TEAM-11

A Consign sentinel

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:

S.No	Name	Designation	Mobile Number
1	Dr. Aarti	Assistant Professor	9991683284 aarti@bharatividyapeeth.edu
2	Ms. Amrita Ticku	Assistant Professor	9910055024 amrita.ticku@bharatividyapeeth.edu
3	Ms. Deepika Yadav	Assistant Professor	8882045399 deepika.yadav@bharatividyapeeth.edu

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-347 Improper Verification of Cryptographic Signature.
3	Injection	CWE-94 Improper Control of Generation of code (“Code Injection”).
4	Insecure Design	CWE-922: Insecure Storage of Sensitive Information.
5	Security Misconfiguration	CWE 260- Password in Configuration File

6	Vulnerable and Outdated Components	CWE-1104: Use of Unmaintained Third-party components.
7	Identification and Authentication Failures	CWE-288: Authentication Bypass using an alternate path or channel.
8	Software and Data Integrity Failures	CWE-494: Download of code without Integrity code.
9	Security Logging and Monitoring Failures	CWE-117: Improper Output Neutralization for Logs.
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 can have significant negative impacts on various levels. Access control refers to the practice of regulating who can access what information, resources, or areas within an organization's digital and physical environment. When access control is not properly managed or enforced, several detrimental consequences can occur.

2. CWE: CWE-347: Improper Verification of Cryptographic Signature

OWASP CATEGORY: A02 2021 Cryptographic Failures

DESCRIPTION: The product does not verify, or incorrectly verifies, the cryptographic signature for data.

BUSINESS IMPACT: Improper verification of cryptographic signatures can have serious consequences for a business, particularly in scenarios where digital signatures are used to ensure the authenticity, integrity, and non-repudiation of digital documents, transactions, or communications. Cryptographic signatures are a fundamental component of secure communication and data integrity, and their improper verification can lead to

various negative impacts.

3. CWE: CWE 94: Improper Control of Generation of code ("Code Injection")

OWASP CATEGORY: A03 2021 Injection

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: Injection problems encompass a wide variety of issues -- all mitigated in very different ways. For this reason, the most effective way to discuss these weaknesses is to note the distinct features which classify them as injection weaknesses. The most important issue to note is that all injection problems share one thing in common -- i.e., they allow for the injection of control plane data into the user-controlled data plane. This means that the execution of the process may be altered by sending code in through legitimate data channels, using no other mechanism. While buffer overflows, and many other flaws, involve the use of some further issue to gain execution, injection problems need only for the data to be parsed. The most classic instantiations of this category of weakness are SQL injection and format string vulnerabilities.

4. CWE: CWE 922: Insecure Storage of Sensitive Information.

OWASP CATEGORY: A04 2021 Insecure Design

DESCRIPTION: The product stores sensitive information without properly

limiting read or write access by unauthorized actors.

BUSINESS IMPACT: If read access is not properly restricted, then attackers can steal the sensitive information. If write access is not properly restricted, then attackers can modify and possibly delete the data, causing incorrect results and possibly a denial of service.

5. CWE: CWE 260- Password in Configuration File

OWASP CATEGORY: A05 2021 Security Misconfiguration

DESCRIPTION: The product stores a password in a configuration file that might be accessible to actors who do not know the password.

BUSINESS IMPACT: This can result in compromise of the system for which the password is used. An attacker could gain access to this file and learn the stored password or worse yet, change the password to one of their choosing.

6. CWE: CWE-1104 Use of Unmaintained Third-Party Components.

OWASP CATEGORY: A06 2021 Vulnerable and Outdated Components

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

BUSINESS IMPACT: A vulnerable and outdated component is a software component that is no longer being supported by the developer, making it susceptible to security vulnerabilities. Applications often become vulnerable to attacks because they use outdated software components with known security vulnerabilities. Hackers can exploit these vulnerabilities to gain access to the application's data or to take control of the application entirely.

7. CWE: CWE: CWE 288 Authentication Bypass Using an Alternate Path or Channel.

OWASP CATEGORY: A07 2021 Identification and Authentication Failures.

DESCRIPTION: A product requires authentication, but the product has an alternate path or channel that does not require authentication.

BUSINESS IMPACT: Authentication bypass using an alternate path or channel can have serious negative impacts on a business. This refers to a situation where an attacker finds a way to bypass the standard authentication process by exploiting alternative methods or channels, such as vulnerabilities in the system or unauthorized access points.

8. CWE: CWE-494 Download of Code Without Integrity Check.

OWASP CATEGORY: A08 2021 Software and Data Integrity Failures

DESCRIPTION: The product downloads source code or an executable from a remote location and executes the code without sufficiently verifying the origin and integrity of the code.

BUSINESS IMPACT: Allowing the download of code without integrity checks can have significant negative impacts on a business's security and operations. This situation refers to the scenario where code, scripts, or software packages are downloaded and executed without verifying their authenticity or integrity.

9. CWE: CWE-117 Improper Output Neutralization for Logs.

OWASP CATEGORY: A09 2021 Security Logging and Monitoring Failures

DESCRIPTION: The product does not neutralize or incorrectly neutralizes output that is written to logs.

BUSINESS IMPACT: Security logging and monitoring failures can have significant and far-reaching impacts on businesses. Effective security logging and monitoring are crucial components of a robust cybersecurity strategy, as they help organizations detect, respond to, and mitigate security incidents and breaches.

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: Server-Side Request Forgery (SSRF) is a security vulnerability that can have various impacts on businesses, depending on the context and severity of the vulnerability. SSRF occurs when an attacker can manipulate the server into making unauthorized requests to internal resources or external systems, often leading to unintended exposure or manipulation of data.

Stage : 2 Report

NESSUS Vulnerability Report

Introduction:

It is essential to perform a vulnerability assessment on a college website in order to identify and fix potential security flaws that could be exploited by assailants. Continuous monitoring and enhancement are required to maintain a strong defense against potential threats. In addition, if you lack the knowledge to conduct a comprehensive assessment, it is prudent to seek the assistance of qualified cybersecurity professionals. Confirm that the website is secure and displays properly on a variety of devices and web browsers. Document all vulnerabilities identified, along with their severity and prospective impact. Assist the college's IT staff or web developers with the remediation process by prioritizing repairs based on their importance. Document all vulnerabilities identified, along with their severity and prospective impact.

Nessus is a well-known vulnerability assessment tool that is extensively used by cybersecurity professionals and organizations to identify and address security vulnerabilities in their networks, systems, and applications. Here are a few of Nessus's most important applications:

Network Security: Nessus is predominantly used for scanning networks to identify vulnerabilities in network infrastructure devices such as routers, switches, and firewalls. It assists administrators in identifying misconfigurations, obsolete software, and possible entrance points for attackers.

System Security: Individual systems, such as servers and workstations, are scanned to identify vulnerabilities in the operating systems, applications, and services running on those systems. This ensures that systems have the most recent security upgrades and

updates installed.

Web Application Security: Nessus can scan web applications for common security vulnerabilities such as SQL injection, cross-site scripting (XSS), and insecure authentication mechanisms. This helps organizations identify and address vulnerabilities that could be exploited by attackers targeting their web applications.

Cloud Infrastructure Security: With the increasing adoption of cloud services, Nessus has extended its capabilities to assess the security of cloud environments such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP). It can identify misconfigurations and security gaps in cloud instances, storage, and services.

Mobile Application Security: Mobile apps can also be scanned for security vulnerabilities that could compromise user data or expose the application to attacks. Nessus helps identify issues such as insecure data storage, improper authentication, and code vulnerabilities.

Compliance Auditing: Many industries and organizations are subject to regulatory compliance requirements (e.g., PCI DSS, HIPAA, GDPR). Nessus can perform compliance audits to ensure that systems and networks adhere to the necessary security standards.

Penetration Testing Support: While Nessus is not a full-fledged penetration testing tool, it can be used as part of a larger penetration testing effort to identify initial vulnerabilities before more advanced testing techniques are employed.

Risk Assessment and Prioritization: Nessus provides risk scores and severity ratings for identified vulnerabilities, helping organizations prioritize which vulnerabilities should be addressed first based on their potential impact and likelihood of exploitation.

Reporting and Documentation: Nessus generates detailed reports with information about the identified vulnerabilities, their severity, and recommended remediation steps. These

reports are useful for communicating security status to stakeholders and for tracking progress in addressing vulnerabilities.

