operator	Type	Total Capacity (MW)
Kaiga	Karnataka	NPCIL	IPHWR-700	1,400
Jaitapur	Maharashtra	NPCIL	EPR	9,900
Kovvada	Andhra Pradesh	NPCIL	AP1000	6,600
Kavali	Andhra Pradesh	NPCIL	VVER	6000
Gorakhpur	Haryana	NPCIL	IPHWR-700	2,800
Mahi Banswara	Rajasthan	NPCIL	IPHWR-700	2,800
Chutka	Madhya Pradesh	NPCIL	IPHWR-700	1,400
Chennai	Tamil Nadu	BHAVINI	FBR	1,200
Tarapur	Maharashtra		AHWR	300
			Total	32,400

Nuclear energy is important for India

Nuclear energy has to play an important role in India's energy scenario from three angles. First is that unlike renewables, nuclear sources can provide bulk energy in a certain manner (without uncertainty) to the base load. The Kudankulam power projects' two reactors have added 2000 MW electricity to the southern states. Secondly, nuclear energy is a clean energy source and hence is very important to attain a carbon free energy economy. Thirdly, nuclear energy enhances energy independence and energy security especially with the potential use of domestically available thorium input use.

Nuclear power industry has developed manifold since its inception in India, studies in nuclear science on a systematic basis began in India during the late forties with the establishment of Tata Institute of Fundamental Research (TIFR) in Mumbai. Exploitation of Nuclear energy for generation of electricity has supplied the country with nearly more electricity so far.Keeping in mind the increasing need of industry and global competitive challenges started, Nuclear Power Corporation of India Limited (NPCIL) with its headquarter at Vikram Sarabhai Bhavan, Mumbai. NPCIL is a wholly owned enterprise of the government of India under the administrative control of the Department of Atomic Energy. It has registered as a Public Limited Company under the Company Act, 1956 in Sept. 1987 with the objection of undertaking design, construction, operation and maintenance of the Atomic Power Station for the generation of the electricity in pursuance of the schemes and programs of the Government of India under its infant status at time of independence. Research and Development is the corporation, as it transforms aspiration and ideas into reality. The technical knowledge, analytical aptitude and investigation imagination are three core competencies required in a research scientist at NPCIL.

Bhabha Atomic Research Centre (BARC) at Mumbai is a premier institute aiming to provide the nucleus of the quality manpower for the NPCIL's nuclear power projects all over the country for the last 35 years through the training in scientific and field. BARC encompasses fields like agriculture, medicine, computer, electronics, R&D and other areas, which are directly relevant to the development of the nuclear resources of the country in a very efficient way.

The fundamental of the electricity generation at atomic power stations is the generation of heat by bombarding neutrons on the isotope of U-235. The heat, which is thus being

generated, is used to heat up the water to convert it into steam in the turbine, which further runs the turbo generator, and thus generates electricity.

It was deemed necessary to have an installed Nuclear Power Capacity 20000 MW by the year to make the country self-sufficient in electricity production. Considering that Nuclear Power is a safe and environmentally clean source of power generation and that India has vast thorium reserves, NPCIL is ever increasingly poised to play a leading role in future to meet energy demands of the country.

TAPS 3&4 site is one of the largest capacity nuclear reactors in India. IT-Group TAPS 3&4 maintains a local web-site on the Local network. On the website different applications are running. This website is one of the most popular websites among all NPCIL units.

CHAPTER 2

Cyber Security

- **What is Cyber Security?**

Cybersecurity refers to the practice of protecting computer systems, networks, software, and data from unauthorised access, attacks, damage, or any form of digital disruption. It involves implementing measures and adopting strategies to ensure the confidentiality, integrity, and availability of information in the digital realm.

With the increasing reliance on technology and interconnected systems, cybersecurity has become a crucial aspect of both individual and organisational security. It encompasses various technologies, processes, and practices that aim to safeguard computer systems and networks from potential threats, such as hackers, malware, viruses, data breaches, and other cyberattacks.

Cyber security is a critical issue for businesses of all sizes. A cyber attack can have a devastating impact on a company's operations, financial well-being, and reputation.

There are many things that businesses can do to protect themselves from cyber threats, including:

1. Having a strong security policy in place.
2. Implementing security controls, such as firewalls, antivirus software, and intrusion detection systems.
3. Educating employees about cyber security risks.
4. Conducting regular security assessments.

- **Types of Cyber Attacks**

1. Malware: Malware is malicious software designed to infiltrate a computer system or network and perform unauthorised actions. This includes viruses, worms, Trojans, ransomware, spyware, and adware. Malware can damage files, steal sensitive information, or grant unauthorised access to attackers.
2. Phishing: Phishing attacks involve tricking individuals into revealing sensitive information, such as passwords, credit card numbers, or social security numbers. Attackers typically masquerade as trustworthy entities via email, instant messaging, or phone calls and deceive victims into clicking on malicious links or providing their confidential data.
3. Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS): In a DoS attack, the attacker overwhelms a targeted system or network with a flood of requests, rendering it unable to respond to legitimate user requests. DDoS attacks involve multiple compromised devices simultaneously attacking the target, amplifying the impact and making it harder to mitigate.
4. SQL Injection: This attack targets web applications that rely on a database backend. By exploiting vulnerabilities in input fields, attackers can inject malicious SQL

statements that manipulate or retrieve unauthorised data, potentially gaining control over the application or accessing sensitive information.

5. Man-in-the-Middle (MitM): In a MitM attack, an attacker intercepts communications between two parties without their knowledge. The attacker can eavesdrop, modify, or inject malicious content into the communication stream, compromising the confidentiality and integrity of the data being transmitted.
6. Cross-Site Scripting (XSS): XSS attacks target web applications that fail to properly validate user input. Attackers inject malicious scripts into web pages viewed by unsuspecting users, allowing them to steal sensitive information, hijack user sessions, or deliver malware.
7. Social Engineering: Social engineering attacks exploit human psychology to manipulate individuals into performing actions or divulging confidential information. This can include impersonating trusted individuals, conducting phishing calls, or using psychological manipulation to gain unauthorised access.
8. Ransomware: Ransomware encrypts a victim's files or locks their system, making them inaccessible until a ransom is paid. Attackers typically demand payment in cryptocurrencies and may threaten to permanently delete or publish the victim's data if the ransom is not paid.

