TEAM II

Submitted By:

Dr.Ajay Kumar	Assistant Professor	9953007789 ajay.kumar@bharatividyapeeth.edu

TEAM –II (BHARATI)

A vulnerability assessment

Part I-Executive summary

Overview

Introduction:
The purpose of this executive summary is to provide an overview of the vulnerability assessment conducted for **Thapar University** . This assessment aimed to identify weaknesses and potential threats in the organization's information systems and infrastructure.
Key Findings:

1. **Critical Vulnerabilities**: During the assessment, 28 critical vulnerabilities were identified across various systems and applications. These vulnerabilities pose a severe risk to the organization's security posture, potentially leading to unauthorized access, data breaches, or service disruptions.
2. **Outdated Software:** A significant number of systems were found to be running outdated software and operating systems, leaving them exposed to known vulnerabilities. Updating these systems is crucial to mitigate risks.
3. **Weak Passwords:** Weak and easily guessable passwords were discovered in 30 of user accounts, increasing the likelihood of unauthorized access. Implementing stronger password policies is recommended.
4. **Lack of Patch Management**: The organization's patch management process was found to be ineffective, resulting in unpatched systems and applications. Improved patch management is essential to address critical vulnerabilities promptly.
5. **Inadequate Network Segmentation:** Network segmentation was insufficient, allowing unrestricted lateral movement within the network once an attacker gains access. Implementing stricter network segmentation can limit the impact of security incidents.

Recommendations:

1. **Prioritize Critical Vulnerabilities:** Address critical vulnerabilities immediately, with a focus on high-impact systems and applications. Develop a remediation plan with clear timelines.
2. **Implement Patch Management:** Enhance the patch management process to ensure timely deployment of security patches and updates.
3. **Password Policy Enhancement:** Strengthen password policies, enforce multi-factor authentication (MFA) where feasible, and conduct user awareness training on password security.
4. **Network Segmentation:** Review and improve network segmentation to restrict lateral movement and isolate critical assets.
5. **Regular Assessments**: Schedule periodic vulnerability assessments to continuously monitor and improve the organization's security posture.

Conclusion: The vulnerability assessment revealed significant risks within the organization's infrastructure, including critical vulnerabilities, outdated software, weak passwords, and inadequate network segmentation. Addressing these issues is essential to mitigate security threats effectively. By implementing the recommended measures and conducting regular assessments, **Thapar university** can strengthen its security posture and reduce the likelihood of security incidents.

For detailed understanding of the assessment results and specific remediation steps, below are to the full assessment report.

This executive summary provides a concise overview of the vulnerability assessment's key findings and recommendations, making it easier for senior executives to understand the security risks and prioritize actions to improve the organization's security posture.

IP address of thapar university / 117.203.246.106

2. Team Members Involved in vulnerability Assessment

S.No	Name	Designation	Mobile Number
1	Dr.Ajay Kumar	Assistant Professor	9953007789 ajay.kumar@bharatividyapeeth.edu
2	Dr.Mahesh Kumar Chaubey	Assistant Professor	9899197995 Maheshkumar.chaubey@bharatividyapeeth.edu
3	Mr. Yashwant Kumar	Assistant Professor	9899025905 yashwant.kumar@@bharatividyapeeth.edu

3. List of Vulnerable Parameter, location discovered

S.No	Name of the Vulnerability	Reference CWE
1	Broken Access Control	CWE 285- Improper Authorization
2	Cryptographic Failures	CWE-916: Use of Password Hash WithInsufficient Computational Effort
3	Injection	CWE-564: SQL Injection: Hibernate
4	Insecure Design	CWE-653: Improper Isolation or Compartmentalization
5	Security Misconfiguration	CWE-614:Sensitive Cookie in HTTPSSession Without 'Secure' Attribute
6	Vulnerable and Outdated Components	CWE-1395: Dependency on VulnerableThird-Party Component
7	Identification and Authentication Failures	CWE-521: Weak Password Requirements
8	Software and Data Integrity Failures	CWE-565C: Reliance on Cookies withoutValidation and Integrity Checking
9	Security Logging and Monitoring Failures	CWE-532: Insertion of Sensitive Informationinto Log File
10	Server Side Request Forgery	CWE-918:Server Side Request Forgery

1. CWE: CWE 285- Improper Authorization

OWASP CATEGORY : A01 2021 Broken Access Control

DESCRIPTION: CWE-285, titled "Improper Authorization," is a common software weakness identified in the Common Weakness Enumeration (CWE) system. It refers to situations where a software application or system fails to properly enforce access controls or authorization mechanisms, allowing unauthorized users to access sensitive resources or perform actions that they should not have permission to do. Improper authorization can lead to security breaches, data leaks, and unauthorized operations, posing significant risks to the confidentiality, integrity, and availability of the system.

