AI-Enhanced Security Analytics Dashboard That Provides Real-Time Insights into Security Events, Trends, And Risks.

Team Cypherers

Team ID: PNT2022TMID593452

Team Members:

Sarika V

Shaik Kaleshavali

Aadish Chougala

Pranavasri Rudrakshala Matam

Problem Statement:

In the current digital landscape, the absence of a centralized, real-time security analytics dashboard that incorporates AI-driven insights impedes organizations ability to swiftly detect, analyse and respond to emerging security threats. This gap leads to delayed threat identification, inefficient resource allocation, and increased vulnerability to potential breaches. Therefore, there is a pressing need for an AI-enhanced security analytics dashboard that can consolidate diverse security data sources, deliver real-time insights, and empower proactive security measures. This project aims to develop a user-friendly and scalable solution that integrates cutting-edge AI algorithms for predictive analysis, anomaly detection, and trend forecasting, facilitating robust security management and safeguarding critical data assets

Abstract:

The online and cyber world has reached a stage where every single person started using services offered online, which proves us that a wide range of people from student to office workers and government officials are also using these services. So, there is wide range of data that has to be protected and privacy has to be maintained. The reported cybercrime in 2021 is 1,402,809 and between Q1 and Q2 2022, it increased by 15.3%. 78% of Indian organizations experienced a ransomware attack in 2021. Thus, there is a desperate need for a product that prevents the users from any attacks online. It is also important that the product is easy to setup, operate and also protect the users from any attacks or vulnerabilities but does not compromise on the security. So our team of engineers focused on creating an AI enhanced security analytics dashboard that provides real-time insights into security events, trends, and risks, to ensure the users safety is ensured online. It has a AI based monitoring system which checks for any action that seems suspicious in real time. It also contains set of major vulnerabilities observed worldwide to prevent them from being exploited. The product also identifies the risks in any website, online platform or any webpage. In addition to identifying it, the user is notified about the risk. The project focuses on developing AI trained with datasets that can easily identify the vulnerabilities, if found as well suspicious or unusual activities. This differs from traditional approaches to security. Machine Learning algorithms are trained using large amount of data to identify patterns and thus responding to threats in real time. This Ai based system can continuously learn and adapt, hence tackling with the new vulnerabilities and attacks. This product has malware detection, on analysing the behaviour of the malwares, it can identify new and unknown malware unlike the traditional antivirus software. It uses dynamic analysis, analysing behaviour of file when executed to find patterns and anomalies. The product also detects phishing using machine learning algorithms to analyse content and structure of emails to identify phishing attacks. This is established by making the algorithm learn from a large amount of data to detect pattern and anomalies that indicate phishing attacks. The Ai based project scans files for malware and prevents any suspicious file from being executed. It also blocks unauthorized access attempts and prevent attackers from gaining access to sensitive data. Ai algorithms can any time learn from new data and adapt it to evolving threats. We have also focused on patch management, where the AI can automatically scan systems and network for vulnerabilities and prioritize them and also

recommend patches or security updates for software and tools. Whenever a threat is detected, the system triggers a real time alert and notifications for the user to decide on the very quick options to resolve them. The AI based systems reduces the time between threat detection and response thus reducing the impact of any attack. Focusing on the revolutionary changes AI has made in various sectors, it also has a great insight for cyber security. Automating the security strengthens the security by improving accuracy and reducing labour and cost. Its potential is also utilized in the field of cyber security.

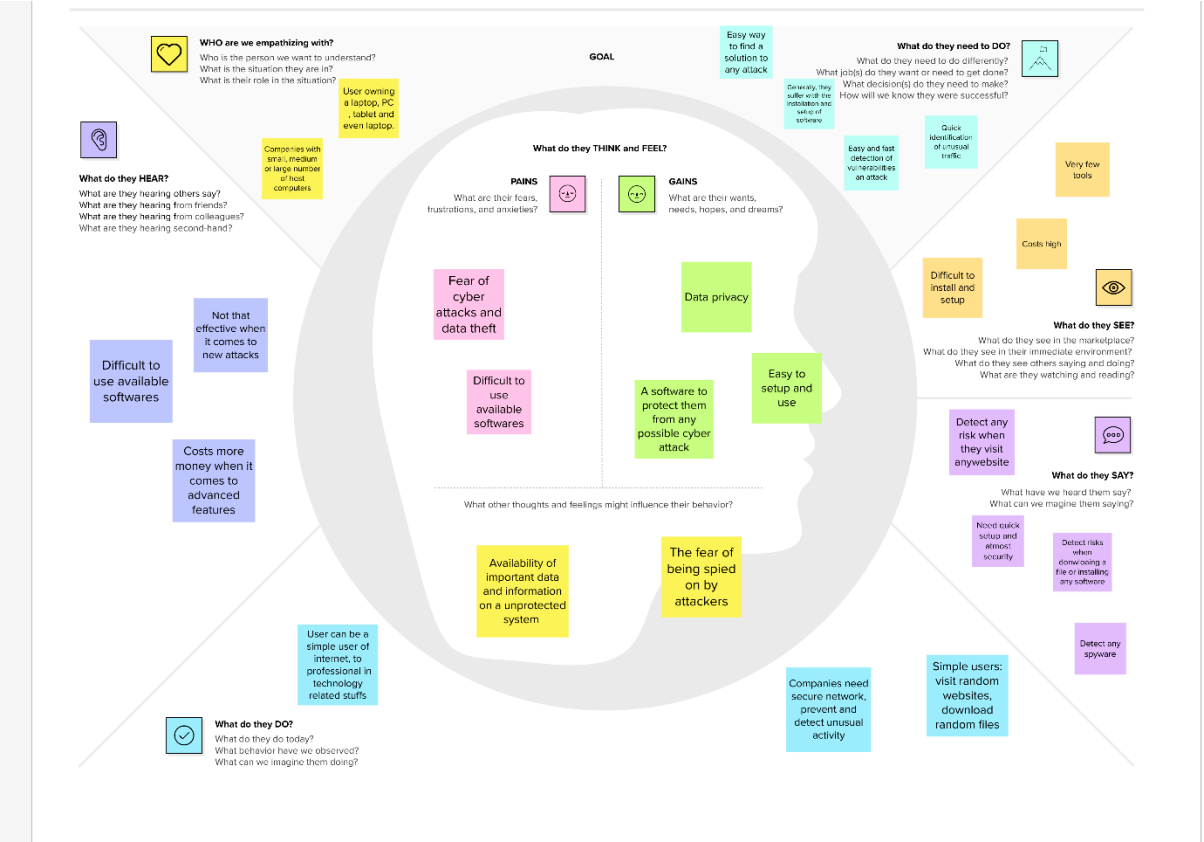

Fig. Users perspective about the dashboard

Sarika V

Hybrid Threat Intelligence Integration: Develop a dashboard that seamlessly integrates both internal and external threat intelligence data sources, combining AI-driven algorithms with human expertise. This approach will enable the system to provide real-time threat insights, correlating external threat data with internal security events for comprehensive risk assessment and proactive threat mitigation.

Aadish

Customizable Visualization and Reporting: Create a customizable dashboard interface that allows security analysts and stakeholders to configure visualizations and reports based on their specific requirements and preferences. Incorporate interactive data visualization techniques to represent complex security data in an easily interpretable format, facilitating quick decision-making and efficient communication of security insights across the organization.

Kalesha

Predictive Analytics and Automated Response: Implement advanced machine learning models within the dashboard to predict potential security incidents based on historical data and ongoing trends. Incorporate automated response mechanisms that can trigger predefined security protocols in response to identified threats, minimizing manual intervention and reducing response time, thereby enhancing the overall security posture.

Pranavasri

Scalable Cloud-Based Architecture: Design the security analytics dashboard using a scalable cloud-based architecture, allowing seamless integration with existing IT infrastructures and the flexibility to handle varying workloads and data volumes. Implement robust security measures within the cloud infrastructure to ensure the confidentiality and integrity of sensitive data while enabling easy access and analysis of security information from multiple locations and devices.

