Title of the project :- PSNR The Hackers

Overview :-

This report provides an assessment of recent cyber attacks targeting the website of one university. The analysis focuses on identifying the nature of the attacks, potential vulnerabilities exploited, and recommended actions to enhance cybersecurity measures.
We have described the nature and scope of recent cyber attacks. Also we have specified affected components, data, and operations. Phishing, malware, and insider threats are used to compromise the security.
Based on the findings and recommendations outlined in this report, it is crucial for organizations to prioritize cybersecurity enhancements to mitigate future cyber threats effectively. By implementing proactive measures and fostering a culture of cybersecurity awareness, the Organization can significantly strengthen its defenses against evolving cyber threats.

List of teammates–

S.no	Name	Collage	Contact Number
1	Dr. Sunil	Nirma University	7677427797
2	Dr. Ramesh R. Naik	Nirma University	9898750778
3	Dr. Nitin Rathore	Nirma University	9713120420
4.	Mr. Nimeshkumar Patel	NFSU, Gandhinagar	9624433667

List of Vulnerability Table

S.no	Vulnerability Name	CWE - No
1	Incorrect Authorization	863
2	Incorrect Default Permissions	276
3	Improper Control of Generation of Code ('Code Injection')	94
4	Improper Privilege Management	269
5	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	362
6	Missing Authentication for Critical Function	306
7	Server-Side Request Forgery (SSRF)	918
8	Improper Authentication	287
9	Missing Authorization	862
10	Improper Input Validation	20

Stage 1 Report

Vulnerability Name:-: Incorrect Authorization

CWE : - CWE-863

OWASP/SANS Category:- 1425C: 2023

Description:- The product performs an authorization check when an actor attempts to access a resource or perform an action, but it does not correctly perform the check. This allows attackers to bypass intended access restrictions.

Business Impact::- Improper authentication can lead to various security threats, such as: Data breaches: Improper authentication can allow unauthorized users to gain access to sensitive data, leading to data breaches, data loss, or unauthorized access to confidential information.

Vulnerability Name:-: Incorrect Default Permissions

CWE : - CWE-276

OWASP/SANS Category:- 1425B : 2023

Description:- During installation, installed file permissions are set to allow anyone to modify those files.

Business Impact: During the installation process, the software may apply unwanted permissions to directories, files, or other objects, which is called this flaw. As a result, a malicious user may be able to override security requirements that were not intended.

Vulnerability Name:-: Improper Control of Generation of Code ('Code Injection')

CWE : - CWE-94:

OWASP/SANS Category:- 1425B : 2023

Description:- The product constructs all or part of a code segment using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the syntax or behavior of the intended code segment.

Business Impact: If a code injection vulnerability exists in an application, the security impact is that an attacker is able to execute arbitrary server-side code. The ability to execute server-side code can result in a total loss of integrity, availability, and confidentiality within the application.

Vulnerability Name:-: Improper Privilege Management

CWE : - CWE-269

OWASP/SANS Category:- 1425B : 2023

Description:- The product does not properly assign, modify, track, or check privileges for an actor, creating an unintended sphere of control for that actor.

Business Impact: Broken access control vulnerability is a security flaw that allows unauthorized users to access, modify, or delete data they shouldn't have access to. This vulnerability is considered one of the most critical web application security risks.

Vulnerability Name:-: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')

CWE : - CWE-362:

OWASP/SANS Category:- 1425C : 2023

Description:- The product contains a code sequence that can run concurrently with other code, and the code sequence requires temporary, exclusive access to a shared resource, but a timing window exists in which the shared resource can be modified by another code sequence that is operating concurrently.

Business Impact:The adversary targets a race condition occurring when multiple processes access and manipulate the same resource concurrently, and the outcome of the execution depends on the particular order in which the access takes place. The adversary can leverage a race condition by "running the race", modifying the resource and modifying the normal execution flow. For instance, a race condition can occur while accessing a file: the adversary can trick the system by replacing the original file with their version and cause the system to read the malicious file.

Vulnerability Name:-:: Missing Authentication for Critical Function

CWE : - CWE-306

OWASP/SANS Category:- 1425B : 2023

Description:- The product does not perform any authentication for functionality that requires a provable user identity or consumes a significant amount of resources.

Business Impact: When authentication checks are not applied, users are able to access data or perform actions that they should not be allowed to access or perform. The lack of authentication checks can cause the exposure of information, denial of service, and arbitrary code execution.

Vulnerability Name:-: Server-Side Request Forgery (SSRF)

CWE : - CWE-918

OWASP/SANS Category:- 1425B : 2023

Description:- The web server receives a URL or similar request from an upstream component and retrieves the contents of this URL, but it does not sufficiently ensure that the request is being sent to the expected destination.

Business Impact: Server-side request forgery is a web security vulnerability that allows an attacker to cause the server-side application to make requests to an unintended location. In a typical SSRF attack, the attacker might cause the server to make a connection to internal-only services within the organization's infrastructure.

Vulnerability Name:-: Improper Authentication

CWE : - CWE-287

OWASP/SANS Category:- 1425 : 2023

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: If software incorrectly validates user logon information or allows using different techniques of malicious credentials gathering (e.g. brute force, spoofing), an attacker can gain certain privileges within the application or disclose sensitive information. Attackers can exploit improper authentication to gain unauthorized access to resources, such as servers, databases, and applications. Impersonation of legitimate users: Attackers can use stolen or weak credentials to impersonate legitimate users and perform actions on their behalf.

Vulnerability Name:-: Missing Authorization

CWE : - CWE-862

OWASP/SANS Category:- 1425C : 2023

Description:- The product does not perform an authorization check when an actor attempts to access a resource or perform an action.

Business Impact: This vulnerability may allow unauthorized users to access critical business data and perform actions they should not be able to accomplish. This can lead to data breaches, sensitive information loss, and financial losses.

Vulnerability Name:-: Improper Input Validation

CWE : - CWE-20

OWASP/SANS Category:- 1425C : 2023

Description:- The product receives input or data, but it does not validate or incorrectly validates that the input has the properties that are required to process the data safely and correctly.

Business Impact: Improper input validation can enable attacks and lead to unwanted behavior. Parts of the system may receive unintended input, which may result in altered control flow, arbitrary control of a resource, or arbitrary code execution.

Stage 2: Report

NESSUS Vulnerability

Overview

It is essential to do a vulnerability assessment on a University website in order to find and fix any security flaws that an attacker might exploit. Continual monitoring and improvement are crucial to maintaining a strong defense against potential threats, as security is a continual activity. Additionally, it's a good idea to get help from certified cybersecurity specialists if you lack the knowledge necessary to perform an exhaustive assessment.

Check to see if the website works properly on different hardware and browser combinations and is safe. List all vulnerabilities that have been found, their impact, and their degree of vulnerability. Sort patches into criticality groups and assist web developers or the college's IT staff with the restoration process.Note down all vulnerabilities that have been found, their impact potential, and their degree of vulnerability. Help the college's IT staff or web developers with the remediation process by ranking patches according to their criticality.
Experts in cybersecurity and enterprises utilise Nessus, a well-liked vulnerability assessment tool, to find and fix security flaws in their networks, systems, and apps. Following are some of the main applications for Nessus:

Viability Scanning: Automated vulnerability scanning is the main use of Nessus. It looks for misconfigurations and known vulnerabilities by scanning servers, networks, endpoints, and applications. This aids in the identification of possible points of entry for hackers and the prioritization of security initiatives by organizations.

