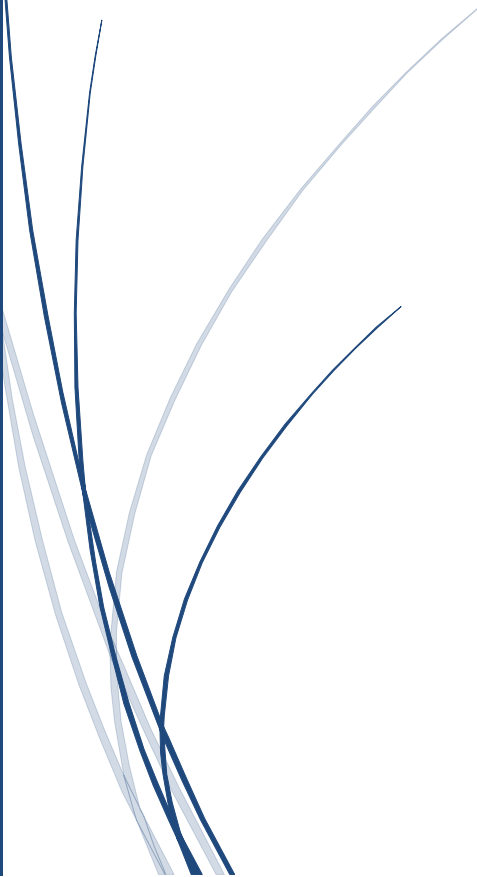




8/27/2023

# Team – III

Stage- I



Dr.Arpit Jain, Ms.D.Sailaja, Ms.B.Sudha Rani, Dr.  
R.Dinesh

## **A TrustDefender**

### **Part I-Executive summary**

#### **Overview**

Implementing cybersecurity in an organization involves a comprehensive and proactive approach to protect its digital assets, data, and infrastructure from cyber threats. The steps to implement cybersecurity effectively at every organization include:

- Develop a clear and well-defined cybersecurity policy and strategy that aligns with the organization's business objectives and risk tolerance.
- Conduct a thorough risk assessment to identify potential cybersecurity threats and vulnerabilities specific to the organization. Prioritize risks based on their potential impact and likelihood of occurrence. Implement risk mitigation measures and create a risk management plan to address identified vulnerabilities.
- Train all employees on cybersecurity best practices and the role they play in safeguarding the organization's information. Educate them about phishing, social engineering, password hygiene, and other common attack vectors to promote a security-conscious culture.
- Implement strong access control measures to ensure that only authorized personnel can access sensitive data and critical systems. Utilize multi-factor authentication (MFA) for an extra layer of security.
- Deploy firewalls, intrusion detection/prevention systems (IDS/IPS), and secure gateways to monitor and control network traffic

- Install antivirus software, endpoint protection tools, and host-based firewalls on all devices to defend against malware and other threats at the device level.
- Install antivirus software, endpoint protection tools, and host-based firewalls on all devices to defend against malware and other threats at the device level.
- Encrypt sensitive data both at rest and in transit to prevent unauthorized access and ensure data confidentiality.
- Establish a systematic process to apply security patches and updates promptly to all software, operating systems, and firmware to address known vulnerabilities.
- Develop a well-defined incident response plan (IRP) to handle cybersecurity incidents effectively. The plan should include clear guidelines on identifying, reporting, containing, eradicating, and recovering from security incidents.
- Conduct regular internal and external security audits and assessments to evaluate the organization's security posture and identify potential weaknesses or gaps.
- Monitoring and Logging: Implement centralized logging and real-time monitoring of network and system activities to detect and respond to suspicious activities promptly.
- Establish clear channels for reporting security incidents and communicating with stakeholders, including employees, customers, partners, and regulatory authorities.

**IP address of irctc.com 103.116.163.23**

## **2. Team Members Involved in vulnerability Assessment**

<b>S.No</b>	<b>Name</b>	<b>Designation</b>	<b>Mobile Number</b>
1	Dr.Arpit Jain	Professor	9411294039 <a href="mailto:arpitjain@kluniversity.in">arpitjain@kluniversity.in</a>
2	Ms.D.Sailaja	Assistant Professor	8985010108 <a href="mailto:ksailaja@kluniversity.in">ksailaja@kluniversity.in</a>
3	Ms.B.Sudha Rani	Assistant Professor	9959377648 <a href="mailto:bsudharani@kluniversity.in">bsudharani@kluniversity.in</a>
4	Dr.R.Dinesh	Professor	9486399714 <a href="mailto:dineshrajavellu@kluniversity.in">dineshrajavellu@kluniversity.in</a>

## **3. List of Vulnerable Parameter, location discovered**

S.No	Name of the Vulnerability	Reference CWE
1	Broken Access Control	CWE 284- Improper Access Control
2	Cryptographic Failures	CWE-310:Cryptographic Issues
3	Injection	CWE-74-Improper Neutralization of special element in output is used by a downstream component.
4	Insecure Design	CWE-657: Violation of secure design principles
5	Security Misconfiguration	CWE-16:Configuration
6	Vulnerable and Outdated Components	CWE-1104: Use of Unmaintained Third Party Components
7	Identification and Authentication Failures	CWE-306: Missing Authentication for Critical Function
8	Software and Data Integrity Failures	CWE-1214: Data Integrity Issues
9	Security Logging and Monitoring Failures	CWE-778: Insufficient Logging
10	Server Side Request Forgery	CWE-918:Server Side Request Forgery

## **1. CWE: CWE 284- Improper Access Control**

**OWASP CATEGORY : A01 2021 Broken Access Control**

**DESCRIPTION:** The product does not restrict or incorrectly restricts access to a resource from an unauthorized actor.

**BUSINESS IMPACT:** Improper access control in a business environment can have significant negative impacts on various aspects of the organization. Access control refers to the processes and mechanisms that ensure the right people have appropriate access to resources, systems, and data while preventing unauthorized individuals from gaining access. Here are some potential business impacts of improper access control.

## **2. CWE: CWE-310: Cryptographic Issues**

**OWASP CATEGORY : A02 2021 Cryptographic Failures**

**DESCRIPTION:** Weaknesses in this category are related to the design and implementation of data confidentiality and integrity. Frequently these deal with the use of encoding techniques, encryption libraries, and hashing algorithms. The weaknesses in this category could lead to a degradation of the quality data if they are not addressed.

**BUSINESS IMPACT:** Cryptographic failures in a business context can have serious and wide-ranging impacts on various aspects of the organization's operations, security, and reputation. Cryptography is the practice of using techniques to secure communication and protect information through encryption, decryption, and other security measures.

## **3. CWE: CWE 74: Improper Neutralization of Special Elements in Output Used by a**

**Downstream Component ('Injection')**

**OWASP CATEGORY : A03 2021 Injection**

**DESCRIPTION:** The product constructs all or part of a command, data structure, or record using externally-influenced input from an upstream component, but it does not neutralize

or incorrectly neutralizes special elements that could modify how it is parsed or interpreted when it is sent to a downstream component.

**BUSINESS IMPACT:** SQL injection is a type of cyberattack where malicious SQL code is inserted into input fields of a web application, with the intent to manipulate the application's database. This can have severe consequences for businesses, as it can lead to unauthorized access to data, data breaches, and various other negative impacts.

#### **4. CWE: CWE 657: Violation of Secure Design Principles**

**OWASP CATEGORY : A04 2021 Insecure Design**

**DESCRIPTION:** The product violates well-established principles for secure design.

**BUSINESS IMPACT:** Insecure design in a business context refers to the development of products, systems, or applications with inherent security vulnerabilities or flaws. These vulnerabilities can be exploited by malicious actors to compromise the security and integrity of the business's operations.