- **How to prevent Cyber attacks?**

Cyber attacks are becoming increasingly common, and it is important to take steps to protect yourself and your organisation from them.

Following are the some ways to prevent it:

1. Keep Software Updated: Regularly update operating systems, applications, and firmware to ensure they have the latest security patches and fixes. Enable automatic updates whenever possible.
2. Use Strong and Unique Passwords: Create strong passwords that include a combination of upper and lowercase letters, numbers, and symbols. Use a unique password for each online account or system and consider using a password manager to securely store and generate passwords.
3. Implement Multi-Factor Authentication (MFA): Enable MFA or two-factor authentication (2FA) wherever possible. This adds an extra layer of security by requiring an additional verification method, such as a fingerprint scan, SMS code, or authentication app, in addition to a password.
4. Educate and Train Users: Conduct regular cybersecurity awareness training for employees, teaching them about common threats, safe browsing practices, recognizing phishing emails, and the importance of strong passwords. Encourage a culture of security throughout the organisation.
5. Use Secure Networks and Encryption: When accessing sensitive information or conducting financial transactions online, ensure you are using a secure network connection. Look for the padlock symbol in the address bar and use websites with "https://" instead of "http://" to ensure encrypted communication.

6. Regularly Back Up Data: Maintain secure and up-to-date backups of important data. In the event of a ransomware attack or data loss, backups can help restore your information without having to pay a ransom or suffer significant consequences.
7. Implement Firewalls and Antivirus Software: Utilise firewalls to monitor and control network traffic, and install reputable antivirus or anti-malware software to detect and remove malicious programs. Keep these tools updated to effectively combat emerging threats.
8. Monitor and Log Activities: Implement robust logging and monitoring systems to track and analyze network and system activities. Monitor for suspicious behaviour, unauthorised access attempts, and signs of compromise. Regularly review logs for any indicators of compromise.

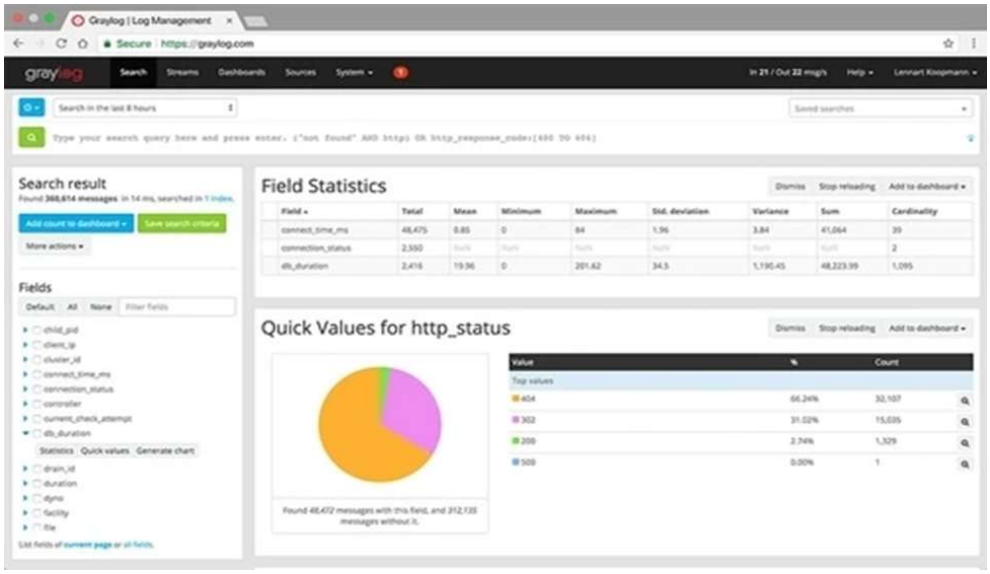
- **Tools required for securing a network**

1. **NMAP :** Nmap (Network Mapper) is an open-source network exploration and security auditing tool. It is widely used by network administrators, security professionals, and ethical hackers to scan and map networks, discover hosts, and gather information about the services running on those hosts.
   Nmap utilises raw IP packets to perform a variety of tasks, including host discovery, port scanning, service and version detection, and OS fingerprinting. It can identify live hosts on a network, determine which ports are open, and provide details about the services running on those ports.

2. **Wireshark** : Wireshark is a powerful and popular open-source network protocol analyzer used for network troubleshooting, analysis, and security investigations. It allows users to capture and analyse network traffic in real-time or from stored capture files. Wireshark is a versatile tool used by network administrators, network engineers, security analysts, and researchers. Its extensive capabilities and user-friendly interface make it a valuable resource for diagnosing network problems, analysing network behaviour, and investigating network security incidents.

3. **Snort** : Snort is a widely used open-source Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) that monitors network traffic for potential security threats.Snort is widely deployed across various industries and organisations to enhance network security and protect against intrusions. Its robust detection capabilities, customization options, and community support make it a valuable tool for network administrators and security professionals in maintaining a secure network environment.
4. **Graylog** : Graylog is an open-source log management and analysis platform that allows organisations to collect, index, and analyze log data from various sources in real-time. It provides a centralized solution for log aggregation, searching, and visualisation, enabling users to gain insights into their systems,

troubleshoot issues, and enhance security. Graylog is utilized by organizations of all sizes and across different industries to manage their log data effectively, gain operational insights, and enhance security monitoring. Its open-source nature, rich feature set, and active community support make it a popular choice for log management and analysis needs.