Patch Management: Nessus scan findings tell you what updates and patches are missing for different programmed and operating systems. This facilitates the upkeep of a current and secure IT environment by making sure that important security updates are installed on time.

Compliance Auditing: Nessus can be used to evaluate if a company's setups and systems adhere to legal and industry standards such PCI DSS, HIPAA, as well as CIS and NIST. It aids businesses in finding weaknesses and achieving best practices compliance for security.

Web Application Scanning: Nessus is capable of scanning web applications to find flaws such as SQL injection, cross-site scripting (XSS), and other problems that could put them at risk of attacks.

N**etwork Inventory and Asset Management:** Nessus can offer useful information about the systems and devices connected to the network, helping to maintain an accurate inventory and asset management. An awareness of the attack surface of the network.

Security Awareness and Training: Nessus gives security teams and IT staff valuable insights into the security posture of their systems by producing comprehensive vulnerability reports. Programmes for training and raising security awareness can benefit from this material.

Risk Assessment: Nessus prioritizes an organization's efforts by concentrating on high-risk vulnerabilities first. It does this by assigning severity levels to vulnerabilities that are found.

Support for Penetration Testing: Before more thorough manual testing is carried out, Nessus can offer an initial overview of potential vulnerabilities. This will help to supplement human penetration testing efforts.

Cloud Infrastructure Security: Cloud infrastructure is being used by a lot of companies these days. Nessus can evaluate cloud environments and find vulnerabilities or misconfigurations that could have an impact on the cloud-based resource security.

Continuous Monitoring: Organizations can utilize Nessus to put continuous monitoring techniques into place, which allow them to periodically evaluate their security posture and identify any changes that could introduce novel weaknesses.

Integration of Threat Intelligence: Nessus can be coupled with threat intelligence feeds to compare scan results to known vulnerabilities and threats, offering a more thorough understanding of probable dangers.

Although Nessus is a great tool for finding existing vulnerabilities and misconfigurations, it should only be used as a component of a comprehensive security plan that also addresses new and zero-day threats via continuing security awareness campaigns, manual assessments on a regular basis, and threat hunting.

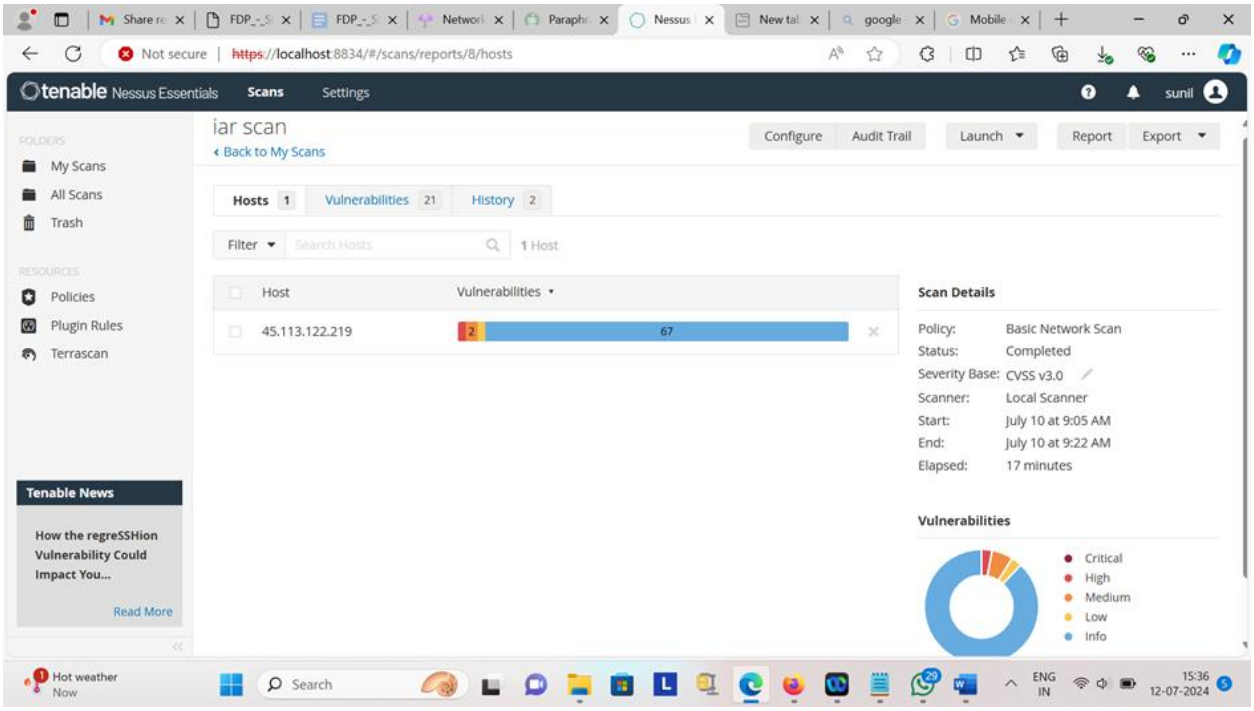
Target WebSite : Institute of Advanced Research, University for Innovation, Gandhinagar website : https://iar.ac.in/
Target IP : 45.113.122.219

S. No.	Vulnerability	Severity	Plugin	Description	Solution	Business Impact	Port
1	SSL Medium Strength Cipher Suites Supported (SWEET32)	High	42873	strength encryption. Nessus regards medium strength as any encryption that uses key lengths	"Reconfigure the affected application if possible to avoid	Medium strength ciphers use encryption methods that may	2083

				at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite. Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.	use of medium strength ciphers."	not be strong enough to resist modern cryptographic attacks, such as brute force or more sophisticated techniques. Compatibility Over Security: These ciphers are often retained for compatibility with older systems and software, but this comes at the cost of reduced security.	
2	SMTP Service Cleartext Login Permitted	Low	54582	The remote host is running an SMTP server that advertises that it allows cleartext logins over unencrypted connections. An attacker may be able to uncover user names and passwords by sniffing traffic to the server if a less secure authentication mechanism (i.e. LOGIN or PLAIN) is used.	"Configure the service to support less secure authentication mechanisms only over an encrypted channel."	Credential Exposure: Usernames and passwords are sent in plain text, making it easy for attackers to capture and misuse them. Data Breach: Compromised credentials can lead to unauthorized access to email accounts,	587

						which can result in data breaches. Man-in-the-Middle Attacks: Attackers can intercept and alter communications between the client and server without detection.	
3.	TLS Version 1.0 Protocol Detection	Medium	104743	"The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible. As of March 31, 2020, Endpoints that arenâ€™t enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors. PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination	Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.	Known Vulnerabilities: TLS 1.0 is susceptible to various attacks, such as BEAST (Browser Exploit Against SSL/TLS). Compliance Issues: Many regulatory standards (e.g., PCI-DSS) require disabling TLS 1.0. Weak Encryption: TLS 1.0 does not support modern, strong cryptographic algorithms.	2083

				points to which they connect) that can be verified as not being susceptible to any known exploits."			
4	TLS Version 1.1 Deprecated Protocol	Medium	157288	The remote service accepts connections encrypted using TLS 1.1. TLS 1.1 lacks support for current and recommended cipher suites. Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1 As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.	Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.	Outdated Cryptography: TLS 1.1 does not support the most current and secure cryptographic algorithms. Compliance Issues: Many regulatory standards (e.g., PCI-DSS) mandate disabling TLS 1.1. Vulnerabilities: Although not as weak as TLS 1.0, TLS 1.1 is still vulnerable to certain attacks and lacks the enhancements introduced in TLS 1.2 and TLS 1.3	2083



Stage 3 :Report

Integrating SOC and SIEM to Achieve Proactive Cybersecurity

- **Soc :**

  In order to continuously monitor an organization's systems, apps, and network, SOC is essential. It is capable of identifying and handling possible security events, such as malware infestations, data leaks, and illegal access attempts. Time is critical in the event of a security crisis. SOC teams are taught to contain and lessen the harm that results from security breaches quickly and skillfully. SOC proactively finds holes and weaknesses in the organization's infrastructure rather than just responding to incidents. Companies may improve their security posture and put safeguards in place to fend off potential threats thanks to this proactive strategy.