BUSINESS IMPACT: The business impact of CWE-285, "Improper Authorization," can be significant and detrimental to an organization. Proper authorization and access control are critical components of any secure software or system, and when they are not implemented correctly, various negative consequences can occur, affecting both the organization and its stakeholders. i.e Data Breaches.

2. CWE: CWE-916: Use of Password Hash With Insufficient Computational Effort

OWASP CATEGORY : A02 2021 Cryptographic Failures

DESCRIPTION: CWE-916, titled "Use of Password Hash With Insufficient Computational Effort," refers to a security weakness where an application or system uses a weak or insufficient computational effort when hashing passwords. Hashing passwords is a fundamental security practice used to protect user credentials, and it's critical that the hashing process is computationally intensive enough to resist various attacks, such as brute-force and dictionary attacks.

BUSINESS IMPACT: "Use of Password Hash With Insufficient Computational Effort," can have significant business impacts due to the increased risk of unauthorized access and potential security breaches.

3. CWE: CWE 564: SQL Injection: Hibernate

OWASP CATEGORY : A03 2021 Injection

DESCRIPTION: "SQL Injection: Hibernate," refers to a specific type of vulnerability related to Hibernate, a popular Object-Relational Mapping (ORM) framework used in Java applications. SQL Injection is a well-known security issue that occurs when untrusted data is included in SQL queries without proper validation or sanitization, allowing attackers to manipulate the queries and potentially gain unauthorized access to a database or perform malicious actions.

In the context of Hibernate, which is commonly used for database interactions in Java applications, CWE-564 typically arises due to improper use of Hibernates Query Language (HQL) or Criteria API.

BUSINESS IMPACT: "SQL Injection: Hibernate," can have significant business impacts due to the inherent security risks associated with SQL injection vulnerabilities in Hibernate-based applications. Loss of Customers

Trust, Data Exposure are major impact

4. CWE: CWE 653: Improper Isolation or Compartmentalization

OWASP CATEGORY: A04 2021 Insecure Design

DESCRIPTION: The product violates well-established principles for secure design. This can introduce resultant weaknesses or make it easier for developers to introduce related weaknesses during implementation. Because code is centered around design, it can be resource-intensive to fix design problems.

BUSINESS IMPACT: "Improper Isolation or Compartmentalization," refers to a security weakness where different components or processes within a software system are not adequately isolated or compartmentalized from each other. This lack of proper isolation can lead to a variety of security risks and potential business impacts: Security Breaches, Data Leakage, Unauthorized Access etc

5. CWE: CWE 614-Sensitive Cookie in HTTPS Session Without 'Secure' Attribute

OWASP CATEGORY : A05 2021 Security Misconfiguration

DESCRIPTION: Sensitive Cookie in HTTPS Session Without 'Secure' Attribute," is a specific security weakness identified in the Common Weakness Enumeration (CWE) system. It relates to the improper handling of sensitive cookies in web applications that use HTTPS (Hypertext Transfer Protocol Secure). The 'Secure' attribute is a standard feature of HTTP cookies that instructs web browsers to only transmit the cookie over secure (HTTPS) connections. Failing to set this attribute when required can introduce security risks

BUSINESS IMPACT: "Sensitive Cookie in HTTPS Session Without 'Secure' Attribute," can have several business impacts, primarily related to security vulnerabilities and potential breaches of sensitive data. Failing to set this attribute when required can introduce security risks. Here are the business impacts associated with CWE-614:

Session Hijacking: When sensitive cookies are not marked with the 'Secure' attribute, they can be transmitted over insecure HTTP connections if the user inadvertently accesses an HTTP version of the website. This can make the session vulnerable to interception by attackers, potentially leading to session hijacking. Attackers who intercept these cookies could impersonate users, gain unauthorized access to their accounts, and perform actions on their behalf. Session hijacking can result in data theft, unauthorized transactions, and reputational damage.

Data Tampering: If sensitive cookies are transmitted over unsecured connections, attackers can intercept and tamper with the cookies' contents. This can lead to data corruption, unauthorized changes to user profiles, and manipulation of application behavior.