Continuous Monitoring: Security is an ongoing process, and Nessus can be scheduled to perform regular scans on a predetermined basis. This helps organizations maintain an up-to-date understanding of their security posture and address new vulnerabilities as they emerge.

Target WebSite : SASI Institute of Technology & Engineering

https://www.sasi.ac.in/

Target IP : 184.168.97.172

Here are some of the Initial screenshot of Nessus doing the vulnerability scanning of IP address 184.168.97.172

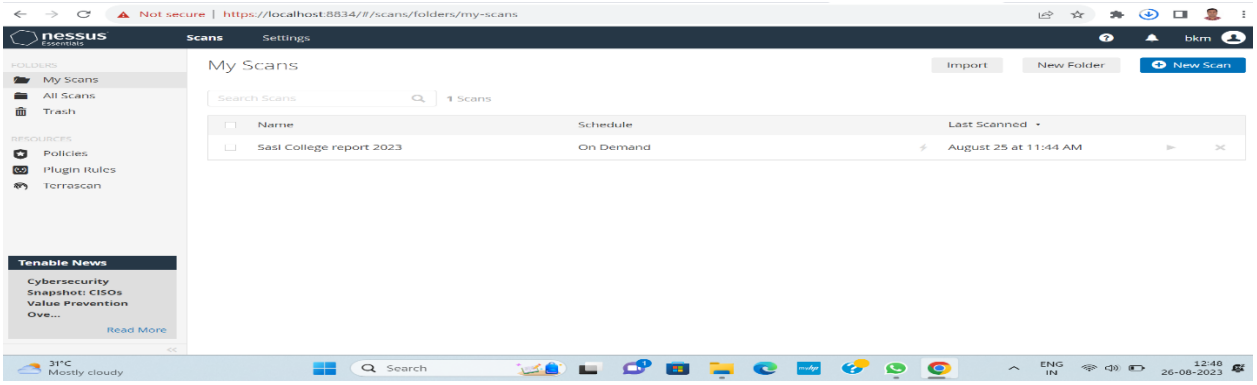


Figure 1: Home page of the Nessus vulnerability scanning

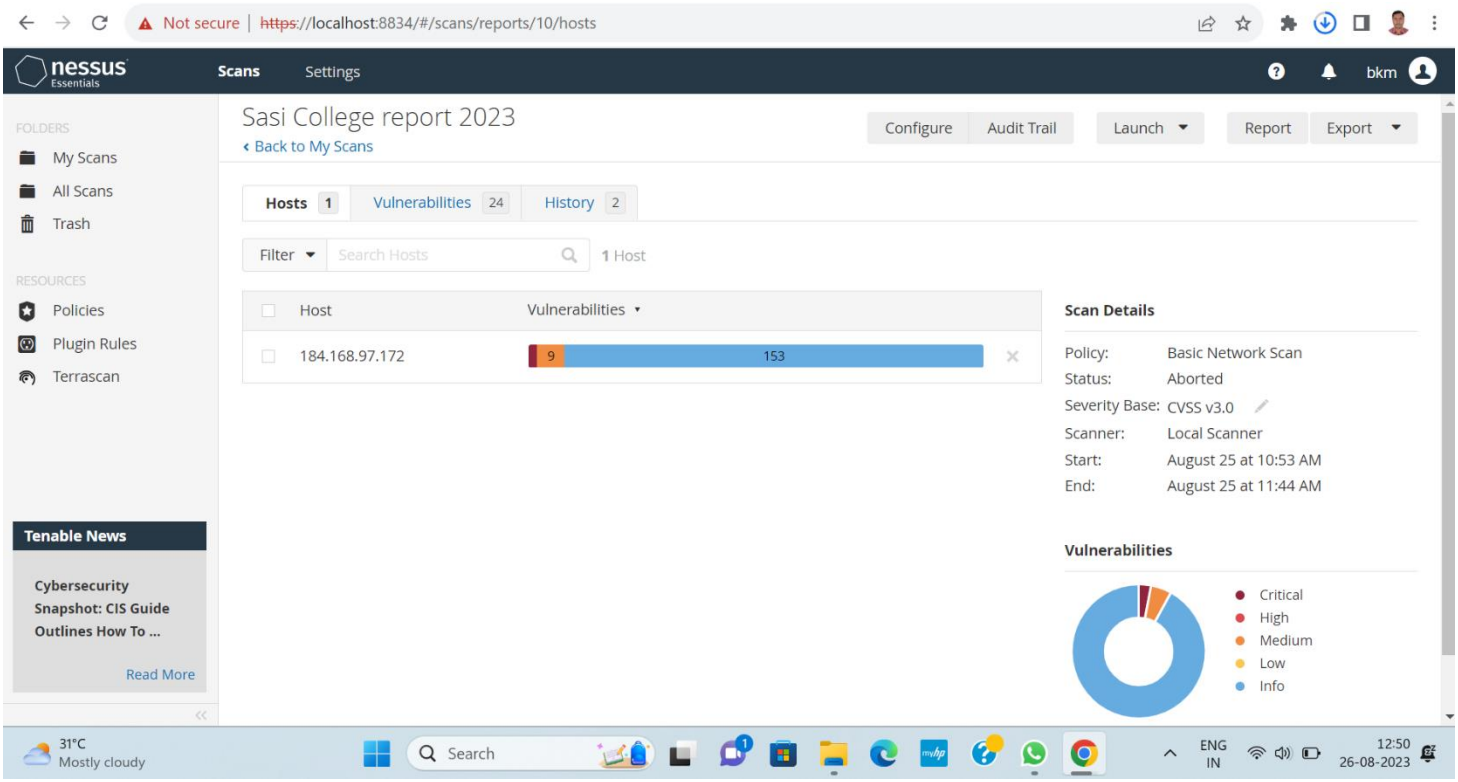


Figure 2: It show Nessus vulnerability scanning details like policy, status, etc.

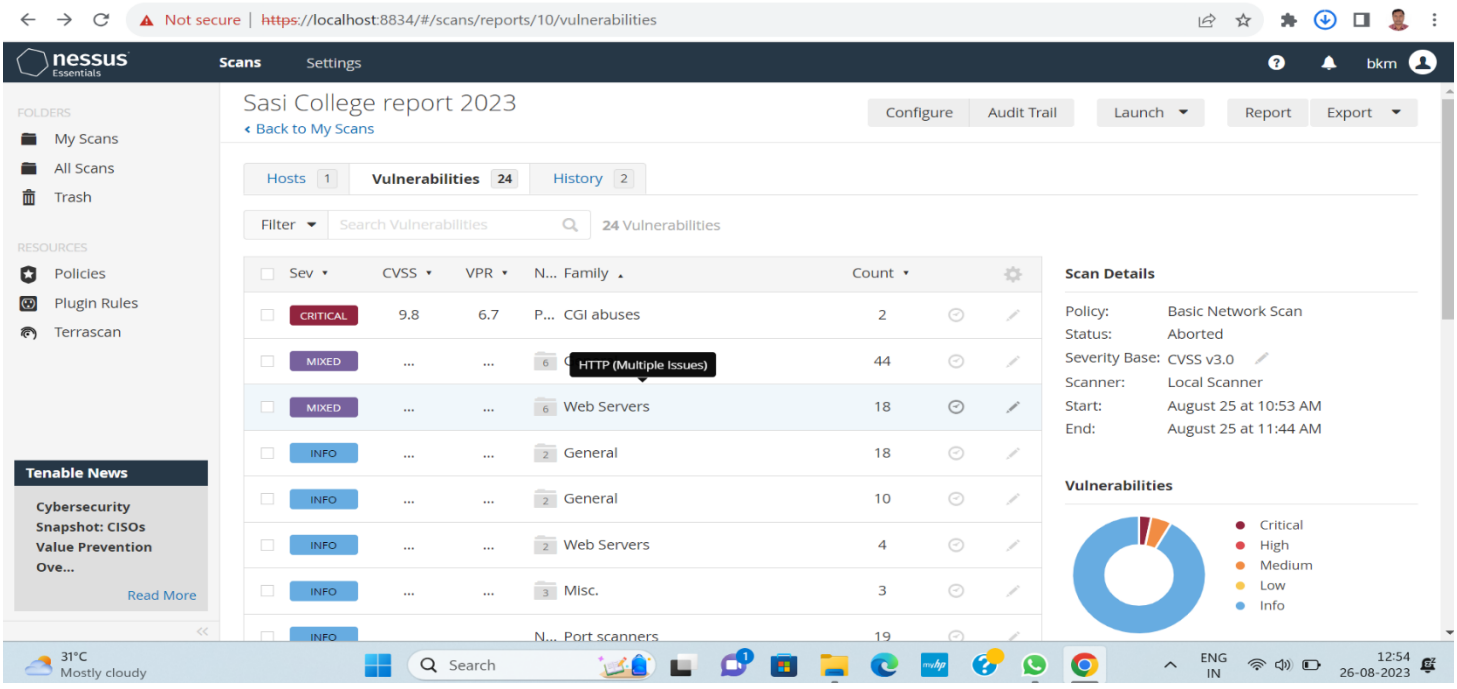


Figure 3: It show number of vulnerability and types.

