

|  |  |
| --- | --- |
| Date | 10 March 2025 |
| Team ID | PNT2025TMID02556 |
| Project Name | Project - Exploring Cyber Security  Understanding Threats and Solutions in the Digital Age |
| Maximum Marks | 8 Marks |

**List of teammates–**

|  |  |  |  |
| --- | --- | --- | --- |
| **S.no** | **Name** | **College** | **Contact no** |
| **1**      **2** | **Dhanraj Pawar**      **Kaushal Chougule** | **DY Patil Agriculture and Technical University, Talsande**    **DY Patil Agriculture and Technical University, Talsande** | **9322825454**      **9960592608** |
| **3**      **4** | **Balaji Patil**      **Atharv Pawar** | **DY Patil Agriculture and Technical**  **University, Talsande**    **DY Patil Agriculture and Technical**  **University, Talsande** | **7498586267**      **8010656042** |

**Abstract:**

In today's digital world, cybersecurity is essential because cyber threats are constantly changing and can affect individuals, businesses, and governments. This project looks at important cybersecurity threats like malware, phishing, ransomware, denial-of-service (DoS) attacks, SQL injection, and zero-day exploits. These threats can lead to serious problems, including data breaches, financial losses, and damage to reputations.

The research reviews both traditional and modern ways to defend against these threats. It assesses the effectiveness of tools like firewalls, intrusion detection systems (IDS), encryption methods, and access controls. It also explores advanced security technologies such as artificial intelligence (AI), machine learning (ML), and blockchain. Furthermore, it emphasizes the importance of security strategies like zero-trust architecture, least privilege access, and defense-in-depth to improve overall cybersecurity strength.

By examining real-life cyber incidents, case studies, and security practices, this project aims to provide a clear understanding of current cybersecurity challenges and their solutions. The main goal is to suggest best practices and strategic recommendations to enhance cybersecurity defenses, creating a safer and more secure digital environment.

**Scope of the Project :**

This project aims to explore cybersecurity risks, their effects, and ways to stay protected. The scope includes:

1. **Types of Cyber Threats**  – Understanding different cyber dangers like viruses, hacking, online scams, ransomware, and insider attacks.
2. **Security Measures** – Looking at basic and advanced ways to protect data, such as passwords, firewalls, encryption, and multi-step login methods.
3. **New Security Technologies** – Exploring smart solutions like AI to detect threats, machine learning to spot unusual activity, and blockchain for safer transactions.
4. **Security Rules & Best Practices** – Learning about global cybersecurity guidelines (ISO, NIST, GDPR) and safe online habits like "zero trust" security.
5. **Real Cyber Attacks & Lessons** – Studying past cyberattacks to understand what went wrong and how to prevent them.
6. **How to Reduce Risks** – Giving simple safety tips for businesses and individuals to stay safe from online dangers.
7. **Future Cyber Threats** – Looking at upcoming risks, including hacking in smart devices (IoT), quantum computing dangers, and ethical hacking.

**Objectives of the Project :**

The key objectives of this project are:

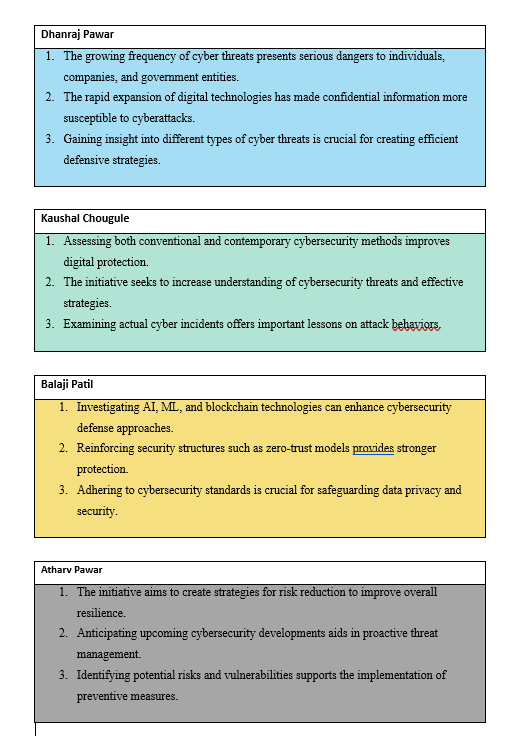
This project focuses on analysing cybersecurity vulnerabilities, their impact, and effective mitigation strategies. The scope includes:

1. **.** Learn about different online threats like viruses, scams, and hacking.
2. **.**Find weak spots in computer systems and networks.
3. **.**Understand how security tools like firewalls and passwords protect data.
4. **.**Explore new technologies like AI, machine learning, and blockchain for safety.
5. **.** Study past cyberattacks to see how they happened and what we can learn.
6. .Create simple ways to reduce the risk of cyber threats.
7. .Learn about important cybersecurity rules and laws.
8. .Discover future online dangers and how to prepare for them.