Security Vulnerabilities: Failure to set the 'Secure' attribute on sensitive cookies may introduce security vulnerabilities that can be exploited by attackers. These vulnerabilities can lead to unauthorized access, data breaches, and other security incidents.

Loss of Customer Trust: Security incidents resulting from the improper handling of sensitive data can erode customer trust in the organization. Users may lose confidence in the security of their data and transactions, leading to a loss of customers and damage to the organization's reputation.

Financial Impact: Addressing security vulnerabilities related to the improper use of the 'Secure' attribute may incur financial costs. Organizations may need to invest in security assessments, vulnerability remediation, incident response, and potential compensation to affected users or clients. Regulatory fines and legal actions can further increase financial burdens.

Regulatory Non-Compliance: Depending on the industry and regulatory environment, failing to set the 'Secure' attribute on sensitive cookies may result in non-compliance with data protection and security standards. This can lead to regulatory fines and legal consequences.

Operational Disruption: Security incidents related to improper cookie handling can disrupt normal business operations. Organizations may need to allocate significant resources to investigate, remediate, and recover from incidents, impacting productivity and increasing operational costs. Here are the business impacts associated with this weakness.

.

6. CWE: CWE 1395: Dependency on Vulnerable Third-Party Component

OWASP CATEGORY: A06 2021 Vulnerable and Outdated Components

DESCRIPTION: The product has a dependency on a third-party component that contains one or many products which are large enough or complex enough and that part of their functionality uses libraries, modules, or other intellectual property developed by third parties who are not the product creator.

BUSINESS IMPACT: "Dependency on Vulnerable Third-Party Component," refers to a security weakness in software development where an application relies on a third-party component that is known to have security vulnerabilities. The business impacts associated with this weakness can be significant and encompass a range of potential consequences:

Security Breaches: Dependency on vulnerable third-party components increases the risk of security breaches. Attackers can exploit known vulnerabilities in these components to gain unauthorized access, execute malicious code, or manipulate data within the application. Such breaches can lead to data theft, unauthorized access to sensitive information, and the compromise of user accounts.

Data Loss or Manipulation: Vulnerable third-party components can be leveraged to manipulate or corrupt data within the application. This can result in data loss, data integrity issues, or the introduction of malicious content into the application's data stores.

Reputation Damage: Security incidents stemming from the use of vulnerable third-party components can severely damage an organization's reputation. Customers and users may lose trust in the application, leading to a loss of business, negative reviews, and public relations challenges.

Financial Impact: Addressing security vulnerabilities in third-party components can be costly. Organizations may incur expenses related to identifying and patching vulnerabilities, responding to security incidents, and potentially compensating affected users or clients. Regulatory fines and legal actions can further increase financial burdens.

Operational Disruption: Security incidents resulting from vulnerable components can disrupt normal operations. Organizations may need to allocate significant resources to investigate and mitigate security incidents, potentially causing downtime, lost productivity, and increased operational costs.

Compliance Violations: Depending on the industry and regulatory environment, the use of vulnerable third-party components may result in compliance violations. Organizations may fail to meet legal and regulatory requirements related to data protection, security, and privacy, potentially leading to fines and legal consequences.

Long-Term Maintenance Issues: Over time, the use of vulnerable third-party components can create long-term maintenance challenges. Constantly addressing security vulnerabilities in these components can be resource-intensive and hinder the development of new features or improvements.

7. CWE: CWE 521-Weak Password Requirements

OWASP CATEGORY: A07 2021 Identification and Authentication Failures

DESCRIPTION: The product does not require that users should have strong passwords, which makes it easier for attackers to compromise user accounts. "Weak Password Requirements," refers to a security weakness where an application or system enforces weak password policies or lacks adequate password complexity requirements.

BUSINESS IMPACT: Weak password requirements can lead to several business impacts:

Security Breaches: Weak passwords are easier for attackers to guess or crack through brute force or dictionary attacks. This increases the risk of unauthorized access to user accounts, systems, and sensitive data. Security breaches can result in data theft, financial losses, and damage to an organization's reputation.

Unauthorized Access: Users who have weak passwords are more vulnerable to unauthorized access to their accounts. This can lead to account compromise, unauthorized actions, and data manipulation. In some cases, weak passwords may enable attackers to gain access to administrative or privileged accounts, causing more significant security incidents.