#### **5. CWE: CWE 16-Configuration**

**OWASP CATEGORY : A05 2021 Security Misconfiguration**

**DESCRIPTION:** Weaknesses in this category are typically introduced during the configuration of the software.

**BUSINESS IMPACT:** The configuration of an organization's IT systems, networks, and software plays a crucial role in maintaining security, efficiency, and functionality. Improper or inadequate configuration can lead to various negative impacts on a business.

#### **6. CWE: CWE 1104: Use of Unmaintained Third Party Components**

**OWASP CATEGORY : A06 2021 Vulnerable and Outdated Components**

**DESCRIPTION:** The product relies on third-party components that are not actively supported or maintained by the original developer or a trusted proxy for the original developer.

**BUSINESS IMPACT:** The use of vulnerable and outdated components in software development and IT infrastructure can have serious consequences for businesses, as it exposes them to a range of security and operational risks. Vulnerabilities and outdated components are common targets for attackers seeking to exploit weaknesses in systems.

## **7. CWE: CWE 306-Missing Authentication for Critical Function**

**OWASP CATEGORY : A07 2021 Identification and Authentication Failures**

**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:** Identification and authentication failures can have serious repercussions for businesses, as they directly affect the security and access controls that protect sensitive information and systems. Proper identification and authentication mechanisms are crucial for ensuring that only authorized individuals have access to resources and data.

## **8. CWE: CWE-1214 Data Integrity Issues**

**OWASP CATEGORY : A08 2021 Software and Data Integrity Failures**

**DESCRIPTION:** Weaknesses in this category are related to a software system's data integrity components. Frequently these deal with the ability to ensure the integrity of data, such as messages, resource files, deployment files, and configuration files. The weaknesses in this category could lead to a degradation of data integrity quality if they are not addressed.



**BUSINESS IMPACT:** Software and data integrity failures can have severe and far-reaching impacts on a business. Both the software applications that a company uses to run its operations and the integrity of the data it processes are crucial for maintaining efficiency, customer trust, and overall success.

## **9. CWE: CWE-778 Insufficient Logging**

**OWASP CATEGORY: A09 2021 Security Logging and Monitoring Failures**

**DESCRIPTION:** When a security-critical event occurs, the product either does not record the event or omits important details about the event when logging it.

**BUSINESS IMPACT:** Security logging and monitoring failures can have significant negative impacts on a business. In today's digital landscape, where cyber threats are constantly evolving, the ability to effectively monitor and log security events is crucial for maintaining the integrity, confidentiality, and availability of data and systems.

## **10. CWE: CWE-918 Server Side Request Forgery**

**OWASP CATEGORY : A10 2021 - Server Side Request Forgery**

**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:** A successful SSRF attack can often result in unauthorized actions or access to data within the organization, either in the vulnerable application itself or on other back-end systems that the application can communicate with.

**Stage : 2 Report**

## Overview

Performing a vulnerability assessment for a college website is crucial to identify and address potential security weaknesses that could be exploited by attackers. Security is an ongoing process, and continuous monitoring and improvement are essential to maintain a robust defense against potential threats. Additionally, if you lack the expertise to conduct a thorough assessment, it is wise to seek assistance from qualified cybersecurity professionals. Verify that the website is secure and displays correctly on various devices and browsers. Document all identified vulnerabilities, along with their severity and potential impact. Prioritize fixes based on criticality and help the college's IT team or web developers with the remediation process. Document all identified vulnerabilities, along with their severity and potential impact. Prioritize fixes based on criticality and help the college's IT team or web developers with the remediation process.

Nessus is a popular vulnerability assessment tool that is widely used by

cybersecurity professionals and organizations to identify and address security weaknesses in their networks, systems, and applications. Here are some of the key uses of Nessus:

**Vulnerability Scanning:** Nessus is primarily used for automated vulnerability scanning. It scans networks, servers, endpoints, and applications to detect known vulnerabilities and misconfigurations. This helps organizations identify potential entry points for attackers and prioritize their security efforts.

**Patch Management:** The scan results generated by Nessus provide information about missing patches and updates for various software and operating systems. This assists in maintaining an up-to-date and secure IT environment by ensuring that critical security patches are applied promptly.

**Compliance Auditing:** Nessus can be used to assess whether an organization's systems and configurations comply with industry standards and regulatory requirements, such as PCI DSS, HIPAA, NIST, CIS, and more. It helps organizations identify gaps and achieve compliance with security best practices.

**Web Application Scanning:** Nessus can scan web applications to identify vulnerabilities like SQL injection, cross-site scripting (XSS), and other issues that may expose web applications to potential attacks.

**Network Inventory and Asset Management:** Nessus can provide valuable information about the devices and systems connected to the network, assisting in maintaining an up-to-date inventory and understanding the network's attack surface.

**Security Awareness and Training:** By generating detailed vulnerability reports, Nessus helps security teams and IT personnel gain insights into the security posture of their systems. This

information can be used to improve security awareness and training programs.

**Risk Assessment:** Nessus assigns severity levels to identified vulnerabilities, helping organizations prioritize their efforts by focusing on high-risk vulnerabilities first.

**Penetration Testing Support:** Nessus can complement manual penetration testing efforts by providing an initial overview of potential vulnerabilities before more extensive manual testing is conducted.

**Cloud Infrastructure Security:** Many organizations are now using cloud infrastructure. Nessus can assess cloud environments and identify misconfigurations or vulnerabilities that might affect the security of cloud-based resources.

**Continuous Monitoring:** Nessus can be used to implement continuous monitoring strategies, enabling organizations to regularly assess their security posture and detect changes that may introduce new vulnerabilities.

**Threat Intelligence Integration:** Nessus can be integrated with threat intelligence feeds to cross-reference scan results with known exploits and threats, providing a more comprehensive view of potential risks.

Nessus is an excellent tool for identifying known vulnerabilities and misconfigurations, it should be part of a comprehensive security strategy that includes regular manual assessments, threat hunting, and ongoing security awareness efforts to address emerging and zero-day threats.

**Target WebSite :** Tagore Engineering College website : [tagore-engg.ac.in](http://tagore-engg.ac.in) **Target IP :**  
103.53.43.82

S. No.	Vulnerability name	Severity	Plugin	Description	Solution	Business Impact	Port
1	SSL Medium strength cipher suits supports (SWEET32)	High	42873	The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken	Purchase or generate a proper SSL certificate for this service.	Encountering an "SSL Certificate Cannot Be Trusted" error can have significant business impacts, primarily centered around trust, security, and user experience. An SSL certificate is essential for securing the communication between a user's browser and a website's server, ensuring that data exchanged is encrypted and secure.	8010
2	HTTS Missing From HTTPS Server	Info	84502	The remote HTTPS server is not enforcing HTTP Strict Transport Security (HSTS). HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.	Configure the remote web server to use HSTS.	The absence of HTTP Strict Transport Security (HSTS) from an HTTPS server can have several business impacts, primarily related to security, user experience, and trust. HSTS is a security policy mechanism that helps protect websites and their users against certain types of attacks, such as SSL stripping and man-in-the-middle attacks.	443, 8010
3		Info	84574	Security patches may have been	Give Nessus credentials to	Detecting backported security	443

	Backported Security Patch Detection (PHP)			<p>'backported' to the remote PHP install without changing its version number.</p> <p>Banner-based checks have been disabled to avoid false positives.</p> <p>Note that this test is informational only and does not denote any security problem. Security patches may have been 'backported' to the remote PHP install without changing its version number.</p>	perform local checks.	<p>patches in PHP or any other programming language is crucial for maintaining a secure software ecosystem. Backported patches involve taking security fixes from newer software versions and applying them to older versions that are still in use.</p>	
--	---	--	--	--	-----------------------	--	--