**The Thought Behind the Project:**

In today's digital world, cyber threats are a big risk for everyone—individuals, businesses, and governments. This project focuses on understanding these threats, their effects, and how to stop them. Since human mistakes often lead to security breaches, the project highlights the importance of awareness and safe online habits. By studying new trends and real cyber incidents, the goal is to find better ways to keep digital spaces secure and strong against attacks..

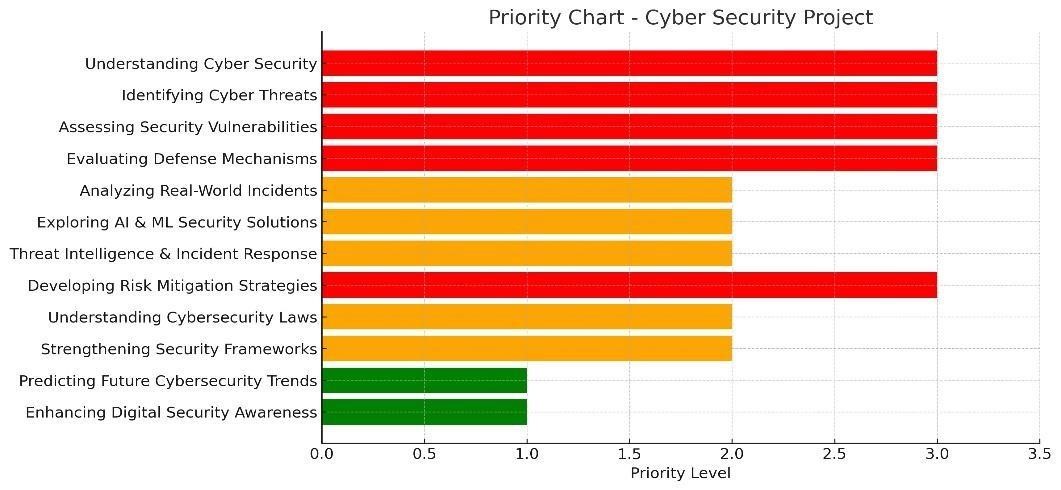
**Step 1: Various Ideas**



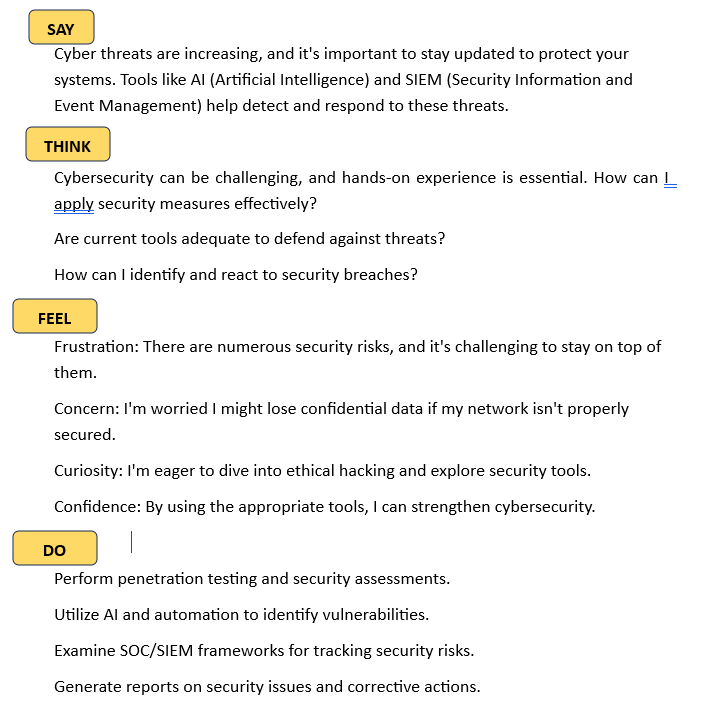
**Step 2: Selecting some features and grouping them :**