Data Exposure: Weak passwords can result in the exposure of sensitive data. If accounts with access to sensitive information have weak passwords, attackers may be able to access and exploit this data, potentially leading to regulatory non-compliance and legal consequences.

Account Lockouts and Support Costs: Organizations may experience an increased number of account lockouts and support requests from users who forget their weak passwords. This can lead to additional support costs and user frustration.

Regulatory Non-Compliance: Depending on the industry and regulatory requirements, weak password policies may lead to non-compliance with data protection and security standards. This can result in regulatory fines and legal liabilities.

Loss of Customer Trust: Security incidents resulting from weak password policies can erode customer trust. Users may lose confidence in the organization's ability to protect their data, leading to a loss of customers and a negative impact on the organization's reputation.

Costly Remediation: After discovering the weaknesses in password policies, organizations may need to invest in remediation efforts, such as implementing stronger password policies, educating users on password security, and potentially implementing multi-factor authentication (MFA) solutions. These efforts can be costly and time-consuming.

Operational Disruption: Dealing with security incidents related to weak passwords can disrupt normal business operations. Resources may need to be diverted to investigate, mitigate, and recover from incidents, impacting productivity and increasing operational costs..

8. CWE: CWE-565C Reliance on Cookies without Validation and Integrity Checking

OWASP CATEGORY: A08 2021 Software and Data Integrity Failures

DESCRIPTION: The product relies on the existence or values of cookies when performing security-critical operations, but it does not properly ensure that the setting is valid for the associated user. Attackers can easily modify cookies, within the browser or by implementing the client-side code outside of the browser. Reliance on cookies without detailed validation and integrity checking can allow attackers to bypass authentication, conduct injection attacks such as SQL injection and cross-site scripting, or otherwise modify inputs in unexpected ways.

BUSINESS IMPACT: "Reliance on Cookies without Validation and Integrity Checking," refers to a security weakness where a web application relies on cookies for session management or data storage but fails to adequately validate and check the integrity of these cookies. This vulnerability can lead to several business impacts:

Session Hijacking: Attackers can manipulate or forge cookies if they are not adequately validated and checked for integrity. This can lead to session hijacking, where attackers impersonate legitimate users, gain unauthorized access to user accounts, and perform actions on behalf of the victim. Session hijacking can result in data theft, unauthorized transactions, and reputational damage.

Data Tampering: If cookies are not validated and their integrity is not checked, attackers may modify the content of cookies to inject malicious data or tamper with session-related information. This can lead to data corruption, unauthorized changes to user profiles, and manipulation of application behavior.

Unauthorized Access: Weak cookie validation can allow attackers to craft cookies that grant them unauthorized access to restricted areas or functionalities of the application. This can lead to unauthorized access to sensitive data or administrative controls, potentially causing data breaches and other security incidents.

Loss of Customer Trust: Security incidents resulting from inadequate cookie validation can erode customer trust in the application. Users may lose confidence in the security of their data and transactions, leading to a loss of customers and damage to the organization's reputation.

Financial Impact: Addressing security vulnerabilities related to cookie validation may incur financial costs. Organizations may need to invest in security assessments, vulnerability remediation, incident response, and potential compensation to affected users or clients. Regulatory fines and legal actions can further increase financial burdens.

Regulatory Non-Compliance: In many regions and industries, there are regulations and compliance requirements (e.g., GDPR, HIPAA) that mandate the secure handling of sensitive data, particularly during session management and data storage. Failing to validate and ensure the integrity of cookies can result in non-compliance with these regulations, leading to legal consequences and fines.

Operational Disruption: Security incidents related to improper cookie handling can disrupt normal business operations. Organizations may need to allocate significant resources to investigate and mitigate security incidents, potentially causing downtime, lost productivity, and increased operational costs.

9. CWE: CWE-918 insertion of Sensitive Information into Log File

OWASP CATEGORY: A09 2021 Security Logging and Monitoring

Failures

DESCRIPTION: While logging all information may be helpful during development stages, it is important that logging levels be set appropriately before a product ships so that sensitive user data and system information are not accidentally exposed to potential attackers.

BUSINESS IMPACT: Insertion of Sensitive Information into Log File," is a security weakness that occurs when sensitive or confidential information is unintentionally logged or recorded in a system's log files. This can have several business impacts:

Data Exposure: When sensitive information such as passwords, personal identification numbers (PINs), credit card numbers, or personally identifiable information (PII) is logged, it becomes exposed in plain text in log files. Unauthorized access to these log files can result in data breaches and the compromise of sensitive data.