4	Service Detection	Info	22964	Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.	A web server is running on this port through TLSv1.	Service detection refers to the process of identifying the specific services and applications running on a network or server. This information is crucial for network management, security, and operational purposes.	443, 8010
5	Apache Banner Linux Distribution Disclosure	Info	18261	Nessus was able to extract the banner of the Apache web server and determine which Linux distribution the remote host is running.	If you do not wish to display this information, edit 'httpd.conf' and set the directive 'ServerTokens Prod' and restart Apache.	The "Apache Banner Linux Distribution Disclosure" refers to the disclosure of information about the specific Linux distribution running Apache web server in the server's banner or response headers. This information can include details about the distribution version and other system information.	NA



6	JQuery 1.2 < 3.5.0 Multiple XSS	Medium	136929	According to the self-reported version in the script, the version of JQuery hosted on the remote web server is greater than or equal to 1.2 and prior to 3.5.0. It is, therefore, affected by multiple cross site scripting vulnerabilities.	Upgrade to JQuery version 3.5.0 or later.	The JQuery 1.2 to 3.5.0 multiple cross-site scripting (XSS) vulnerabilities refer to a range of security issues in the jQuery JavaScript library. These vulnerabilities could potentially allow attackers to inject malicious code into web applications and compromise user data and experiences.	443
7	HTTP TRACE / TRACK Methods Allowed	Medium	11213	The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections.	Disable these HTTP methods. Refer to the plugin output for more information.	Allowing the HTTP TRACE or TRACK methods can potentially have serious security implications for your web application. These methods are used for debugging and diagnostics, but they can also expose sensitive information and introduce security vulnerabilities.	443

8	Web Server No 404 Error Code Check	Info	10386	The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page.	The following string will be used : TYPE= password	Failing to properly handle and implement 404 error code checks on a web server can have several business impacts, primarily affecting user experience, security, and brand reputation	8010

--	--	--	--	--	--	--	--	--

9	TCP/IP Timestamps Supported	Info	25220	Failing to properly handle and implement 404 error code checks on a web server can have several business impacts, primarily affecting user experience, security, and brand reputation	No output recorded.	Enabling or supporting TCP/IP timestamps in a network environment can have both positive and negative business impacts, primarily related to network performance, security, and compatibility	NA

## **Stage-3**

### **Enhancing Cyber security: Strategies for Effective SOC and SIEM Integration under the Indian Penal Code**

**SOC:** A Security Operations Center (SOC) is a centralized team and facility responsible for monitoring, detecting, responding to, and mitigating cybersecurity threats and incidents within an organization's IT infrastructure. A Security Operations Center (SOC) is a centralized team and facility responsible for monitoring, detecting, responding to, and mitigating cybersecurity threats and incidents within an organization's IT infrastructure.

**SOC – Cycle:** The SOC operates in a continuous cycle to ensure the organization's security posture is maintained and threats are promptly addressed. This cycle typically involves several key stages:

#### **1. Threat Identification and Detection:**

- In this stage, the SOC monitors network traffic, system logs, and security event data to identify potential threats and anomalies.
- Various tools, such as intrusion detection systems (IDS), intrusion prevention systems (IPS), and security information and event management (SIEM) solutions, are used to collect and analyze data.
- SOC analysts analyze alerts and events to determine if they indicate actual security incidents or false positives.

#### **2. Incident Analysis and Prioritization:**

- Once potential incidents are detected, the SOC team analyzes the data to understand the nature and scope of the threat.
- Analysts assess the severity, potential impact, and likelihood of compromise associated with each incident.
- Incidents are prioritized based on the risk they pose to the organization.

### **3. Incident Response:**

- After prioritization, the SOC initiates an incident response plan tailored to the severity of the threat.
- The response may involve containment, isolation of affected systems, and preservation of evidence.
- SOC analysts work to mitigate the threat, eradicate malicious activity, and restore normal operations.

### **4. Communication and Reporting:**

- During and after incident response, clear communication is crucial. SOC teams collaborate with other relevant departments, such as IT, legal, and management.
- Regular updates are provided to stakeholders, and incident reports are generated to document the details of the incident, response actions, and outcomes.

### **5. Lessons Learned and Improvement:**

- After the incident is resolved, the SOC conducts a post-incident review to understand what went well and identify areas for improvement.
- This stage helps refine incident response processes, update detection rules, and enhance overall security measures.

### **6. Continuous Monitoring and Adaptation:**

- The SOC's work doesn't stop after responding to an incident. Continuous monitoring of systems, networks, and user activities remains ongoing.
- The SOC team adapts to new threat vectors, emerging attack techniques, and changes in the organization's infrastructure.

### **7. Threat Intelligence and Proactive Defense:**

- The SOC integrates threat intelligence data to anticipate and prepare for potential threats.
- By staying informed about the latest attack trends, the SOC can implement proactive measures to prevent or mitigate threats before they impact the organization.

### **8. Vulnerability Management:**

- The SOC is involved in identifying vulnerabilities within the organization's systems and applications.
- Vulnerabilities are assessed for risk, and measures are taken to address or mitigate them to reduce the potential for exploitation.

**SIEM:** SIEM stands for Security Information and Event Management. It is a comprehensive approach to security management that combines the capabilities of security information management (SIM) and security event management (SEM). SIEM technology provides a centralized platform for collecting, correlating, analyzing, and responding to security-related information and events from various sources within an organization's IT infrastructure. Here's an overview of the key components and functions of a SIEM system:

### **1. Log Collection:**

SIEM solutions collect log data from a wide range of sources, including network devices, servers, applications, operating systems, and security appliances. These logs contain valuable information about user activities, system events, and potential security incidents.

### **2. Event Correlation:**

SIEM systems correlate and analyze the collected data to identify patterns, anomalies, and potential security threats. By correlating events from different sources, SIEM can provide a more comprehensive view of complex attacks or unauthorized activities.

### **3. Alerting and Notification:**

When the SIEM system detects a potential security incident or policy violation, it generates alerts. These alerts are typically prioritized based on their severity and impact. Security analysts are notified in real-time, allowing them to respond promptly.

### **4. Threat Detection and Monitoring:**

SIEM systems use predefined rules and algorithms to detect known attack patterns and suspicious behavior. They can also employ machine learning and behavioral analytics to identify previously unknown threats or deviations from normal behavior.

### **5. Incident Response:**

SIEM plays a crucial role in incident response by providing detailed information about the scope, timeline, and impact of security incidents. Analysts can investigate incidents using historical data and track how they

have evolved over time.

#### **6. Forensic Analysis:**

SIEM solutions store historical data, enabling security teams to perform forensic analysis of past incidents. This capability assists in understanding the root cause of incidents and improving future security measures.

#### **7. Compliance and Reporting:**

SIEM systems help organizations meet regulatory compliance requirements by generating reports that demonstrate adherence to security policies and regulations. These reports can be essential for audits and legal purposes.

#### **8. Centralized Visibility:**

One of the primary benefits of SIEM is its ability to provide a centralized view of an organization's security posture. This visibility helps security teams quickly identify and respond to threats across the entire IT environment.