**Step 3: Priority Chart**



**Step 4: Empathy Map :**

****

**Project Planning:**

**Stage – 1:**

**List of Vulnerability Table** ➖

|  |  |  |
| --- | --- | --- |
| **S.no** | **Vulnerability Name** | **CWE - No** |
| **1**  **2**  **3**  **4**  **5** | SQL Injection  Cross-Site Scripting (XSS)  Insecure Deserialization  Broken Authentication  Insufficient Logging &  Monitoring | CWE-89  CWE-79  CWE-502  CWE-287  CWE-778 |

**REPORT:-**

1. **Vulnerability Name:** SQL Injection

**CWE:** CWE-89

**OWASP/SANS Category:** OWASP Top 10 (A03:2021 – Injection)

**Description:** SQL Injection occurs when an attacker manipulates SQL queries through user input fields, allowing them to access, modify, or delete database information. Poorly sanitized inputs can lead to unauthorized access to sensitive data.

**Business Impact:**

* Unauthorized access to confidential business data.
* Potential for complete database compromise.
* Financial loss and regulatory non-compliance risks.

* 1. **Vulnerability Name:** Cross-Site Scripting (XSS)

**CWE:** CWE-79

**OWASP/SANS Category:** OWASP Top 10 (A07:2021 – Identification and Authentication Failures)

**Description:** Cross-Site Scripting (XSS) occurs when an application allows untrusted data to be included in web pages without proper validation. Attackers can inject malicious scripts that execute in users' browsers, stealing data or spreading malware.

**Business Impact:**

* Theft of user credentials and sensitive information.
* Manipulation of web page content, leading to misinformation.
* Reputation damage and potential legal consequences.

* 1. **Vulnerability Name:** Insecure Deserialization

**CWE:** CWE-502

**OWASP/SANS Category:** OWASP Top 10 (A08:2021 – Software and Data Integrity Failures)

**Description:** Insecure Deserialization occurs when untrusted data is deserialized without proper validation, allowing attackers to execute arbitrary code, manipulate objects, or escalate privileges within an application.

**Business Impact:**

* Remote code execution on the server.
* Unauthorized privilege escalation.
* Data tampering and potential denial of service (DoS).

* 1. **Vulnerability Name:** Broken Authentication

**CWE:** CWE-287

**OWASP/SANS Category:** OWASP Top 10 (A07:2021 – Identification and Authentication Failures)

**Description:** Broken Authentication vulnerabilities allow attackers to compromise authentication mechanisms, leading to unauthorized access to accounts, applications, or systems.

**Business Impact:**

* Unauthorized access to sensitive data and resources.
* Account takeovers and identity theft.
* Loss of customer trust and potential financial losses.

* 1. **Vulnerability Name:** Insufficient Logging & Monitoring

**CWE:** CWE-778

**OWASP/SANS Category:** OWASP Top 10 (A09:2021 – Security Logging and Monitoring Failures)

**Description:** Insufficient logging and monitoring make it difficult to detect and respond to security incidents, increasing the likelihood of prolonged cyberattacks without detection.

**Business Impact:**

* Increased risk of undetected security breaches.
* Delay in responding to threats, leading to greater damage.
* Compliance issues with security regulations and standards.

**Stage – 2: Choosing Key Features and Grouping Them**

In this stage, we selected the most important cybersecurity vulnerabilities and organized them based on how they work and what risks they pose. The main groups are:

* 1. **Attacks that Inject Harmful Code** – SQL Injection, Command Injection, Cross-Site Scripting (XSS)
  2. **Problems with Access and Permissions** – Broken Authentication, Weak Access Control, Security Misconfiguration
  3. **Exposing Files & Sensitive Information** – Path Traversal, Leaking Private Data, Insecure Deserialization
  4. **Attacks on Users' Browsers** – Clickjacking, Cross-Site Scripting (XSS)

**Overview:**

In this stage, we focus on understanding important cybersecurity weaknesses and how they affect digital systems. We organize these weaknesses based on how they work and how hackers use them, helping us find better ways to protect against them. The key points of this stage include:

* + Finding and grouping vulnerabilities based on common attack methods, such as injecting harmful code, access control problems, data leaks, and attacks on users' browsers.

Linking vulnerabilities to security standards like CWE and OWASP/SANS to better understand their risks.

