AI System To Verify User Identities Based On Behavioral Patterns

Overview :-

In today's world where there are security concerns about our data and therefore there is an increased need for a system that can understand the behaviour of the user and act accordingly this can help us to prevent any data breaches that may occur and compromise our data.The topic we have chosen is related to the back-end AI system which develops some recommendations on various online platforms. So the user identification becomes easier as their behavior patterns can be recognized after multiple interactions with the websites. There are many behavioral patterns of the users which include web interactions, keystrokes, mouse movements, and more. We have to design and implement data collection mechanisms that capture user behaviour in real time. And then we will normalize the collected data to ensure uniformity. Development of accurate AI models for behaviour analysis is at the core of the behaviour-based identity verification system. Training the models to accommodate different user behavior patterns. Then the last step would be adding an extra layer of security to prevent any sort of cyber threats. These behavioural patterns are very important to be studied to keep the websites secure from any safety issues related to the security. The behaviour studying will also help in identifying bots and preventing them from entering the websites which helps in increasing the safety of the website.

This is the a vast field that is growing each day as there is an increase in the amount of e-commerce websites and everything getting online there is an increased requirement for the protection of these websites from the attackers. And using AI to understand the users behaviour and understanding how they behave. This can help in securing the websites accordingly and use AI to prevent any security issues.

List of teammates–

Sno	Name	College	Contact
1	**Vibhuti Saini**	**VIT AP**	**7505666563**
2	**Tanay Bhoyar**	**VIT AP**	**9136348753**

List Of Vulnerabilities

Sno	Vulnerability	CWE
1	HTML Injection	CWE-79
2	iFrame Injection	CWE-829
3	Mail Header Injection	CWE-93
4	OS Command Injection	CWE-78
5	Broken Authentication And Captcha Bypassing	CWE-287
6	Cross Site Scripting(JSON)	CWE-914
7	Server Side Includes Injection	CWE-97
8	Clickjacking	CWE-1021
9	Directory Traversal	CWE-22
10	Restrict Device Access	CWE-264

REPORT

1)**Vulnerability Name**:HTML Injection
CWE:CWE-79
OWASP Category:A7-Cross Site Scripting
Description:The product does not neutralize or incorrectly neutralizes
user-controllable input before it is placed in output that is used as a web page that
is served to other users.
Business Impact:It can cause various losses to the organization like financial losses reputation
damage,legal issues and operational disruptions. It can also make the system vulnerable to
various attacks like Session hijacking and phishing etc.
2)**Vulnerability Name**:iFrame Injection
CWE:CWE-829
OWASP Category:A1-2021-Injection
Description:When including third-party functionality, such as a web widget, library,
or other source of functionality, the product must effectively trust that functionality.
Without sufficient protection mechanisms, the functionality could be malicious innature (either by coming from an untrusted source, being spoofed, or being
modified in transit from a trusted source). The functionality might also contain its
own weaknesses, or grant access to additional functionality and state information
that should be kept private to the base system, such as system state information,
sensitive application data, or the DOM of a web application.
Business Impact:It can cause various losses to the organization like financial losses of
reputation damage,legal issues and operational disruptions. This makes the websites vulnerable

to various attacks like Phishing, Data Leakage, Malware Distribution
3)**Vulnerability Name**:Mail Header Injection
CWE:CWE-93
OWASP Category:A1-Injection
Description:The product uses CRLF (carriage return line feeds) as a special element,
e.g. to separate lines or records, but it does not neutralize or incorrectly neutralizes
CRLF sequences from inputs.
Business Impact:It can cause various losses to the organization like financial losses of
reputation damage,legal issues and operational disruptions. It also makes the sites vulnerable
to attacks like Email Spoofing, Phishing etc.
4)**Vulnerability Name**:OS Command Injection
CWE:CWE-78
OWASP Category:A1:2021-Injection
Description: The product constructs all or part of an OS command using
externally-influenced input from an upstream component, but it does not neutralize
or incorrectly neutralizes special elements that could modify the intended OS
command when it is sent to a downstream component.
Business Impact: It can cause various losses to the organization like financial losses of
reputation damage,legal issues and operational disruptions.It makes websites vulnerable to
attacks like Unauthorize access, DOS etc.
5)**Vulnerability Name**:Broken Authentication And Captcha Bypassing
CWE:CWE-287
OWASP Category: A2:2021-Broken Authentication And A7:2021-Security Misconfiguration
Description: When an actor claims to have a given identity, the product does not