- **Cyber Security Architecture**

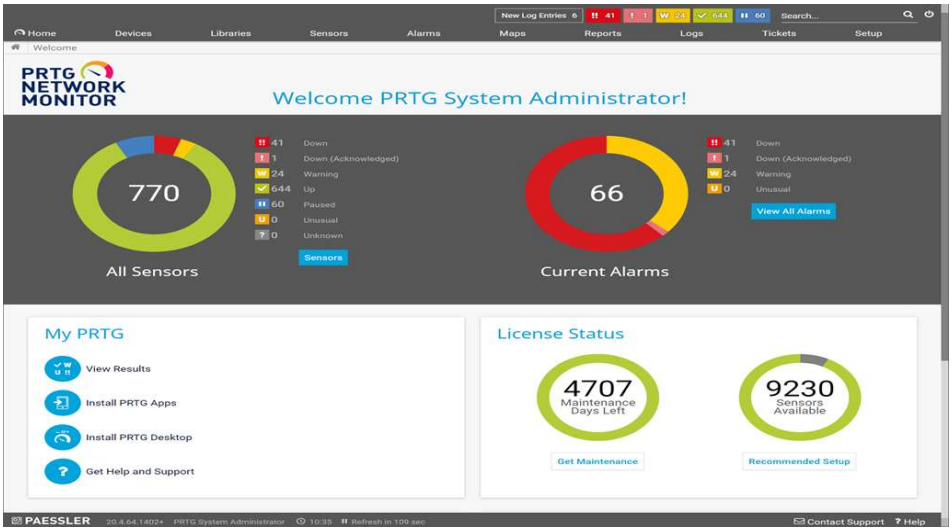
1. **Firewall:** A firewall is a network security device or software that acts as a barrier between an internal network and external networks, such as the internet. It helps protect the internal network from unauthorised access, malicious activities, and potential security threats. Firewalls enforce a set of rules or policies to control incoming and outgoing network traffic based on defined criteria. Firewalls are a fundamental component of network security, providing an essential layer of defence for protecting networks and resources from unauthorised access and malicious activities. They are deployed in various network environments, from small home networks to large enterprise networks, to enforce security policies, control network traffic, and mitigate potential threats.

2. **Proxy server:** A proxy server is an intermediary server that acts as a gateway between clients (such as computers or devices) and other servers (such as web servers). When a client makes a request to access a resource, the request is first sent to the proxy server, which then forwards the request to the appropriate server on behalf of the client. The proxy server receives the response from the server and forwards it back to the client. Proxy servers play a crucial role in network infrastructure by improving performance, enhancing security, and providing additional control over network traffic. They are used in various environments, from home networks to enterprise networks, to optimise resource utilisation, protect privacy, and enforce network policies.

3. Controlling Server:

➢ NAC (Network Access Control) : It is a security framework and set of technologies that are used to enforce security policies and control access to a network. NAC solutions are designed to ensure that only authorised and compliant devices and users can connect to a network, while preventing unauthorised or potentially risky devices from gaining access.
By implementing NAC, organizations can strengthen network security, mitigate risks associated with unauthorised access, enforce compliance with security policies, and improve overall visibility and control over network resources.

➢ PRTG(Paessler Router Traffic Grapher): Is a comprehensive network monitoring and management tool developed by Paessler AG. It allows network administrators to monitor various aspects of their network infrastructure in real-time, providing insights into the performance, availability, and health of network devices, systems, and applications. PRTG simplifies network monitoring by providing a user-friendly interface, extensive monitoring capabilities, and customizable alerting and reporting functionalities.



➢ Log server: A log server, also known as a syslog server or log management server, is a centralized system that collects, stores, and manages log files generated by various devices, applications, and systems within a network. Its primary purpose is to centralise log data for analysis, troubleshooting, compliance, and security purposes. Log servers help organizations streamline log management, improve system troubleshooting, enhance security monitoring, and meet compliance requirements. They provide a centralized repository for log data, making it easier to analyze and derive valuable insights from the vast amount of log information generated within a network environment.

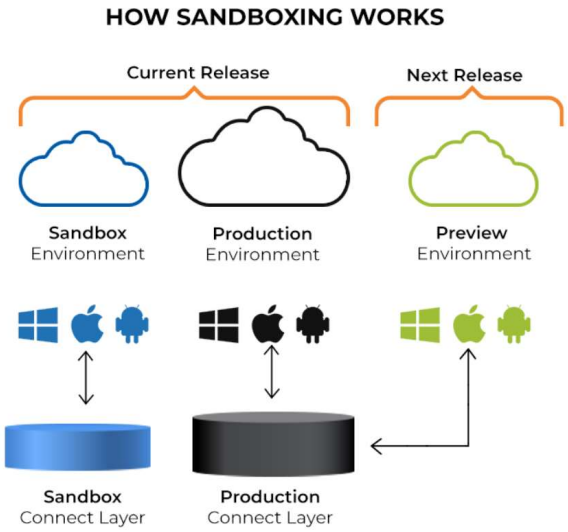
- ➢ Email server: An email server, also known as a mail server, is a computer or software application that handles the sending, receiving, storage, and delivery of email messages. It is responsible for managing email communication within an organisation or between different domains on the internet. Email servers are crucial for efficient and reliable email communication. They provide the infrastructure and protocols necessary for sending, receiving, and managing email messages, ensuring reliable delivery and secure transmission of information across networks.

- ➢ SIEM (Security Information and Event Management): It is a comprehensive approach to security management that combines security information management (SIM) and security event management (SEM) into a unified solution. SIEM systems provide real-time analysis of security alerts and log data from various sources to detect and respond to security incidents effectively. SIEM systems play a crucial role in enhancing an organisation's security posture by providing real-time threat detection, incident response capabilities, and compliance management. By consolidating and analysing security data from multiple sources, SIEM systems enable proactive identification of security incidents, rapid response to threats, and effective management of security risks.