  Security analysts are always on guard and prepared to react to new threats at all times of day because to SOC's round-the-clock monitoring. A strong cybersecurity plan must include SOC. As the digital ecosystem grows more interconnected and dangerous, it gives organisations the ability to recognise, stop, and neutralise cyber threats, protecting confidential information, ensuring business continuity, and protecting their brand. Central coordination and communication for incidents is handled by SOC. To ensure a coordinated and effective response to security issues, it makes it easier for different teams, including IT, legal, communications, and top management, to collaborate.

- **Soc Cycle:**

The process that describes the essential actions required in managing an organization's cybersecurity is called the SOC (Security Operations Centre) cycle, sometimes referred to as the SOC workflow or SOC lifecycle. It includes everything from incident response and recovery to threat identification. Typically, the SOC cycle includes the following stages:

Threat Detection and Monitoring:
The network, systems, and applications of the company are continuously monitored to spot any irregularities or potential security concerns. utilising a range of security tools, including firewalls, threat intelligence feeds, intrusion prevention systems, intrusion detection systems, and SIEM (Security Information and Event Management) systems.

Alert Triage and Analysis:
evaluating and ranking security warnings produced by the monitoring tools according to their seriousness and possible consequences. figuring out whether an alert is a false positive or a real security event.
Incident Investigation and Response:
The SOC team investigates an alert thoroughly to determine the scope and nature of the assault if it is determined to be a real security issue.
assembling proof, examining logs, and carrying out digital forensics to ascertain the incident's cause and consequences.
starting the incident response procedure, which can include containing the threat, averting additional harm, and isolating the impacted systems.

Incident Containment and Eradication:
implementing quick measures to contain the issue and stop it from propagating throughout the network of the company.
Restoring the compromised systems to a secure condition by eliminating the threat and removing the harmful components.

Recovery and Remediation:
The SOC team's first goal after neutralising the threat is getting the impacted systems and services back up and running.
putting corrective measures in place to deal with the incident's underlying cause and stop similar attacks in the future.

Post-Incident Analysis and Lessons Learned:
analysing the incident in detail post-mortem in order to determine how it occurred, what effect it had, and what actions were made in response.

determining what aspects of the organization's incident response and security posture need to be improved.
modifying security guidelines and practices in light of the incident's lessons learnt.

Threat Intelligence and Proactive Measures:
To keep ahead of known attack patterns and developing threats, incorporate threat intelligence into the SOC workflow.
actively looking for early warning indicators of possible dangers and weaknesses to prevent them from developing into serious security incidents.

Continuous Monitoring and Improvement:
In order to keep up with the always changing threat landscape, security measures are continuously monitored, analysed, and improved as part of the SOC cycle.
The SOC team may minimise the impact of cyberthreats on the organization's assets and data by adhering to this cycle, which enables them to detect, respond to, and recover from security incidents.

● SIEM
SIGMA An organisation can identify and resolve any security risks and vulnerabilities with the use of security information and event management, or SIEM, before they have an opportunity to interfere with regular business operations. Artificial intelligence (AI) is used by business security teams to automate many of the manual processes involved in threat detection and incident response, and SIEM systems assist them in identifying abnormalities in user behaviour.
advantages It is imperative for all organisations, regardless of size, to adopt proactive measures to identify and address IT security threats. Enterprises can gain from SIEM systems in many ways, and they are now an important part of security process optimisation.

Real-time threat recognition
Over a whole company infrastructure, centralised compliance auditing and reporting are made possible by SIEM solutions. Strict compliance reporting Standards are met while minimising internal resource consumption through the efficient gathering and analysis of system logs and security events made possible by advanced automation.

AI-driven automation
As IT teams manage company security, today's next-generation SIEM solutions interact with robust security orchestration, automation, and response (SOAR) platforms, saving time and resources. These technologies can perform sophisticated threat identification and incident response

protocols far faster than physical teams because to deep machine learning, which automatically learns from network behaviour.

Improved organizational efficiency
SIEM can be a key factor in increasing interdepartmental efficiencies due to the enhanced visibility of IT infrastructures it offers.
Teams can communicate and work together more effectively when responding to threats and security issues when they have a central dashboard that offers a unified view of system data, warnings, and notifications.

Detecting advanced and unknown threats
Organisations need to be able to rely on solutions that can identify and address both known and new security threats, given how quickly the cybersecurity landscape is changing. Security teams may respond to a variety of cyberattacks more skillfully with the use of SIEM solutions, which use AI and integrated threat intelligence feeds. These assaults include:

Insider threats - ssecurity flaws or attacks that come from those who are allowed access to company networks and digital assets.

Phishing - communications that seem to come from a reliable source are frequently used to acquire bank information, login passwords, user names, and other private company data.

Ransomware - malicious software that locks down a victim's information or device and threatens to keep it locked or worse unless the victim pays the attacker a ransom.

Distributed denial of service (DDoS) attacks - attacks that overload systems and networks with excessive traffic from a dispersed botnet (a network of compromised devices), rendering servers and webpages useless.

Data exfiltration –the intentional or unintentional stealing of data from a computer or other device using malware.

Conducting forensic investigations :

After a security incident, SIEM solutions are perfect for carrying out computer forensic investigations. With the help of SIEM systems, businesses can effectively gather and examine log data from all of their digital assets in one location. This enables them to evaluate suspicious activities and put in place more efficient security procedures by reproducing previous instances or analysing new ones.

Assessing and reporting on compliance

Evaluate and document adherence.For many organisations, compliance audits and reporting are important but difficult tasks. By offering real-time audits and on-demand reporting of regulatory compliance when needed, SIEM solutions significantly lower the resource expenditures needed to run this process.

Monitoring Users and Applications

With the growing prevalence of BYOD (bring your own device) rules, SaaS apps, and remote workforces, enterprises want the amount of visibility required to reduce network threats from outside the conventional network perimeter. SIEM solutions greatly increase infrastructure transparency by monitoring all network activity across users, devices, and applications. They also detect threats regardless of the location from which digital assets and services are accessed.

Five Predictions For The Future Of SIEM :

1. Pricing schemes based on usage will proliferate. Teams only pay for the exact amount of data processing and throughput used each month when using these models. This pattern enables service consumption predictability and is consistent with cloud infrastructure platforms like AWS and GCP. There won't be any more pressure on security teams to use less data.

2. As SIEM platforms continue to be decoupled, which has already begun with SOAR derived from SIEM and other extract, transform, and load (ETL) tools, I believe the next stage will involve developing analysis tools on top of a single SIEM data platform. In this approach, the businesses creating tools are able to concentrate on particular industries and create the most reliable, superior, and expandable software.