prove or insufficiently proves that the claim is correct.
Business Impact: It can cause various losses to the organization like financial losses of
reputation damage,legal issues and operational disruptions. It makes the websites vulnerable to
other attacks like Unauthorize access, Data breaches, Data Manipulation etc which can cause
other issue about the security of users.
6)**Vulnerability Name**:Cross Site Scripting(JSON)
CWE: CWE-914
OWASP Category:A7:2021-Cross-Site Scripting (XSS).
Description: Many languages offer powerful features that allow the programmer to
access arbitrary variables that are specified by an input string. While these features
can offer significant flexibility and reduce development time, they can be extremely
dangerous if attackers can modify unintended variables that have security
implications.
Business Impact: It can cause various losses to the organization like financial losses of
reputation damage,legal issues and operational disruptions.It also makes the website vulnerable
to issues like Data Theft, Session Hijacking, Phishing etc. which makes it the website more
vulnerable and also causes security issues.
7)**Vulnerability Name**:Server Side Includes Injection
CWE: CWE-97
OWASP Category: A1:2021-Injection
Description: The product generates a web page, but does not neutralize or
incorrectly neutralizes user-controllable input that could be interpreted as a
server-side include (SSI) directive.
Business Impact: It can cause various losses to the organization like financial losses of

reputation damage,legal issues and operational disruption. It makes the website vulnerable to
attacks like data leakages, Unauthorized access, Defacement etc.
8)**Vulnerability Name**:Clickjacking
CWE: CWE-1021
OWASP Category: A6:2021-Security Misconfiguration
Description:A web application is expected to place restrictions on whether it is
allowed to be rendered within frames, iframes, objects, embed or applet elements.
Without the restrictions, users can be tricked into interacting with the application
when they were not intending to.
Business Impact: It can affect the website negatively and cause issues like loss in users
loosing trust, and can also lead to financial frauds.It can also cause issues like Resource
Allocation, Operational Disruption etc.
9)**Vulnerability Name**:Directory Traversal
CWE: CWE-22
OWASP Category: A6:2021-Security Misconfiguration
Description: Many file operations are intended to take place within a restricted
directory. By using special elements such as ".." and "/" separators, attackers can
escape outside of the restricted location to access files or directories that are
elsewhere on the system. One of the most common special elements is the "../"
sequence, which in most modern operating systems is interpreted as the parent
directory of the current location. This is referred to as relative path traversal. Path
traversal also covers the use of absolute pathnames such as "/usr/local/bin", which

may also be useful in accessing unexpected files. This is referred to as absolute
path traversal.
Business Impact: It can cause various issues to the website like losing the users trust it can
also cause issues like compromising user data and also financial issues and also can cause
issues with resource allocation.
10)**Vulnerability Name**:Restrict Device Access
CWE: CWE-264
OWASP Category:Description: Weaknesses in this category are related to the management of
permissions, privileges, and other security features that are used to perform access
control.
Business Impact:
The Organizations cannot use their documents and data because of this restricted access of devices.

NESSUS

Nessus is a widely used vulnerability assessment and management software developed by Tenable Network Security. It is designed to identify and assess vulnerabilities in computer systems, networks, and applications. Nessus helps organizations detect and address security weaknesses and potential threats in their IT infrastructure. Here are some key features and information about Nessus:

Vulnerability Scanning: Nessus performs active and passive scans to identify vulnerabilities and security issues. It can scan a wide range of devices and operating systems, including servers, workstations, network devices, and more.

Extensive Vulnerability Database: Nessus uses a vast and continuously updated vulnerability database to compare scan results against known vulnerabilities. This database includes information about common vulnerabilities and exposures (CVEs).

Policy Compliance Checking: In addition to identifying vulnerabilities, Nessus can check systems for compliance with various security policies and industry standards, such as PCI DSS, HIPAA, NIST, and more.

Customizable Scans: Nessus allows users to create custom scans to target specific systems, IP ranges, or vulnerabilities. You can adjust scan policies and schedules to fit your organization's needs.