- ➢ SOAR (Security Orchestration, Automation, and Response): It is a technology solution that integrates security tools, processes, and workflows to streamline and automate security operations. SOAR platforms provide organizations with the ability to respond to security incidents more efficiently and effectively. SOAR platforms enhance an organisation's security operations by enabling efficient incident response, automating security processes, and promoting collaboration among security teams. They help organizations reduce response times, mitigate risks, and improve overall security posture by leveraging orchestration, automation, and standardised workflows.

4. **Sandboxing:** Sandboxing is a security mechanism that isolates running programs or processes from the rest of the system to prevent potentially malicious or unintended actions. It creates a restricted environment where the execution of software is limited and controlled, minimizing the potential damage that a program can cause.
   The main purpose of sandboxing is to provide an additional layer of protection and mitigate the risks associated with running untrusted or unknown code. By isolating the execution of an application, sandboxing can prevent unauthorised access to system resources, protect against malware infections, and reduce the impact of software vulnerabilities.
   Sandboxing can be implemented using various techniques, such as virtualization, containerization, or software-based restrictions. Virtualization creates a virtual machine or environment where the application runs independently from the host system. Containerization utilises lightweight containers to isolate applications, allowing them to share the host's operating system kernel. Software-based sandboxes employ access controls and restrictions within the operating system to limit the actions of the application.

Sandboxing is widely used in several domains, including web browsers, operating systems, software development, and network security. Web browsers often employ sandboxing to confine JavaScript code within a restricted environment, reducing the risk of malicious scripts compromising the user's system. Operating systems may use sandboxes to contain untrusted applications or processes, ensuring that they cannot access sensitive resources. In software development, sandboxes provide developers with controlled environments to test and debug code without affecting the production system. Network security tools may utilise sandboxing to analyze suspicious files or behaviours in a controlled environment before them to execute on the network.



5. **Antivirus:** An antivirus, also known as antivirus software or anti-malware software, is a computer program designed to detect, prevent, and remove malicious software, commonly referred to as malware. The primary purpose of antivirus software is to protect computers and networks from various types of threats, including viruses, worms, Trojans, spyware, adware, and other forms of malware.

   Antivirus software works by employing different techniques to identify and eliminate malware. Here are some common functionalities and features of antivirus programs:

- ➢ Virus detection: Antivirus software scans files, programs, and the system memory for patterns or signatures that match known malware. These signatures are stored in a database that is regularly updated to include the latest threats.
- ➢ Heuristic analysis: Antivirus programs use heuristic techniques to identify suspicious behaviour or characteristics of potentially new or unknown malware. By analysing code and behaviour, the software can detect malware that hasn't been specifically identified yet.
- ➢ Real-time scanning: Antivirus software provides real-time protection by continuously monitoring the system for any malicious activity. It scans files and programs as they are accessed or executed to prevent infection.
- ➢ Quarantine or isolation: When malware is detected, antivirus software typically isolates the infected files or programs, placing them in a secure area called quarantine.

This prevents the malware from spreading and causing further harm. Users can then choose to remove or disinfect the infected files.

- ➢ Automatic updates: Antivirus software regularly updates its virus definitions to stay up to date with the latest threats. These updates ensure that the software can recognize and defend against newly emerged malware.
- ➢ Web protection: Many antivirus programs include features to protect users while browsing the internet. This may include blocking access to malicious websites, scanning downloads for malware, and detecting phishing attempts.

It's important to note that while antivirus software is an essential part of computer security, it is not foolproof. New and sophisticated malware can sometimes evade detection, and antivirus programs may have limitations. Therefore, it is crucial to practise safe computing habits, such as regularly updating software, being cautious with email attachments and downloads, and using a combination of security measures (firewalls, secure browsing, etc.) in addition to antivirus software.It's also worth mentioning that the field of cybersecurity extends beyond antivirus software, encompassing various other security measures like firewalls, intrusion detection systems, encryption, and user education to ensure comprehensive protection against threats.

6. **Hardening :** Hardening refers to the process of strengthening the security of a system or network by implementing various measures to reduce vulnerabilities and protect against potential attacks. The goal of hardening is to minimise the risk of unauthorised access, data breaches, and other security incidents. Here are some common practices for hardening systems:

- ➢ Patch management: Keep the system up to date with the latest security patches and updates for the operating system, software applications, and firmware. Regularly install patches to address known vulnerabilities and enhance system security.
- ➢ Secure configuration: Configure the system and its components to follow secure practices. This may involve disabling unnecessary services and ports, enabling encryption protocols, using strong passwords and authentication mechanisms, and enforcing security policies. When hardening a system for security, it often involves configuring network services and applications to operate on specific ports. Here are some commonly used ports associated with security hardening:
    - ❖ Port 22: This port is used for Secure Shell (SSH) communication. It is commonly hardened by implementing measures such as disabling root login, enforcing strong authentication methods (e.g., key-based authentication), and limiting access to specific IP addresses or networks.
    - ❖ Port 443: This port is used for HTTPS traffic, which employs SSL/TLS encryption for secure web communication. It is important to ensure the proper configuration of SSL/TLS certificates and enforce strong cipher suites and protocols to harden this port.

- ❖ Port 80: This port is used for unencrypted HTTP traffic. If not needed, it is often recommended to disable or redirect HTTP traffic to HTTPS (port 443) to enforce encryption.
- ❖ Port 3389: This port is used for Remote Desktop Protocol (RDP) on Windows systems. It is commonly hardened by implementing measures such as enabling strong password policies, using network-level authentication, and limiting access to specific IP addresses or networks.
- ❖ Port 25: This port is used for Simple Mail Transfer Protocol (SMTP), which is responsible for email transmission. It is important to secure this port by implementing measures such as enabling SMTP authentication, configuring proper spam filtering, and preventing open relay configurations.
- ❖ Port 123: This port is used for Network Time Protocol (NTP) communication, which synchronises system clocks. Hardening this port involves configuring proper access controls, limiting queries to trusted sources, and ensuring NTP server security.
- ❖ Port 53: This port is used for Domain Name System (DNS) communication. Hardening DNS involves implementing measures such as securing DNS zone transfers, using DNSSEC for data integrity, and properly configuring access controls.