3. Security firms will form solid alliances as decoupling progresses to offer a tasteful integration and accelerate time-to-value. By referring business to one another, these alliances should advance the security sector, promote mutual corporate growth, and guarantee the greatest user experience for security teams.

4. As cloud services become more accessible, the price and complexity of SIEMs will continue to drop, making it possible for fresher and smaller security teams to become up to speed even faster. The onboarding of data, analysis, and alerting integrations are not simple tasks with traditional SIEMs, as teams may need over six months to get started.
By enhancing quality and simplicity, next-generation SIEMs let security teams work more efficiently and concentrate on important tasks. The productivity of a security team and the financial health of a company will depend on this trend of decreasing starting times.

5. Funding for further businesses to tackle the complex issues of maintaining robust security will not stop. All sizes of businesses, including the big, highly developed Fortune 1000 corporations, are still having security breaches, and venture funding is at an all-time high.
A single corporation won't hold a monopoly on the market share due to healthy competition. Security teams can choose to use alternative platforms if they so choose thanks to this competition. The conflict will then centre on functionality, adaptability, and ease of use.

● Siem Cycle:
A Security Information and Event Management (SIEM) system's lifespan consists of multiple interrelated steps that guarantee the successful installation, running, and upkeep of the SIEM solution. The following stages are commonly included in the SIEM life cycle:

Planning and Assessment:
Considering the organization's security needs and compliance objectives, define the goals and scope of the SIEM installation.
To find weaknesses and determine what needs to be improved, do a comprehensive evaluation of the current security setup, data sources, and log management procedures.
Create a comprehensive deployment strategy for the SIEM solution that outlines the roles, deadlines, and resource allocation.

Design and Architecture:Build the SIEM architecture with performance, redundancy, and scalability in mind, taking into account the organization's needs and data sources.
Ascertain whether deployment model—cloud-based, hybrid, or on-premises—best suits the requirements and available resources of the company.
As you plan the data sources' integration with the SIEM, make sure that pertinent security events are gathered and analysed centrally.

Data Collection and Integration:
To collect logs and events from a variety of sources, including firewalls, network devices, servers, apps, and endpoints, use data collectors and agents.
To enable effective analysis and correlation, normalise and enhance the gathered data.

Set up connections and parsers to allow data feeds from different sources and security devices to be integrated into the SIEM platform.
Correlation and Analysis of Events:
To find harmful activity patterns and security issues, create and improve correlation rules and use cases.
Create actionable warnings for possible security incidents by analysing and correlating events in real-time.

Incident detection and response: Look into possible security incidents in response to notifications that are issued.
To ascertain the extent and significance of detected security occurrences, conduct in-depth analysis.
Start incident response actions, such as cleanup, recovery, and containment.

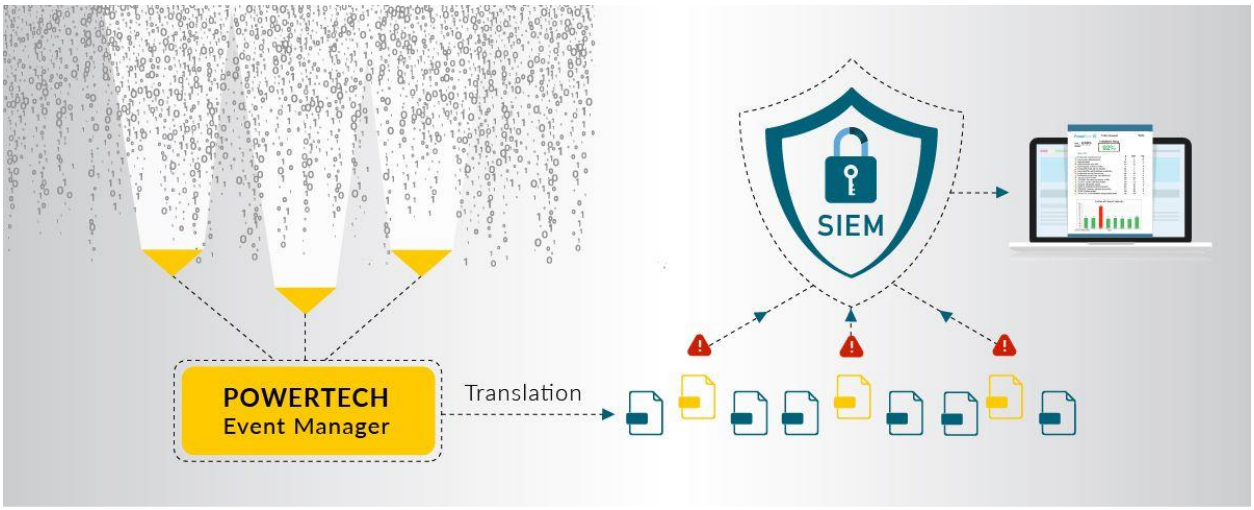
Forensics and investigation: Perform thorough forensic analysis to identify the underlying causes of incidents and the attack vectors.Maintain and record evidence for future legal or regulatory needs.

Reporting and Compliance: Create and deliver security dashboards and reports to CEOs, IT management, auditors, and regulatory bodies, among other stakeholders.
Monitor and report on security events and incidents to ensure adherence to pertinent industry standards and legislation.
Continuous Maintenance and Monitoring: To ensure peak performance, keep an eye on the SIEM infrastructure and make necessary configuration adjustments.
Maintain the effectiveness of the SIEM against emerging risks by routinely updating correlation rules, threat intelligence feeds, and other components.
To find opportunities for improvement, do recurring evaluations and assessments of the SIEM's efficacy and performance.

Instruction and Transfer of Knowledge: Educate SOC employees and IT professionals on how to use the SIEM system efficiently.
Encourage the organisation to share best practices and knowledge gained from incident investigations and analysis.
Every stage of the SIEM lifecycle builds on the knowledge and expertise acquired in earlier ones, and it is an ongoing, iterative process. By using this strategy, organisations can be guaranteed that the SIEM solution will always be useful, efficient, and effective in identifying and addressing security threats.