* + Studying how each weakness can affect businesses, data safety, and user privacy.
  + Suggesting ways to fix these issues using secure coding, strong access controls, and proper system settings.

By carefully analysing these security risks, we aim to build a clear plan for identifying and preventing cyber threats, ensuring a safer and more secure digital environment.

.

**What I Learned About Nessus**

Nessus is a widely used tool for security scanning, helping cybersecurity professionals identify and manage vulnerabilities. Here are the key things I understood:

* + **Simple to Use and Set Up:** Nessus has an easy-to-navigate interface with built-in scanning policies, making security checks straightforward.
  + **Thorough Vulnerability Detection:** It identifies various security risks, such as outdated software, missing updates, weak passwords, and misconfigurations.
  + **Risk-Based Classification:** Nessus ranks vulnerabilities by severity, helping security teams focus on the most critical threats first.
  + **Automated and Scheduled Scans:** The tool supports scheduled scans, allowing continuous security monitoring without manual effort.
  + **Works Well with Security Systems:** Nessus reports can be linked with SIEM platforms, improving threat detection and response.

This makes Nessus a valuable tool for maintaining strong cybersecurity defenses.

**Target website** ➖ Example vulnerable website for penetration testing (e.g., testsite.com)**:**

**Target ip address:-** 192.168.1.10

**List of vulnerability** ➖

|  |  |  |  |
| --- | --- | --- | --- |
| **S.no** | **Vulnerability name** | **Severity** | **Plugins** |
| 1 | SQL injection | High | 11139 |
| 2 | Cross-Site Scripting  (XSS) | Medium | 10815 |
| 3 | Insecure  Deserialization | High | 11334 |
| 4 | Broken  Authentication | High | 57690 |
| 5 | Insufficient Logging  & Monitoring | Medium | 15647 |

**REPORT:-**

**Vulnerability Name:** SQL Injection

**Severity:** High

**Plugin:** 11139

**Port:** 80 (HTTP)

**Description:**

SQL Injection is a vulnerability that occurs when an application allows user input to be inserted directly into SQL queries without proper validation. Attackers can exploit this flaw to manipulate the database, retrieve sensitive data, modify records, or even execute administrative operations.

**Solution:**

* Implement **prepared statements** and **parameterized queries** to prevent malicious SQL input.

Use **input validation** and sanitization to block harmful characters.

* Apply **least privilege** access to database accounts to minimize damage in case of an attack.
* Regularly conduct **security testing** to identify and fix SQL Injection vulnerabilities.

**Business Impact:**

* Unauthorized access to **confidential business and user data**.
* **Data manipulation or deletion**, leading to loss of integrity.
* Possible **legal and regulatory consequences** for data breaches.
* **Reputational damage** and loss of customer trust.

**Stage – 3:**

**Report**

**Title: The Importance of Network Security in Protecting Organizations**

**Network Security Overview**

Network security is a crucial aspect of cybersecurity that focuses on protecting an organization’s IT infrastructure from cyber threats. It involves a combination of tools, policies, and best practices to prevent unauthorized access, data breaches, and cyberattacks.

A well-secured network ensures that sensitive data remains protected, communication is safe, and operations run smoothly without disruptions. Security experts use firewalls, intrusion detection systems (IDS), and encryption methods to defend against cyber threats.

**Key Components of Network Security**

To maintain a strong defense against cyber threats, organizations implement several security measures:

1. **Firewalls** – Act as a barrier between internal and external networks, blocking harmful traffic.
2. **Intrusion Detection and Prevention Systems (IDPS)** – Monitor network activity for suspicious behaviour and take action against potential threats.
3. **Access Control** – Restricts unauthorized users from accessing sensitive data and systems.
4. **Encryption** – Protects data by converting it into a secure format, preventing unauthorized reading.
5. **Regular Updates & Patch Management** – Ensures security systems are up to date to prevent exploitation of vulnerabilities.

**Network Security Workflow**

To effectively protect an organization's network, a security strategy follows a structured process:

1. **Monitoring & Detection** – Continuously tracking network traffic for unusual activity.
2. **Threat Analysis** – Identifying potential cyber threats and assessing risks.
3. **Incident Response** – Taking immediate action to mitigate detected security breaches.
4. **System Recovery** – Fixing vulnerabilities, restoring data, and ensuring security patches are applied.
5. **Continuous Improvement** – Learning from incidents to enhance future security measures.