S.No.	Vulnerability name	Security	Plugin	Description	Solution	Business Impact	Port
1	*PHP 8.1.x < 8.1.22 Multiple Vulnerabilities*	*CRITICAL*	*179317*	The version of PHP installed on the remote host is prior to 8.1.22. It is, therefore, affected by multiple vulnerabilities as referenced in the Version 8.1.22 advisory. Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.	Upgrade to PHP version 8.1.22 or later.	Vulnerabilities in software, including programming languages like PHP, can have significant business impacts depending on the nature of the vulnerabilities, the systems affected, and the potential for exploitation.	443
2	*SSL Certificate with Wrong Hostname*	*MEDIUM*	*45411*	The 'commonName' (CN) attribute of the SSL certificate presented for this service is for a different machine.	Purchase or generate a proper SSL certificate for this service.	Identify Affected Systems, Assess Risk Replace or Update Certificates	2078, 2080, 110, 143, 993, 2083, 995, 2096

3	*HSTS Missing From HTTPS Server (RFC 6797)*	*MEDIUM*	*142960*	The remote web server is not enforcing HSTS, as defined by RFC 6797. 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.	Understand the Risk, Implement HSTS Headers	443
4	*Reverse NAT/Intercepting Proxy Detection*	*Info*	*31422*	Reverse NAT is a technology which lets multiple computers offer public services on different ports via the same IP address. Based on OS fingerprinting results, it seems that different operating systems are	Make sure that this setup is authorized by your security policy	Analyze Network Traffic Patterns, Examine HTTP Headers, Check for Forwarded Headers	N/A

				listening on different remote ports. Note that this behavior may also indicate the presence of a intercepting proxy, a load balancer or a traffic shaper.			
5	*SSL Certificate Signed Using Weak Hashing Algorithm (Known CA)*	*INFO*	*95631*	The remote service uses a known CA certificate in the SSL certificate chain that has been signed using a cryptographically weak hashing algorithm (e.g., MD2, MD4, MD5, or SHA1). These signature algorithms are known to be vulnerable to collision attacks (CVE-2004-2761, for example). An attacker can exploit this to generate another certificate with the same digital signature, allowing the	Contact the Certificate Authority to have the certificate reissued.	Identify Affected Certificates, Certificate Replacement, Configuration Updates, Certificate Revocation	2078, 2080, 110, 143, 993, 2083, 995, 2096

				attacker to masquerade as the affected service. Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire after January 1, 2017 as vulnerable. This is in accordance with Google's gradual sunsetting of the SHA-1 cryptographic hash algorithm. Note that this plugin will only fire on root certificates that are known certificate authorities as listed in Tenable Community Knowledge Article 000001752. That is what differentiates this plugin from plugin 35291, which will fire on any certificate,			

				not just known certificate authority root certificates. Known certificate authority root certificates are inherently trusted and so any potential issues with the signature, including it being signed using a weak hashing algorithm, are not considered security issues.			
6	*Additional DNS Hostnames*	*INFO*	*46180*	Hostnames different from the current hostname have been collected by miscellaneous plugins. Nessus has generated a list of hostnames that point to the remote host. Note that these are only the alternate hostnames for vhosts discovered on a web server.	If you want to test them, re-scan using the special vhost syntax, such as : www.example.com[192.0.32.10]	SSL/TLS Configuration, TTL Configuration	N/A

				Different web servers may be hosted on name-based virtual hosts.			
7	*SSL/TLS Recommended Cipher Suites*	*INFO*	*156899*	The remote host has open SSL/TLS ports which advertise discouraged cipher suites. It is recommended to only enable support for the following cipher suites: TLSv1.3: - 0x13,0x01 TLS13_AES_128_GCM_SHA256 - 0x13,0x02 TLS13_AES_256_GCM_SHA384 - 0x13,0x03 TLS13_CHACHA20_POLY1305_SHA256 TLSv1.2: - 0xC0,0x2B ECDHE-ECDSA-AES128-GCM-SHA256 - 0xC0,0x2F ECDHE-RSA-AES128-GCM-SHA256 - 0xC0,0x2C	Only enable support for recommened cipher suites.	Perfect Forward Secrecy (PFS), Disable Weak Algorithms, Cipher Suite Order	443

				ECDHE-ECDSA-AES256-GCM-SHA384 - 0xC0,0x30 ECDHE-RSA-AES256-GCM-SHA384 - 0xCC,0xA9 ECDHE-ECDSA-CHACHA20-POLY1305 - 0xCC,0xA8 ECDHE-RSA-CHACHA20-POLY1305 - 0x00,0x9E DHE-RSA-AES128-GCM-SHA256 - 0x00,0x9F DHE-RSA-AES256-GCM-SHA384 This is the recommended configuration for the vast majority of services, as it is highly secure and compatible with nearly every client released in the last five (or more) years.			
8	*Traceroute Information*	*INFO*	*10287*	Makes a traceroute to the remote host.	To see debug logs, please visit	Identify Bottlenecks, Monitor	0

					individual host	Service Providers, perform traceroute tests to identify unauthorized network routes or unexpected hops that might indicate potential security breaches	
9	*POP3 Service STLS Command Support*	*INFO*	*42087*	The remote POP3 service supports the use of the 'STLS' command to switch from a cleartext to an encrypted communications channel.	The remote POP3 service responded to the 'STLS' command with an '+OK' response code, suggesting that it supports that command. However, Nessus failed to negotiate a TLS connection or get the	Understand POP3 and TLS, Client Compatibility, Configure your email clients to validate the server's SSL/TLS certificate. This helps prevent man-in-the-middle attacks	110

					associated SSL certificate, perhaps because of a network connectivity problem or the service requires a peer certificate as part of the negotiation.		
10	*TLS Version 1.2 Protocol Detection*	*info*	*136318*	The remote service accepts connections encrypted using TLS 1.2.	TLSv1.2 is enabled and the server supports at least one cipher.	Certificate Transparency Logs, Regular Audits	2078, 2080, 443, 110, 143, 993, 2083, 995, 2096
11	*POP Server Detection*	*Info*	*10185*	The remote host is running a server that understands the Post Office Protocol (POP), used by email clients to retrieve messages from a server, possibly across a network	Disable this service if you do not use it.	Implement network monitoring solutions that can detect and monitor POP server traffic. This helps identify existing and new POP server	110, 995

				link.		instances	
12	*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. Nessus has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate.	CGI scanning will be disabled for this host because the host responds to requests for non-existent URLs with HTTP code 301 rather than 404. The requested URL was : http://172.97.168.184.host.secureserver.net/jxfPiQYWWNOs.html	Review and ensure that your web server's configuration is set up to generate and return proper "404 Not Found" responses when a requested resource is not available	80, 2083, 2096
13	*WebDAV Detection*	Info	*11424*	WebDAV is an industry standard extension to the HTTP specification. It adds a capability for authorized users	http://support.microsoft.com/default.aspx?kbid=241520	WebDAV (Web Distributed Authoring and Versioning) is an extension of the HTTP protocol that	2078

				to remotely add and manage the content of a web server. If you do not use this extension, you should disable it.		allows collaborative editing and management of files on remote web servers. Detecting WebDAV usage on your network is important for security and network management	
14	*Apache HTTP Server Version*	Info	*48204*	The remote host is running the Apache HTTP Server, an open source web server. It was possible to read the version number from the banner.	https://httpd.apache.org/	Managing the version of your Apache HTTP Server is crucial for security and compatibility reasons. Older versions may have known vulnerabilities that attackers can exploit	80, 443
15	*Nessus SYN scanner*	Info	*11219*	This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target. Note that SYN	Protect your target with an IP filter.	Nessus is a widely used vulnerability scanning tool that offers various scanning methods, including the	21, 22, 25 , 80, 110 , 143, 443, 993, 995, 2000, 2077, 2078,

				scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.		SYN scanner. The SYN scanner is used to identify open ports and potential vulnerabilities on target systems by sending SYN packets as part of a TCP handshake	2080, 2082, 2083, 2095, 2096, 3306, 5060