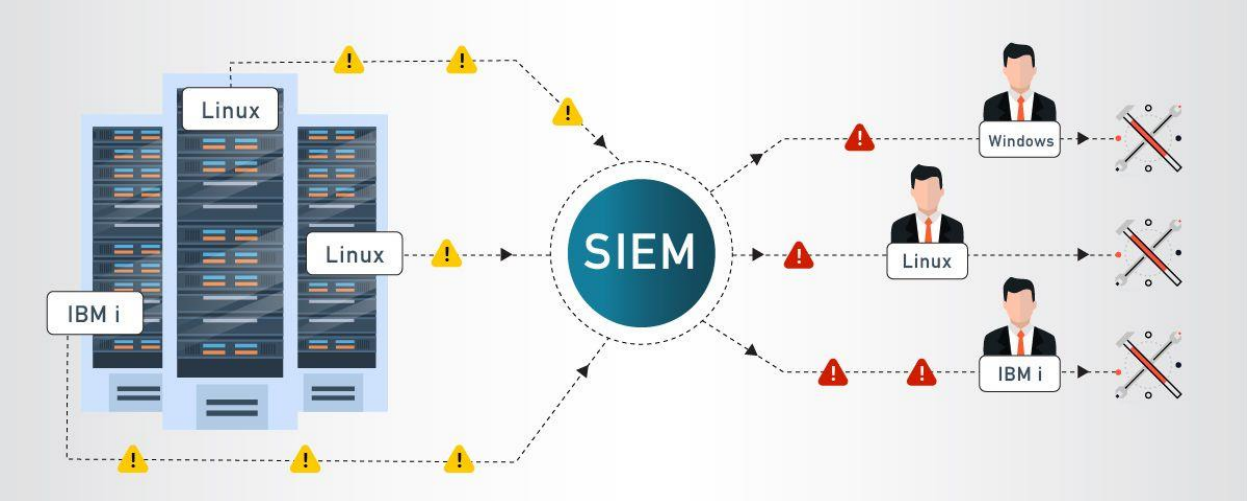
Threat Detection

Translation



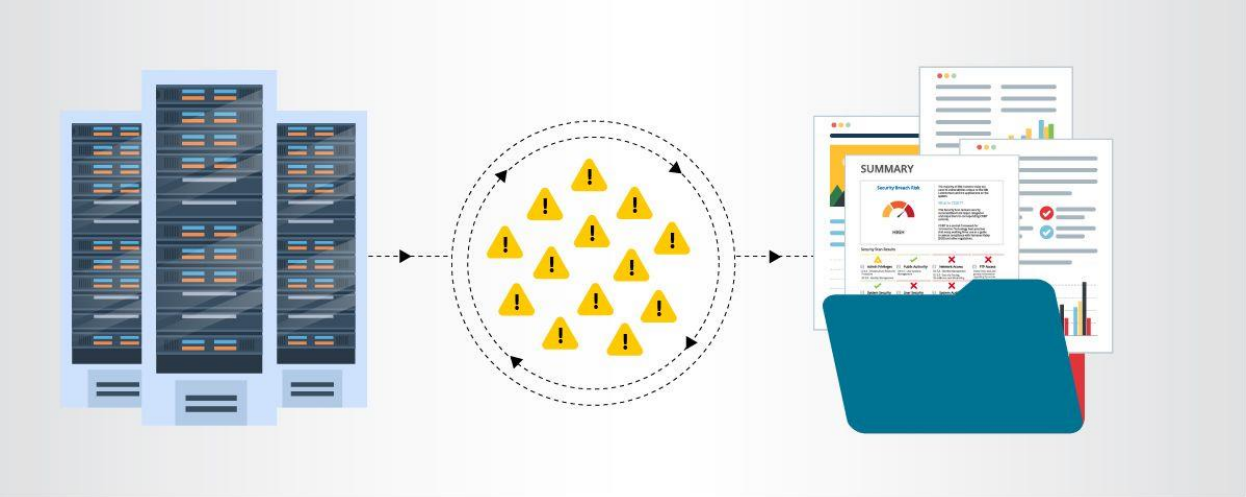
Prioritization

Escalation



Analysis

Compliance



● MISP

Core features of the Malware Information Sharing Platform and Threat Sharing, or MISP, include: An effective indicators database and IOC that stores both technical and non-technical data regarding malware samples, incidents, attackers, and intelligence.

Features of MISP, the open source threat sharing platform
An information platform for threat intelligence that allows the exchange, archiving, and correlation of threat intelligence, financial fraud, vulnerability, and even counterterrorism indicators of compromise of specific assaults. Find out how MISP is currently being used by various organisations. In addition to storing, exchanging, and working together on malware analysis and cyber security indicators, the information and IoCs can be used to identify and stop threats, attacks, and frauds against ICT infrastructures, businesses, or individuals.
The ability to store technical and non-technical data on malware samples, incidents, attackers, and intelligence is provided by an effective IoC and indicators database.

A data architecture with flexibility that allows complicated things to be linked and presented in order to convey occurrences, threat intelligence, or related aspects.
Integrated sharing features to make data sharing across distribution models easier. Events and properties across various MISPs can be automatically synchronised. To comply with each organization's sharing policy, advanced filtering features, such as an attribute-level distribution process and a flexible sharing group capacity, can be employed.

An easy-to-use interface enabling end users to create, edit, and work together on attributes and indicators. An intuitive graphical user interface for moving between events and their relationships. Create and view relationships between objects and attributes using the event graph feature. To assist analysts in contributing events and attributes, advanced filtering features and a warning list are provided.

storing information in an organised manner with strong support for fraud and cyber security indications, similar to what is seen in the financial industry, to enable automated usage of the database for a variety of uses.

To integrate with other systems (network IDS, host IDS, custom tools),
export: generate IDS (Suricata, Snort, and Bro are supported by default), OpenIOC, plain text, CSV, MISP XML, or JSON output.
Import: bulk-import, batch-import, free-text import, import from OpenIOC, GFI sandbox, ThreatConnect CSV or MISP format.

MISP users can suggest modifications or updates to characteristics/indicators through a gentle method for collaboration on events and attributes.

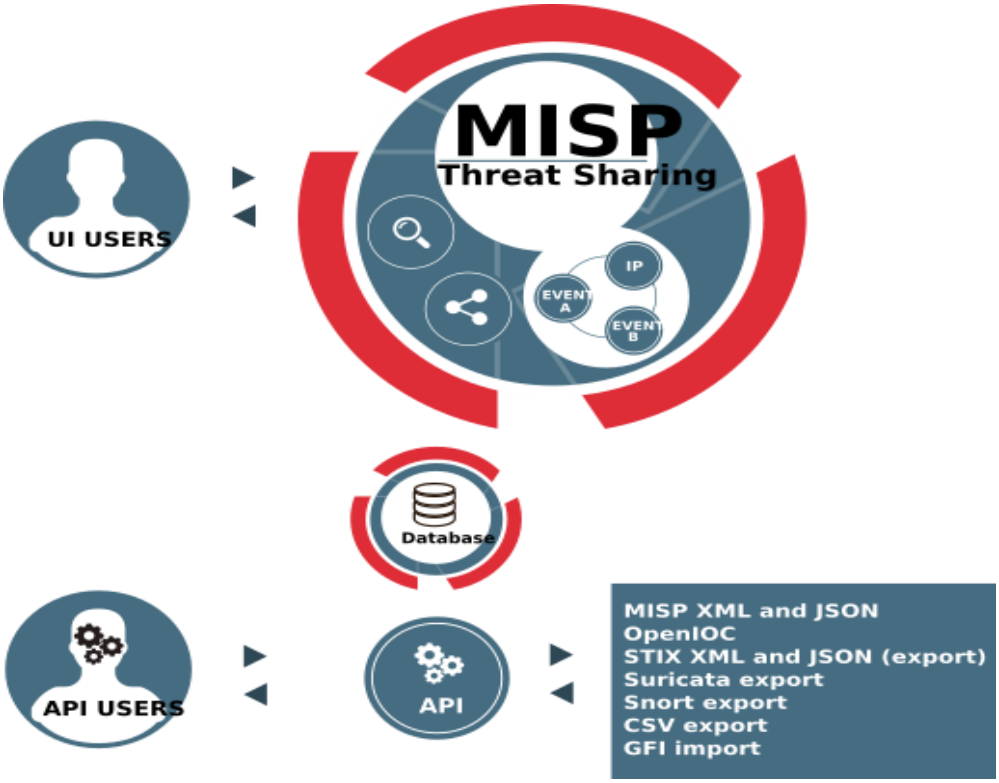
Data-sharing is the automatic MISP-based synchronisation and exchange of information with other parties and trust groups.
A versatile method for integrating and importing threat intelligence and open-source intelligence feeds from outside sources is feed import. Standard MISP installations come with a number of default feeds installed.
Delegating sharing enables an organisation to assign the dissemination of events or indicators to another party using a straightforward pseudo-anonymous method.
Adaptable API to incorporate MISP into your own programmes. PyMISP, a versatile Python library that can handle malware samples, search for attributes, and fetch, add, or change event attributes, is packed with MISP.