➢ Access controls: Implement appropriate access controls to limit user privileges and restrict access to sensitive resources. This includes employing the principle of least privilege, implementing strong authentication mechanisms, and regularly reviewing and revoking unnecessary user accounts and permissions.

➢ Encryption: Utilise encryption techniques to protect sensitive data in transit and at rest. This includes encrypting network traffic using protocols like SSL/TLS, implementing full-disk encryption, and encrypting data stored in databases or file systems.

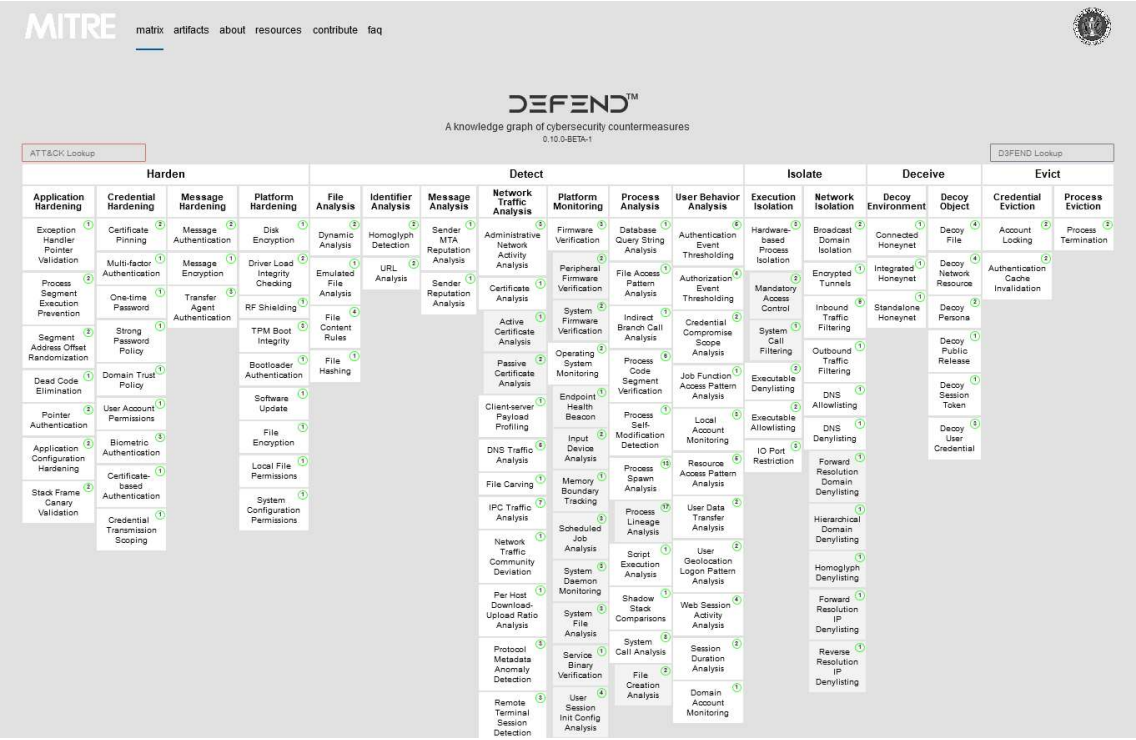
➢ Security awareness and training: Promote security awareness among users and provide training on best practices, such as recognizing and avoiding social engineering attacks, phishing attempts, and other common security threats. Educated users are less likely to fall victim to security breaches.

➢ Regular backups: Maintain regular backups of critical data to ensure it can be restored in the event of a security incident or system failure. Test the backup and restore processes periodically to ensure their effectiveness.

➢ Monitoring and logging: Implement robust monitoring and logging mechanisms to detect and investigate security incidents. Monitor system logs, network traffic, and user activities for any signs of unauthorised access or suspicious behaviour.

Hardening is an ongoing process that requires continuous monitoring, evaluation, and adaptation to address emerging threats and vulnerabilities. It is essential to conduct regular security assessments, vulnerability scans, and penetration tests to identify potential weaknesses and apply appropriate measures to strengthen system security.

- **MITRE DEFENCE FRAMEWORK**



MITRE D3FENSE Matrix

While the MITRE ATT&CK framework is branched into three main variants known as Matrices (Enterprise, Mobile, and ICS), there is currently only one MITRE D3FENSE Matrix. D3FEND's countermeasure information is organised similarly to ATT&CK's hierarchy of adversary TTP but from a defensive perspective. Tactics are the highest-level classification in the D3FENSE hierarchy and correspond to the specific goals defenders must achieve to counter specific phases of a cyberattack. Each Tactic contains multiple Techniques and Sub-Techniques that describe technical methods for accomplishing the associated defensive tactical goals and include references to relevant IT security industry standards, tools, and patents.

MITRE D3FENSE Tactics and Highest-Level Techniques

- **Harden**
  - Application Hardening
  - Credential Hardening
  - Message Hardening
  - Platform Hardening
- **Detect**
  - File Analysis
  - Identifier Analysis
  - Message Analysis
  - Network Traffic Analysis

Platform Monitoring
Process Analysis
User Behavior Analysis

- **Isolate**

Execution Isolation
Network Isolation

- **Deceive**

Decoy Environment
Decoy Object

- **Evict**

Credential Eviction
Process Eviction

D3FEND also has a unique hierarchical catalogue of associative information known as "Digital Artefacts" not found in ATT&CK. Digital Artefacts represent digital concepts and objects, and the catalogue has four primary classes: Top-Level Artefacts, Files, Network Traffic, and Software. A portion of ATT&CK's offensive TTPs have been mapped to DeFEND Techniques using Digital Artefacts for use as a reference to identify related countermeasures and vice-versa. Those associations can be searched for and viewed within the Digital Artefacts Ontology.