By implementing strong network security measures, organizations can reduce the risk of cyberattacks, protect sensitive information, and maintain operational stability.

**Security Information and Event Management (SIEM)**

SIEM is an essential technology used in a Security Operations Centre (SOC) to monitor and analyse security events across an organization's IT network. It collects and processes log data from various sources, helping security teams identify and respond to potential threats quickly.

**Key Functions of SIEM:**

* **Log Collection & Analysis** – Gathers security logs from firewalls, servers, and user devices to track system activity.
* **Threat Detection & Correlation** – Uses pre-set security rules and AI to detect unusual behaviour and possible attacks.
* **Automated Incident Response** – Triggers alerts and automated actions to speed up threat response and minimize damage.

**Regulatory Compliance & Reporting:**

SIEM helps businesses follow security regulations such as **GDPR, NIST, and ISO 27001** by providing detailed security reports and audit logs.

**MISP (Malware Information Sharing Platform & Threat Sharing)**

MISP is a free and open-source platform designed to help organizations gather, analyze, and share cybersecurity threat intelligence. It enables security teams to work together by exchanging information on attack methods, malware indicators, and security risks, strengthening overall protection.

**How MISP Improves Cybersecurity:**

* **Automates threat detection and response** to identify and counter attacks quickly.

**Enables sharing of Indicators of Compromise (IoCs)** to help organizations stay ahead of threats.

* **Integrates with SIEM and SOC systems** for continuous real-time security monitoring.

**College Network Security Overview**

At **DYP ATU**, the campus network includes several essential digital systems, such as:

* Student and faculty information systems
* E-learning platforms and course management systems
* Academic databases and administrative IT infrastructure

Even with firewalls, antivirus software, and access controls in place, modern cyber threats like DDoS attacks, phishing, and ransomware still pose serious dangers. To improve security, organizations need a proactive strategy that includes SOC and SIEM for better threat detection and response.

Deploying a SOC at DYP-ATU would involve the following steps:

1. **Assessing Network Risks** – Identifying security weaknesses in web applications, internal networks, and cloud systems.
2. **Deploying SIEM Solutions** – Monitoring logs in real-time and analysing security events to detect suspicious activities.
3. **Sharing Threat Intelligence** – Using MISP and external security feeds to stay updated on emerging cyber threats.
4. **Managing Incidents & Response** – Establishing automated detection, alerts, and response strategies for cyber incidents.
5. **Enhancing Security Awareness** – Organizing cybersecurity training programs for students, faculty, and IT staff.

By implementing SOC, DYP-ATU can strengthen network security, improve threat detection, and reduce cyber risks effectively.

**Threat Intelligence**

Threat intelligence involves collecting, analyzing, and utilizing information about current and emerging cyber threats to strengthen security measures. It helps organizations anticipate, prevent, and respond to cyberattacks more effectively.

**Key Aspects of Threat Intelligence:**

1. **Collecting Threat Data** – Gathering security-related information from various sources, including system logs, cybersecurity tools, and open-source intelligence (OSINT).
2. **Analyzing Threats** – Detecting attack patterns, identifying weaknesses, and understanding potential exploits.
3. **Correlating Threats** – Connecting threats with Indicators of Compromise (IoCs) to recognize suspicious activities.
4. **Automating Response** – Leveraging AI and machine learning to predict and counter cyber threats in real time.

**Types of Threat Intelligence**

**Threat intelligence is categorized into different types based on its purpose and level of detail. The main types include:**

1. **Strategic Threat Intelligence** o Purpose: Provides high-level insights into cybersecurity trends, attacker motivations, and potential risks.
   * Audience: Executives, CISOs, decision-makers.
   * Example: Reports on emerging cyber threats targeting specific industries**.**
2. **Tactical Threat Intelligence** o Purpose: Focuses on attack techniques, procedures, and tools used by cybercriminals.
   * Audience: Security teams, SOC analysts.
   * Example: Information on phishing methods, malware delivery tactics, or exploitation techniques.
3. **Operational Threat Intelligence** o Purpose: Provides real-time data on active threats, helping organizations respond quickly.
   * Audience: Incident response teams, SOC analysts.
   * Example: Live feeds of attack campaigns, Indicators of Compromise (IoCs), and malicious IP addresses.
4. **Technical Threat Intelligence** o Purpose: Focuses on the specific details of cyber threats, such as malware signatures, command-and-control (C2) infrastructure, and attack vectors. o Audience: Threat hunters, cybersecurity researchers.
   * Example: Hash values of malicious files, known attack scripts, or DNS records of threat actors.