Privacy Violations: Logging sensitive information without proper protection can lead to privacy violations and regulatory non-compliance. In many regions and industries, there are strict regulations governing the handling and storage of sensitive data, such as the General Data Protection Regulation (GDPR) or the Health Insurance Portability and Accountability Act (HIPAA). Failure to comply with these regulations can result in legal consequences, fines, and reputational damage.

Reputation Damage: Security incidents related to the exposure of sensitive data can severely damage an organization's reputation. Customers and users may lose trust in the organization's ability to protect their data, leading to a loss of customers and negative publicity.

Operational Disruption: Dealing with security incidents related to the insertion of sensitive information into log files can disrupt normal business operations. Organizations may need to allocate significant resources to investigate, remediate, and recover from these incidents. This can impact productivity and increase operational costs.

Legal and Regulatory Consequences: Depending on the nature of the sensitive information and the applicable laws and regulations, organizations may face legal consequences for not adequately protecting this data. Legal actions, fines, and legal liabilities can result from data exposure incidents.

Costly Remediation: Identifying and addressing vulnerabilities related to the insertion of sensitive information into log files can be costly. Organizations may need to invest in security assessments, vulnerability remediation, incident response, and potentially compensating affected individuals or entities.

Loss of Competitive Advantage: If a security incident becomes public knowledge, it can erode an organization's competitive advantage and market position. Potential customers may choose to do business with competitors with better security practices.

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 weakness that occurs when an attacker can manipulate a web application into making unauthorized requests to internal or external resources on behalf of the server. This can have several business impacts:

Data Exposure: An attacker can use SSRF to access and retrieve sensitive data from internal resources, such as databases, file systems, or configuration files. This can result in the exposure of confidential information, customer data, or intellectual property, leading to data breaches.

Unauthorized Access: SSRF can allow attackers to bypass security controls and gain unauthorized access to internal systems, services, or interfaces that should not be accessible from the internet. This can lead to unauthorized manipulation of systems, data, or configurations.

Server Misuse: Attackers can abuse SSRF to make the server perform unintended actions, such as initiating attacks on other systems, scanning internal networks, or launching distributed denial-of-service (DDoS) attacks on external targets. This can lead to legal liabilities and damage to an organization's reputation.

Regulatory Non-Compliance: Depending on the industry and regulatory environment, the misuse of SSRF may result in non-compliance with data protection and security standards. This can lead to regulatory fines and legal consequences.

Reputation Damage: Security incidents related to SSRF can severely damage an organization's reputation. Customers, partners, and users may lose trust in the organization's security practices, leading to a loss of business and negative publicity.

Operational Disruption: Dealing with security incidents related to SSRF can disrupt normal business operations. Organizations may need to allocate significant resources to investigate, remediate, and recover from these incidents, impacting productivity and increasing operational costs.

Financial Impact: Addressing security vulnerabilities related to SSRF can be costly. Organizations may incur expenses related to vulnerability assessments, remediation efforts, incident response, and potential compensation to affected parties.

Loss of Competitive Advantage: Security incidents, especially those involving data breaches or misuse of resources, can erode an organization's competitive advantage and market position. Potential customers and partners may choose to do business with competitors with better security practices.

Stage : 2 Report

NESSUS Vulnerability Report

Overview

Conducting a vulnerability assessment for a college website is of utmost importance in order to detect and address potential security weaknesses that may be exploited by malicious attackers. It is imperative to note that security is a continuous process, and it is essential to continuously monitor and improve security measures to maintain a robust defense against potential threats. In the event that one lacks the necessary expertise to conduct a comprehensive assessment, it is advisable to seek the assistance of qualified cybersecurity professionals. It is also important to ensure that the website is secure and displays correctly on various devices and browsers. All identified vulnerabilities, along with their severity and potential impact, should be documented. Fixes should be prioritized based on criticality, and assistance should be provided to the college's IT team or web developers in the remediation process. It is recommended to document all identified vulnerabilities, along with their severity and potential impact, and prioritize fixes based on criticality while providing assistance to the college's IT team or web developers in 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 : thaper.edu