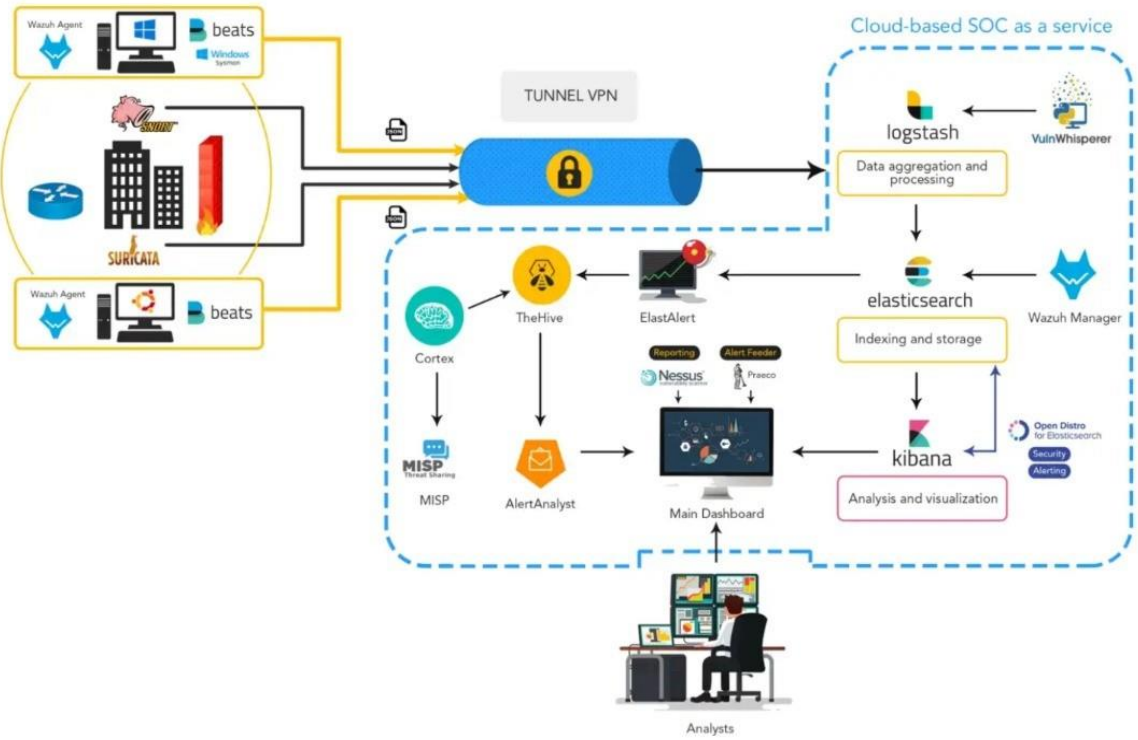
Stage 3 Report

"Unveiling the Power of SOC/SIEM"

- **Soc:**

A Security Operations Center (SOC) is a centralized unit within an organization that is responsible for monitoring, detecting, analyzing, and responding to various security incidents and threats in real-time. Its primary goal is to ensure the confidentiality, integrity, and availability of an organization's digital assets and information systems. A well-functioning SOC serves as the nerve center for an organization's cybersecurity efforts, providing a proactive and coordinated approach to identifying and mitigating potential security risks.

- **Soc Cycle:**



The SOC (Security Operations Center) cycle refers to the continuous and iterative process that a SOC follows to manage and respond to security incidents and threats effectively. It encompasses various stages that help the SOC team detect, analyze, respond to, and learn from security events. The SOC cycle typically consists of the following phases:

Detection: This is the initial phase where the SOC team monitors various data sources, such as network traffic, system logs, and security alerts generated by different tools and technologies. The goal is to identify anomalies, suspicious activities, and potential security incidents.

Analysis: Once an event or potential incident is detected, the SOC analysts dive deeper into the data to understand the nature of the event. They analyze the event's context, severity, and potential impact on the organization's systems and data.

Prioritization: After analysis, the SOC team determines the severity and criticality of

the event. Not all events are equal in terms of risk, so the team needs to prioritize their response efforts based on the potential impact on the organization's operations and security.

Containment: If an incident is confirmed, the SOC initiates containment measures to prevent the incident from spreading further. This might involve isolating affected systems, restricting access, or taking other measures to limit the incident's impact.

Eradication: After containment, the SOC focuses on eliminating the root cause of the incident. This might involve removing malicious software, applying patches, or implementing other corrective actions to ensure that the incident doesn't recur.

Recovery: Once the threat is eliminated, the SOC team works on restoring affected systems and services to their normal state. This phase ensures that the organization's operations can resume without significant disruptions.

Lessons Learned: After the incident is resolved, the SOC conducts a post-incident review. This review involves assessing how well the incident was handled, identifying any gaps in processes or tools, and determining what improvements can be made to enhance the organization's overall security posture.

Documentation: Throughout the entire SOC cycle, thorough documentation is crucial. Detailed records of the incident, analysis, response actions, and outcomes are maintained. This documentation serves as a valuable resource for future incident investigations and for refining incident response procedures.

Continuous Improvement: The insights gained from the post-incident review feed into the SOC's continuous improvement efforts. The team uses this information to update and refine their detection and response strategies, as well as to enhance training and skill development.

Threat Hunting: In addition to responding to incidents, the SOC may also proactively

hunt for threats. This involves actively searching for signs of hidden or advanced threats that may not be immediately apparent from automated alerts.

The SOC cycle is iterative, meaning that the process is ongoing and adapts to the changing threat landscape and evolving organizational needs. By following a well-defined cycle, a SOC can effectively manage security incidents, minimize the impact of breaches, and continuously enhance the organization's overall cybersecurity posture.

- **SIEM:** SIEM stands for Security Information and Event Management. It refers to a comprehensive approach to security management that combines the capabilities of two distinct types of tools: Security Information Management (SIM) and Security Event Management (SEM). SIEM systems provide a centralized platform for collecting, analyzing, and correlating security-related data from various sources across an organization's IT infrastructure.

  Key features and functions of SIEM systems include:

  - Log Collection: SIEM systems gather log data from a wide range of sources, including network devices, servers, operating systems, applications, firewalls, intrusion detection/prevention systems, and more. This data is collected in real time and used to gain insights into the organization's security posture.
  - Event Correlation: SIEM tools correlate events and log entries from different sources to identify patterns, anomalies, and potential security incidents. Correlation helps in detecting sophisticated threats that might go unnoticed when analyzing individual events.
  - Alerting and Notification: When the SIEM system identifies an event or pattern that matches predefined rules or baselines, it generates alerts or notifications. These alerts can be sent to SOC analysts for further investigation and response.
  - Threat Detection: SIEM systems use advanced analytics and machine learning techniques to detect both known and unknown

threats. This includes identifying unauthorized access, malware infections, insider threats, and other suspicious activities.

- Incident Response: SIEM platforms facilitate incident response by providing SOC teams with contextual information about incidents, helping them assess the severity and scope of the threat, and guiding them in taking appropriate response actions.
- Compliance Monitoring: SIEM systems assist organizations in meeting regulatory and compliance requirements by monitoring and reporting on security events and activities. They can generate audit trails and reports for compliance audits.
- User and Entity Behavior Analytics (UEBA): Some SIEM solutions incorporate UEBA capabilities to analyze user and entity behavior over time. This helps in identifying deviations from normal behavior that could indicate a compromised account or insider threat.
- Data Correlation: SIEM tools correlate data from various sources, such as user activity, network traffic, and system logs, to provide a holistic view of security events. This helps in identifying multi-stage attacks that span different parts of the organization's infrastructure.
- Forensic Analysis: SIEM systems support forensic investigations by providing historical data and context around security incidents. This is essential for understanding the timeline and impact of an incident.
- Dashboard and Reporting: SIEM solutions offer customizable dashboards and reports that provide visual insights into an organization's security posture. These tools help management and analysts understand the effectiveness of security measures.
- Integration: SIEM systems can integrate with other security tools and technologies, enhancing their capabilities by combining data from various sources. This can include threat intelligence feeds, endpoint detection and response (EDR) systems, and more.
- In essence, SIEM systems play a critical role in aggregating, analyzing, and responding to security events and incidents within

an organization's environment. They provide a centralized platform for improving threat detection, incident response, compliance monitoring, and overall security management.