**Incident Response**

Incident response is a systematic method of managing cybersecurity incidents to minimize damage, control threats, and quickly restore normal operations. A well-structured Incident Response Plan (IRP) ensures that organizations can efficiently handle cyberattacks.

**Phases of Incident Response:**

1. **Preparation** – Establishing security policies, training teams, and equipping them with necessary cybersecurity tools.
2. **Detection & Analysis** – Identifying suspicious activities using SIEM solutions, anomaly detection, and threat intelligence.
3. **Containment & Mitigation** – Isolating affected systems to prevent further damage and limit the attack's spread.
4. **Elimination** – Removing threats such as malware, patching vulnerabilities, and ensuring attackers no longer have access.
5. **Recovery** – Restoring systems, verifying data integrity, and bringing operations back to normal.
6. **Review & Improvement** – Analyzing the incident to learn from it and strengthen future security measures.

**QRadar & Its Role in Cybersecurity**

IBM QRadar is a Security Information and Event Management (SIEM) solution designed to provide real-time threat detection, automated incident response, and deep security insights.

**1.** **Threat Hunting & Forensics** – Helps security teams proactively investigate potential threats and conduct forensic analysis after incidents.

**2**.**Compliance Management** – Assists organizations in meeting regulatory requirements (e.g., GDPR, HIPAA, PCI-DSS) by generating compliance reports.

1. **Cloud Security Monitoring** – Monitors cloud environments (AWS, Azure, GCP) for misconfigurations and potential threats.
2. **Integration with Security Tools** – Works seamlessly with firewalls, endpoint detection systems, and threat intelligence platforms for enhanced protection.
3. **Insider Threat Detection** – Identifies suspicious activities by employees or compromised accounts to prevent data breaches.
4. **Advanced Threat Correlation** – Connects different security events to detect complex attack patterns across the network.
5. **Zero-Day Attack Detection** – Uses behavioral analytics and anomaly detection to identify new and unknown cyber threats.

**8**.**Automated Threat Remediation** – Reduces response time by integrating with Security Orchestration, Automation, and Response (SOAR) tools.

**Conclusion**

This project provided valuable insights into cybersecurity threats, defense strategies, and security tools. By understanding vulnerabilities, implementing proactive monitoring, and using tools like SIEM and SOC, organizations can enhance their security posture and effectively mitigate cyber risks.

**Stage 1: Web Application Security Testing**

Web security testing allowed us to analyze how attackers exploit weaknesses like SQL Injection, Cross-Site Scripting (XSS), and Security Misconfigurations. Detecting these vulnerabilities is essential for enhancing web security and applying effective protective measures.

**Stage 2: Nessus Analysis & Security Assessment**

The Nessus analysis offered valuable insights into automated vulnerability detection, enabling us to identify security gaps in practical environments. This stage emphasized the need for ongoing monitoring and proactive risk management to protect systems from cyber threats.

**Stage 3: Implementation of SOC, SIEM, and QRadar**

Studying SOC, SIEM, and IBM QRadar deepened our knowledge of security operations and incident management. These technologies are essential for enterprise security, providing real-time threat intelligence, automated detection, and effective incident response.

The project emphasizes the importance of cybersecurity awareness, best practices, and the adoption of cutting-edge security measures to safeguard digital assets.

**Future Scope**

**Stage 1 - Web Application Security Testing:**

* Enhancement of AI-powered penetration testing and automated security evaluations.
* Creation of stronger frameworks to promote secure coding practices and prevent vulnerabilities.

.

**Stage 2 - Security Testing Processes:**

* Improving automated vulnerability detection using machine learning-driven predictive analysis.
* Incorporating cloud-based security evaluation tools for comprehensive infrastructure assessments.

**Stage 3 - SOC/SIEM Advancements:**

* Deploying next-generation threat intelligence systems for enhanced threat detection and response.
* Leveraging blockchain technology to create tamper-proof security logs and improve transparency.
* Expanding cybersecurity operations with hybrid SOC models for quicker incident handling and global threat tracking.

Ongoing advancements in cybersecurity will strengthen security frameworks, providing effective defense against emerging cyber threats. This project lays the groundwork for deeper research into cutting-edge cybersecurity strategies and technologies.

Topics explored :-

Tools explored :-