Fig. Different Ideas for the Problem statement by team members

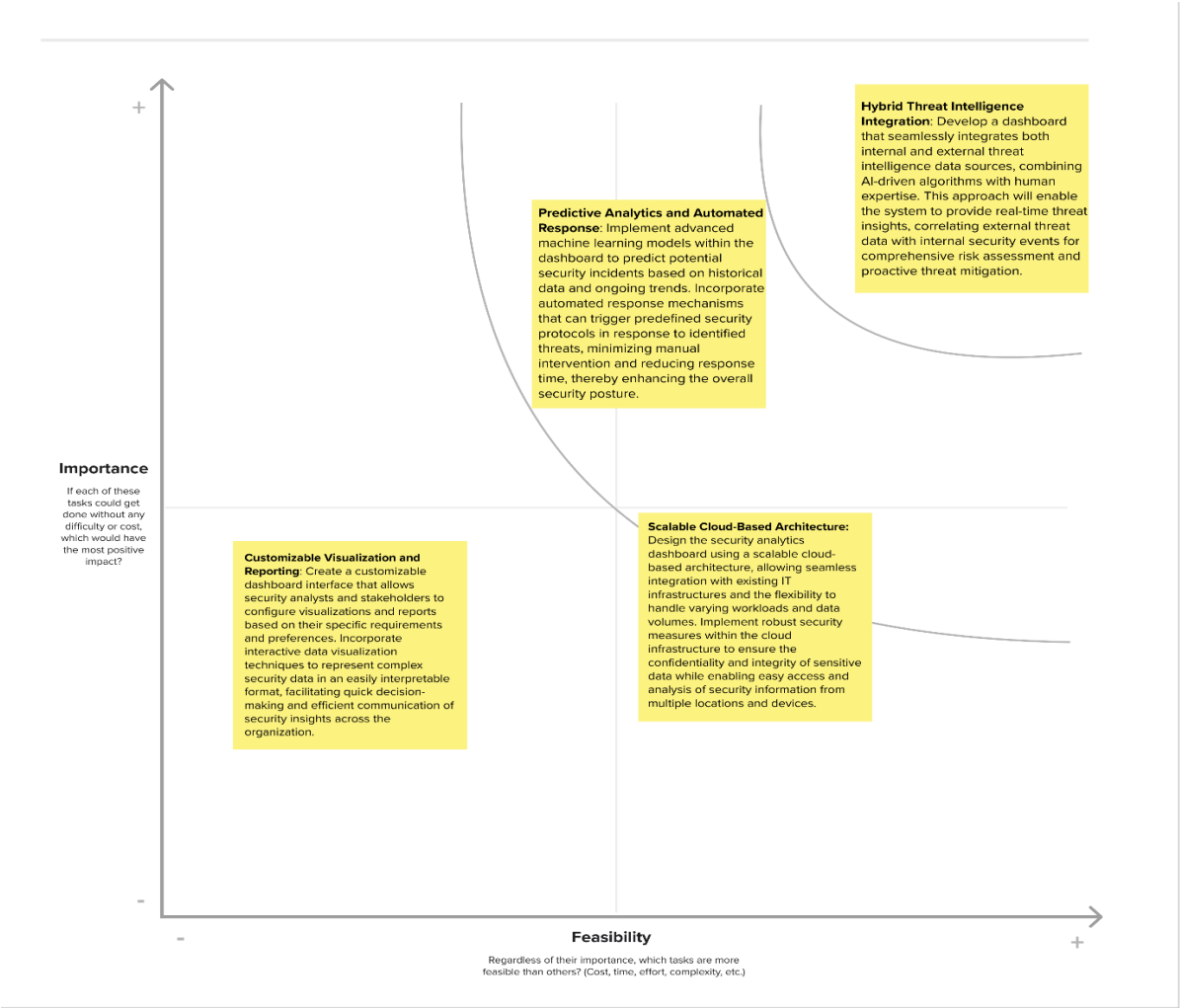

Fig. Prioritizing the ideas given by team members

Table1. Proposed Solution

S. No	Parameter	Description
1.	Problem Statement (Problem to be solved)	In the current digital landscape, the absence of a centralized, real-time security analytics dashboard that incorporates AI-driven insights impedes organizations ability to swiftly detect, analyze and respond to emerging security threats. This gap leads to delayed threat identification, inefficient resource allocation, and increased vulnerability to potential breaches. Therefore, there is a pressing need for an AI-enhanced security analytics dashboard that can consolidate diverse security data sources, deliver real-time insights, and empower proactive security measures. This project aims to develop a user-friendly and scalable solution that integrates cutting-edge AI algorithms for predictive analysis, anomaly detection, and trend forecasting ,facilitating robust security management and safeguarding critical data assets

2.	Idea / Solution description	The proposed solution is a scalable security analytics dashboard that leverages leading-edge AI techniques such as: • **Statistical analysis and machine learning** for baseline modeling and anomaly detection from network, endpoint, and user activity data • **Natural language processing** to parse through unstructured threat intelligence and log data • **Scene graph analytics** to identify relationships between threats, users, and infrastructure • **Graph neural networks** to detect suspicious behavioral patterns and trends The dashboard will provide security analysts with real-time visibility through customizable alerting, dynamic visualizations, and role-based access controls. Users can prioritize and investigate security events, perform root cause analysis, and initiate automated response workflows. Built-in reporting capabilities will facilitate risk monitoring and communication across stakeholders. The solution will ingest data from existing security tools via API integrations and normalize/enrich data for AI analytics. The platform will be scalable to accommodate large enterprises and offer robust data protection compliant with industry standards. An intuitive, responsive UI will provide users a simple yet powerful security analytics experience.
3.	Novelty / Uniqueness	• It takes an AI-first approach to security analytics, unlike most solutions that apply AI as an afterthought. Advanced AI algorithms are deeply integrated for automated threat detection, analysis, and response. • The dashboard uniquely combines statistical, NLP, graph-based, and computer vision AI to extract insights from diverse data types in a holistic manner. This overcomes the limitations of point analytics tools. • A key innovation is the use of scene graph analytics to model relationships between security entities. This enables complex threat hunting and risk monitoring across the attack surface.
4.	Social Impact / Customer Satisfaction	• Improved cybersecurity and reduced data breaches through proactive threat detection can build public trust and reputation for organizations using the dashboard. • Faster incident response enabled by the dashboard translates to minimizing customer data and privacy violations in the event of attacks. • By detecting insider threats and cyber risks, the dashboard helps companies avoid IP theft and maintains shareholder value. • Scalable architecture and cloud deployment ensure affordable access to advanced analytics, especially for smaller businesses or non-profits.

5.	Business Model (Revenue Model)	The dashboard will be offered as a Software-as-a-Service (SaaS) model to provide easy access without extensive setup and maintenance overhead for customers. **Target Customers** The platform is designed for organizations of all sizes across industries looking to augment their security operations through AI automation and actionable insights from data. **Revenue Streams** • Subscription plans for dashboard access based on number of users, data sources, and platform features • Professional services for onboarding, training, and ongoing enhancement • Ongoing customer support and maintenance contracts **Key Metrics** • Number of customers across tiers and segments • Data sources and events processed per customer • Renewal and retention rates • Customer lifetime value • Customer acquisition cost • Cost per incident detected/prevented
6.	Scalability of the Solution	Here is a concise overview of how the proposed security analytics dashboard solution scales: • Distributed microservices architecture spreads workload across servers as data volumes grow. Just add more servers. • Cloud deployment provides unlimited computing power for storage, processing, and analysis as needed. • Modular components can be independently scaled - ex: scale AI modelling servers separately from app servers. • Stateless design prevents bottlenecks. No single point of failure.