Reporting and Remediation: Nessus generates detailed reports that provide information on discovered vulnerabilities, including severity, potential impact, and remediation recommendations. This helps organizations prioritize and address security issues.
Scanning Frequency: Nessus supports regular and automated scanning, enabling organizations to monitor their security posture continuously.

Agent-Based Scanning: In addition to network-based scanning, Nessus offers agent-based scanning, which can be installed on individual systems to provide deeper visibility into host-specific vulnerabilities.

Integration: Nessus can be integrated with other security tools and platforms, such as Security Information and Event Management (SIEM) systems, to streamline the vulnerability management process.

User Access Control: Nessus provides role-based access control, allowing organizations to assign different levels of

access to their security team members and control who can initiate scans and view scan results.

Licensing: Nessus offers various licensing options, including free and commercial versions. The free version is called Nessus Essentials and has limitations compared to the commercial offerings, such as Nessus Professional and Nessus Manager.

It's important to note that while Nessus can help identify vulnerabilities, it is essential for organizations to have a robust vulnerability management process in place to prioritize and remediate these issues. Vulnerability scanning is just one component of a comprehensive security strategy.

Nessus is widely used by organizations of all sizes to improve their security posture by identifying and addressing vulnerabilities and ensuring compliance with industry standards and regulations.

Target website ─ bWAPP

Target ip address:- 220.158.183.5

REPORT Of Nessus Scan

Vulnerabilities Total: 59

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	9.2	133845	Apache Tomcat 7.0.x < 7.0.100 / 8.5.x < 8.5.51 / 9.0.x < 9.0.31 Multiple Vulnerabilities
CRITICAL	9.8	6.7	111069	Apache Tomcat 9.0.0 < 9.0.10 Multiple Vulnerabilites
HIGH	8.6	5.5	161159	Apache Tomcat 9.0.0.M1 < 9.0.21 vulnerability
HIGH	8.1	9.2	103699	Apache Tomcat 9.0.0.M1 < 9.0.1 Multiple Vulnerabilities
HIGH	7.5	3.6	121124	Apache Tomcat 8.0.x < 8.0.52 / 8.5.x < 8.5.31 / 9.0.x < 9.0.8 Denial of Service
HIGH	7.5	4.4	166906	Apache Tomcat 9.0.0-M1 < 9.0.68 Request Smuggling Vulnerability
HIGH	7.5	4.4	176310	Apache Tomcat 9.0.0.M1 < 9.0.10 multiple vulnerabilities
HIGH	7.5	6.7	126312	Apache Tomcat 9.0.0.M1 < 9.0.16 DoS
HIGH	7.5	6.7	126245	Apache Tomcat 9.0.0.M1 < 9.0.20 DoS
HIGH	7.5	6.7	132419	Apache Tomcat 9.0.0.M1 < 9.0.30 Privilege Escalation Vulnerability
HIGH	7.5	4.4	138098	Apache Tomcat 9.0.0.M1 < 9.0.36 DoS
HIGH	7.5	5.1	138591	Apache Tomcat 9.0.0.M1 < 9.0.37 Multiple Vulnerabilities
HIGH	7.5	8.4	147164	Apache Tomcat 9.0.0.M1 < 9.0.43 Multiple Vulnerabilities
HIGH	7.5	4.4	171657	Apache Tomcat 9.0.0.M1 < 9.0.71
HIGH	7.5	3.6	122447	Apache Tomcat 9.0.0.M1 < 9.0.8 Denial of Service Vulnerability
HIGH	7.5	5.1	144050	Apache Tomcat 9.x < 9.0.40 Information Disclosure
HIGH	7.0	8.4	136806	Apache Tomcat 9.0.0 < 9.0.35 Remote Code Execution