Target IP : 117.203.246.106

S.No.	Vulnerability name	Severity	Plugin	Description	Solution	Business Impact	Port
1	HSTS 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) on an HTTPS server can have various business impacts. This omission can expose the website and its users to security vulnerabilities, potentially leading to data breaches and financial losses. Additionally, it may negatively affect search engine rankings, user trust, and compliance with security standards, resulting in decreased website	443 / tcp / www

						traffic and potential legal consequences. Immediate implementation of HSTS is essential to enhance security, trust, and regulatory compliance.	
2	TLS Version 1.1 Protocol Deprecated	MEDIUM	157288	The remote service accepts connections encrypted using TLS 1.1. TLS 1.1 lacks support for current and recommended cipher suites. Ciphers that support encryption before MAC computation, and authenticat	Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.	The deprecation of TLS Version 1.1 has a significant business impact. It results in decreased security for data transmission, increasing the risk of data breaches and potential legal and compliance	443 / tcp / www

				ed encryption modes such as GCM cannot be used with TLS 1.1 As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.		issues. Immediate action is required to upgrade to a more secure TLS version to mitigate these risks and maintain customer trust.	
3	SSL Self-Signed Certificate	Medium	medium	he X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.	Using self-signed SSL certificates can provide a cost-effective solution for encrypting web traffic. However, they lack third-	Self-signed SSL certificates pose a significant business impact as they lack third-party validation. They can trigger security warnings for users, eroding trust and hindering secure online transactions. Inadequate security	25 / tcp / smtp

				Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.	party validation, potentially leading to security warnings for users. Self-signed certificates are suitable for internal systems or environments where security trust isn't a primary concern.	measures may result in data breaches and reputational damage.	
4	**TLS Version 1.0 Protocol Detection**	**medium**	**104743**	**The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these**	**Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.**	**Detecting the use of TLS version 1.0 is critical for businesses as it indicates outdated and insecure encryption. Continued support of TLS 1.0 exposes organizations to significant security risks, potential data breaches, and regulatory non-**	

				flaws and should be used whenever possible. As of March 31, 2020, Endpoints that aren’t enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors. PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.		compliance, which can lead to financial losses and reputational damage. Upgrading to secure TLS versions is imperative.	
5	**SSL Medium Strength Cipher Suites Supported (SWEET32)**	**medium**	**42873**	**The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or**	**Reconfigure the affected application if possible to avoid use of medium strength**	**The presence of SSL medium-strength cipher suites (SWEET32) in a business environment poses serious security risks. These weak ciphers are vulnerable to attacks, potentially exposing sensitive data to unauthorized**	**42873**

				else that uses the 3DES encryption suite. Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network	ciphers	access. Non-compliance with security standards may result in legal and regulatory consequences, including fines. Mitigating SWEET32 vulnerabilities is essential to maintain data integrity, protect customer trust, and adhere to compliance requirements, reducing the risk of financial and reputational damage.	
6	SSL Certificate Expiry	Mediium	15901	This plugin checks expiry dates of certificates associated with SSL-enabled services on the target and reports whether any have already expired.	Purchase or generate a new SSL certificate to replace the existing one.	SSL certificate expiry can disrupt online services, leading to loss of user trust, site inaccessibility, and reduced revenue. It exposes websites to security risks, including data breaches. Non-compliance with certificate management can lead	8383 / tcp / www

						to legal penalties and damage an organization's reputation, impacting customer confidence and brand image.	
7	HSTS Missing From HTTPS Server (RFC6797)	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-	Configure the remote web server to use HSTS.	The absence of HTTP Strict Transport Security (HSTS) on an HTTPS server can lead to severe security risks, including potential man-in-the-middle attacks and data interception. This can erode user trust, damage the reputation of the business, and result in data breaches, financial losses, and legal liabilities	443 / tcp / www

				hijacking protections.			
8	TLS Version 1.1 Protocol Deprecated	Medium	157288	The remote service accepts connections encrypted using TLS 1.1. TLS 1.1 lacks support for current and recommended cipher suites. Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1 As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly	Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.	The deprecation of TLS 1.1 protocol can have significant business impacts as it poses security vulnerabilities. Failure to update can expose sensitive data to potential breaches, erode customer trust, and lead to regulatory non-compliance, resulting in financial penalties, legal consequences, and reputational damage. Upgrading to more secure protocols is essential.	25 / tcp / smtp