- **SIEM Cycle:** The lifecycle of a Security Information and Event Management (SIEM)system involves several interconnected stages that ensure the effective implementation, operation, and maintenance of the SIEM solution. The SIEM life cycle typically includes the following phases:

Planning and Assessment:

Define the objectives and scope of the SIEM implementation, considering the organization's security requirements and compliance goals.

Conduct a thorough assessment of the existing security infrastructure, data sources, and log management practices to identify gaps and necessary improvements.

Develop a detailed plan for deploying the SIEM solution, including resource allocation, timeline, and responsibilities.

Design and Architecture:

Design the SIEM architecture based on the organization's requirements and data sources, considering factors like scalability, redundancy, and performance.

Determine the best deployment model (on-premises, cloud-based, hybrid) that aligns with the organization's needs and resources.

Plan the integration of data sources into the SIEM, ensuring that relevant security events are collected and centralized for analysis.

Data Collection and Integration:

Implement data collectors and agents to gather logs and events from

various sources, such as firewalls, network devices, servers, applications, and endpoints.

Normalize and enrich the collected data to facilitate efficient analysis and correlation.

Configure connectors and parsers to integrate data feeds from security devices and other sources into the SIEM platform.

Event Correlation and Analysis:

Develop and fine-tune correlation rules and use cases to identify patterns of malicious activity and security threats.

Conduct real-time event correlation and analysis to generate actionable alerts for potential security incidents.

Utilize threat intelligence feeds to enhance the SIEM's ability to detect emerging threats and known attack vectors.

Incident Detection and Response:

Respond to generated alerts by investigating potential security incidents.

Perform detailed analysis to determine the scope and impact of identified security events.

Initiate incident response activities, including containment, eradication, and recovery.

Forensics and Investigation:

Conduct in-depth forensics analysis to understand the root cause of incidents and the methods used by attackers.

Preserve and document evidence for potential legal or regulatory purposes.

Reporting and Compliance:

Generate and present security reports and dashboards for various stakeholders, including IT management, executives, auditors, and regulatory authorities.

Ensure compliance with relevant industry standards and regulations by monitoring and reporting on security events and incidents.

Continuous Monitoring and Maintenance:

Continuously monitor the SIEM infrastructure and adjust the configuration as needed to maintain optimal performance.

Regularly update correlation rules, threat intelligence feeds, and other components to keep the SIEM effective against evolving threats.

Conduct periodic reviews and assessments of the SIEM's performance and effectiveness to identify areas for improvement.

Training and Knowledge Transfer:

Train SOC personnel and IT staff on the effective use of the SIEM solution.

Foster knowledge sharing and best practices from incident investigations and analysis within the organization.

The SIEM lifecycle is a continuous and iterative process, with each phase building upon the insights and experiences gained from previous stages. This approach ensures that the SIEM solution remains relevant, efficient, and effective in helping organizations detect and respond to security threats.

As a syslog server incessantly pings with every security notification, security teams can feel as though they are drowning in a sea of security warnings. Without a SIEM, it’s difficult to know which events are trulycritical and which can be ignored. However, when a SIEM has been implemented, security teams get a much clearer picture of their environment’s security. There could truly be no threats, or multiple incidents may be occurring that simply have not yet affected performance.

- **MISP:** MISP stands for "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 communities. MISP provides a collaborative environment for collecting, storing, sharing, and correlating information about threats, indicators of compromise (IoCs), attack techniques,

vulnerabilities, and more. It aids in the dissemination of timely and actionable threat intelligence, enabling organizations to enhance their cybersecurity efforts and response capabilities.

Key features and components of MISP include:

- Event Management: MISP allows users to create and manage "events," which represent specific threat intelligence reports, observations, or incidents. Each event can contain a variety of information, including indicators, threat actor details, malware samples, and more.
- Indicator Sharing: Users can input and share various types of indicators, such as IP addresses, domain names, hashes (MD5, SHA-1, SHA-256), email addresses, and more. These indicators help identify potential threats in an organization's environment.
- Taxonomies: MISP supports multiple taxonomies and classification systems, allowing users to categorize and label threat intelligence data according to different standards, such as ATT&CK, CAPEC, and more.
- Collaboration: MISP encourages collaboration among different organizations and teams by enabling the sharing of threat intelligence data in a controlled manner. Users can choose who to share their data with and set access levels.
- Correlation and Enrichment: MISP allows users to correlate and enrich data by linking related indicators and attributes within events. This helps in identifying complex attack patterns and attributing them to specific threat actors or campaigns.

- **YOUR COLLEGE INFORMATION:**
- **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:

- 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.

Budget and Resource Allocation:

- Determine the budget and resource requirements forestablishing and maintaining the SOC.
- Allocate personnel, hardware, software, and other necessaryresources to support the SOC operations.

Build a Skilled Team:

- Recruit or assign skilled security professionals to form the SOCteam.
- The team should include security analysts, incident responders,threat hunters, and SOC management personnel.

Infrastructure and Technology Setup:

- Establish the physical or virtual infrastructure for the SOC,including servers, network equipment, and storage.
- Deploy the required security technologies, such as SIEM, intrusion detection and prevention systems (IDS/IPS), firewalls,endpoint protection, and threat intelligence feed

Integration and Data Collection:

- Integrate security tools and systems with the SIEM to centralizelog and event data collection.
- Ensure that critical data sources, such as firewalls, servers,network devices, and applications, are sending logs to the SIEM.

Establish Processes and Procedures:

- Define standard operating procedures (SOPs) for various SOCactivities, including incident handling, response protocols, escalation procedures, and communication guidelines.
- Implement incident categorization and prioritizationmechanisms.

Implement Monitoring and Alerting:

- Configure the SIEM to generate real-time alerts based onpredefined correlation rules and security use cases.
- Fine-tune alerting thresholds to minimize false positives andfocus on critical alerts.

Incident Response and Escalation:

- Develop a formal incident response plan that outlines the stepsto be taken in the event of a security incident.
- Define roles and responsibilities for incident handling andescalation path for severe incidents.

Training and Skill Development:

- Provide comprehensive training to the SOC team on the use ofsecurity tools, incident analysis, threat hunting, and incident response best practices.
- Keep the team updated on the latest cybersecurity trends,attack techniques, and relevant certifications.

Testing and Continuous Improvement:

- Conduct regular tabletop exercises and simulated cyber-attackscenarios to test the SOC team's response capabilities.
- Use the insights gained from testing to improve and refine the SOC's processes and procedures.

Monitoring and Reporting:

- Continuously monitor the SOC's performance and effectiveness in detecting and responding to security incidents.

- Generate regular reports and metrics to measure the SOC's performance and communicate its value to stakeholders.

Integration with IT and Business Functions:

- Foster collaboration between the SOC and other IT and business units to ensure a coordinated approach to security.
- Engage with executive management and board members to gain support and buy-in for SOC initiatives.
- Deploying a SOC is an ongoing process that requires adaptability and continuous improvement. Regular assessments, training, and updates are essential to ensure that the SOC remains effective in addressing

the organization's evolving security challenge.

- **THREAT INTELLIGENCE:** Threat intelligence refers to the knowledge and insights gained from analyzing information about potential or actual cybersecurity threats, vulnerabilities, attack techniques, and malicious actors. It involves collecting, processing, and analyzing data from various sources to understand the tactics, techniques, and procedures (TTPs) that adversaries use to target organizations' information systems, networks, and digital assets. Threat intelligence helps organizations proactively identify and mitigate risks, enhance their cybersecurity posture, and make informed decisions to protect their assets.