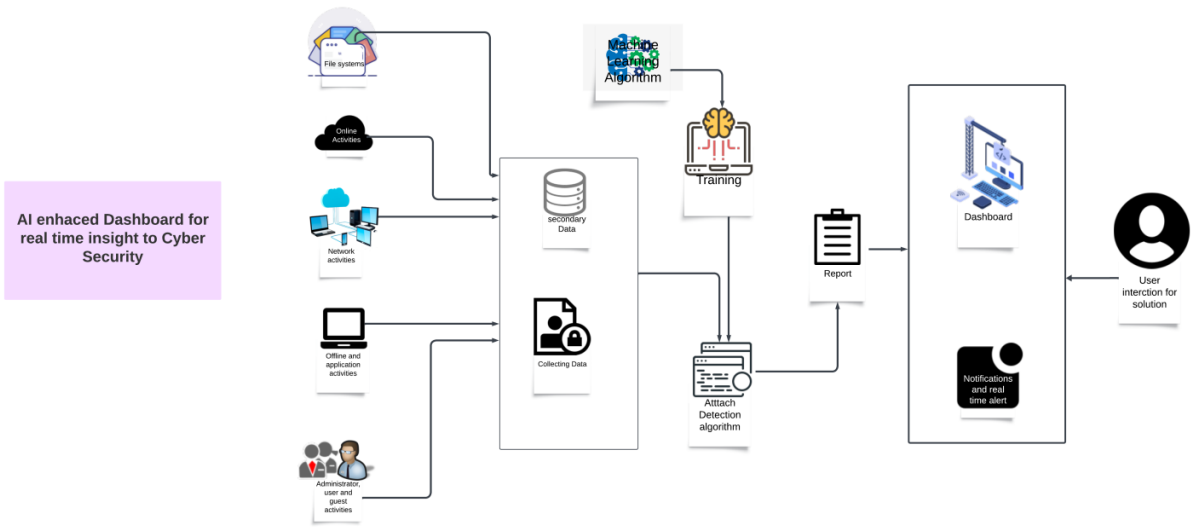

Fig. Solution Architecture

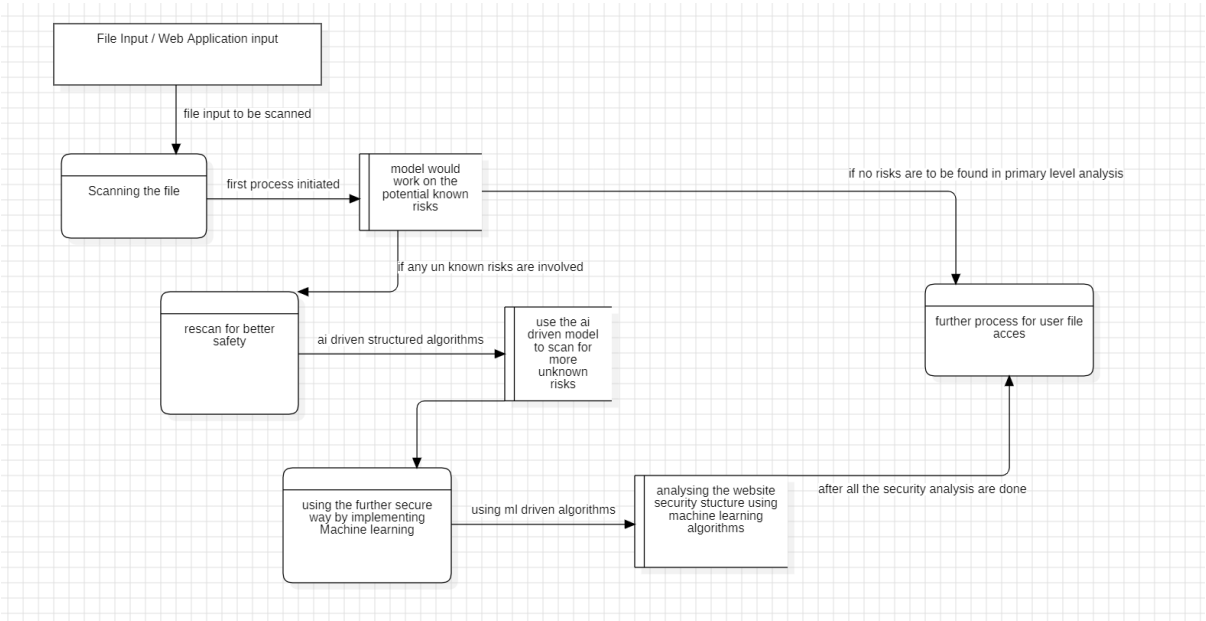

Fig. Dataflow Diagram

User Type	Functional Requirement (Epic)	User Story Number	User Story / Task	Acceptance criteria	Priority	Release
Customer (Mobile user)	Registration	USN-1	As a user, I can register for the application by entering my email, password, and confirmingmy password.	I can access my account / dashboard	High	Sprint-1
Customer (mobile, laptop and pc user)	Confirmation mails	USN-2	As a user, I will receive confirmation email once I have registered for the application	I can receive confirmation email & click confirm	High	Sprint-1
Customer (mobile and laptop user)	Register via Facebook	USN-3	As a user, I can register for the application through Facebook	I can register & access the dashboard with Facebook Login	Low	Sprint-2
Customer (all users)	Register via Gmail	USN-4	As a user, I can register for the application through Gmail	I can register & access the dashboard with GMail Login	Medium	Sprint-1
Customer (all users)	Login	USN-5	As a user, I can log into the application by entering email & password	I can register & access the dashboard with a new Login created	High	Sprint-1
Customer (all users)	Dashboard	USN-6	As a user, I can view my dashboard with information about vulnerabilities in my system	I can view my system vulnerabilities	High	Sprint-1
Customer (Web user)	Risks Online	USN-7	As a user, I can view risks from the websites that I visit, if any	I can view the risk of visiting a page	High	Sprint-1
Customer Care Executive	Privileges	USN-8	As a customer care executive, I have access to the programmer the customer has opted fro	I can view the privileges customers are allowed to enjoy	Medium	Spirint-2
Administrator	Logs	USN-9	As a administrator, I can have access to the logs of the users system.	I can view the logs of user	Medium	Sprint-2
Customer Care Executive	Manuals	USN-10	As a customer care executive, I have a manual to be followed when the customer faces with some issue	I have a procedure to deal with customers	Medium	Sprint-2
Customer (all)	Privacy	USN-11	As a user, only I can view my dashboard and details	I have privacy to my activities on my system	High	Sprint-1
Customer (all)	Notification and alert	USN-12	As a user, I must be notified every time a vulnerability is found in my system or every time my system is attacked.	I am notified to take necessary actions for my system security	High	Sprint-1

Table 2- User stories

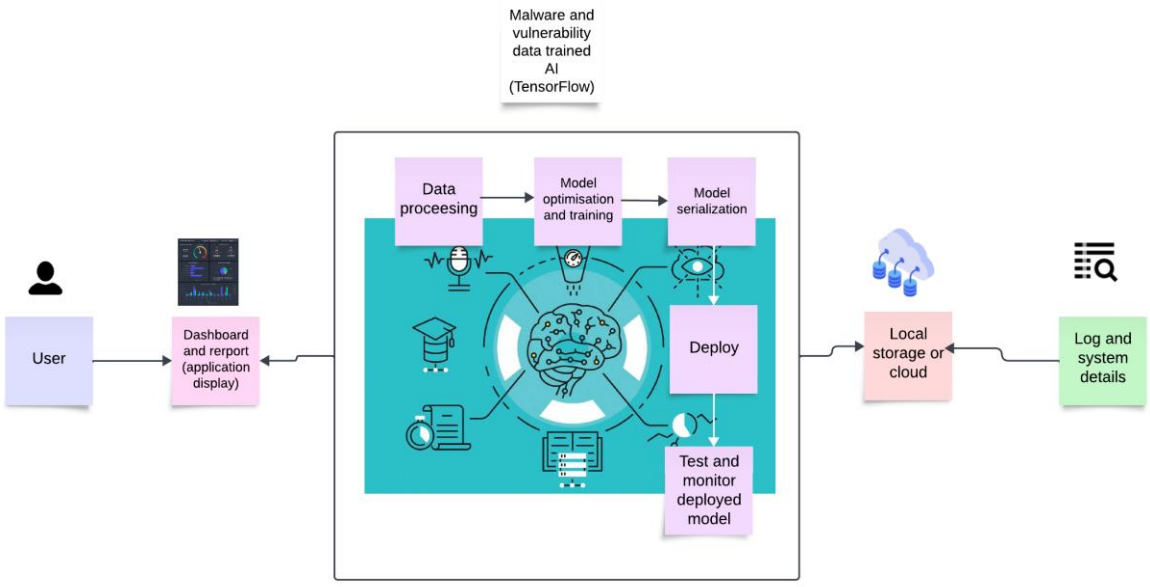

Fig. Technology stack

Table-3: Components & Technologies

S.No	Component	Description	Technology
1.	User Interface	Graphical interface for user interaction	HTML, CSS, JavaScript / Angular Js / React Js
2.	AI-Based Monitoring System	Real-time monitoring for suspicious actions	AI Algorithms, Real-time Data Analysis
3.	Vulnerability Detection	Identify and prevent major vulnerabilities	Machine Learning, Global Vulnerability Databases
4.	Risk Identification & Notification	Identify and notify users about risks	AI Algorithms, Risk Assessment Modules
5.	Dynamic Malware Analysis	Analyze malware behavior for detection	Dynamic Analysis Techniques, Machine Learning
6.	Phishing Detection	Analyze content and structure of emails	Machine Learning, Email Analysis Algorithms
7.	File-Level Malware Scanning	Scan files for malware and prevent execution	Malware Scanning Engines, Threat Intelligence
8.	Unauthorized Access Prevention	Block unauthorized access attempts	Access Control Systems, Intrusion Detection
9.	Patch Management	Automatically scan for vulnerabilities	Automated Patch Management Tools, Vulnerability Scanners
10.	Database	Data Type, Configurations etc.	MongoDB, MySQL
11.	External API-1	For data about existing vulnerabilities	Vulnerability API
12.	External API-2	For data about existing malwares	Malware API
13.	Machine Learning Model	Detect and analyze vulnerabilities and risks	Vulnerability and anomalies detection model
14.	Infrastructure (Server / Cloud)	Application Deployment on Local System / Cloud	Local, Cloud

Table-4: Application Characteristics

S.No	Characteristics	Description	Technology
1.	Open-Source Frameworks	Utilizing open-source frameworks for development	Technology of Opensource framework
2.	Security Implementations	Implementation of robust security measures	e.g. SHA-256, Encryptions, IAM Controls, OWASP etc.
3.	Scalable Architecture	Employing a scalable architecture for flexibility	3-tier, Micro-services
4.	Availability	Ensuring high availability through advanced techniques	Load balancers, Distributed servers
5.	Performance	Design considerations for optimal performance	Requests per second, Cache usage, CDN integration

Table-5: Project planning

Sprint	Functional Requirement (Epic)	User Story Number	User Story / Task	Story Points	Priority	Team Members
Sprint-1	Registration	USN-1	As a user, I can register for the application by entering my email, password, and confirming my password.	2	High	4
Sprint-1	Confirmation mails	USN-2	As a user, I will receive confirmation email once I have registered for the application	2	High	4
Sprint-2	Register via Facebook	USN-3	As a user, I can register for the application through Facebook	2	Low	4
Sprint-1	Register via Gmail	USN-4	As a user, I can register for the application through Gmail	2	Medium	4
Sprint-1	Login	USN-5	As a user, I can log into the application by entering email & password	2	High	4
Sprint-1	Dashboard	USN-6	As a user, I can view my dashboard with information about vulnerabilities in my system	4	High	4
Sprint-1	Risks Online	USN-7	As a user, I can view risks from the websites that I visit, if any	2	High	4
Sprint-2	Privileges	USN-8	As a customer care executive, I have access to the programmer the customer has opted from	5	Medium	4
Sprint-2	Logs	USN-9	As a administrator, I can have access to the logs of the users system.	8	Medium	4
Sprint-2	Manuals	USN-10	As a customer care executive, I have a manual to be followed when the customer faces with some issue	5	Medium	4
Sprint-1	Privacy	USN-11	As a user, only I can view my dashboard and details	4	High	4
Sprint-1	Notification and alert	USN-12	As a user, I must be notified every time a vulnerability is found in my system or every time my system is attacked.	2	High	4