MEDIUM	6.5	4.2	151502	Apache Tomcat 7.0.x <= 7.0.108 / 8.5.x <= 8.5.65 / 9.0.x <= 9.0.45 / 10.0.x <= 10.0.5 vulnerability
MEDIUM	6.5	4.4	106978	Apache Tomcat 9.0.0.M1 < 9.0.5 Insecure CGI Servlet Search Algorithm Description Weakness
MEDIUM	6.5	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.5	-	157288	TLS Version 1.1 Protocol Deprecated
MEDIUM	6.1	3.8	180194	Apache Tomcat 9.0.0.M1 < 9.0.80
MEDIUM	5.3	1.4	152182	Apache Tomcat 9.0.0.M1 < 9.0.48 vulnerability
MEDIUM	5.3	-	12085	Apache Tomcat Default Files
MEDIUM	4.3	1.4	141446	Apache Tomcat 8.5.x < 8.5.58 / 9.0.x < 9.0.38 HTTP/2 Request Mix-Up
MEDIUM	4.3	2.2	118037	Apache Tomcat 9.0.0.M1 < 9.0.12 Open Redirect Weakness
MEDIUM	4.3	2.2	173251	Apache Tomcat 9.0.0.M1 < 9.0.72
LOW	3.7	2.2	159464	Apache Tomcat 9.0.0.M1 < 9.0.62 Spring4Shell (CVE-2022-22965) Mitigations
LOW	3.7	1.4	106713	Apache Tomcat 9.0.0.M22 < 9.0.2 Insecure CGI Servlet Search Algorithm Description Weakness
INFO	N/A	-	39446	Apache Tomcat Detection
INFO	N/A	-	166602	Asset Attribute: Fully Qualified Domain Name (FQDN)
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	54615	Device Type
INFO	N/A	-	84502	HSTS Missing From HTTPS Server
INFO	N/A	-	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	46215	Inconsistent Hostname and IP Address
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification

INFO	N/A	-	66334	Patch Report
INFO	N/A	-	31422	Reverse NAT/Intercepting Proxy Detection
INFO	N/A	-	56984	SSL / TLS Versions Supported
INFO	N/A	-	45410	SSL Certificate 'commonName' Mismatch
INFO	N/A	-	83298	SSL Certificate Chain Contains Certificates Expiring Soon
INFO	N/A	-	42981	SSL Certificate Expiry - Future Expiry
INFO	N/A	-	10863	SSL Certificate Information
INFO	N/A	-	95631	SSL Certificate Signed Using Weak Hashing Algorithm (Known CA)
INFO	N/A	-	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	-	21643	SSL Cipher Suites Supported
INFO	N/A	-	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	94761	SSL Root Certification Authority Certificate Information
INFO	N/A	-	156899	SSL/TLS Recommended Cipher Suites
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	121010	TLS Version 1.1 Protocol Detection
INFO	N/A	-	136318	TLS Version 1.2 Protocol Detection
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	20108	Web Server / Application favicon.ico Vendor Fingerprinting

* indicates the v3.0 score was not available; the v2.0 score is shown

REPORT

● SOC

A security operations center (SOC) – sometimes called an information security operations center, or ISOC – is an in-house or outsourced team of IT security professionals that monitors an organization’s entire IT infrastructure, 24/7, to 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 cybersecurity technologies, and continually analyzes threat data to find ways to improve the organization's security posture.The chief benefit of operating or outsourcing an SOC is that 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.

● SOC - cycle

The SOC (Security Operations Center) cycle refers to the recurring processes and activities that a Security Operations Center follows to detect, respond to, and mitigate security incidents. The goal of a SOC is to proactively monitor an organization's IT infrastructure, networks, and systems to identify and respond to security threats. The SOC cycle typically consists of several key stages:

Identification: In this stage, the SOC team monitors and collects data from various sources, such as network traffic, logs, and security tools, to identify potential security incidents. This includes setting up monitoring alerts and analyzing the data for unusual or suspicious activities.

Detection: Once potential security incidents are identified, the SOC team investigates further to determine if they are indeed security threats. They use various tools, techniques, and expertise to validate the alerts and assess the severity and impact of the incidents.

Analysis: In this stage, the SOC analysts conduct in-depth analysis of the detected incidents. They try to understand the nature of the threats, how they may have entered the network, and what vulnerabilities may have been exploited. This information helps in crafting an effective response.

Prioritization: After analyzing the incidents, they are prioritized based on their severity and potential impact on the organization. This helps the SOC team allocate resources to address the most critical threats first.

Containment: Once an incident is confirmed, the SOC team takes steps to contain and mitigate the threat. This can involve isolating affected systems, blocking malicious activity, or taking other measures to prevent further damage.
Eradication: After containment, the SOC works on eliminating the root cause of the incident. This may involve patching vulnerabilities, removing malware, or taking other actions to prevent the threat from recurring.

Recovery: In this stage, the SOC helps the organization recover from the incident. This may include restoring affected systems and services to normal operation and ensuring that data and resources are safe.