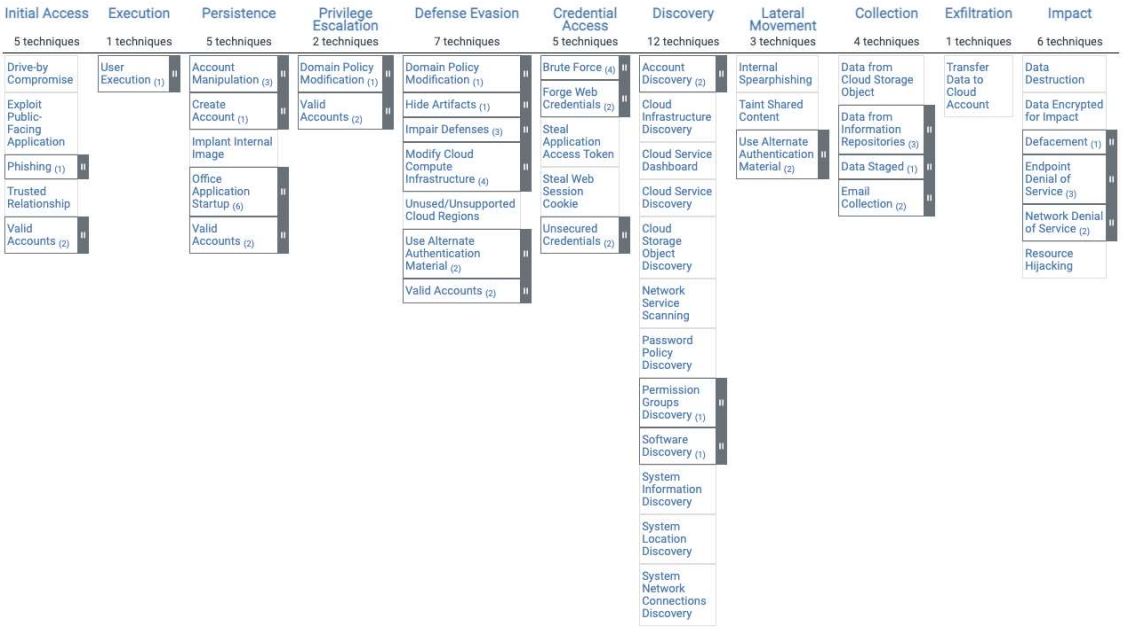
How to Use the MITRE D3FENSE Framework

D3FEND validates a common defensive cybersecurity language and classification hierarchy that can be used between stakeholders when developing a cybersecurity program from the ground up or evaluating an existing cyber program, assessing and comparing the security posture of software or cloud vendors' products, or informing acquisition and investment.

D3FEND has practical applications for organisations of all sizes, from SMBs to large enterprises. The D3FEND Tactics and Techniques can serve as a checklist for security planners, architects, and decision-makers planning and designing integrated network defences and software products that will ultimately be the barrier between adversaries and the organisation's digital assets.

Although the ATT&CK framework includes some limited mitigation advisory, D3FEND provides more formalised and organised insight into defensive countermeasures that mitigate and enable a long-term strategy to monitor, detect, and respond to cyberattacks.

- **MITRE ATTACK FRAMEWORK**



The MITRE ATT&CK matrix contains a set of techniques used by adversaries to accomplish a specific objective. Those objectives are categorised as tactics in the ATT&CK Matrix. The objectives are presented linearly from the point of reconnaissance to the final goal of exfiltration or "impact". Looking at the broadest version of ATT&CK for Enterprise, which includes Windows, macOS, Linux, PRE, Azure AD, Office 365, Google Workspace, SaaS, IaaS, Network, and Containers, the following adversary tactics are categorised:

1. Reconnaissance: gathering information to plan future adversary operations, i.e., information about the target organisation
2. Resource Development: establishing resources to support operations, i.e., setting up command and control infrastructure
3. Initial Access: trying to get into your network, i.e., spear phishing
4. Execution: trying the run malicious code, i.e., running a remote access tool
5. Persistence: trying to maintain their foothold, i.e., changing configurations
6. Privilege Escalation: trying to gain higher-level permissions, i.e., leveraging a vulnerability to elevate access
7. Defence Evasion: trying to avoid being detected, i.e., using trusted processes to hide malware
8. Credential Access: stealing accounts names and passwords, i.e., keylogging
9. Discovery: trying to figure out your environment, i.e., exploring what they can control
10. Lateral Movement: moving through your environment, i.e., using legitimate credentials to pivot through multiple systems
11. Collection: gathering data of interest to the adversary goal, i.e., accessing data in cloud storage

12. Command and Control: communicating with compromised systems to control them, i.e., mimicking normal web traffic to communicate with a victim network
13. Exfiltration: stealing data, i.e., transfer data to cloud account
14. Impact: manipulate, interrupt, or destroy systems and data, i.e., encrypting data with ransomware

Within each tactic of the MITRE ATT&CK matrix there are adversary techniques, which describe the actual activity carried out by the adversary. Some techniques have sub-techniques that explain how an adversary carries out a specific technique in greater detail.

CHAPTER 3

ETHICAL HACKING

Ethical hacking involves an authorised attempt to gain unauthorised access to a computer system, application, or data. Carrying out an ethical hack involves duplicating strategies and actions of malicious attackers. This practice helps to identify security vulnerabilities which can then be resolved before a malicious attacker has the opportunity to exploit them.
Also known as “white hats,” ethical hackers are security experts that perform these security assessments. The proactive work they do helps to improve an organisation’s security posture. With prior approval from the organisation or owner of the IT asset, the mission of ethical hacking is opposite from malicious hacking.