Sprint	Total Story Points	Duration	Sprint Start Date	Sprint End Date (Planned)	Story Points Completed (as on Planned End Date)	Sprint Release Date (Actual)
Sprint-1	20	10 Days	11 Oct 2023	21 Oct 2023	20	21 Oct 2023
Sprint-2	20	10 Days	21 Oct 2023	31 Oct 2023	20	31 Oct 2023

Velocity:

Imagine we have a 10-day sprint duration, and the velocity of the team is 20 (points per sprint). Let's calculate the team's average velocity (AV) per iteration unit (story points per day)

Sprint duration = 10-days

Velocity of team =20 per sprint

Average Velocity = 20/10 = 2 story points per day

Stage 1:

Title of the Project: AI-Enhanced Security Analytics Dashboard That Provides Real-Time Insights into Security Events, Trends, And Risks

Overview:

The proposed solution is a scalable security analytics dashboard that leverages leading-edge AI techniques such as:

- Statistical analysis and machine learning for baseline modeling and anomaly detection from network, endpoint, and user activity data
- Natural language processing to parse through unstructured threat intelligence and log data
- Scene graph analytics to identify relationships between threats, users, and infrastructure
- Graph neural networks to detect suspicious behavioral patterns and trends

The dashboard will provide security analysts with real-time visibility through customizable alerting, dynamic visualizations, and role-based access controls. Users can prioritize and investigate security events, perform root cause analysis, and initiate automated response workflows.

Built-in reporting capabilities will facilitate risk monitoring and communication across stakeholders. The solution will ingest data from existing security tools via API integrations and normalize/enrich data for AI analytics.

The platform will be scalable to accommodate large enterprises and offer robust data protection compliant with industry standards. An intuitive,

responsive UI will provide users a simple yet powerful security analytics experience.

The dashboard will be offered as a Software-as-a-Service (SaaS) model to provide easy access without extensive setup and maintenance overhead for customers.

Target Customers.

The platform is designed for organizations of all sizes across industries looking to augment their security operations through AI automation and actionable insights from data.

Revenue Streams.

- Subscription plans for dashboard access based on number of users, data sources, and platform features
- Professional services for onboarding, training, and ongoing enhancement
- Ongoing customer support and maintenance contracts

Key Metrics.

- Number of customers across tiers and segments
- Data sources and events processed per customer
- Renewal and retention rates
- Customer lifetime value
- Customer acquisition cost
- Cost per incident detected/prevented

Team 10.2

List of Teammates:

S.no	Name	College	Contact
1	Sarika V	Vellore Institute of Technology	sarika.v2021@vitstudent.ac.in
2	Shaik Kalesha Vali	Vellore Institute of Technology	shaikkalesha.vali2021@vitstudent.ac.in
3	Aadish Chougala	Vellore Institute of Technology	aadishrakesh.chougala2021@vitstudent.ac.in
4	Pranavasri Rudrakshala Matam	Vellore Institute of Technology	rudrakshala.matam2021@vitstudent.ac.in

List of Vulnerabilities:

Test Website: https://testphp.vulnweb.com/

S. No	Vulnerability Name	CWE - No
1	SQL Injection	89
2	Cross-site Scripting (Self)	79,80,116
3	Cross-domain referral leakage	200
4	Directory Index	548
5	Email addresses disclosed	200
6	Web Parameter Tampering	472
7	Insecure Direct Object Reference	639
8	Server-Side Request Forgery	918
9	Brute force attack	307
10	Improper signup process	665

Team 10.2

Report:

1. SQL Injection

Vulnerability Name: SQL Injection

CWE - 89: Improper Neutralization of Special Elements used in an SQL Command

OWASP Category: A03:2021 - Injection

Description: SQL Injection is a type of security vulnerability that occurs when untrusted data is inserted into SQL queries without proper validation or sanitization. Attackers exploit this vulnerability by inserting malicious SQL statements into the input fields of an application, manipulating the database query to perform unauthorized actions or retrieve sensitive data. This can lead to the exposure of confidential information, unauthorized access to the database, data manipulation, and in some cases, the complete takeover of the application or the underlying server.

Business Impact:

1.Data Breaches: Broken Access Control can lead to unauthorized access to sensitive data, resulting in data breaches. This can damage the reputation of the business and result in legal consequences, especially if the data belongs to customers or partners.

2.Financial Loss: Unauthorized access can lead to financial losses, such as theft of intellectual property, loss of sensitive financial information, or fraudulent transactions.

Vulnerability Path: http://testphp.vulnweb.com/listproducts.php?cat=1

SQL map injection:

sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 —dbs

sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart columns

2. Cross-site Scripting

Vulnerability Name: Cross-site Scripting (Self)

CWE - 79,80,116,159

OWASP Category: A03:2021 – Injection

Description: Cross-Site Scripting (XSS) is a type of security vulnerability typically found in web applications. In the case of Cross-site Scripting (Self), the vulnerability allows an attacker to inject malicious scripts directly into the web application, which are then executed in the context of the user's browser. This means that the attacker can essentially hijack the user's session, manipulate web page content, or redirect the user to malicious sites.

The vulnerability arises due to a lack of proper validation and sanitization of user inputs on the web application's side. Attackers exploit this weakness by injecting scripts, usually in the form of HTML or JavaScript, into the application, which is then unknowingly executed by other users

Business Impacts:

1.Data Theft: Attackers can use XSS to steal sensitive user data such as login credentials, session tokens, or other personal information.

2.Website Defacement: Malicious scripts can modify the content of the web pages, leading to a negative impact on the company's reputation and brand image.

3.Phishing Attacks: XSS vulnerabilities can be exploited to redirect users to fake or malicious websites designed to steal sensitive information.

3. Cross-domain referral leakage

Vulnerability Name: Cross-domain referral leakage

CWE - 200: Information Exposure

OWASP Category: A01:2021 - Broken Access Control

Description: Cross-domain referral leakage typically transpires when a web application fails to adequately restrict the data it shares with external domains or websites. This can happen due to lax implementation of security protocols,

leading to the exposure of sensitive user data, such as authentication tokens, session IDs, or other critical information, to unauthorized third parties.

Business Impact:

The consequences of cross-domain referral leakage can be far-reaching and detrimental for both users and the organization managing the vulnerable application. The potential business impacts include, but are not limited to:

1.Data breaches: Exposure of sensitive data can pave the way for unauthorized access to user accounts, potentially leading to data breaches and violations of user privacy.

2.Reputational damage: Any data breach resulting from cross-domain referral leakage can severely tarnish the organization's reputation, eroding customer trust and potentially leading to reduced revenue and market share.

3.Legal consequences: Non-compliance with data protection regulations, as a result of the exposure of sensitive information, can trigger legal repercussions and financial penalties for the organization.

Issue detail

The page was loaded from a URL containing a query string:

●http://testphp.vulnweb.com/listproducts.php

The response contains the following links to other domains:

●http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab

●http://www.acunetix.com/

●https://www.acunetix.com/blog/articles/prevent-sql-injection-vulnerabilities-inphp- applications/

●https://www.acunetix.com/vulnerability-scanner/

●https://www.acunetix.com/vulnerability-scanner/php-security-scanner/

●http://www.eclectasy.com/Fractal-Explorer/index.htm

4. Directory Index

Vulnerability Name: Directory Index

CWE - 548: Exposure of Information Through Directory Listing

OWASP Category: A05:2021 – Security Misconfiguration

Description: Directory Indexing is a web server feature that allows the contents of a directory to be displayed when there is no index file (such as index.html or index.php) present in that directory. When directory indexing is enabled, it can potentially expose sensitive information about the directory structure and the files it contains to users or attackers who can access the directory. This vulnerability can be exploited by malicious actors to gather information about the file system structure, identify potential targets for further attacks, and potentially retrieve sensitive files that were not meant to be publicly accessible.

Business Impact:

The exposure of directory listings can lead to various business impacts and security risks, including:

1.Information Leakage: The exposed directory listings can inadvertently reveal the internal structure of the web application or website, which can include sensitive information such as file names, directory paths, and potentially confidential data.

2.Targeted Attacks: Attackers can use the information obtained from directory listings to identify potential vulnerabilities in the web application or to craft more sophisticated attacks, such as directory traversal attacks or brute force attacks on specific files or directories.

3.Data Breach: If sensitive files or data are exposed through directory listings, it can lead to unauthorized access and potential data breaches, resulting in the loss of sensitive information, intellectual property, or customer data.