				with major web browsers and major vendors.			
9.	SSL Certificate Expiry	Medium	15901	This plugin checks expiry dates of certificates associated with SSL-enabled services on the target and reports whether any have already expired.	Purchase or generate a new SSL certificate to replace the existing one.	SSL certificate expiry can disrupt online services, leading to loss of user trust, site inaccessibility, and reduced revenue. It exposes websites to security risks, including data breaches. Non-compliance with certificate management can lead to legal penalties and damage an organization's reputation, impacting customer confidence and brand image.	8383 / tcp / www
10.	SSL Anonymous Cipher Suites Supported	Medium	31705	The remote host supports the use of anonymous SSL	Reconfigure the affected application if possible to avoid	Supporting SSL anonymous cipher suites can have a detrimenta	

				ciphers. While this enables an administrator to set up a service that encrypts traffic without having to generate and configure SSL certificates, it offers no way to verify the remote host's identity and renders the service vulnerable to a man-in-the-middle attack.	use of weak ciphers.	l business impact. These suites allow for encrypted connections without authentication, making them vulnerable to eavesdropping and man-in-the-middle attacks. This can lead to data breaches, loss of customer trust, legal liabilities, and damage to brand reputation. To maintain security and compliance, it's crucial for businesses to disable SSL anonymous cipher suites and prioritize stronger encryption methods and authentication protocols.	

Stage 3 Report

Achieving Proactive Cybersecurity with SOC and SIEM Integration

- **Soc**

SOC plays a crucial role in continuously monitoring an organization's network, systems, and applications. It can detect and respond to potential security incidents, including malware infections, data breaches, and unauthorized access attempts. When a security incident occurs, time is of the essence. SOC teams are trained to respond swiftly and effectively to contain and mitigate the damage caused by security breaches. SOC doesn't merely react to incidents; it proactively identifies vulnerabilities and weaknesses in the organization's infrastructure. This proactive approach enables companies to strengthen their security posture and implement measures to prevent future attacks. SOC provides 24/7 monitoring, ensuring that security analysts are constantly vigilant and ready to respond to emerging threats, regardless of the time of day. SOC is a critical component of a robust cybersecurity strategy. It empowers organizations to detect, respond to, and prevent cyber threats, safeguarding sensitive data, maintaining business continuity, and preserving the organization's reputation in an increasingly interconnected and threat-prone digital landscape. SOC acts as the central hub for incident coordination and communication. It facilitates collaboration among various teams, such as IT, legal, communications, and executive management, ensuring a cohesive and efficient response to security incidents.

- **SOC - cycle**

The SOC (Security Operations Center) cycle, also known as the SOC lifecycle or SOC workflow, is a continuous process that outlines the key steps involved in managing an organization's cybersecurity. It encompasses activities from threat detection to incident response and recovery. The SOC cycle typically consists of the following stages:

Threat Detection and Monitoring:

Continuous monitoring of the organization's network, systems, and applications to identify potential security threats and anomalies.

Leveraging various security tools, such as intrusion detection systems (IDS), intrusion prevention systems (IPS), firewalls, SIEM (Security Information and Event Management) solutions, and threat intelligence feeds.

Alert Triage and Analysis:

Analyzing and prioritizing security alerts generated by the monitoring tools based on their severity and potential impact.

Determining if an alert indicates a genuine security incident or a false positive.

Incident Investigation and Response:

If an alert is confirmed as a legitimate security incident, the SOC team conducts a thorough investigation to understand the nature and extent of the attack.

Gathering evidence, analyzing log data, and performing digital forensics to determine the source and impact of the incident.

Initiating the incident response process, which may involve isolating affected systems, containing the threat, and preventing further damage.

Incident Containment and Eradication:

Taking immediate actions to contain the incident and prevent it from spreading further within the organization's network.

Removing the malicious elements and eradicating the threat to restore the affected systems to a secure state.

Recovery and Remediation:

After the threat is eradicated, the SOC team focuses on restoring affected systems and services to normal operation.

Implementing remediation measures to address the root cause of the incident and prevent similar attacks in the future.

Post-Incident Analysis and Lessons Learned:

Conducting a thorough post-mortem analysis of the incident to understand how it happened, what was the impact, and what steps were taken to respond.

Identifying areas of improvement in the organization's security posture and incident response procedures.

Updating security policies and procedures based on the lessons learned from the incident.

Threat Intelligence and Proactive Measures:

Integrating threat intelligence into the SOC workflow to stay ahead of emerging threats and known attack patterns.

Proactively hunting for signs of potential threats and vulnerabilities before they lead to full-fledged security incidents.

Continuous Monitoring and Improvement:

The SOC cycle is a continuous process, with ongoing monitoring, analysis, and improvement of security measures to adapt to the evolving threat landscape.