Lessons Learned: After resolving an incident, the SOC team conducts a post-incident review to analyze what went right and what went wrong during the incident response process. This information is used to improve the organization's security posture and response procedures.

Documentation: All activities related to the incident, including the identification, response, and recovery steps, are documented for future reference, compliance, and reporting purposes.

Reporting: The SOC team provides reports and updates to senior management and stakeholders on the status of incidents, actions taken, and the overall security posture of the organization.

The SOC cycle is a continuous and iterative process that helps organizations better understand and manage their security threats. It involves the use of security technologies, skilled personnel, and well-defined procedures to detect, respond to, and mitigate security incidents effectively. The goal is to minimize the impact of security breaches and ensure the ongoing security of an organization's IT environment.

- **Siem**

Security information and event management, SIEM for short, is a solution that helps organizations detect, analyze, and respond to security threats before they harm business operations.

SIEM, pronounced “sim,” combines both security information management (SIM) and security event management (SEM) into one security management system. SIEM technology collects event log data from a range of sources, identifies activity that deviates from the norm with real-time analysis, and takes appropriate action.

In short, SIEM gives organizations visibility into activity within their network so they can respond swiftly to potential cyberattacks and meet compliance requirements

SIEM tools collect, aggregate, and analyze volumes of data from an organization’s applications, devices, servers, and users in real-time so security teams can detect and block attacks. SIEM tools use predetermined rules to help security teams define threats and generate alerts..

In the past decade, SIEM technology has evolved to make threat detection and incident response smarter and faster with artificial intelligence.

- Log management: SIEM systems gather vast amounts of data in one place, organize it, and then determine if it shows signs of a threat, attack, or breach.
- Event correlation: The data is then sorted to identify relationships and patterns to quickly detect and respond to potential threats.
- Incident monitoring and response: SIEM technology monitors security incidents across an organization’s network and provides alerts and audits of all activity related to an incident.

SIEM systems can mitigate cyber risk with a range of use cases such as detecting suspicious user activity, monitoring user behavior, limiting access attempts and generating compliance reports.

● Siem Cycle

SIEM (Security Information and Event Management) is a comprehensive approach to security that involves the collection, correlation, analysis, and monitoring of security-related data and events from various sources within an organization's IT environment. The SIEM cycle is the

recurring process that a SIEM system follows to provide visibility into an organization's security posture and facilitate effective incident detection, response, and compliance. It typically consists of the following stages:

Data Collection: The SIEM system collects a wide range of security-related data and event logs from various sources, including network devices, servers, applications, and endpoints. These sources may include firewalls, intrusion detection systems (IDS), antivirus software, authentication systems, and more.

Normalization: Once the data is collected, it is normalized to ensure that all the incoming logs and events are in a consistent format. This is important because different sources may produce data in various formats, and normalization makes it easier to correlate and analyze the data.

Data Storage: The normalized data is then stored in a secure and centralized repository, often referred to as a "data lake" or "data warehouse." This storage allows for historical analysis, forensic investigations, and compliance reporting.

Correlation: The SIEM system correlates data and events by comparing them with predefined rules, policies, and baselines. Correlation helps identify suspicious or anomalous patterns that may indicate a security threat. It can also help in detecting complex attacks that may involve multiple events from different sources.

Alerting: When the SIEM system detects potential security incidents through correlation, it generates alerts. These alerts are sent to the security operations team, which then investigates further to determine the severity and validity of the incidents.

Incident Investigation: Security analysts within the organization's SOC (Security Operations Center) or IT security team investigate the alerts generated by the SIEM system. They analyze the incident, gather additional context, and assess its impact on the organization's security.

Incident Response: If an incident is confirmed, the security team takes appropriate actions to respond to and mitigate the threat. This may involve isolating affected systems, removing malware, and taking steps to prevent further damage.

Reporting: SIEM systems provide reporting and visualization capabilities to present security-related information to various stakeholders within the organization, including security teams, management, and compliance auditors. Reports can include information about detected incidents, compliance status, and overall security trends.

Compliance Monitoring: SIEM systems often include features to monitor and report on compliance with various security standards and regulations, such as PCI DSS, HIPAA, or GDPR. This helps organizations ensure they are meeting legal and industry-specific requirements.