5. Email addresses disclosed

Vulnerability Name: Email addresses disclosed

CWE - 200: Information exposure

OWASP Category: A01:2021 - Broken Access Control

Description: Broken Access Control refers to the failure of a web application to enforce restrictions on what authenticated users are allowed to do. This could mean that users can perform certain actions that they shouldn't have access to, such as viewing sensitive files, modifying other users' data, or changing access rights. It can occur due to various reasons, including incorrect configuration settings, improper session management, or lack of proper access control checks within the application.

Business Impact:

1.Data Breaches: Broken Access Control can lead to unauthorized access to sensitive data, resulting in data breaches. This can damage the reputation of the business and result in legal consequences, especially if the data belongs to customers or partners.

2.Financial Loss: Unauthorized access can lead to financial losses, such as theft of intellectual property, loss of sensitive financial information, or fraudulent transactions.

Vulnerability Path: https://testphp.vulnweb.com/

There are 4 instances of this issue:

- /
- /categories.php
- /guestbook.php
- /listproducts.php

6. Web Parameter Tampering

Vulnerability Name: Web Parameter Tampering using Man-in-the-middle attack

CWE – 472: External Control of Assumed-Immutable Web Parameter

OWASP Category: A01:2021 - Broken Access Control

Description: The Web Parameter Tampering attack is based on the manipulation of parameters exchanged between client and server in order to modify application data, such as user credentials and permissions, price and quantity of products, etc. Usually, this information is stored in cookies, hidden form fields, or URL Query Strings, and is used to increase application functionality and control.

This attack can be performed by a malicious user who wants to exploit the application for their own benefit, or an attacker who wishes to attack a third-person using a Man-in-the-middle attack. The attack success depends on integrity and logic validation mechanism errors, and its exploitation can result in other consequences including XSS, SQL Injection, file inclusion, and path disclosure attacks.

Business Impact:

It enables threat actors to modify data application like user credentials, user permissions and the number, quantity or price of products listed on website.

Financial Loss: Businesses can suffer substantial financial losses due to data tampering. For example, tampering with financial records can result in inaccurate reporting and decision-making, leading to costly errors.

7. IDOR

Vulnerability Name: Insecure Direct Object Reference (IDOR)

CWE – 639: Authorization Bypass Through User-Controlled Key

OWASP Category: A01:2021 - Broken Access Control

Description: Insecure Direct Object Reference (IDOR) is a vulnerability that arises when attackers can access or modify objects by manipulating identifiers used in a web application's URLs or parameters. It occurs due to missing access

control checks, which fail to verify whether a user should be allowed to access specific data.

Business Impact:

This can lead to disclosure of sensitive information. Sometimes the attack can be used to modify data like manipulating parameters in an HTTP POST request. IDOR can also be abused to impact the availability of resources as unauthorized person has access to database and files.

8. Server-Side Request Forgery

Vulnerability Name: Server-Side Request Forgery

CWE – 918: Server-Side Request Forgery (SSRF)

OWASP Category: A10: 2021-Server-Side Request Forgery (SSRF)

Description: In a Server-Side Request Forgery (SSRF) attack, the attacker can abuse functionality on the server to read or update internal resources. The attacker can supply or modify a URL which the code running on the server will read or submit data to, and by carefully selecting the URLs, the attacker may be able to read server configuration such as AWS metadata, connect to internal services like http enabled databases or perform post requests towards internal services which are not intended to be exposed.

Business Impact:

SSRF leads to unauthorized actions or access to data within organization. Sometimes, it allows the threat actors to perform arbitrary command execution. The exploits causes connection to third-party systems which acts like a backdoor for further attacks, which can seem to originate from organization.

9. Brute force attack

Vulnerability Name: Brute force attack

CWE – 307: Improper Restriction of Excessive Authentication Attempts

OWASP Category: A01: 2021- Broken Access Control

Description: A brute force attack can manifest itself in many different ways, but primarily consists in an attacker configuring predetermined values, making requests to a server using those values, and then analysing the response. For the sake of efficiency, an attacker may use a dictionary attack (with or without mutations) or a traditional brute-force attack (with given classes of characters e.g.: alphanumeric, special, case (in)sensitive). Considering a given method, number of tries, efficiency of the system which conducts the attack, and estimated efficiency of the system which is attacked the attacker is able to calculate approximately how long it will take to submit all chosen predetermined values.

Business Impact:

There are chances of stealing valuable personal information, personal identity details and more. It also enables attackers to spread malware into your systems. Upon compromising a website, they can set website links to redirect to malicious websites infected with malware and entice users to download them, threat actors can put spam ads on compromised websites, earn money from them and install spyware to track the activities of website visitors. The impacts of a brute force attack can be significant and have far-reaching consequences for the targeted system or organization

10. Improper signup process

Vulnerability Name: Improper signup process

CWE – 665: Improper Initialization

OWASP Category: A04: 2021 - Insecure Design

Description: The product does not initialize or incorrectly initializes a resource, which might leave the resource in an unexpected state when it is accessed or used.

Business Impact:

Ineffective authentication leads to compromise in CIA triads. The website can have many weaknesses.

Main Website: https://internshala.com/

Team 10.2

S. No	Vulnerability Name	CWE - No
1	Cleartext Transmission of Sensitive Information	319
2	Improper Certificate Validation (if SSL/TLS implementation is flawed)	295
3	Improper Access Control	284
4	Exposure of Sensitive Information to an Unauthorized Actor	200

Report:

1.

Vulnerability Name: Cleartext Transmission of Sensitive Information

C**WE:** 319

OWASP Category: A06:2021 - Security Misconfiguration

Description:

Port 80 is commonly used for unencrypted HTTP communication. When data is transmitted over HTTP, it is susceptible to interception and eavesdropping, as the information is sent in plain text. This can lead to a variety of security issues:

Man-in-the-Middle Attacks: Without encryption, attackers can intercept and read sensitive data such as login credentials, personal information, and session tokens.

Data Tampering: Attackers can modify the data being transmitted, potentially leading to unauthorized access, injection attacks, or other forms of data manipulation.

Session Hijacking: Session IDs can be captured, allowing attackers to impersonate authenticated users.

Business Impact:

Data Exposure: Sensitive information can be easily intercepted, potentially leading to data breaches.

Reputation Damage: Customers may lose trust in the website's security, affecting the reputation of the organization.

Mitigation:

Implement HTTPS: All communication should be redirected from port 80 to port 443 to ensure encryption.

HSTS (HTTP Strict Transport Security): Implementing HSTS headers enforces the use of secure connections and helps prevent downgrade attack.

2.

Vulnerability Name: Improper Certificate Validation (if SSL/TLS implementation is flawed)

CWE: 295

OWASP Category: A06:2021 - Security Misconfiguration

Description: Port 443 is used for secure, encrypted HTTPS communication. However, even with encryption, there can be vulnerabilities if not configured correctly:

Weak Cipher Suites: Outdated or weak encryption algorithms can leave the communication vulnerable to attacks.

Improper Certificate Validation: If the SSL/TLS implementation doesn't properly validate certificates, it can expose users to man-in-the-middle attacks.

Misconfigurations: Incorrect configurations of SSL/TLS settings can lead to security holes.

Business Impact:

Data Exposure: Misconfigurations can result in the unintentional exposure of sensitive information.

Man-in-the-Middle Attacks: If SSL/TLS is not implemented correctly, attackers can intercept and manipulate the communication.

Mitigation:

SSL/TLS Best Practices: Ensure that SSL/TLS configurations are up-to-date and follow best practices to maintain a high level of security.

Certificate Management: Regularly update SSL certificates to prevent expiration or misuse.

Security Audits and Testing: Perform regular security audits and penetration testing to identify and address potential vulnerabilities.

3.

Vulnerability Name: Improper Access Control

CWE: 284

OWASP Category: A01:2021 – Broken Access Control

Description:

If the SSH protocol is left open without adequate security measures, it can be vulnerable to various exploits and attacks. Some of the potential vulnerabilities include:

Brute force attacks: Attackers may attempt to guess the SSH username and password combination through successive login attempts.

SSH key compromise: If SSH keys are not protected securely, they may be stolen or leaked, allowing attackers to gain unauthorized access to systems using those keys

Denial of Service (DoS) attacks: Attackers can flood the SSH server with excessive connections or malformed packets to overwhelm its resources, making it inaccessible to legitimate users.

Password-based attacks: Weak or easily guessable passwords can be exploited, allowing unauthorized access to the system.

Business Impact:

Security risks: Opening port SSH can expose the system to potential security threats if not properly secured. Attackers may attempt to compromise the SSH service, exploit vulnerabilities, or use brute force attacks to gain unauthorized access to the system.

Compliance concerns: Depending on the industry and regulatory requirements, open SSH ports may violate security standards. Organizations need to ensure they comply with relevant regulations and protect sensitive data

4.

Vulnerability Name: Exposure of Sensitive Information to an Unauthorized Actor

CWE: 200

OWASP Category: A01:2021 – Broken Access Control

Description:

Opening port 8083 on a system may expose it to certain vulnerabilities, depending on the specific services running on that port. Here are some potential vulnerabilities associated with an open port 8083:

Misconfigured or vulnerable service: If there is a service running on port 8083, it could have misconfigurations or security vulnerabilities. Attackers could potentially exploit these vulnerabilities to gain unauthorized access, execute arbitrary code, or manipulate sensitive data.