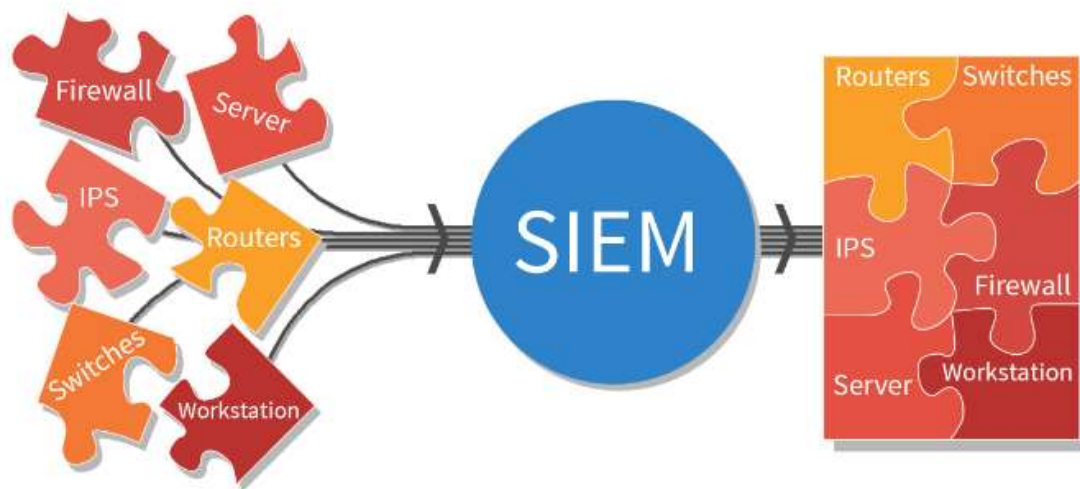
#### **9. Integration with Other Security Tools:**

Many SIEM solutions can integrate with other security tools, such as intrusion detection systems (IDS), intrusion prevention systems (IPS), firewalls, and vulnerability scanners. This integration enhances the overall security ecosystem.

#### **10. Threat Intelligence Integration:**

SIEM systems can incorporate external threat intelligence feeds, enhancing their ability to detect new and emerging threats by comparing internal data with known threat indicators.





**SIEM Cycle:** Certainly, let's break down the SIEM (Security Information and Event Management) cycle into distinct phases:

### 1. Data Collection:

- SIEM begins by collecting data from various sources, such as network devices, servers, endpoints, applications, and security tools.
- Logs, events, and data are aggregated from different systems and devices, creating a centralized repository.

### 2. Data Normalization and Enrichment:

- The collected data can come in various formats from different sources. In this phase, the data is normalized and standardized to a common format for better analysis.
- Additional context and information might be added to the data through enrichment, making it more valuable for analysis.

### 3. Data Correlation and Analysis:

- SIEM systems analyze the normalized data to identify patterns, anomalies, and potential security threats.

- Correlation rules and algorithms are applied to detect relationships between different events and identify complex attack sequences.

#### **4. Alert Generation:**

- When the SIEM detects an event or pattern that matches predefined correlation rules, it generates alerts.
- Alerts are categorized based on their severity and potential impact on security.

#### **5. Alert Prioritization and Escalation:**

- Security analysts assess the alerts to determine their urgency and potential significance.
- Alerts are prioritized based on the level of threat and the criticality of affected systems.
- High-priority alerts are escalated to the appropriate teams for further investigation.

#### **6. Incident Investigation:**

- Analysts investigate the alerts and events to understand the context and potential implications.
- They use historical data and correlation capabilities to trace the events leading up to the alert.

#### **7. Incident Response:**

- If an alert is confirmed as a security incident, the incident response process is initiated.
- Actions are taken to contain and mitigate the incident, such as isolating affected systems and blocking malicious activities.

#### **8. Forensic Analysis and Root Cause Identification:**

- For more complex incidents, forensic analysis is conducted to determine the root cause and extent of the breach.
- Analysts use historical data to reconstruct the sequence of events and understand how the incident occurred.

### 9. Remediation and Recovery:

- After containing the incident, steps are taken to remediate affected systems.
- Vulnerabilities that were exploited are patched, and security measures are enhanced to prevent similar incidents.

### 10. Reporting and Documentation:

- SIEM systems generate reports detailing the incidents, response actions, and outcomes.
- These reports are valuable for auditing, compliance, and management decision-making.

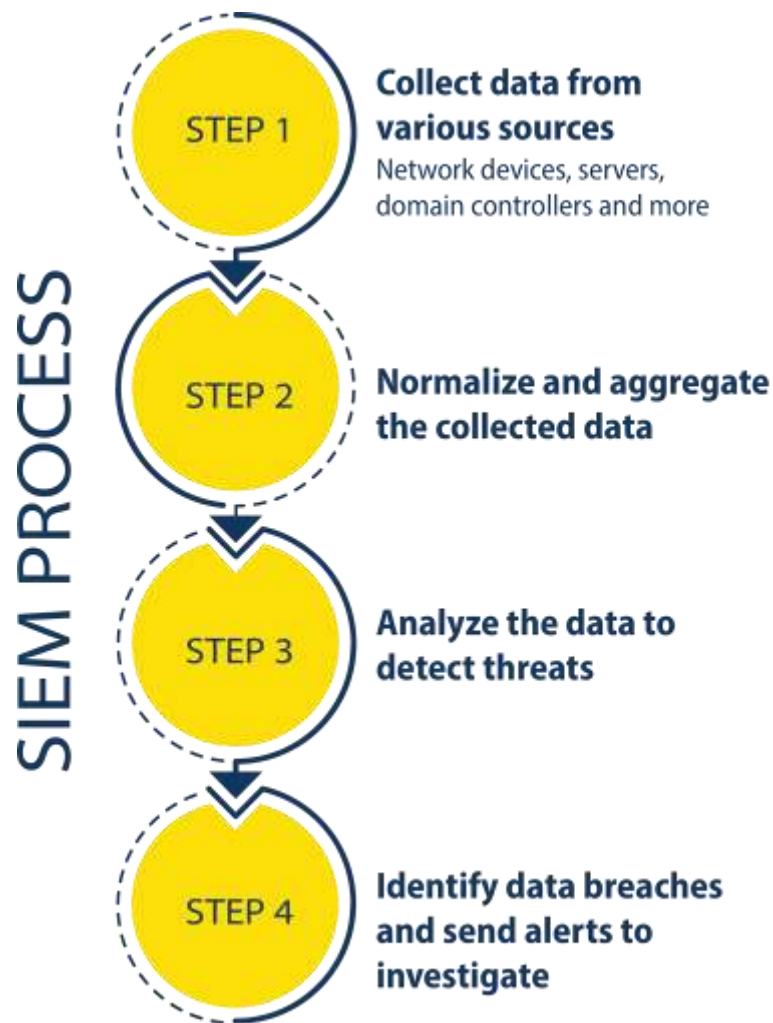
### 11. Continuous Improvement:

- The SIEM cycle is continuous, with ongoing monitoring and analysis of security events.
- The SIEM's rules, correlation patterns, and response procedures are refined based on lessons learned from previous incidents.

### 12. Threat Intelligence Integration:

- SIEM incorporates external threat intelligence feeds to enhance its ability to detect new and emerging threats.





**MISP:** Malware Information Sharing Platform & Threat Sharing. It's an open-source threat intelligence platform designed to improve the sharing of structured threat information between organizations and cybersecurity professionals. MISP allows users to collect, manage, share, and collaborate on threat intelligence data, helping to enhance overall security posture and enable proactive defense against cyber threats. Here are some key features and functions of MISP:

#### **1. Data Collection and Management:**

- MISP allows users to collect various types of threat intelligence data, including indicators of compromise (IoCs), threat actor information, attack techniques, malware samples, and more.
- Users can organize and manage this data within the platform, enabling efficient storage and retrieval.

## **2. Standardized Data Format:**

- MISP uses a standardized data format, known as the MISP format, which allows for consistent representation of threat intelligence data. This format includes details about threat indicators, attributes, relationships, and more.

## **3. Collaborative Sharing:**

- MISP supports collaborative threat intelligence sharing among different organizations, communities, and security teams.
- Users can share specific threat intelligence with trusted partners, fostering a more proactive response to threats.

## **4. Flexible Data Correlation:**

- MISP provides mechanisms to correlate different pieces of threat intelligence data, helping users understand the relationships between various indicators and threats.

## **5. Event and Object Management:**

- Users can create and manage "events" in MISP, which represent a collection of related threat intelligence data.
- Within events, users can create and manage various "objects," such as indicators, attributes, and related information.