The company that owns the system or network allows Cyber Security engineers to perform such activities in order to test the system’s defences. Thus, unlike malicious hacking, this process is planned, approved, and more importantly, legal.
Ethical hackers aim to investigate the system or network for weak points that malicious hackers can exploit or destroy. They collect and analyse the information to figure out ways to strengthen the security of the system/network/applications. By doing so, they can improve the security footprint so that it can better withstand attacks or divert them.
Ethical hackers are hired by organisations to look into the vulnerabilities of their systems and networks and develop solutions to prevent data breaches. Consider it a high-tech permutation of the old saying “It takes a thief to catch a thief.”
They check for key vulnerabilities include but are not limited to:

- Injection attacks
- Changes in security settings
- Exposure of sensitive data
- Breach in authentication protocols
- Components used in the system or network that may be used as access points

Different security training manuals explain the process of ethical hacking in different ways, but for me as a Certified Ethical Hacker, the entire process can be categorised into the following six phases.

➢ Reconnaissance: Reconnaissance is the phase where the attacker gathers information about a target using active or passive means. The tools that are widely used in this process are NMAP, Hping, Maltego, and Google Dorks.

➢ Scanning: In this process, the attacker begins to actively probe a target machine or network for vulnerabilities that can be exploited. The tools used in this process are Nessus, Nexpose, and NMAP.

➢ Gaining Access: In this process, the vulnerability is located and you attempt to exploit it in order to enter into the system. The primary tool that is used in this process is Metasploit.

➢ Maintaining Access: It is the process where the hacker has already gained access into a system. After gaining access, the hacker install some backdoors in order to enter into the system when he needs access in this owned system in future. Metasploit is the preferred tool in this process.

➢ Clearing Tracks: This process is actually an unethical activity. It has to do with the deletion of logs of all the activities that take place during the hacking process.

➢ Reporting: Reporting is the last step of finishing the ethical hacking process. Here the Ethical Hacker compiles a report with his findings and the job that was done such as the tools used, the success rate, vulnerabilities found, and the exploit processes.

Ethical hacking Tools

Automation has left its imprint on every industry out there, and the realm of ethical hacking is no different. With the onset of various tools in the ethical hacking industry, it has been transformed. Ethical hacking tools help in information gathering, creating backdoors and payloads, cracking passwords and an array of other activities.

- Acunetix
- Nmap
- Metasploit
- Wireshark
- Nikto
- SQLninja
- Wapiti

CHAPTER 4

Security Operation Centre (SOC)

A Security Operations Center (SOC) is a centralised unit within an organisation that is responsible for monitoring, detecting, and responding to security incidents and threats. It serves as a command centre for security operations, providing continuous monitoring and analysis of security events and activities.

The primary functions of a Security Operations Center include:

1. Monitoring and Detection: SOC teams continuously monitor network and system logs, security devices, and other data sources to identify security incidents and potential threats. They use various tools and technologies, such as Security Information and Event Management (SIEM) systems, intrusion detection systems (IDS), and threat intelligence feeds, to gather and analyse information.

2. Incident Response: When a security incident is detected, SOC teams initiate an incident response process. This involves investigating and containing the incident, analysing the impact and root cause, and taking appropriate actions to mitigate the threat and minimise damage. Incident response may include isolating affected systems, removing malicious software, and restoring normal operations.

3. Threat Hunting: SOC teams proactively search for indications of compromise or potential threats within the organisation's network and systems. They conduct in-depth analysis and use advanced techniques to identify and investigate suspicious activities that may go undetected by automated security controls.

4. Vulnerability Management: SOC teams collaborate with other departments, such as IT and cybersecurity, to manage vulnerabilities within the organisation's infrastructure. They perform vulnerability assessments and track patching and remediation activities to address identified vulnerabilities and reduce the attack surface.

5. Threat Intelligence and Analysis: SOC teams gather, analyse, and disseminate threat intelligence to stay informed about the latest attack techniques, malware trends, and emerging threats. This helps them proactively identify potential risks and take preventive measures to strengthen the organisation's security posture.

6. Reporting and Communication: SOC teams prepare reports and communicate security incidents, trends, and risks to management, stakeholders, and relevant teams within the organisation. Clear and timely communication ensures that the organisation remains aware of security issues and can make informed decisions.

To effectively operate a SOC, organisations require skilled personnel with expertise in cybersecurity, incident response, threat intelligence, and security analysis. SOC teams often work in a 24/7 environment, ensuring round-the-clock monitoring and response capabilities.

The establishment of a SOC demonstrates an organisation's commitment to maintaining a proactive and robust security posture. By centralising security operations, organisations can better detect and respond to security incidents, protect sensitive data, and reduce the impact of potential security breaches.

Working

The primary mission of the SOC is security monitoring and alerting. This includes the collection and analysis of data to identify suspicious activity and improve the organisation’s security. Threat data is collected from firewalls, intrusion detection systems, intrusion prevention systems, security information and event management (SIEM) systems and threat intel. Alerts are sent out to SOC team members as soon as discrepancies, abnormal trends or other indicators of compromise are picked up.

A SOC is primarily responsible for detecting and responding to cyber incidents and threats. SOCs can also conduct vulnerability assessments, penetration testing, threat hunting, and auditing for regulatory compliance. SOCs performs the following activities:

- **Monitor**
  Continuously collect security and event data in real-time from across your organisation’s IT infrastructure. This includes data from on-premises (on-prem) devices, the cloud, ICS and OT systems, remote systems, and mobile devices.

- **Detect**
  Identify abnormal trends, discrepancies, or other indicators of compromise (IoCs) from the volumes of data collected. Potential threats are categorised by severity and evaluated to determine whether they are actual threats your organisation should be concerned about. Automated detection tools can also be used to isolate real threats.

- **Respond**
  Take immediate action to respond to incidents and deploy appropriate mitigation measures to address the threat. Following an incident, SOCs will restore your network and systems back to their baseline state and recover any lost or compromised data.