Information disclosure: Depending on the service listening on port 8083, there may be a risk of unintentional information disclosure. If the service is not properly secured, sensitive data could be exposed, leading to privacy breaches or unauthorized access to confidential information.

Brute-force attacks: If port 8083 is open, it might be the default port for a service that requires authentication. Attackers could launch brute-force attacks attempting to guess usernames and passwords to gain access to the system.

Business Impact:

Increased network vulnerability: Open ports can be potential entry points for hackers and unauthorized access to a network. If port 8083 has security vulnerabilities, it can lead to data breaches or unauthorized activities within the business network.

Increased risk of malware or viruses: If port 8083 is left open, it can expose the network to various malware or virus attacks that specifically target open ports. This can result in compromised systems, data loss, or disruptions to business operations.

Compliance and regulatory concerns: Depending on the industry or nature of the business, there might be specific regulations or compliance requirements

that dictate which ports should be closed or restricted. Having an open port 8083 without proper justifications can lead to non-compliance and potential legal consequences.

Stage 2:

Overview:

Nessus is a popular vulnerability scanner developed by Tenable, Inc. It is used to scan IT infrastructure for potential vulnerabilities that could be exploited by attackers.

The key functionality of Nessus includes:

Vulnerability scanning: Nessus can scan networks, operating systems, web applications, databases etc. for known vulnerabilities based on its continuously updated vulnerability database. It uses techniques like port scanning, banner grabbing, version detection etc. to identify misconfigurations and weaknesses.

Compliance audits: Nessus provides pre-defined compliance audit templates for standards like PCI-DSS, HIPAA etc. This allows organizations to audit their infrastructure for compliance to various industry standards and regulations.

Malware detection: Nessus has plugins that can detect presence of malware like viruses, spyware, rootkits etc. on hosts. This allows identifying compromised systems.

Sensitive data discovery: Plugins can detect storage of sensitive data like credit card numbers and social security numbers on hosts. This helps identify potential data breaches.

Reporting: Nessus presents detailed reports on all vulnerabilities and issues discovered during a scan. These reports help security teams analyze risks and prioritize remediation.

Nessus Architecture

Nessus has a client-server architecture. The Nessus server does the actual scanning while the Nessus client is used to configure and schedule scans and view reports.

The key components of Nessus architecture include:

Nessus Manager: This is the central management component that oversees all the Nessus scanners deployed in an organization. It provides a single dashboard to operate Nessus infrastructure.

Nessus Scanner: This component does the actual scanning by running plugins for identification of vulnerabilities. Multiple scanners can be deployed and controlled centrally via the Nessus Manager.

Plugins: Nessus has thousands of plugins which implement the actual checks for vulnerabilities. Plugins are written in NASL language. Tenable continuously updates the plugins to detect new vulnerabilities.

Agent: Nessus agent can be installed on endpoints like laptops, desktops and servers to report data to scanners. This allows deeper scanning and visibility of endpoints.

CLI: Nessus provides a command line interface for administrators who prefer automation and scripting. All key functions are accessible via CLI.

REST API: Nessus provides RESTful API for integration with other tools like SIEMs, ticketing systems etc. The API allows automation of security workflows.

Nessus Scanning process

When a scan is kicked off in Nessus, it goes through the following key stages:

Discovery - This stage involves host discovery where Nessus identifies live hosts on the target network. Techniques like ping sweeps, port scanning etc. are used here.

Enumeration - Nessus gathers information about target hosts by identifying open ports, determining services, OS fingerprinting etc.

Vulnerability detection - This is the core scanning stage where thousands of vulnerability plugins are run on target hosts based on the enumeration data.

Reporting - Once scanning is complete, Nessus generates a detailed report with all findings and vulnerabilities discovered.

The scanning process is highly customizable in Nessus. For instance, users can choose between host-based or credentialed scanning, tweak plugin selection for focused audits, customize reports etc.

Target website: https://testphp.vulnweb.com/

Team 10.2

Target Ip address: 44.228.249.3

List of Vulnerability:

S. No	Vulnerability Name	Severity	Plugins
1	DNS Amplification Attack	Medium	35450
2	DNS Recursive Query Poisoning	Medium	10539
3	DNS Server Detection	Info	11002
4	Nessus SYN Scanner	Info	11219
5	ICMP Timestamp Disclosure	Info	10114
6	Traceroute Information	Info	10287
7	OS Identification	Info	11936
8	FQDN Resolution	Info	12053
9	Nessus Scan Information	Info	19506
10	TCP Timestamps Enabled	Info	25220
11	CPE Matching	Info	45590
12	Device Type Detection	Info	54615

Report:

Vulnerability Name: DNS Amplification Attack

Severity: Medium

Plugin: 35450

Port: 53/udp

Description: The remote DNS server could be used in a DDoS amplification attack. It answers queries from anyone and the responses are larger than the requests.

Solution: Restrict access to your DNS server from public network or reconfigure it to reject such queries.

Business Impact: This could allow an attacker to leverage the DNS server to amplify traffic in a DDoS attack against other victims. It could lead to denial of service.

Vulnerability Name: DNS Recursive Query Poisoning

Severity: Medium

Plugin: 10539

Port: 53/udp

Description: The remote DNS server allows recursive queries from anyone. This could allow cache poisoning attacks.

Solution: Restrict recursive queries to the hosts that should use this nameserver (such as those on the LAN).

Business Impact: This could allow an attacker to inject false DNS records into the cache, redirecting victims to malicious sites or IP addresses.

Vulnerability Name: DNS Server Detection

Severity: Info

Plugin: 11002

Port: 53/tcp, 53/udp

Description: A DNS server is listening on the remote host.

Solution: Disable this service if not needed or restrict access to internal hosts only if exposed externally.

Business Impact: A publicly reachable DNS server could be vulnerable to attacks like amplification or cache poisoning if not properly secured.

Vulnerability Name: Nessus SYN Scanner

Severity: Info

Plugin: 11219

Port: 53/tcp, 80/tcp

Description: A SYN scan found TCP ports 53 and 80 open.

Solution: Protect your target with an IP filter.

Business Impact: Open ports could be accessed by attackers if not properly secured.

Vulnerability Name: ICMP Timestamp Disclosure

Severity: Info

Plugin: 10114

Port: ICMP

Description: The remote host reveals its date/time via ICMP timestamp requests.

Solution: Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Business Impact: An attacker could defeat time-based authentication by knowing the exact time set on the host.

Vulnerability Name: Traceroute Information

Severity: Info

Plugin: 10287

Port: UDP

Description: A traceroute to the host was performed.

Solution: N/A

Business Impact: Traceroute exposes network topology information.

Team 10.2

Vulnerability Name: OS Identification

Severity: Info

Plugin: 11936

Port: TCP

Description: The remote OS appears to be CentOS Linux 7 Kernel 3.10.

Solution: N/A

Business Impact: Attackers can use OS fingerprinting for reconnaissance.

Vulnerability Name: FQDN Resolution

Severity: Info

Plugin: 12053

Port: TCP

Description: The remote host name resolves to ec2-44-228-249-3.us-west-2.compute.amazonaws.com.

Solution: N/A

Business Impact: Could help attackers determine host ownership and geography.

Vulnerability Name: Nessus Scan Information

Severity: Info

Plugin: 19506

Port: TCP

Description: Displays Nessus scan information like plugin feed version, scan duration, etc.

Solution: N/A

Team 10.2

Business Impact: Informational plugin.

Vulnerability Name: TCP Timestamps Enabled

Severity: Info

Plugin: 25220

Port: TCP

Description: The remote service implements TCP timestamps.

Solution: N/A

Business Impact: Could allow uptime estimation.

Vulnerability Name: CPE Matching

Severity: Info

Plugin: 45590

Port: TCP

Description: The remote OS matched CPE cpe:/o:centos:centos.

Solution: N/A

Business Impact: Assists in precise OS identification.

Vulnerability Name: Device Type Detection

Severity: Info

Plugin: 54615

Port: TCP

Description: The remote device type is unknown.

Solution: N/A

Business Impact: Attempts to classify device type.

Stage 3:

Title: Roles of SOC/SEIM

SIEMs tools are used to produce alerts and store the logs that generated those alerts for full analysis. The alerts themselves need to be reviewed by humans who then confirm if the alert is meaningful or a false positive. SIEM software can be used to assist security professionals by prioritizing alerts and highlighting specific devices or activities, along with AI gives chance of using fully automated system for security.

The human experts within SOCs can operate without a SIEM, but then they will need to find an alternative way to organize the log data or to flag key security events among the sea of data. For larger organizations, this homebrew-style approach to security can be clumsy and make it difficult to meet compliance reporting and other requirements.

However, SIEMs cannot effectively provide security without SOCs at this time. SIEMs issue alerts, but cannot act or even suggest appropriate actions so human security professionals must still use their experience to determine the response.