## **6. Integration and Automation:**

- MISP offers APIs and integration capabilities to automate the sharing of threat intelligence and the integration with other security tools and platforms.

## **7. Stix and CybOX Support:**

- MISP supports the STIX (Structured Threat Information eXpression) and CybOX (Cyber Observable eXpression) standards for representing threat intelligence in a structured and standardized way.

## 8. Taxonomies and Tags:

- MISP provides taxonomies and tags that help categorize and classify threat intelligence data. This allows for better organization and searching.

## 9. Customization and Extensions:

- MISP is customizable and extensible. Users can define their own data models, create custom attributes, and tailor the platform to their specific needs.

## 10. Visualization and Analysis:

- MISP provides visualization tools to help users understand and analyze complex relationships between threat intelligence data points.

## 11. Community Involvement:

- MISP has an active user community that contributes to its development, shares threat intelligence, and collaborates on improving the platform's features and capabilities.



## Your college network information

- Total Number of the Labs: 52

- Total Number of the System: 3400

## **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:

### **1. Assessment and Requirements Gathering:**

- Conduct a thorough assessment of the organization's current cybersecurity posture, including existing security measures, tools, and processes.
- Identify the specific security challenges, risks, and compliance requirements that a SOC will address.
- Define the goals and objectives of the SOC deployment to align with the organization's overall security strategy.

### **2. Budget and Resource Allocation:**

- Determine the budget and resource requirements for establishing and maintaining the SOC.
- Allocate personnel, hardware, software, and other necessary resources to support the SOC operations.

## **Threat intelligence:**

Threat intelligence refers to the process of collecting, analyzing, and interpreting information about potential or existing cyber threats. It involves gathering data about threat actors, their motives, tactics, techniques, procedures, vulnerabilities, and other factors that could pose risks to an organization's cybersecurity. The goal of threat intelligence is to provide actionable insights that enable organizations to proactively defend against cyber threats and make informed decisions to enhance their security posture. Here are some key aspects of threat intelligence:

## **Types of Threat Intelligence**

### **1. Strategic Intelligence:**

- Provides high-level information about threat landscapes, trends, and potential future threats. It helps organizations understand the broader context of cybersecurity risks.

- **Tactical Intelligence:** Focuses on specific threats, vulnerabilities, and attack techniques. It helps organizations understand how threats operate and provides information to improve detection and response capabilities.
- **Operational Intelligence:** Offers real-time information about ongoing threats and incidents. It helps organizations respond to immediate threats and mitigate risks.

## **2. Sources of Threat Intelligence:**

- **Open-Source Intelligence (OSINT):** Publicly available information from websites, social media, forums, and other online sources.
- **Closed-Source Intelligence (CSINT):** Proprietary or commercial threat intelligence feeds and reports.
- **Human Intelligence (HUMINT):** Insights gathered from experts, analysts, and security researchers.
- **Technical Intelligence (TECHINT):** Information extracted from technical sources such as network traffic, malware samples, and system logs.

## **3. Collection and Analysis:**

- Threat intelligence teams collect data from various sources, including indicators of compromise (IoCs), threat actor profiles, vulnerabilities, and attack patterns.
- They analyze this data to identify patterns, trends, and correlations that help in understanding the behavior of threat actors and their methods.

## **4. Threat Indicators:**

- Threat intelligence often revolves around identifying and monitoring threat indicators, which are pieces of information that suggest malicious activity. Indicators can include IP addresses, domain names, file hashes, email addresses, and more.

## **5. Sharing and Collaboration:**

- Threat intelligence is most effective when shared among organizations and security communities.



- Sharing threat intelligence helps others stay informed about emerging threats and enhances collective defense capabilities.

#### **6. Proactive Defense:**

- Threat intelligence enables organizations to anticipate and prepare for potential threats by understanding attack techniques and motivations.
- It allows for the identification of vulnerabilities and weaknesses that could be exploited by threat actors.

#### **7. Incident Response and Mitigation:**

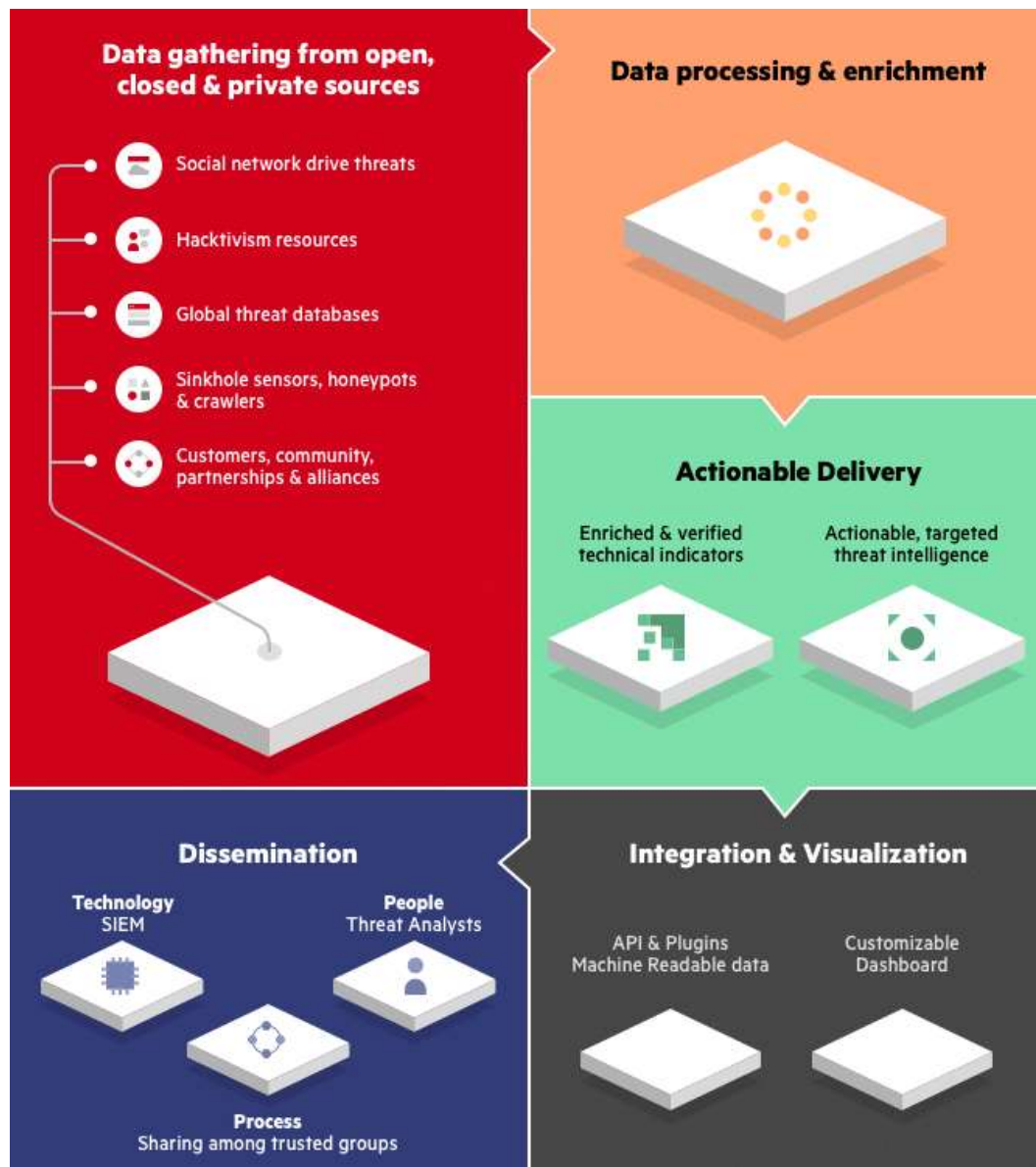
- Threat intelligence assists in rapid incident response by providing context and insights into ongoing incidents.
- It helps in understanding the nature of the attack, its impact, and the appropriate response actions.