- **Analyze**
  Conduct root cause investigation using log data and other information to determine the source of the incident. This can help prevent similar incidents from happening in the future

Key Security Operations Center (SOC) team members

• **The SOC manager**, who runs the team, oversees all security operations, and reports to the organisation's CISO (chief information security officer).

• **Security engineers**, who build out and manage the organisation's security architecture. Much of this work involves evaluating, testing, recommending, implementing and maintaining security tools and technologies. Security engineers also work with development or DevOps/DevSecOps teams to make sure the organisation's security architecture includes application development cycles.

• **Security analysts** – also called security investigators or incident responders – who are essentially the first responders to cybersecurity threats or incidents. Analysts detect, investigate, and triage (prioritise) threats; then they identify the impacted hosts, endpoints and users, and take the appropriate actions to mitigate and contain the impact or the threat or incident. (In some organisations, investigators and incident responders are separate roles classified as Tier 1 and Tier 2 analysts, respectively.)

• **Threat hunters** (also called expert security analysts) specialise in detecting and containing advanced threats – new threats or threat variants that manage to slip past automated defences. The SOC team may include other specialists, depending on the size of the organisation or the industry in which it does business. Larger companies may include a Director of Incident Response, responsible for communicating and coordinating incident response. And some SOCs include forensic investigators, who specialise in retrieving data – clues – from devices damaged or compromised in a cybersecurity incident.

Considerations when establishing your SOC

With cyber attacks becoming more frequent and complex, the question is not if an attack will happen, but when. This is something your organisation should keep in mind. A SOC can help to increase your organisation’s resilience against cyber threats and minimise the impact in the event of a compromise. The following are some best practices to consider when setting up and operating a SOC:

- **Develop a SOC strategy with the appropriate scope.**
    - Identify which organisational assets, like systems and data, are highly valuable or sensitive and need to be monitored and protected.
    - Perform a cyber security risk assessment to understand the threats your organisation faces. It can also be useful to understand the level of sophistication of threat actors targeting your organisation. For Government of Canada (GC) departments, refer to ITSG-33, Annex A, Table 5 for description of threat agents. For non-GC organisations, consult the structured threat

information expression (STIX) v2.1 framework for description of threat actor skill levels.
    - Understand the legal, regulatory, and compliance requirements that your organisation operates under to know what the SOC is required to do or protect.

➢ **Design a SOC solution that meets organisational needs.**
    - Select a SOC model that is comparable to your organisation's threat profile and is achievable given your resources. Your requirements and the threats you face will change over time, so your model should be easily adapted to keep pace.
    - Incorporate threat-oriented defence into the routine security operations including those from threat frameworks such as MITRE ATT&CK and OWASP top ten.
    - For large organisations with broad geographical coverage, like hospitals and schools, consider integrating or consolidating multiple SOCs into a regional SOC. This enables SOCs to share information, jointly invest in tools and expert staff, and increase the situational awareness for the participating organisations.

➢ **Implement and operate the solution efficiently.**
    - Collect meaningful data from sensors and logs generated from applications, operating systems, the network, the cloud, and ICS/OT systems.
    - Use automated technologies as part of your incident response strategy.
    - Select an event management solution that includes log collection and processing, storage, querying, alerting, and incident management. A number of commercial and open-source security information and event management (SIEM) platforms are available to help your organisation derive value from the volumes of event data collected daily. Consider the ongoing configuration, support and licensing requirements when choosing the appropriate SIEM platform.
    - Establish a clear incident response plan, and test it regularly, to ensure critical functions can be restored and recovered in a timely manner. Simulate the issue response within an isolated testing zone so that the production environment is not affected.
    - Ensure SOC services operate within their legal and regulatory requirements. Appropriate security controls should be in place and enforced, like data validation to identify sensitive information.
    - Develop clear documentation of processes and procedures to enable SOC team members to work efficiently.
    - Build the right SOC team by hiring people with a wide range of technical skills and experience. Create a retention strategy to minimise staff turnover.

- **Maintain and update the solution as necessary over time.**
    - Encourage regular communication and collaboration amongst SOC team members and various stakeholders, like users, management, and system owners, across the organisation. This can create a valuable feedback mechanism for the SOC to provide better services to your clients.
    - Collect metrics to measure SOC performance and effectiveness which will allow you to adjust the SOC operations accordingly.
    - Enhance SOC activities to include attack simulation and assessments, cyber deception, and insider threat hunting in order to stay ahead of sophisticated threat actors.

Benefits of a SOC

- Continuous monitoring and analysis of system activity.
- Improved incident response.
- Decreased timeline between when a compromise occurs and when it is detected.
- Reduced downtime.
- Centralization of hardware and software assets leading to a more holistic, real time approach to infrastructure security.
- Effective collaboration and communication.
- Reduction in direct and indirect costs associated with the management of cyber security incidents.
- Employees and customers trust the organisation and become more comfortable with sharing their confidential information.
- Greater control and transparency over security operations.
- Clear chain of control for systems and data, something that's crucial for the successful prosecution of cybercriminals.

CHAPTER 5

Conclusion

In conclusion, implementing cybersecurity measures within an organisation is crucial in today's digital landscape. It helps protect sensitive data, safeguard critical systems and infrastructure, and mitigate the risk of cyber threats and attacks. By taking cybersecurity seriously, organisations can ensure business continuity, maintain customer trust, and avoid the potentially devastating consequences of security breaches.

In today's interconnected world, cybersecurity is an ongoing effort that requires a combination of technical measures, employee awareness and training, incident response planning, and continuous monitoring and improvement. By investing in cybersecurity, organisations can better protect their assets, maintain a competitive edge, and safeguard their long-term success in the digital age.

CHAPTER 6

References

1. https://www.wikipedia.org/
2. https://attack.mitre.org/
3. https://d3fend.mitre.org/