Adaptable taxonomy allows you to tag and classify events using pre-existing taxonomies or your own custom classification schemes. In addition to being local to your MISP, the taxonomy can be shared with other MISP instances. A default collection of widely recognised taxonomies and classification schemes is included with MISP to facilitate standard categorization, which is utilised by numerous organisations such as ENISA, Europol, DHS, and CSIRTs.

Support for STIX: export and import of data in STIX 2.0 format, as well as data export in XML and JSON formats.
incorporated PGP, S/MIME, or both encryption and signing of the notifications, based on user preferences.
A real-time publish-subscribe channel within MISP that allows for the automatic retrieval of all changes (such as new events, indications, sightings, or tagging) in Kafka or ZMQ (such as the misp-dashboard).

MISP enables you to automatically import data into your detection systems, leading to better and faster intrusion detection through the generation of STIX, OpenIOC, text, or csv exports, as well as Snort/Suricata/Bro/Zeek IDS rules.
Furthermore options for importing data include batch import, OpenIOC, free-text import, sandbox result import, and custom or predefined template import. Data can also be uploaded and downloaded automatically from and to externally hosted MISP instances if MISP is operating internally. You no longer need to put in any extra work to obtain useful compromise indicators because of this automation and the efforts of others.

cooperative exchange of correlation and analysis
How often has your team completed an analysis only to find out afterwards that a team member had previously worked on a comparable threat? or that a report from outside has already been produced? MISP will instantly display relationships with other observables and indicators as new data is introduced. This leads to an analysis that is more effective while also giving you a clearer understanding of the TTPs, associated campaigns, and attribution.



Organization network information

A total of 24 labs and approximately 1200 systems are available.

- How you think you deploy soc in your college
  Deploying a Security Operations Center (SOC) in an organization involves careful planning, resource allocation, and a structured approach. Here are the key steps to deploy a SOC:

Assessment and Requirements Gathering:

- Evaluate the organization's present cybersecurity posture in detail, taking into account all of the tools, procedures, and security measures in place.

Determine the precise security obstacles, hazards, and regulatory obligations that a SOC will tackle.

- Establish the SOC deployment's aims and objectives in accordance with the organization's overall security plan.

Budget and Resource Allocation:

- Allocate staff, hardware, software, and other resources required to support the SOC operations. Establish the financial and resource needs for setting up and maintaining the SOC.

Create a Skilled Team:

- Assemble the SOC team by hiring or allocating qualified security experts.
- The team should consist of threat hunters, security analysts, incident responders, and SOC management staff.

Infrastructure and Technology Setup:

- Assemble servers, network hardware, and storage as well as the real or virtual infrastructure for the SOC.
- Install the necessary security solutions, including firewalls, endpoint protection, intrusion detection and prevention systems (IDS/IPS), SIEM, and threat intelligence feeds.

Data Collection and Integration:

- Centralise the collection of log and event data by integrating security systems and tools with the SIEM.
- Verify that pertinent data sources are submitting logs to the SIEM, including servers, firewalls, network devices, and apps.

Create Processes and Procedures:

- Standard operating procedures (SOPs) for incident handling, response protocols, escalation procedures, and communication guidelines should be defined for different SOC activities. Put incident classification and prioritisation procedures into action.

Execute Monitoring and Alerting:

- Set up the SIEM to provide alerts in real time according to pre-established correlation criteria and security use cases. Adjust levels for alerts to reduce false positives and concentrate on important warnings.

Escalation and Incident Response:

- Create a formal incident response strategy that describes what should be done in case of a security occurrence.
- Clearly define roles and duties for managing occurrences, and provide a defined route for reporting serious incidents.

Training and Skill Development:

- Give the SOC team thorough instruction on event analysis, threat hunting, incident response best practices, and the use of security tools.
- Keep the group informed about the most recent advancements in cybersecurity, including attack strategies and certifications.

Testing and Continual Improvement:

- Test the SOC team's reaction skills through regular tabletop exercises and realistic cyberattack situations. To enhance and optimise the SOC's procedures and processes, apply the knowledge acquired from testing.

Monitoring and Reporting:

- Constantly assess how well the SOC is performing in terms of identifying and handling security events.
- Create measurements and reports on a regular basis to assess the SOC's effectiveness and convey its importance to stakeholders.

Connectivity with IT and Business Functions:

- Promote cooperation between the SOC and other IT and business divisions to guarantee a synchronised security strategy. Talk to the board and upper management to get their support and buy-in for SOC initiatives.
- SOC deployment is a continuous process that calls for flexibility and constant advancement. Maintaining the SOC's efficacy in handling the organization's changing security problem requires regular evaluations, training, and modifications.
- Threat intelligence

Data that is gathered, processed, and examined in order to comprehend the goals, objectives, and attack patterns of a threat actor is known as threat intelligence. Threat intelligence helps us to shift from reactive to proactive behaviour in the battle against threat actors by enabling us to make security decisions more quickly, more intelligently, and with evidence to support them.

Threat intelligence is important for the following reasons:

- clarifies the unclear, empowering security teams to make wiser choices Enhances the ability of cyber security stakeholders to make informed decisions by exposing the tactics, techniques, and procedures (TTPs) of adversaries.
- Aids security experts in comprehending the decision-making process of threat actors.
- Empowers business stakeholders, including executive boards, CISOs, CIOs, and CTOs, to make better decisions, reduce risk, and invest their money.

From top to bottom, threat intelligence offers unique advantages to every member of a security team, including:

- Sec/IT Analyst
- SOC
- CSIRT
- Intel Analyst
- Executive Management

- Incident response

- A clear incident response plan ought to be in place for all organisations, at the very least. This plan should specify what the organisation considers an incident and outline a precise, well-defined procedure that must be followed in the event that one arises.
- It's also a good idea to identify the teams, workers, or leaders who are in charge of overseeing the incident response initiative as a whole and who are accountable for carrying out each of the actions listed in the incident response plan.

Which Person Responds to Incidents?

Usually, an organization's cyber incident response team, sometimes referred to as the computer incident response team (CIRT), handles incident response. Members of the legal, human resources, and public relations departments are typically included in CIRTs, in addition to security and general IT personnel. CIRTs are tasked with responding to security breaches, viruses, and other potentially catastrophic situations in companies that face severe security risks, according to Gartner's description of the group. It should include professionals who can advise firm executives on proper communication following such situations, in addition to technological specialists qualified to handle particular dangers.

Six Steps for Effective Incident Response

Preparation :

Being ready for the eventual security breach is the most crucial stage of incident response. The process of preparation, which includes policy, communication, documentation, identification of CIRT members, access control, tools, and training, aids organisations in gauging the effectiveness with which their CIRT will be able to handle an incident.

Identification :

The process of identification involves locating occurrences as soon as possible to allow for a quick response, which lowers expenses and damages. IT personnel gathers events from log files, monitoring tools, error messages, intrusion detection systems, and firewalls to discover and ascertain occurrences and their extent in this phase of successful incident response.

Containment :

The first priority after an event is discovered or identified is to contain it. As said in step number two, the sooner events are discovered, the sooner they may be contained to minimise harm. The primary goal of containment is to limit the damage and stop more damage from happening. It is noteworthy that all of the containment phase's SANS-recommended actions ought to be followed, particularly the one to “avoid the destruction of any evidence that may be needed later for prosecution.”