#### **8. Strategic Decision-Making:**

- Organizations can use threat intelligence to make informed decisions about security investments, risk management strategies, and resource allocation.

#### **9. Continuous Monitoring and Adaptation:**

- The threat landscape is dynamic, so threat intelligence efforts must be ongoing to keep up with evolving risks.
- Organizations should regularly update their threat intelligence to adapt to new attack techniques and emerging threats.



**Incident Response:** Incident response is a structured approach taken by organizations to manage and mitigate the effects of a cybersecurity incident. A cyber security incident is any unauthorized or unexpected event that could potentially compromise the confidentiality, integrity, or availability of an organization's information systems, data, or networks. Incident response aims to minimize the damage caused by incidents, reduce recovery time and costs, and prevent future occurrences. Here's an overview of the key phases involved in an incident response process:

## 1. Preparation:

- Establish an incident response plan (IRP) outlining roles, responsibilities, and procedures for responding to different types of incidents.
- Identify a dedicated incident response team (IRT) or individuals responsible for coordinating and executing the response efforts.
- Develop communication plans that define how stakeholders will be informed during and after an incident.
- Ensure necessary tools, technologies, and resources are readily available.

## **2. Identification:**

- Detect and identify potential incidents through various means, such as security monitoring, intrusion detection systems, and user reports.
- Monitor network and system logs for suspicious activities, anomalies, or indicators of compromise.

## **3. Containment:**

- Isolate affected systems, devices, or network segments to prevent further spread of the incident.
- Implement temporary measures to halt the attacker's progress and minimize damage.

## **4. Eradication:**

- Identify the root cause of the incident and remove any malicious code, malware, or unauthorized access from the affected systems.
- Address vulnerabilities that were exploited to prevent future incidents of the same nature.

## **5. Recovery:**

- Restore affected systems, services, and data to their normal operational state.
- Validate the integrity of restored systems and perform testing to ensure they are fully functional.

## **6. Lessons Learned:**

- Conduct a post-incident review to assess the effectiveness of the incident response efforts.
- Identify what worked well and areas that need improvement in the response process.
- Document lessons learned to enhance future incident response activities.

## **7. Communication:**

- Maintain transparent and clear communication with stakeholders, including employees, customers, partners, and regulatory authorities.
- Provide regular updates on the incident's status, actions taken, and expected outcomes.

## **8. Documentation:**

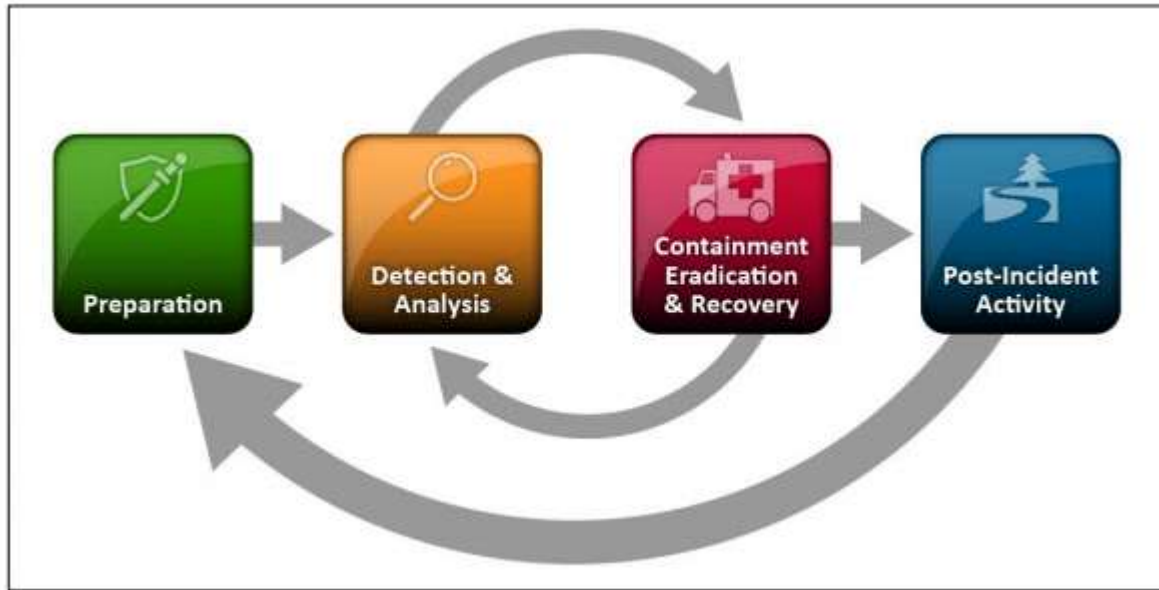
- Document all aspects of the incident, including the timeline, actions taken, evidence collected, and communication logs.
- This documentation is valuable for legal, regulatory, and auditing purposes.

## **9. Regulatory Reporting:**

- If the incident involves personally identifiable information (PII) or falls under regulatory requirements, report the incident to the relevant authorities as needed.