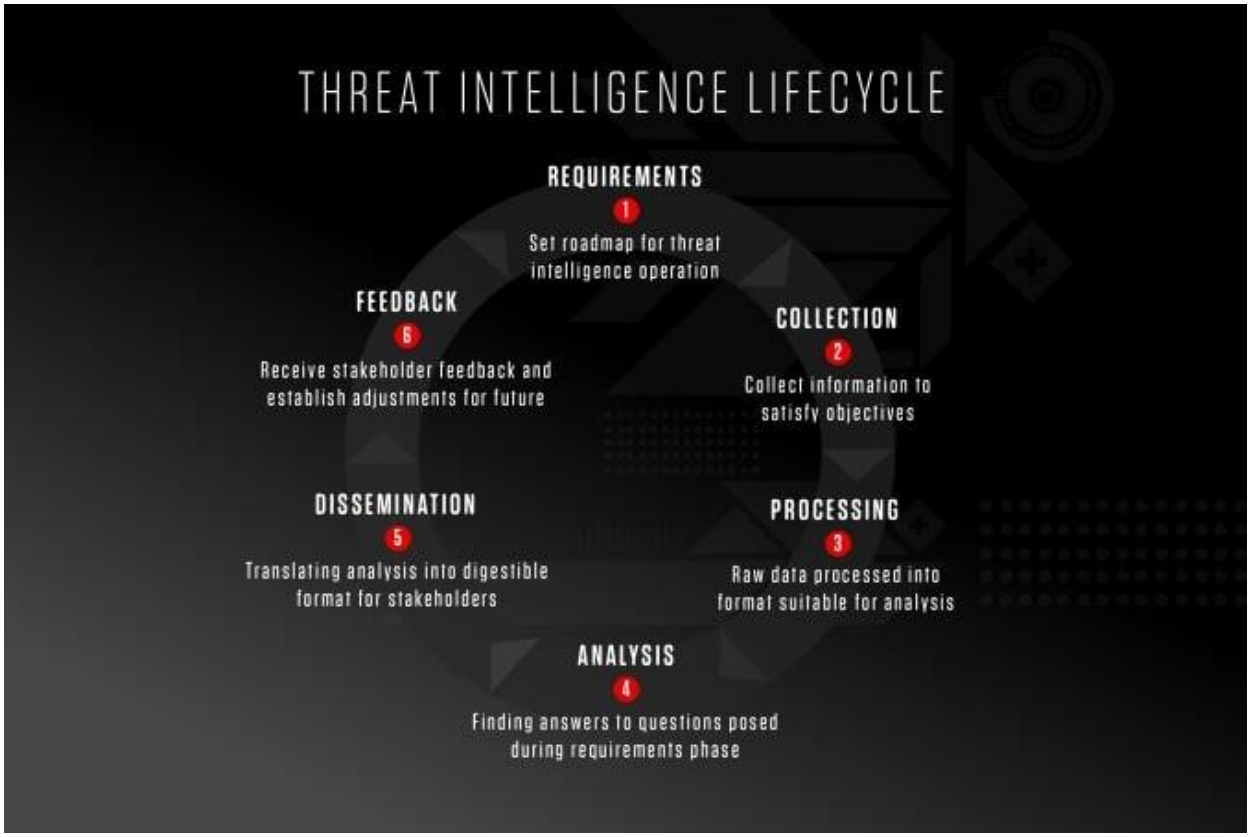
  Key aspects of threat intelligence include:

  - Indicators of Compromise (IoCs): IoCs are specific pieces of information that indicate a potential security threat. These can include IP addresses, domain names, URLs, hashes, filenames, email addresses, and more. IoCs are used to identify malicious activity and protect against attacks.
  - Tactics, Techniques, and Procedures (TTPs): Threat intelligence provides insights into the methods attackers use to compromise systems and evade detection. Understanding TTPs helps organizations detect and defend against sophisticated attacks.
  - Threat Actors: Threat intelligence identifies and profiles malicious actors, such as hacker groups, cybercriminals, state-sponsored attackers, hacktivists, and insiders. Understanding the motives, capabilities, and targets of threat actors aids in preemptive defense.
  - Attack Surfaces: Threat intelligence helps organizations identify vulnerabilities and weaknesses in their systems, networks, and applications that attackers might exploit. This information guides vulnerability management and patching

efforts.

- Cyber Threat Landscape: Threat intelligence provides a comprehensive view of the current and evolving cybersecurity threat landscape. This includes emerging threats, attack trends, and new attack vectors.
- Strategic and Tactical Insights: Threat intelligence can be categorized as strategic or tactical. Strategic intelligence focuses on long-term trends, threat actor motivations, and geopolitical factors influencing cyber threats. Tactical intelligence provides specific details about recent attacks and vulnerabilities.
- Internal and External Intelligence: Organizations can gather threat intelligence from internal sources (logs, network traffic, endpoint data) as well as external sources (open-source threat feeds, commercial threat intelligence providers, cybersecurity communities).
- Sharing and Collaboration: Threat intelligence sharing allows organizations to collaborate with peers, industry groups, and government agencies. Sharing helps warn others about emerging threats and improves overall collective defense.
- Contextual Analysis: Threat intelligence should provide context around threats, including information about the target industry, geographical location, and possible impact. This context helps organizations prioritize and respond to threats effectively.
- Automated Threat Intelligence: Advanced tools and platforms automate the collection, analysis, and dissemination of threat intelligence. This speeds up response times and allows for real-time threat detection.
- Incident Response: Threat intelligence informs incident response teams about the nature of ongoing or potential incidents. It aids in rapid detection, containment, eradication,

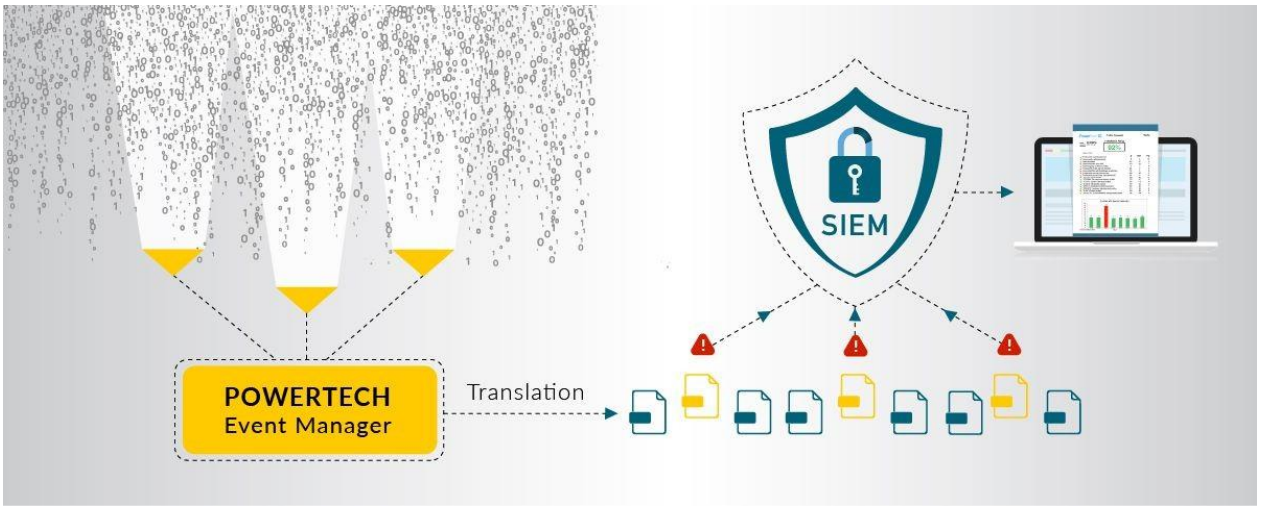
and recovery efforts.