Three of these processes are system backup, long-term containment, and short-term containment.

Eradication :

Eradication is the step of effective incident response that involves eliminating the threat and, ideally, minimising data loss, returning afflicted systems to their pre-attack state. Ensuring that all necessary precautions have been performed up to this stage, such as removing the harmful information and making sure the impacted systems are entirely clean, are the primary acts related to eradication.

Recovery:

The primary responsibilities related to this incident response stage include testing, monitoring, and validating systems as they are put back into production to ensure they are not compromised or re-infected. In this phase, decisions are also made regarding the best time and date to resume operations, the compromised systems are tested and verified, anomalous behaviours are observed, and methods for testing, monitoring, and validating system behaviour are used.

Lessons Learned :

A crucial part of incident response is the lessons learned phase, which aids in enlightening and enhancing subsequent incident response initiatives.

In addition to updating their incident response plans with any information that may have been overlooked during the incident, organisations can take advantage of this step to ensure that all paperwork is comprehensive and available in case of future incidents. Lessons learned reports provide an in-depth analysis of the entire incident and can be utilised as training materials for new members of the CIRT, at recap sessions, or as standards for comparison.

The series of actions an organisation takes in the wake of a cybersecurity event is known as the incident response process. Businesses should keep records of their incident response plans and procedures, including details on who is in charge of carrying out the various tasks included in them. It is far more difficult for a corporation to effectively respond to and recover from cyberattacks if they do not have an incident response plan.

The incident response method comprises five steps, sometimes known as pillars.

Identify – Organisations must recognise all forms of dangers and the resources they may compromise. This entails making a risk assessment and taking an environment inventory.

Protect: Every important asset has to be covered by a protection plan that includes employee security awareness training and protective technology solutions.

Detect - Organisations try to find dangers early on in this process so that they can't have a chance to seriously harm the environment.

React: Upon detection of a threat or incident, a well-defined plan of action needs to be implemented to minimise harm and stop it from spreading to other infrastructure elements.

Recover: The affected system resumes regular operations after completing the recovery stage. Additionally, it assesses the incident's origin.

What is the NIST incident response model?

The NIST incident response model involves four phases recommended to effectively handle cybersecurity incidents.

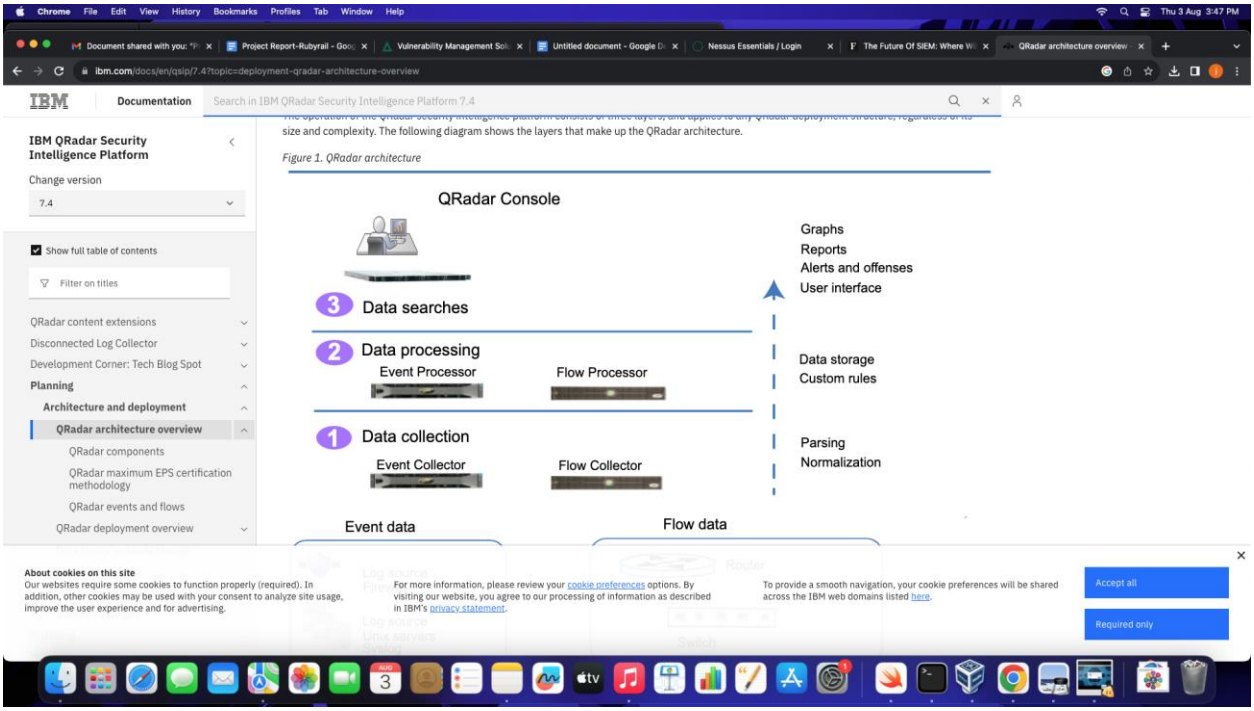
Preparation - Organizations should take the necessary steps to be prepared for a cybersecurity incident when one occurs.

Detection and analysis - The cybersecurity response team is responsible for detecting and analyzing incidents to determine how to proceed and who needs to be notified.

Containment, eradication, and recovery: Following an incident, the response team should work to prevent further spread of the threat, eliminate it from the surrounding area, and start the process of restoring any compromised systems.

Post-incident activity: The goal of post-incident activity is to determine the lessons learnt and apply them to fortify defences in order to reduce the likelihood of future incidents that are similar.

- Qradar & understanding about tool



Regardless of the size or quantity of components in a deployment, the QRadar architecture operates in an identical manner. The fundamental features of every QRadar system are represented by the following three layers in the diagram.

Data collection :

Event data collection and flow collecting are the main functions of QRadar SIEM.Event data is a representation of things that happen in the user's environment at a specific moment, like email connections, VPN connections, firewall denies, proxy connections, user logins, and anything else you might want to record in your device logs.

Flow data, which QRadar converts into flow records, is network activity information or session information shared by two hosts on a network. In order to create flow records—which essentially depict a session between two hosts—Quadar transforms or normalises raw data into IP addresses, ports, byte and packet counts, and other information. Full packet capture is possible with the QRadar Incident Forensics component in addition to gathering flow data with a Flow Collector.

Data processing:

An All-in-One appliance can process both event and flow data; additional event or flow processors are not required. You might need to add Event Processors, Flow Processors, or any other processing appliance to address the additional requirements if the All-in-One appliance's

processing capability is surpassed. It's possible that you'll also need more storage, in which case adding Data Nodes can help.

Additional features that gather different kinds of data and offer more capabilities are QRadar Risk Manager (QRM), QRadar Vulnerability Manager (QVM), and QRadar Incident Forensics.

Your network topology is mapped out and network infrastructure configuration is gathered by QRadar Risk Manager. By simulating different network scenarios and making changes to setups and rules in your network, you may utilise the data to manage risk.

To scan your network for vulnerabilities and handle the information gathered from other scanners like Nessus and Rapid7, use QRadar Vulnerability Manager. The information gathered about vulnerabilities is utilised to pinpoint different security threats within your network.

Use QRadar Incident Forensics to perform in-depth forensic investigations,
and replay full network sessions.

Data searches :

All data is gathered, processed, and stored on the All-in-One appliance in an All-in-One system.