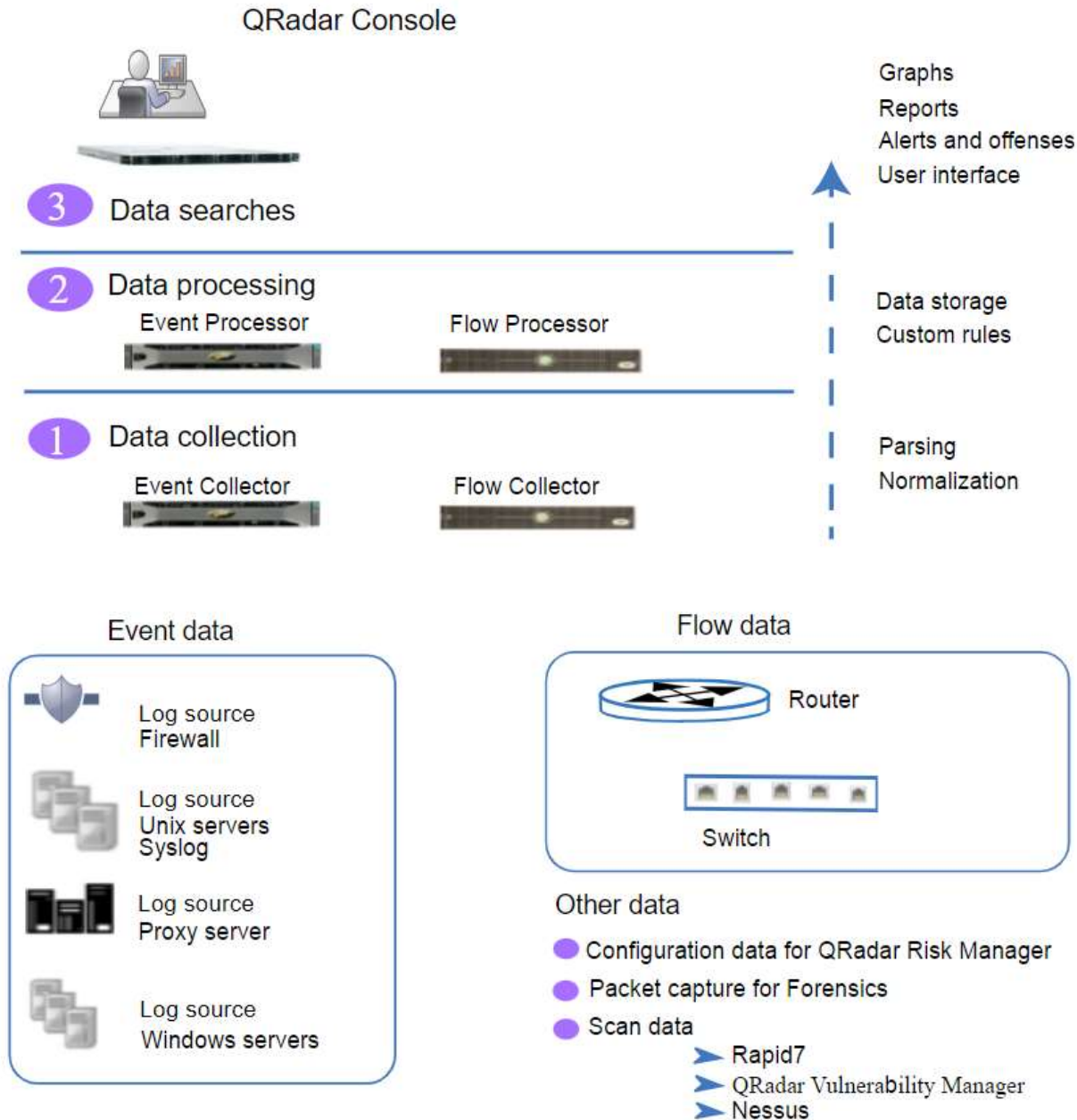
## **10. Continuous Improvement:**

- Use the insights gained from the incident to update and refine the incident response plan and procedures.
- Conduct regular training and simulations to ensure the incident response team is well-prepared for future incidents.



## Qradar & understanding about tool

IBM Security® QRadar® Suite is a modernized threat detection and response solution designed to unify the security analyst experience and accelerate their speed across the full incident lifecycle. The portfolio is embedded with enterprise-grade AI and automation to dramatically increase analyst productivity, helping resource-strained security teams work more effectively across core technologies. It offers integrated products for endpoint security (EDR, XDR, MDR), log management, SIEM and SOAR—all with a common user interface, shared insights and connected workflows.



## Data collection

Data collection is the first layer, where data such as events or flows is collected from your network. The All-in-One appliance can be used to collect the data directly from your network or you can use collectors such as QRadar Event Collectors or QRadar QFlow Collectors to collect event or flow data. The data is parsed and normalized before it is passed to the processing layer. When the raw data is parsed, it is normalized to present it in a structured and usable format.

The core functionality of QRadar SIEM is focused on event data collection, and flow collection.

Event data represents events that occur at a point in time in the user's environment such as user logins,

email, VPN connections, firewall denys, proxy connections, and any other events that you might want to log in your device logs.

Flow data is network activity information or session information between two hosts on a network, which QRadar translates in to flow records. QRadar translates or normalizes raw data in to IP addresses, ports, byte and packet counts, and other information into flow records, which effectively represents a session between two hosts. In addition to collecting flow information with a Flow Collector, full packet capture is available with the QRadar Incident Forensics component.

## **Data processing**

After data collection, the second layer or data processing layer is where event data and flow data are run through the Custom Rules Engine (CRE), which generates offenses and alerts, and then the data is written to storage.

Event data, and flow data can be processed by an All-in-One appliance without the need for adding Event Processors or Flow Processors. If the processing capacity of the All-in-One appliance is exceeded, then you might need to add Event Processors, Flow Processors or any other processing appliance to handle the additional requirements. You might also need more storage capacity, which can be handled by adding Data Nodes.

Other features such as QRadar Risk Manager (QRM), QRadar Vulnerability Manager (QVM), or QRadar Incident Forensics collect different types of data and provide more functions.

QRadar Risk Manager collects network infrastructure configuration, and provides a map of your network topology. You can use the data to manage risk by simulating various network scenarios through altering configurations and implementing rules in your network.

Use QRadar Vulnerability Manager to scan your network and process the vulnerability data or manage the vulnerability data that is collected from other scanners such as Nessus, and Rapid7. The vulnerability data that is collected is used to identify various security risks in your network.

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

## **Data searches**

In the third or top layer, data that is collected and processed by QRadar is available to users for searches, analysis, reporting, and alerts or offense investigation. Users can search, and manage the security admin

tasks for their network from the user interface on the QRadar Console.

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

In distributed environments, the QRadar Console does not perform event and flow processing, or storage. Instead, the QRadar Console is used primarily as the user interface where users can use it for searches, reports, alerts, and investigations.

### **QRadar components**

Use IBM QRadar components to scale a QRadar deployment, and to manage data collection and processing in distributed networks.

### **QRadar maximum EPS certification methodology**

IBM QRadar appliances are certified to support a certain maximum events per second (EPS) rate. Maximum EPS depends on the type of data that is processed, system configuration, and system load.

### **QRadar events and flows**

The core functions of IBM QRadar SIEM are managing network security by monitoring flows and events.

## **Conclusion**

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



Web application testing refers to the process of evaluating and validating a web application's functionality, performance, security, and overall user experience. The goal of web application testing is to identify and address any issues or vulnerabilities in the application before it is released to the public. This process involves a variety of testing techniques and methodologies to ensure that the application meets its intended requirements and performs well under different conditions. Key aspects of web application testing include:

**Functionality Testing:** This involves testing the application's features and functionalities to ensure they work as intended. Testers check whether buttons, links, forms, navigation, and other interactive elements function correctly.

**Usability Testing:** This assesses the user-friendliness of the application. Testers evaluate the application's user interface, design, and overall user experience to ensure that users can easily navigate and use the application.

**Performance Testing:** Performance testing involves evaluating the application's responsiveness, speed, and scalability. This includes load testing (checking how the application performs under various levels of user traffic) and stress testing (testing the application's limits to identify potential bottlenecks or crashes).

**Security Testing:** Security testing aims to identify vulnerabilities and weaknesses that could be exploited by malicious users. It involves assessing the application for potential security breaches, data leaks, and other vulnerabilities. Common security testing techniques include penetration testing, vulnerability scanning, and code review.

**Compatibility Testing:** Compatibility testing ensures that the web application works correctly across different devices, browsers, and operating systems. This helps ensure a consistent user experience regardless of the user's setup.

**Regression Testing:** This involves retesting the application after changes or updates have been made to ensure that new modifications haven't introduced new issues or broken existing functionality.

**Accessibility Testing:** Accessibility testing ensures that the application is usable by people with disabilities. Testers evaluate whether the application adheres to accessibility standards, making it usable by individuals with various impairments.

**Localization and Internationalization Testing:** For applications intended for a global audience, this testing verifies that the application displays content correctly in different languages, cultures, and regions.

**Database Testing:** This involves checking the integrity and accuracy of data stored within the application's databases. It ensures that data retrieval, storage, and manipulation functions as expected.

**User Acceptance Testing (UAT):** UAT involves end-users testing the application in a real-world environment to ensure it meets their needs and expectations. Their feedback is valuable for making final adjustments before the application's release.

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

A Nessus report is a structured document generated by the Nessus vulnerability scanning tool, which is widely used for identifying security vulnerabilities, misconfigurations, and weaknesses in computer systems, networks, and applications. Nessus is developed by Tenable, and it helps organizations assess the

security posture of their IT infrastructure and take proactive measures to address vulnerabilities and enhance security. A Nessus report typically includes the following key elements:

**Executive Summary:** This section provides a high-level overview of the scan results, highlighting critical vulnerabilities and risks. It often includes a risk rating, a summary of vulnerabilities by severity level, and an overall assessment of the system's security status.

**Host and Asset Information:** The report includes details about the scanned hosts or assets, such as IP addresses, hostnames, operating systems, and other relevant information.

**Vulnerability Details:** This section provides a comprehensive list of identified vulnerabilities, categorized by severity levels (e.g., critical, high, medium, low). Each vulnerability entry includes details such as the vulnerability name, description, CVSS (Common Vulnerability Scoring System) score, potential impact, and recommendations for remediation.