Continuous Improvement: Organizations continuously fine-tune and improve their SIEM systems by updating correlation rules, adding new data sources, and enhancing their incident response procedures. This iterative process ensures that the SIEM system remains effective in addressing evolving security threats.

The SIEM cycle is a critical component of an organization's security strategy, providing a proactive approach to identifying and responding to security incidents, as well as facilitating compliance and risk

management. It helps organizations gain better visibility into their IT environment and enhances their ability to detect and respond to security threats in a timely manner.

- **MISP**

MISP, which stands for Malware Information Sharing Platform & Threat Sharing, is an open-source threat intelligence platform designed to facilitate the sharing of structured threat information among cybersecurity professionals and organizations. MISP was developed to help improve the collective defense against cyber threats by enabling the sharing of threat indicators, such as malware samples, IP addresses, domain names, and other attributes, in a standardized and structured format. Here is some key information about MISP:

Information Sharing and Collaboration: MISP is primarily used for sharing threat intelligence within and between organizations. It allows cybersecurity teams to share information about new and emerging threats, as well as indicators of compromise (IOCs) with their trusted partners and communities.

Data Standardization: MISP uses the STIX (Structured Threat Information eXpression) format and other standardized data models to ensure that threat information is structured, consistent, and easily consumable by different security tools and platforms. This helps in improving the quality and effectiveness of threat sharing.

Customizable Data Models: MISP allows users to define and customize data models and taxonomies, enabling organizations to adapt the platform to their specific needs and industry requirements.

Correlation and Analysis: MISP provides features for correlating and analyzing shared threat data. Analysts can search for related indicators and assess the potential impact of a specific threat on their environment.

Integration: MISP offers various integration options, allowing organizations to connect it with other security tools and platforms, such as SIEMs, IDS/IPS systems, and threat feeds. This integration helps automate the detection and response to threats.
Indicator Feeds: MISP can consume and distribute threat intelligence feeds from various sources, including open-source threat feeds and commercial threat intelligence providers. This enables organizations to stay up-to-date with the latest threat information.

Community and Sharing: MISP has a thriving community of users who actively share threat intelligence with one another. Users can establish trusted sharing relationships with other organizations and participate in global or sector-specific information-sharing communities.

Security and Privacy: While sharing threat data is essential for collective defense, MISP also prioritizes the privacy and security of the shared information. The platform allows users to control access to their shared data and apply access restrictions as needed.

Event and Attribute Management: In MISP, threat data is organized into events, which can contain multiple attributes (e.g., indicators). This structure provides a clear way to manage and understand shared information.

Open Source: MISP is an open-source project, and its code is available on GitHub. This allows organizations to deploy and customize the platform to meet their specific

requirements and integrate it into their existing security infrastructure.

MISP has become an integral part of threat intelligence sharing efforts and collaboration within the cybersecurity community. By providing a standardized and structured way to share threat information, it helps organizations better defend against cyber threats and respond to incidents more effectively.

● Your college network information

Deploying a SOC is a complex and resource-intensive process that requires careful planning and ongoing dedication to maintaining security operations. It is essential for protecting an organization's digital assets and data in an increasingly complex threat landscape.
Deploying a SOC is a complex and resource-intensive process that requires careful planning and ongoing dedication to maintaining security operations. It is essential for protecting an organization's digital assets and data in an increasingly complex threat landscape.

College Website Link:
vtop2.vitap.ac.in
College Website IP Address:
220.158.183.5

● Threat intelligence

Threat intelligence is information that helps organizations understand and defend against cybersecurity threats. It encompasses a wide range of data and analysis related to potential and current cyber threats. The primary goal of threat intelligence is to provide organizations with the knowledge they need to make informed decisions and take proactive steps to protect their digital assets and data. Here are key aspects of threat intelligence:

Types of Threat Intelligence:

Strategic Threat Intelligence: This type of intelligence focuses on long-term trends and provides a high-level view of the threat landscape. It helps organizations make strategic decisions about their security posture.
Operational Threat Intelligence: Operational threat intelligence is more immediate and is used for day-to-day security operations. It includes information about specific threats, vulnerabilities, and attack tactics.
Tactical Threat Intelligence: Tactical threat intelligence is often real-time and includes actionable information to assist in the detection and mitigation of threats.
Sources of Threat Intelligence:

Open Sources: These are publicly available sources of information, such as blogs, news articles, forums, and social media, where threat information may be disclosed or discussed.
Commercial Threat Intelligence Providers: Organizations can subscribe to commercial threat intelligence services that offer curated, timely, and in-depth threat information.
Government and Law Enforcement Agencies: Government agencies, such as CERTs (Computer Emergency Response Teams), often provide threat intelligence to the private sector.
Information Sharing and Analysis Centers (ISACs): ISACs are industry-specific organizations that facilitate the sharing of threat intelligence within particular sectors, like financial services, healthcare, and energy.
[7:33 PM]
Components of Threat Intelligence:

Indicators of Compromise (IOCs): These are specific pieces of data that indicate a potential security threat,

such as IP addresses, domain names, file hashes, or patterns of suspicious behavior.
Tactics, Techniques, and Procedures (TTPs): TTPs describe the methods and strategies employed by threat actors in carrying out cyberattacks. Understanding TTPs helps in identifying and responding to threats.
Context and Attribution: Threat intelligence often provides information about the identity and motivations of threat actors, their tools, infrastructure, and tactics.
Use Cases:

Incident Detection and Response: Threat intelligence can help organizations identify security incidents and respond to them more effectively.
Vulnerability Management: Understanding emerging threats can aid in prioritizing and addressing vulnerabilities in a timely manner.
Security Awareness: Threat intelligence can inform security awareness training for employees, helping them recognize and avoid potential threats.
Compliance and Reporting: Many compliance standards require organizations to use threat intelligence to assess and improve their security posture.
[7:33 PM]
Challenges: Threat intelligence is constantly evolving, and organizations may face challenges in collecting, analyzing, and applying intelligence effectively. It can also be challenging to distinguish between actionable intelligence and noise.

Sharing and Collaboration: Many organizations participate in information-sharing initiatives, sharing threat data and collaborating with trusted partners to enhance their collective defense.

Security Tools: Threat intelligence is often integrated into security tools like SIEMs (Security Information and Event

Management), IDS/IPS (Intrusion Detection System/Intrusion Prevention System), and endpoint security solutions to improve threat detection and response.

Human Expertise: While technology is essential, human analysts play a critical role in making sense of threat intelligence, contextualizing it, and applying it effectively to an organization's security practices.

In summary, threat intelligence is a crucial element of modern cybersecurity, providing organizations with the knowledge and insights needed to defend against a constantly evolving threat landscape. It helps organizations make informed decisions, detect and respond to threats, and proactively strengthen their security posture.

- **Incident response**

Incident response is a structured approach to managing and addressing cybersecurity incidents effectively. A cybersecurity incident is any event that could potentially harm an organization's information systems, data, or overall security posture. Incident response is essential for minimizing the impact of incidents, mitigating threats, and restoring normal operations. Here are the key aspects of incident response:

Preparation:

Incident Response Plan: Organizations develop an incident response plan (IRP), which outlines the procedures, roles, and responsibilities for addressing security incidents. The IRP is a critical component of preparedness and helps ensure a coordinated response.

Incident Response Team: A dedicated incident response team is assembled, consisting of security experts and

relevant stakeholders. This team should include roles such as an incident manager, technical analysts, legal advisors, and communication personnel.

Training and Drills: Regular training and simulation exercises are conducted to prepare the team for various incident scenarios. These exercises help test the effectiveness of the IRP and improve the response process.

Identification:

Event Monitoring: Organizations continually monitor their networks, systems, and applications for security events that might indicate an incident. This involves using security tools and techniques to detect anomalies, such as unauthorized access or unusual patterns of behavior.

Incident Classification: When a potential incident is identified, it is classified based on its severity and impact. This classification helps determine the appropriate response actions.

Containment:

The incident response team takes immediate steps to contain the incident to prevent it from spreading further. This may involve isolating affected systems, disabling compromised accounts, or blocking network traffic associated with the incident.

Eradication:

After containment, the root cause of the incident is identified and eliminated. Vulnerabilities are patched, malware is removed, and any unauthorized access is revoked.