SOC

SOC is in-housed or out-sourced team of IT security professionals that monitors organization’s entire IT infrastructure, 24/7 detect cybersecurity events in real time and address them as quickly and effectively as possible. An SOC also selects, operates, and maintains the organization’s cyber security technologies, and continually analyzes threat data to find ways to improve the organization's security posture. It unifies and coordinates an organization’s security tools, practices, and response to security incidents. This usually results in improved preventative measures and security policies, faster threat detection, and faster, more effective and more cost-effective response to security threats. An SOC can also improve customer confidence, and simplify and strengthen an organization's compliance with industry, national and global privacy regulations.

Preparation, planning and prevention
Monitoring, detection and response
Recovery, refinement and compliance

SOC – cycle

SOC Cycle has several key stages, repeated continuously to ensure security of an enterprise.

1. Threat detection: SOC monitors network and system activities in real-time to detect vulnerabilities and risks, using IDS, IPS, firewalls, and endpoint security systems. Analysts analyse logs and alerts to find suspicious or anomalous activities.

2. Alert Triage: When alert is generated, security analysts triage determines its severity and validity. Investigating the alert, analyzing associated data, and deciding the genuine security incident or a false positive are some of the process involved.

3. Incident investigation: If an alert is confirmed to be a security incident, the SOC team starts a deeper investigation. They research about the incident, the scope, impact and methods used by attacker. Digital forensics and threat intelligence analysis also help them in the investigation.

4. Incident Containment: After identifying the threat SOC takes action to contain it, like isolating affected systems, blocking malicious network traffic, and other actions to prevent them from spreading.

5. Eradication: This involves removing threat form environment, like removing malware, closing vulnerabilities.

6. Recovery: SOC restores the affected systems to normal operation by applying patches and updates, restoring data, and verifying integrity of the systems.

7. Lessons Learned: A post incident review is conducted by assessing incident response process, identifying any weaknesses or areas for improvement, and updating security policies and procedures accordingly.

8. Continuous monitoring: SOC continues to monitor environment for any signs of further threat. This is important to identify and address new security risks.

7. Tuning and optimization: SOC regularly reviews and fine-tunes the security tools and procedures based on lesson learned and monitoring, to improve organization's security.

SIEM

SIEM is a security solution that helps organizations recognize and address potential security threats and vulnerabilities before they have a chance to disrupt business operations. SIEM systems help enterprise security teams detect user behavior anomalies and use artificial intelligence (AI) to automate many of the manual processes associated with threat detection and incident response.
Log management tool, security information management and analysis of security-related events and tacking and logging security data
Used in SOC for security management and compliance management use cases.
It performs data aggregation, consolidation and sorting functions to find threats.

Some functions of SIEM are:
Log management
Event Correlation and Analytics
Incident monitoring and security alerts
Compliance management and reporting
Real time threat recognition
Improved organizational efficiency
Detecting advanced and unknown threats
Conducting forensic investigations
Assessing and reporting in compliance
Monitoring users and applications

SIEM Cycle

The SIEM cycle involves several stages to effectively use this technology for threat detection, incident response, and ongoing security management.

1. Data Collection: The SIEM system collects data from various sources from include firewalls, intrusion detection systems, antivirus software, and other security tools. This data includes log files, network traffic data, endpoint information, and more.

2. Data Normalization: Raw data comes in various formats and structures. The SIEM normalizes this data, converting it into a standardized format to facilitate

correlation and analysis. Normalization involves parsing and categorizing events for consistency.

3. Event Correlation: The SIEM system correlates events to identify patterns and potential security incidents. It uses predefined rules, heuristics, and threat intelligence to detect anomalies, suspicious activities, or known attack patterns.

4. Alert Generation: When the SIEM system detects an event that matches predefined correlation rules or is otherwise deemed suspicious, it generates alerts which are prioritized based on severity and are sent to security analysts for further investigation.

5. Alert Triage: Security analysts review the generated alerts to determine their validity and significance. This involves investigating the context of the alert, the affected systems, and any associated indicators of compromise (IoCs).

6. Incident Investigation: If an alert is confirmed as a security incident, the SIEM system assists security analysts in conducting a deeper investigation. It provides relevant data, historical logs, and contextual information to help analysts understand the scope and impact of the incident.

7. Incident Response: Based on the findings of the investigation, the security team takes action to contain and mitigate the incident. This may involve isolating affected systems, blocking malicious activity, and applying countermeasures to limit the damage.

8. Documentation and Reporting: Throughout the SIEM cycle, documentation is essential. Security analysts maintain records of their findings, actions taken, and other relevant information. This documentation is crucial for compliance, legal, and post-incident analysis.

9. Lessons Learned: After an incident is resolved, the organization conducts a post-incident review to assess the effectiveness of the SIEM system, its rules, and the incident response process. Lessons learned are used to fine-tune the SIEM rules and processes.

10. Continuous Improvement: The SIEM system is continually optimized based on lessons learned and changing threat landscapes. This includes updating correlation rules, adding new data sources, and refining response procedures.

11. Compliance and Reporting: SIEM systems often provide reporting features to help organizations comply with regulatory requirements. They can generate reports on security incidents, user activities, and other relevant metrics.

MISP

MISP (Malware Information Sharing Platform & Threat Sharing), is an open-source threat intelligence platform used in the field of cyber security, designed to assist organizations and security professionals in collecting, storing, sharing, and correlating structured threat information. MISP provides a centralized repository for threat intelligence and facilitates collaboration between different organizations and security teams.

1. Threat Intelligence Sharing: MISP allows organizations to share threat intelligence, including indicators of compromise (IoCs), threat feeds, and contextual information, with trusted partners and the broader cybersecurity community. Sharing threat intelligence helps to enhance collective cybersecurity defense and incident response capabilities.

2. Data Structuring: MISP enables the structured representation of threat information. It uses standardized data models and taxonomies to describe threat indicators, events, and attributes. This structured approach makes it easier to understand, correlate, and analyze threat data.

3. IoC Management: MISP helps organizations manage IoCs, such as IP addresses, domains, file hashes, and more. It provides a platform for collecting and organizing IoCs, making them available for security operations and incident response.

4. Data Enrichment: MISP supports the enrichment of threat data by integrating with various external sources and tools. It can automatically pull in additional context, such as threat feeds, WHOIS information, and other relevant data, to provide a more comprehensive view of threats.

5. Correlation and Analysis: MISP offers correlation and analysis features to identify relationships and patterns among different indicators. This can help security teams understand the broader context of a threat and its potential impact.

6. Stix and TAXII Support: MISP adheres to the Structured Threat Information eXpression (STIX) and Trusted Automated Exchange of Indicator Information

(TAXII) standards, allowing for interoperability and integration with other threat intelligence platforms and tools that support these standards.

7. Sharing Communities: MISP can be used to create or join sharing communities, where organizations with similar interests or threats can collaborate on sharing and analyzing threat data. This collaborative approach enhances collective situational awareness and threat detection.

8. Integration with Other Tools: MISP is designed to work in conjunction with other security tools and technologies, such as SIEM systems, IDS/IPS solutions, and security orchestration and automation platforms (SOAR). Integration with these tools can streamline incident response and remediation.

9. Customization and Extensions: MISP is highly customizable and extensible. Organizations can tailor it to their specific needs by creating custom data models, taxonomies, and modules to support their unique threat intelligence requirements.

10. Open Source and Active Community: MISP is an open-source project with an active community of users and contributors. This means that it is continuously evolving, with new features and updates being developed and shared by the community.

College network information

The network of the college is vast and complex. Like any other network it is used to provide connectivity, resources and services to students, faculties, and staffs while maintaining security. It contains hierarchical architecture of core, distribution, and access layers. Both wired and wireless components are used. It is connected to internet for use. Security is considered to be top priority in the college network. Access controls and authentication is used because of storing and using sensitive information. Wi-Fi is made available for use by many in the campus.

Deploying SOC in my college

Implementing a Security Operations Center (SOC) in a college network can greatly enhance the security posture of the institution. It monitors, detects, responds to, and mitigates security threats and incidents. Once the scale of the network is known, SOC can be deployed to protect the data. A dedicated team of security professionals should be built to staff the SOC. This includes security analysts, incident responders and SOC manager. A SIEM tool is chose along

with IDS/IPS, firewall, antivirus, and endpoint security solutions. Update the SOC with latest threat information. A detailed infrastructure for SOC is to be planned. Develop a standard Operating Procedure (SOP) for incident detection, response and report. Continuous monitoring is required along with a proper Incident Response Plan and proper documentation for reporting any vulnerability. Along with these continuous update should be made on the software as well the knowledge of the SOC team.

Threat intelligence

Threat intelligence refers to information that is collected, analyzed, and disseminated to help organizations understand and defend against cyber security threats, obtained from various sources and provides insights into the tactics, techniques, procedures, and intentions of cyber adversaries. Threat intelligence plays a crucial role in enhancing an organization's cyber security posture and proactive defense.

Incident Response

Incident response is a structured and organized approach to addressing and managing cyber security incidents and data breaches. The goal of an incident response program is to reduce the impact of incidents, quickly mitigate the threat, and restore normal operations while preserving and analyzing data to prevent future incidents. Here are the key steps and elements of an incident response process:

1. Preparation:

=> Establish an incident response team: Assemble a dedicated team of individuals with defined roles and responsibilities in responding to incidents.