**Risk Assessment:** The report often assigns a risk score or rating to each vulnerability, helping organizations prioritize which vulnerabilities should be addressed first based on their potential impact and exploitability.

**Detailed Findings:** For each vulnerability, the report may offer more in-depth information, including technical details about the vulnerability, affected systems, and steps to reproduce or verify the issue.

**Remediation Recommendations:** The report provides actionable recommendations for mitigating each vulnerability. These recommendations may include links to official security advisories, patches, configuration changes, or best practices to resolve the identified issues.

**Compliance and Policy Checks:** Nessus can also perform checks against various compliance standards and security policies (such as CIS benchmarks), and the report may include information about how well the scanned systems adhere to these standards.

**Appendices and Supporting Data:** Some Nessus reports include additional information, such as raw scan data, a summary of applied plugins or checks, and details about the scanning configuration.

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

**SOC (Security Operations Center):** A Security Operations Center (SOC) is a centralized team, facility, or department within an organization responsible for monitoring, detecting, analyzing, and responding to security threats and incidents. The primary goal of a SOC is to ensure the security of an organization's information systems and data. SOC teams use various tools, technologies, and processes to monitor network and system activities, identify potential security incidents, investigate anomalies, and respond to incidents in a timely and effective manner.

**SIEM (Security Information and Event Management):** SIEM stands for Security Information and Event Management. It refers to a technology solution that aggregates, correlates, and analyzes security-related data from various sources within an organization's IT environment. The goal of a SIEM system is to provide real-time insights into security events, help identify patterns of suspicious behavior, and facilitate the detection and response to security incidents. SIEM systems collect logs and data from networks, servers, applications, and other sources, and then use advanced analytics to generate alerts and reports for SOC teams to investigate.

**QRadar Dashboard (IBM QRadar Dashboard):** IBM QRadar is a popular SIEM solution that provides tools for security information and event management. A QRadar dashboard is a graphical interface within the QRadar system that displays visual representations of security-related data and information. Dashboards are customizable and allow SOC analysts to visualize and monitor security events, alerts, vulnerabilities, and other key metrics in real time. QRadar dashboards often include widgets, charts, graphs, tables, and maps that help analysts quickly assess the security posture of their environment and take appropriate actions. Future Scope

### Stage 1 :- Future scope of web application testing

The future scope of web application testing is evolving in response to advancements in technology, development methodologies, and the changing landscape of cybersecurity. Here are some key trends and areas of focus that are likely to shape the future of web application testing:

**Automation and AI/ML Integration:** Automation will continue to play a significant role in web application testing. Test automation frameworks, scripting languages, and tools will become more sophisticated, allowing testers to create and execute tests more efficiently. The integration of Artificial Intelligence (AI) and Machine Learning (ML) will enable the creation of smarter test scripts that adapt to changes in the application and its environment.

**Shift-Left Testing:** There's an increasing emphasis on shifting testing activities to earlier stages of the development lifecycle. This involves involving testers in the requirements and design phases to identify potential issues before coding begins, resulting in higher-quality code and faster development cycles.

**DevSecOps Integration:** The integration of security testing into the DevOps pipeline, often referred to as DevSecOps, will become more widespread. Security testing, including vulnerability scanning and penetration testing, will be seamlessly integrated into the development process to identify and address security weaknesses early on.

**Microservices and API Testing:** With the growing adoption of microservices architecture, there will be an increased need for testing APIs and interactions between microservices. Specialized tools and methodologies for API testing will gain prominence.

## Stage 2 :- Future scope of testing process you understood.

The future scope of web application testing is evolving in response to advancements in technology, development methodologies, and the changing landscape of cybersecurity. Here are some key trends and areas of focus that are likely to shape the future of web application testing:

**Automation and AI/ML Integration:** Automation will continue to play a significant role in web application testing. Test automation frameworks, scripting languages, and tools will become more sophisticated, allowing testers to create and execute tests more efficiently. The integration of Artificial Intelligence (AI) and Machine Learning (ML) will enable the creation of smarter test scripts that adapt to changes in the application and its environment.

**Shift-Left Testing:** There's an increasing emphasis on shifting testing activities to earlier stages of the development lifecycle. This involves involving testers in the requirements and design phases to identify potential issues before coding begins, resulting in higher-quality code and faster development cycles.

**DevSecOps Integration:** The integration of security testing into the DevOps pipeline, often referred to as DevSecOps, will become more widespread. Security testing, including vulnerability scanning and penetration testing, will be seamlessly integrated into the development process to identify and address security weaknesses early on.

**Microservices and API Testing:** With the growing adoption of microservices architecture, there will be an increased need for testing APIs and interactions between microservices. Specialized tools and methodologies for API testing will gain prominence.

## Stage 3 :- future scope of SOC / SEIM

The future scope of Security Operations Centers (SOCs) and Security Information and Event Management (SIEM) systems is continually evolving to address the dynamic and complex landscape of cybersecurity threats. Here are some key trends and areas of focus that are likely to shape the future of SOCs and SIEM systems:

**Threat Intelligence and Contextual Analysis:** SOCs will increasingly integrate threat intelligence feeds,

both internal and external, to enhance their ability to detect and respond to sophisticated threats. SIEM systems will incorporate advanced analytics and machine learning to provide contextual analysis of security events, enabling more accurate threat detection and reduced false positives.

**Behavioral Analytics and User-Centric Monitoring:** Behavioral analytics will become a core component of SIEM systems, allowing for the identification of abnormal user behaviors and insider threats. User-centric monitoring will help organizations detect unauthorized access, data exfiltration, and other malicious activities.

**Automation and Orchestration:** SOCs will leverage automation and orchestration to streamline incident response processes. Automated incident response workflows will help in rapidly containing and mitigating threats, minimizing the manual effort required for routine tasks.

**Cloud and Hybrid Environments:** As organizations increasingly migrate to cloud and hybrid environments, SOCs and SIEM systems will adapt to monitor and protect these dynamic infrastructures. Cloud-native SIEM solutions will become more prevalent.

**IoT and OT Security:** The growth of Internet of Things (IoT) and Operational Technology (OT) devices introduces new security challenges. SOCs will expand their capabilities to monitor and protect these connected devices, industrial control systems, and critical infrastructure.

**Zero Trust and Identity-Centric Security:** The adoption of Zero Trust architectures will require SOCs to focus on identity-centric security. SIEM systems will monitor user and entity behaviors to ensure that access is granted based on continuous verification of identities.

**Integrated Threat Hunting:** SOC teams will increasingly adopt proactive threat hunting practices. This involves actively searching for signs of advanced threats and vulnerabilities that might not be detected by automated tools alone.

**Regulatory Compliance and Reporting:** With stricter data protection regulations, SOCs and SIEM systems will play a crucial role in helping organizations achieve compliance with standards like GDPR, CCPA, and others. Reporting and audit capabilities will be vital.

**Managed Detection and Response (MDR):** Organizations will continue to explore outsourcing their SOC functions to managed security service providers (MSSPs) that offer MDR services. This allows organizations to leverage external expertise and resources for threat detection and incident response.

**Integration with DevSecOps:** The integration of security practices into DevOps processes will lead to the evolution of DevSecOps. SOCs and SIEM systems will work closely with development and operations teams to ensure security is baked into the entire software development lifecycle.

advancements. The future scope of SOC and SIEM will involve increased automation, advanced threat detection, integration with emerging technologies, and a proactive approach to cybersecurity. Organizations will need to invest in the latest tools and technologies while continuously developing the expertise of their cybersecurity teams to stay ahead of evolving threats.

### **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, chaptgpt, wepik.com (AI image editor), Gamma (AI based PPT), 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