Recovery:

Once the threat is removed, the organization focuses on restoring affected systems and services to normal operation. This includes data recovery, system hardening, and verification of a secure and stable environment.
Lessons Learned:

After the incident is resolved, a post-incident review is conducted to analyze what went well and what could be improved. This information is used to update the incident response plan and enhance security measures.
Documentation:

Throughout the incident response process, detailed records are maintained. These records include information about the incident, response actions, and lessons learned. Documentation is crucial for compliance and future reference.
Communication:

Effective communication is critical during an incident. The incident response team communicates with stakeholders, management, employees, customers, and sometimes the public to provide updates and instructions, maintain trust, and manage the reputation of the organization.
Legal and Regulatory Compliance:
Organizations must consider legal and regulatory requirements when responding to incidents, particularly regarding data breaches. Legal advisors may be involved to ensure compliance with relevant laws.
External Reporting:

In some cases, organizations are required to report incidents to regulatory authorities, law enforcement, and affected parties. Timely and accurate reporting is essential.
Incident response is an ongoing and cyclical process that focuses on minimizing the impact of security incidents,

improving security practices, and enhancing an organization's ability to detect, respond to, and recover from threats effectively. A well-prepared and well-executed incident response plan is a crucial element of a strong cybersecurity strategy.

- **Qradar & understanding about tool**

IBM QRadar is a popular security information and event management (SIEM) solution designed to help organizations monitor, detect, and respond to security incidents and threats effectively. QRadar offers a wide range of features and capabilities that enhance an organization's ability to safeguard its digital assets. Here's an overview of IBM QRadar and its key components:

Log Collection and Normalization: QRadar collects and normalizes logs and events from various sources across an organization's IT infrastructure, including firewalls, network devices, servers, applications, and more. The normalization process standardizes the data for consistent analysis.

Real-Time Event Correlation: QRadar performs real-time correlation of log and event data to identify potential security incidents. It applies predefined rules and policies to detect suspicious patterns and anomalies. Correlation helps in identifying threats and reducing false positives.

Anomaly Detection: QRadar uses machine learning and behavioral analysis to detect unusual and potentially malicious activities that may not be identified by signature-based methods.
Threat Intelligence Integration: QRadar can ingest threat intelligence feeds and use this information to enhance its ability to detect known threats and indicators of compromise (IOCs).

User and Entity Behavior Analytics (UEBA): QRadar includes UEBA capabilities to monitor user and entity behavior for signs of insider threats and abnormal activities. It can identify deviations from normal behavior patterns.

Incident Management: QRadar provides a centralized console for managing security incidents. It helps incident responders track, prioritize, and document incident response activities.

Vulnerability Assessment Integration: QRadar can integrate with vulnerability assessment tools to correlate vulnerabilities with real-time threat data, allowing organizations to prioritize remediation efforts.

Customizable Dashboards: Users can create custom dashboards and reports to visualize security data and key performance indicators (KPIs). These dashboards provide insights into an organization's security posture.
Network Flow Analysis: QRadar can analyze network flows to detect unusual network traffic and patterns that may indicate a breach or cyberattack.

Data Retention and Forensics: The platform stores log and event data for extended periods, facilitating forensic investigations, compliance reporting, and historical analysis.

Compliance Reporting: QRadar includes predefined compliance templates and reporting capabilities to assist organizations in meeting regulatory and industry-specific requirements.

Integration with Other Security Tools: QRadar can be integrated with various security tools and technologies,

such as endpoint detection and response (EDR) solutions, threat intelligence platforms, and incident response tools.

User Access Control: Role-based access control (RBAC) allows organizations to grant appropriate access to different users and roles within the QRadar platform.

Understanding the tools within QRadar requires cybersecurity expertise and training. Effective usage of the platform involves configuring data sources, creating custom rules, tuning alert thresholds, and effectively responding to incidents. QRadar is a versatile and powerful tool, but it's most effective when used by experienced security professionals who understand the intricacies of threat detection and response. IBM typically provides training and certification programs to help users become proficient with QRadar.

Overall, IBM QRadar is a robust SIEM solution that plays a crucial role in modern cybersecurity by helping organizations monitor, detect, and respond to security threats and incidents efficiently.

Conclusion :-

- Stage 1 :- what you understand from Web application testing .
- Stage 2 :- what you understand from the nessus report .
- Stage 3 :- what you understand from SOC / SEIM / Qradar Dashboard .

Topics explored :-
Vulnerabilities of websites,SOC,SIEM,IBM Qradar,Threat Intelligence,MISP,Incident Response Team
Tools explored :- burpSuit,Nessus,Kali Linux Tools

_____THE END_____