The QRadar Console does not handle event and flow processing or storage in distributed systems. Rather, the main purpose of the QRadar Console is to serve as the user interface for searches, reports, alarms, and investigations.

The components of QRadar

Managing data collection and processing across distant networks and scaling a QRadar system are made easier with IBM QRadar components.

Certification technique for QRadar Maximum EPS

The maximum events per second (EPS) rate that IBM QRadar appliances can sustain is certified. System configuration, system load, and the type of data handled all affect maximum EPS.

Events and flows in QRadar

Network security management through flow and event monitoring is one of IBM QRadar SIEM's primary uses.

Conclusion

Stage 1 :- what you understand from Web application testing .

Web application testing gives the assurance that the programme is dependable, safe, and functions as intended. Finding and fixing potential flaws, vulnerabilities, and usability is the goal of the testing process. Problems that can affect the functionality and user experience of the programme. Web application testing is the process of evaluating and verifying that a web application functions correctly and meets specified requirements before it goes live. This involves a variety of testing types and methodologies to ensure the application is reliable, secure, and performs well under different conditions. Here's an overview of the key aspects of web application testing:

Functional Testing: Ensures that the application works according to the specified requirements. This includes testing all features, such as forms, buttons, links, and other user interactions.

Usability Testing: Evaluates how user-friendly and intuitive the application is. This involves testing the navigation, layout, and overall user experience.

Interface Testing: Checks the interaction between different components of the application, including the server, database, and web services. It ensures that data is correctly exchanged and processed.

Compatibility Testing: Verifies that the application works across different browsers, devices, and operating systems. This ensures a consistent experience for all users.

Performance Testing: Measures the application's performance under various conditions, such as load testing (how it performs under heavy traffic) and stress testing (how it handles extreme conditions).

Security Testing: Identifies vulnerabilities and potential threats to the application. This includes testing for common security issues like SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF).

Database Testing: Ensures the application's database performs correctly, including data integrity, data retrieval, and data storage processes.

Regression Testing: Ensures that new code changes do not adversely affect existing functionalities. This involves re-running previous tests to confirm that existing features still work as expected.

Acceptance Testing: Conducted to determine if the application meets the acceptance criteria and is ready for deployment. This is often performed by the end-users or clients.

Effective web application testing requires a combination of manual and automated testing approaches. Automation tools (like Selenium, JUnit, and LoadRunner) are commonly used to streamline repetitive tasks and enhance testing efficiency.

The goal of web application testing is to identify and fix any issues before the application is released to users, ensuring a high-quality, robust, and secure application.

Stage 2 :- what you understand from the nessus report.

A Nessus report is the output generated by Nessus, a widely used vulnerability assessment tool developed by Tenable, Inc. Nessus scans a network or a specific system for vulnerabilities that could be exploited by attackers. Understanding a Nessus report involves interpreting various sections and details provided in the report to identify and mitigate security risks. A thorough understanding of a Nessus report is essential for effective vulnerability management and for maintaining the security posture of an organization.

Stage 3 :- what you understand from SOC / SEIM / Qradar Dashboard.

Security Operations Centers (SOCs) use Security Information and Event Management (SIEM) tools like IBM QRadar to monitor, detect, and respond to security incidents. A SOC/SIEM/QRadar dashboard provides a centralized view of security-related data and alerts. Here's an overview of each component and what they typically display:

Security Operations Center (SOC)

A SOC is a centralized unit that deals with security issues on an organizational and technical level. It involves:

Monitoring: Continuous monitoring of network traffic, systems, and data for potential security threats.
Detection: Identifying unusual activities or anomalies that could indicate a security incident.
Response: Taking appropriate actions to mitigate identified threats and prevent damage.
Analysis: Investigating security incidents to understand their impact and origin.
Reporting: Generating reports for management and compliance purposes.

Security Information and Event Management (SIEM)

SIEM tools aggregate and analyze security data from across the network to provide a comprehensive view of an organization’s security posture. They offer:

Log Collection: Gathering log data from various sources such as firewalls, intrusion detection/prevention systems (IDS/IPS), and servers.

Event Correlation: Linking related security events to identify patterns that may indicate a security threat.
Alerting: Generating alerts for potential security incidents based on predefined rules and patterns.
Reporting: Creating detailed reports on security events, trends, and compliance status.
Forensic Analysis: Enabling detailed investigation of security incidents.

QRadar Dashboard
IBM QRadar is a popular SIEM solution. Its dashboard typically includes:

Summary Overview

Security Posture Summary: High-level view of the current security status, including key metrics and trends.
Incident Overview: Summary of recent and ongoing security incidents.
Alerts and Incidents

Real-time Alerts: List of current security alerts, categorized by severity (e.g., critical, high, medium, low).
Incident Management: Details on open incidents, their status, assigned analysts, and response actions.
Log Activity

Log Volume: Charts showing log volume over time, which can help detect unusual spikes or drops.
Log Sources: Breakdown of log data by source (e.g., firewalls, servers, endpoints).
Offense Management

Offense List: Detailed list of offenses (grouped security events) with information on severity, source, destination, and description.
Offense Details: In-depth view of individual offenses, including timeline, related events, and impacted assets.
Network Activity

Network Traffic Analysis: Visualizations of network traffic patterns, highlighting unusual activity or potential threats.
Flow Data: Information on network flows, including source/destination IPs, ports, and protocols.
User Activity

User Behavior Analytics: Monitoring user activity to detect anomalies that could indicate insider threats or compromised accounts.
Access Logs: Details on user access to systems and data.

Compliance Reporting

Compliance Status: Overview of compliance with relevant standards and regulations (e.g., PCI DSS, HIPAA).
Audit Reports: Detailed reports for auditors and regulatory bodies.
Threat Intelligence

Threat Feeds: Integration with external threat intelligence sources to provide context on emerging threats.
Indicators of Compromise (IoCs): Information on known IoCs to aid in threat detection and response.
Key Features and Benefits
Centralized Visibility: Provides a unified view of the security landscape, making it easier to detect and respond to threats.
Automated Alerting: Reduces the need for manual monitoring by automatically generating alerts for potential threats.
Advanced Analytics: Uses machine learning and advanced analytics to identify patterns and anomalies that may indicate security issues.
Incident Response: Streamlines incident response by providing tools for investigation, analysis, and remediation.
Compliance Management: Helps ensure compliance with industry regulations and standards by providing detailed reporting and audit trails.
Understanding and effectively using a SOC/SIEM/QRadar dashboard is crucial for maintaining a strong security posture, quickly detecting threats, and efficiently responding to incidents.

Topics explored :-
Introduction to cybersecurity, Growth of cybersecurity, Data sanity, Cloud service and cloud security, Data breach, Firewall, Antivirus, Digital ecosystem, Data protection, Types of cyber attacks, Essential terminology, Introduction to networking, Web APIs, web hooks, Web shell concepts, Vulnerability stack,OWASP top 10 applications, QRadar, SOC, SIEM

Tools explored :-
Nessus, cybermap.kaspersky.com, thehackersone.com, OWASP top 10 vulnerabilities(2021), thehackersnews.com, CWE, exploitDB, virtual box, live websites-bugcrowd, nslookup.io, OSINT framework, mitre framework, IBM fix central, QRadar Installation, mobaxterm, tools-nmtui, Nmap, sqlmap, Identify fixes-wincollect agent, metasploitable, malware bytes, Linux cheatsheet, QRadar for SOC dashboard presentation, Kali linux