=> Develop an incident response plan: Create a comprehensive plan that outlines the organization's strategy, procedures, and guidelines for responding to different types of incidents.

=> Establish communication protocols: Define how the team will communicate internally and externally during an incident.

=> Conduct training and drills: Regularly train and test the incident response team to ensure they are prepared to respond effectively.

2. Identification:

=> Monitor for signs of incidents: Continuously monitor network and system activities for indicators of compromise (IoCs) and other suspicious activities.

=> Detect incidents: Use intrusion detection systems (IDS), security information and event management (SIEM) tools, and other security measures to identify incidents.

3. Containment:

=> Isolate affected systems: Take immediate steps to contain the incident, which may involve isolating affected systems from the network to prevent the threat from spreading.

=> Block malicious activity: Apply measures to prevent the attacker from causing further damage or exfiltrating data.

4. Eradication:

=> Identify and remove the root cause: Determine how the incident occurred and take steps to remove any malware or vulnerabilities.

=> Patch or update systems: Apply security patches or updates to eliminate vulnerabilities that were exploited.

5. Recovery:

=> Restore systems and data: After the incident is contained and eradicated, work on restoring affected systems and data to their normal state.

=> Monitor for recurrence: Continue monitoring to ensure that the incident does not recur after recovery.

6. Lessons Learned:

=> Conduct a post=>incident review: Analyze the incident response process and the incident itself to identify strengths, weaknesses, and areas for improvement.

=> Update incident response procedures: Based on the lessons learned, update the incident response plan and improve the organization's security posture.

7. Documentation:

=> Document the incident: Keep detailed records of the incident, including timelines, actions taken, and the impact of the incident.

=> Legal and compliance requirements: Ensure that all documentation is in compliance with legal and regulatory requirements, which may involve notifying authorities or affected parties.

8. Communication:

=> Notify stakeholders: Communicate with relevant internal and external stakeholders, including executive management, affected individuals, customers, and regulatory authorities, as required.

9. Continuous Improvement:

=> Implement changes: Based on the lessons learned from the incident, make improvements to security measures, incident response procedures, and ongoing monitoring.

10. Legal and Regulatory Compliance:

=> Comply with legal and regulatory requirements: Ensure that the incident response process adheres to relevant laws and regulations, which may include data breach notification requirements.

Qradar and understanding about the tool

The IBM QRadar is a security information and event management or SIEM product that is designed for enterprises. The tool collects data from the organization and the network devices. It also connects to the operating systems, host assets, applications, vulnerabilities, user activities, and behaviors. IBM QRadar is used to perform analysis of the log data and the network flows in real-time so that malicious activities can be identified and stopped as soon as possible. Thus, the main aim of the IBM QRadar is to prevent or minimize the damage to its host organization.
The IBM QRadar SIEM uses a real-time integrated Cybersecurity AI, machine learning, and behavior analytics to prevent the attacks in the blink of an eye and with a very less cost compared to what human supervision can ensure. QRadar can address the bulk security issues that the companies face and save a lot of money. The security teams that struggle with patching endpoints properly and updating them can get their problems solved with IBM BigFix that has QRadar SIEM integrated into it. Most of the common issues are solved with this.

Deployment of the IBM QRadar SIEM is possible in the form of software, hardware, or a product meant for virtual application. Event processors for the

collection, storage, and analysis of event collectors and event data make up the architecture of the product. They help to capture and forward the data.

Management of SIEM can be performed by the SOC or Security Operations Center through centralized consoles. The flow processors are similar to the event processors, however, these are meant for network flows. The consoles offer a lot of help to the people who are managing or using the SIEM.

Comprehensive visibility - The product helps to gain a centralized insight into the data flows, events, and logs on the SaaS (software-as-a-service) and IaaS (infrastructure-as-a-service) environments and on-premises.

Elimination of manual tasks - All the events in a certain threat can be centrally seen in one place and the expensive manual tracking can be eliminated. Analysts can focus on investigating the matter (security threat), followed by a proper response.

Easily cater to the compliance protocols - It becomes easier to comply with the international policies and the external regulations that are achieved by leveraging the pre-built reports and templates.

Real-time threat detection - Out-of-the-box analysis is leveraged that analyzes the network flows and logs automatically and generates proper alerts and the attacks are then directed via the proper kill chain.

Conclusion:

Stage 1:

It is the process of evaluating and assessing web application to ensure it functions as desired and securely. It involves testing to identify and address issues, vulnerabilities that could affect the application's performance. The testing involves testing features, user interfaces, navigation and workflows. Security testing of web application involves identifying and mitigating vulnerability and threat that can lead to data breaches, unauthorized access, XSS, CSRF, SQL injection or other issues. Penetration testing is done to find vulnerability in application's security defenses. It also makes sure that data entered by user should be validated and sanitized. It also tests how the application manages user sessions, including authentication, authorization, and

the prevention of session hijacking or fixation. Thorough testing it helps identify and address issues before they impact users and helps maintain the security and reliability of the application.

Stage 2:

A Nessus report on security vulnerabilities, misconfigurations, and potential threats within computer systems, networks, and web applications. These reports provide detailed information about the security posture of the scanned environment. It has executive summary, an overview of the most critical vulnerabilities and risks identified during the scan. Scan Information, the details about the scan, such as the scan start and end times, the IP addresses or domains scanned, and the version of Nessus used. Risk severity includes risk levels to vulnerabilities, typically using a scale that ranges from Low to Critical. The report categorizes vulnerabilities by their risk severity, helping organizations prioritize mitigation efforts. It also has vulnerability details(vulnerability name, CVE), technical details, mitigation advice and more. Nessus reports are essential for organizations, IT team, security teams to understand the security posture of their systems, prioritize remediation efforts, and demonstrate compliance with security standards. These reports help identify and address vulnerabilities and improve the security.

Stage 3: what you understand fromSOC / SEIM / Qradar Dashboard .

IBM QRadar is a Security Information and Event Management (SIEM) solution that provides comprehensive security intelligence for organizations. In the context of QRadar, a dashboard is a customizable, visual interface that presents real-time and historical information about the security of an organization's IT infrastructure. Dashboards in QRadar help security professionals and administrators quickly gain insights into security events, threats, vulnerabilities, and compliance status.

It has real-time data visualization in the form of charts, graphs, tables, and widgets. They offer an at-a-glance view of what's happening in the IT environment, including security incidents, events, and network traffic. Itr also have a security overview, alerts and offenses, event and log sources, incident response, User and Entity Behavior Analytics (UEBA(, Network Traffic and Flow Data, Drill-Down Capabilities and so on.

QRadar dashboards play a critical role in providing situational awareness, supporting incident response, and ensuring that organizations have a clear understanding of their security posture.

Future Scope:

Stage 1:

The future scope of web application testing is promising and continues to evolve in response to technological advancements and changing user expectations. As organizations rely on web applications to deliver services and conduct business, the demand for high-quality, secure, and user-friendly web applications remains strong. AI and automation is a major future technology to be focused on. Artificial Intelligence (AI) and machine learning are expected to play a significant role in web application testing. AI can help automate test case generation, analyze large datasets for testing insights, and enhance the efficiency of test scripts. Automating security testing, penetration testing, performance and scalability testing can be implemented.

Stage 2:

As organizations adopt CI/CD practices, web application testing will need to align with the rapid development and frequent deployments of software. This requires automated testing to ensure that changes don't introduce new issues. Web application security is a top concern. Security testing will continue to evolve to address emerging threats, including better defenses against cyber attacks and the detection of vulnerabilities. With the proliferation of mobile devices and web browsers, testing for compatibility across various platforms and configurations is crucial. Responsive design and cross-browser testing is important and an area to be focused on. Also, testing for applications that incorporate blockchain and smart contracts will become more specialized to ensure the reliability and security of blockchain-based features. Augmented Reality (AR), Virtual Reality (VR), and WebXR technologies will require testing are also emerging field.

Stage 3: future scope of SOC / SEIM

The future scope of Security Operations Centers (SOCs) and Security Information and Event Management (SIEM) systems is highly promising, as the

cybersecurity landscape continues to evolve, presenting new challenges and opportunities. The ongoing expansion of digital ecosystems and the sophistication of cyber threats are driving the need for more robust and advanced SOC and SIEM capabilities. Enhanced integration with external threat intelligence feeds will help SOCs stay updated with the latest threat information, making it easier to detect and respond to emerging threats. Automation will play a significant, automating routines, incident response workflows and threat containment measures. SOCs and SIEM solutions will need to extend their monitoring and analysis capabilities to cover cloud-based resources and applications. It should be expanded to IoT environments.

Topics Explored:

Cyber Security, Artificial Intelligence, SOC, SIEM, Penetration testing, web application testing, Incident response, threat intelligence, , malware, vulnerabilities and risks, OWASP top 10, data sanity, IDS, IPS, web services, APIs, CIS Top 20.

Tools Explored:

- IBM Qradar
- Nessus
- Kali Linux
- Nmap
- Metasploitable 2
- Nikto
- Accunetix
- Sqlmap
- Metasploitable framework
- Burpsuite