LIFE CYCLE OF THREAT INTELLIGENCE

- **Threat Detection:**

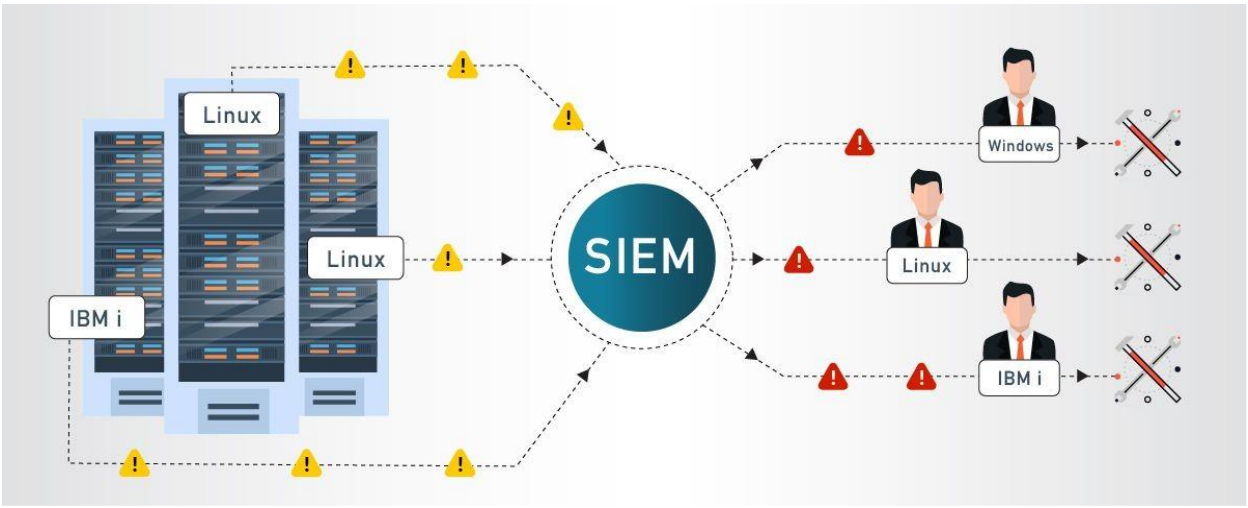
Translation:



Prioritization:

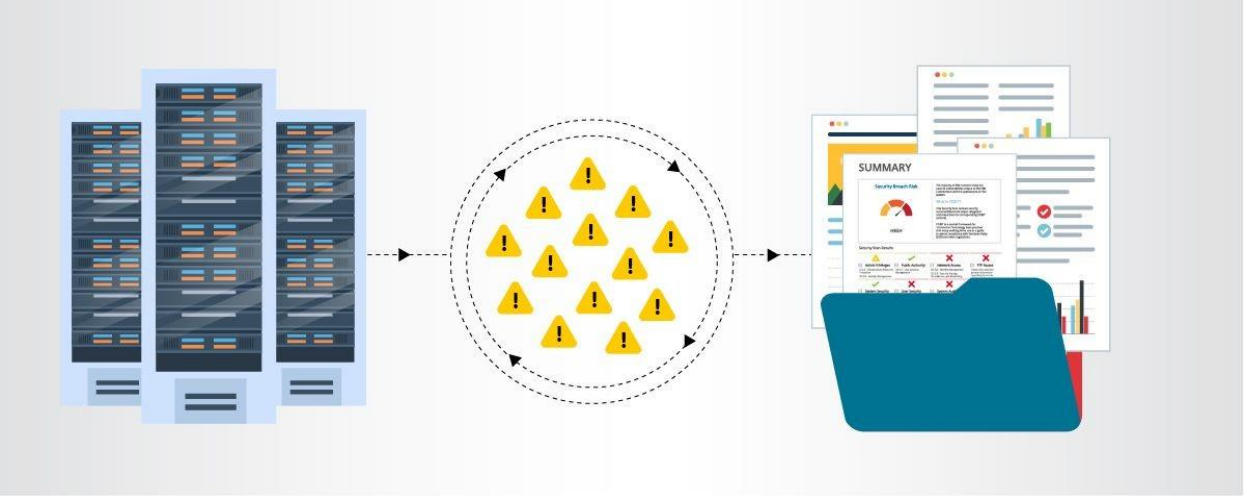

SIEM
HIGHLIGHTED EVENT
SECURITY THREAT
SECURITY INCIDENT

Escalation:



Analysis:

Compliance:



- **Incident response**

Incident response is a term used to describe the process by which an organization handles a data breach or cyberattack, including the way the organization attempts to manage the consequences of the attack or breach (the "incident"). Ultimately, the goal is to effectively manage the incident so that the damage is limited and both recovery time and costs, as well as collateral damage such as brand reputation, are kept at a minimum.

Organizations should, at minimum, have a clear incident response plan in place. This plan should define what constitutes an incident for the company and provide a clear, guided process to be followed when an incident occurs. Additionally, it's advisable to specify the teams, employees, or leaders responsible for both managing the overall incident response initiative and those tasked with taking each action specified in the incident response plan.

Who Handles Incident Responses?

Typically, incident response is conducted by an organization's computer incident response team (CIRT), also known as a cyber incident response team. CIRTs usually are comprised of security and general IT staff, along with members of the legal, human resources, and public relations departments. As Gartner describes, a CIRT is a group that "is responsible for responding to security breaches, viruses, and other potentially catastrophic incidents in enterprises that face significant security risks. In addition to technical specialists capable of dealing with specific threats, it should include experts who can guide enterprise executives on appropriate communication in the wake of such incidents."

Six Steps for Effective Incident Response

Preparation - The most important phase of incident response is preparing for an inevitable security breach. Preparation helps organizations determine how well their CIRT will be able to respond to an incident and should involve policy, response plan/strategy, communication, documentation, determining the CIRT members, access control, tools, and training.

Identification - Identification is the process through which incidents are detected, ideally promptly to enable rapid response and therefore reduce costs and damages. For this step of effective incident response, IT staff gathers events from log files, monitoring tools, error messages, intrusion detection systems, and firewalls to detect and determine incidents and their scope.

Containment - Once an incident is detected or identified, containing it is a top priority. The main purpose of containment is to contain the damage and prevent further damage from occurring (as noted in step number two, the earlier incidents are detected, the sooner they can be contained to minimize damage). It's important to note that all of SANS' recommended steps within the containment phase should be taken, especially to "prevent the destruction of any evidence that may be needed later for prosecution." These

steps include short-term containment, system back-up, and long-term containment.

Eradication - Eradication is the phase of effective incident response that entails removing the threat and restoring affected systems to their previous state, ideally while minimizing data loss. Ensuring that the proper steps have been taken to this point, including measures that not only remove the malicious content but also ensure that the affected systems are completely clean, are the main actions associated with eradication.

Recovery - Testing, monitoring, and validating systems while putting them back into production in order to verify that they are not re-infected or compromised are the main tasks associated with this step of incident response. This phase also includes decision making in terms of the time and date to restore operations, testing and verifying the compromised systems,

monitoring for abnormal behaviors, and using tools for testing, monitoring, and validating system behavior.

Lessons Learned - Lessons learned is a critical phase of incident response because it helps to educate and improve future incident response efforts. This is the step that gives organizations the opportunity to update their incident response plans with information that may have been missed during the incident, plus complete documentation to provide information for future incidents. Lessons learned reports give a clear review of the entire incident and may be used during recap meetings, training materials for new CIRT members, or as benchmarks for comparison.

Proper preparation and planning are the key to effective incident response. Without a clear-cut plan and course of action, it's often too late to coordinate effective response efforts and a communication plan after a breach or attack has occurred when future attacks or security events hit. Taking the time to create a comprehensive incident response plan can save your company substantial time and money by enabling you to regain control over your systems and data promptly when an inevitable breach occurs.

The incident response process is the set of procedures taken by an organization in response to a cybersecurity incident. Companies should document their incident response plans and procedures along with information regarding who is responsible for performing the various activities they contain. The failure to develop an incident response plan makes it much more difficult for a business to successfully respond and recover from cyber attacks.

Following are the five steps or pillars of the incident response process.

Identify - Companies need to identify all types of threats and the assets they could affect. This involves inventorying the environment and conducting a

risk assessment.

Protect - All critical assets need to have a protection plan that involves protective technological solutions and employee security awareness training.

Detect - In this step, organizations attempt to detect threats promptly before they have a chance to cause extensive damage to the environment.

Respond - After a threat or incident is detected, a defined response should be put into action to mitigate its damage and prevent its spread to other infrastructure components.

Recover - The recovery step returns the system affected to normal operations. It also evaluates the source of the incident with the goal of identifying improved security measures to prevent its recurrence.

What is the NIST incident response model?

The NIST incident response model involves four phases recommended to effectively handle cybersecurity incidents. Some of the phases can befurther subdivided to provide more steps.

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 - After an incident, the response team should stop its spread, remove the threat from the environment, and begin the process of recovering affected systems.

Post-incident activity - The focus of post-incident activity is identifying lessons learned and using them to strengthen defenses to minimize the probability of similar incidents in the future.

- **Qradar & understanding about tool**

The operation of the QRadar security intelligence platform consists of three layers, and applies to any QRadar deployment structure, regardless of its size and complexity. The following diagram shows the layers that make up

the QRadar architecture.

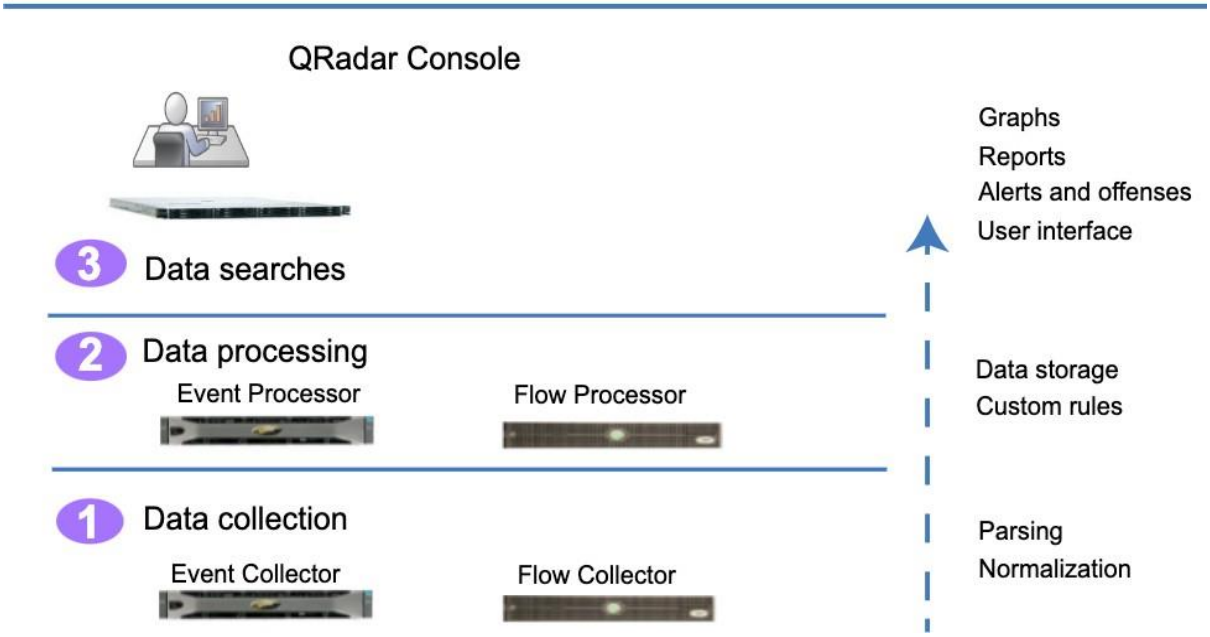


Figure 1. QRadar architecture

The QRadar architecture functions the same way regardless of the size or number of components in a deployment. The following three layers that are represented in the diagram represent the core functionality of any QRadar system.

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 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 .

The outcome of web application testing is to ensure that the application is secure, reliable, and meets its intended functionality. The testing process aims to identify and address potential vulnerabilities, bugs, and usability issues that could impact the application's performance and user experience. The specific outcomes of web application testing include:

- Identification of Security Vulnerabilities
- Bug Detection and Resolution
- Validation of Functional Requirements
- Usability and User Experience Evaluation
- Performance and Load Testing Results
- Compatibility Testing Insights
- Accessibility Compliance
- Security Compliance and Risk Mitigation
- Optimization Recommendations

- Enhanced Quality Assurance
- Increased Customer Confidence
- Compliance with Regulatory Requirements

In summary, the outcome of web application testing is an enhanced, secure, and reliable web application that meets user expectations and delivers a smooth and seamless experience to its users. It provides developers and stakeholders with the confidence that the application is ready for deployment and can withstand potential security threats and performance challenges.

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

Nessus is a vulnerability scanning tool used to identify and report security issues in computer systems and networks.

The outcome of a Nessus report will depend on the specific target scanned and the vulnerabilities found. Typically, a Nessus report will list the identified vulnerabilities along with their severity levels, detailed descriptions, and recommendations for remediation. The severity levels are usually categorized as critical, high, medium, and low, depending on the potential impact and exploitability of the vulnerability.

Conclusion :-

Stage 1 : Understanding about Web application testing.

Web application testing is the systematic evaluation of web-based software applications' functionality, security, performance, and usability. It entails conducting a series of testing and evaluations to identify potential vulnerabilities, guarantee proper functionality, and improve the user experience overall. Web application testing aims to uncover issues, validate compliance with requirements, and provide actionable insights for developers and stakeholders to improve the application's quality, reliability, and resiliency in an ever-changing online environment.

Stage 2 :- Understand about Nessus report .

A Nessus report is a detailed document generated by the Nessus vulnerability scanning utility that outlines the findings and assessment results of a network or system scan. It provides a comprehensive summary of identified vulnerabilities, misconfigurations, and potential security threats within the scanned environment. The report categorizes vulnerabilities by severity, providing insight into critical, high-, medium-, and low-risk issues and recommending corrective actions. The report may also include evidence of the vulnerabilities, affected systems, and CVE (Common Vulnerabilities and Exposures) identifiers. IT teams, security professionals, and stakeholders can comprehend the security posture of their systems, prioritize remediation efforts, and improve overall cybersecurity measures with the assistance of Nessus reports.

Stage 3 Understand from SOC / SEIM / Qradar Dashboard .

Security Information and Event Management (SIEM) systems, such as QRadar, are utilized by a Security Operations Center (SOC) to improve cybersecurity monitoring and response. A QRadar dashboard is a graphical user interface within the SIEM that displays real-time and archival information about security incidents and events. It condenses complex information into readily interpretable charts, graphs, and widgets, enabling SOC analysts to assess the overall security posture, detect anomalies, and identify potential threats with speed. The dashboard offers insights into network traffic, user behavior, and system activities, enabling analysts to identify suspicious patterns and make informed decisions. By consolidating pertinent data and highlighting critical indicators, QRadar dashboards enable SOC

teams to effectively respond to emergent threats, streamline incident investigations, and proactively protect their organization's digital assets.

Future Scope :-

Stage 1 :- future scope of web application testing

Future web application testing will be characterized by a dynamic environment driven by technological advances and changing user expectations. Automation, AI, and machine learning will continue to expedite testing processes, enabling rapid and accurate detection of vulnerabilities and ensuring optimal platform performance. With the proliferation of microservices, APIs, and IoT integration, testing strategies will transition to ensure seamless interactions and security across interconnected components. For inclusive and compliant applications, accessibility testing and strict compliance with data privacy regulations will be required. In addition, the incorporation of testing within

DevSecOps frameworks will cultivate a proactive and continuous approach to security,

while innovative techniques such as red teaming and ethical hacking will play a crucial role in identifying vulnerabilities. The future of testing will revolve around adaptability, automation, and a holistic concentration on security, usability, and compliance as web applications continue to evolve.

Stage 2 :- future scope of testing process you understood .

As a result of technological advancements and shifting development paradigms, the future scope of the testing procedure is likely to change. Automation and AI-powered testing tools will become indispensable, permitting rapid and accurate testing throughout the development lifecycle's various phases. Testing will be seamlessly incorporated into

DevOps and Agile methodologies, allowing for continuous testing that guarantees quality throughout the software delivery pipeline. The transition to cloud-native architectures and microservices will necessitate testing strategies that accommodate dynamic and scalable environments. As IoT and peripheral computing proliferate, testing will encompass a wide variety of devices and platforms. In addition, data-driven insights and analytics will improve testing efficiency and enable data-supported optimization decisions. As the software landscape evolves, the future of software testing will center on sustaining user-centric, secure, and high-performance software solutions.

Stage 3 :- future scope of SOC / SEIM

In response to the ever-changing cybersecurity landscape, the future scope of Security Operations Centers (SOCs) and Security Information and Event Management (SIEM) systems is expected to expand. In response to the increasing complexity and frequency of cyber threats, SOCs will incorporate advanced technologies such as artificial intelligence (AI), machine learning, and automation to improve threat detection and response capabilities. SIEM platforms will evolve to provide real-time insights, predictive analytics, and anomaly detection to facilitate proactive threat mitigation. Integration with cloud services, Internet of Things (IoT) devices, and a wider variety of terminals will expand the monitoring and defense capabilities. In addition, SOCs will collaborate more closely with threat intelligence sharing networks and engage in rapid incident response in order to mitigate the effects of cyber incidents. The future of SOC and SIEM will involve a comprehensive, adaptive, and collaborative approach to cybersecurity, ensuring that organizations remain resilient against evolving threats.

Topics explored :- Kali Linux, Nessus, QRadar,SOC,SIEM,MISP,Theart Intelligence, Incidence Response.

Tools explored :- Metasploit, Traceroot, logstash,Elasticsearch,kibana.