By following this cycle, the SOC team can effectively detect, respond to, and recover from security incidents, minimizing the impact of cyber threats on the organization's assets and data.

- **SIEM**

SIEM Security information and event mangement, or SIEM, is a security solution that helps organizations recognize and address potential security threats and vulnerabilities before they have a chance to disrupt business operations. SIEM systems help enterprise security teams detect user behavior anomalies and use artificial intelligence (AI) to automate many of the manual processes associated with threat detection and incident response.

Benefits Regardless of how large or small an organization may be, taking proactive steps to monitor for and mitigate IT security risks is essential. SIEM solutions benefit enterprises in a variety of ways and have become a significant component in streamlining security workflows.

Real-time threat recognition

SIEM solutions enable centralized compliance auditing and reporting across an entire business infrastructure. Advanced automation streamlines the collection and analysis of system logs and security events to reduce internal resource utilization while meeting strict compliance reporting standards.

AI-driven automation

Today's next-gen SIEM solutions integrate with powerful security orchestration, automation and response (SOAR) systems, saving time and resources for IT teams as they manage business security. Using deep machine learning that automatically learns from network behavior, these solutions can handle complex threat identification and incident response protocols in significantly less time than physical teams.

Improved organizational efficiency

Because of the improved visibility of IT environments that it provides, SIEM can be an essential driver of improving interdepartmental efficiencies. A central dashboard provides a unified view of system data, alerts and notifications, enabling teams to communicate and collaborate efficiently when responding to threats and security incidents.

Detecting advanced and unknown threats

Considering how quickly the cybersecurity landscape changes, organizations need to be able to rely on solutions that can detect and respond to both known and unknown security threats. Using integrated threat intelligence feeds and AI technology, SIEM solutions can help security teams respond more effectively to a wide range of cyberattacks including:

Insider threats - security vulnerabilities or attacks that originate from individuals with authorized access to company networks and digital assets.

Phishing - messages that appear to be sent by a trusted sender, often used to steal user data, login credentials, financial information, or other sensitive business information.

Ransomware - malware that locks a victim's data or device and threatens to keep it locked—or worse—unless the victim pays a ransom to the attacker.

Distributed denial of service (DDoS) attacks - attacks that bombard networks and systems with unmanageable levels of traffic from a distributed network of hijacked devices (botnet), degrading performance of websites and servers until they are unusable.

Data exfiltration – theft of data from a computer or other device, conducted manually, or automatically using malware.

Conducting forensic investigations

SIEM solutions are ideal for conducting computer forensic investigations once a security incident occurs. SIEM solutions allow organizations to efficiently collect and analyze log data from all of their digital assets in one place. This gives them the ability to recreate past incidents or analyze new ones to investigate suspicious activity and implement more effective security processes.

Assessing and reporting on compliance

Compliance auditing and reporting is both a necessary and challenging task for many organizations. SIEM solutions dramatically reduce the resource expenditures required to manage this process by providing real-time audits and on-demand reporting of regulatory compliance whenever needed.

Monitoring Users and Applications

With the rise in popularity of remote workforces, SaaS applications and BYOD (bring your own device) policies, organizations need the level of visibility necessary to mitigate network risks from outside the traditional network perimeter. SIEM solutions track all network activity across all users, devices, and applications, significantly improving transparency across the entire infrastructure and detecting threats regardless of where digital assets and services are being accessed.

Five Predictions For The Future Of SIEM

1. Usage-based pricing models will become the norm. With these models, teams only pay for precisely the data throughput and processing incurred each month. This trend follows suit with cloud infrastructure platforms such as AWS and GCP and gives predictability to service usage. Pressure for security teams to reduce the amount of data they use will become a thing of the past.

2. The decoupling of SIEM platforms — which has already started with SOAR coming from SIEM and other extract, transform and load (ETL) tools — will continue, and I suspect that the next phase would be building analysis tools on top of a universal SIEM data platform. This way, the companies building tools can focus on specific verticals and produce the most robust, high-quality and scalable software possible.

3. As decoupling continues to occur, security companies will create strong partnerships to provide an elegant integration and improve the time-to-value. These partnerships should help push the security industry forward, help with mutual company growth by referring customers to each other and ensure security teams have the best possible user experience.

4. The cost and complexity of a SIEM will continue to be reduced (per the availability of cloud services), enabling smaller and newer security teams to get up to speed even quicker. With legacy SIEMs, it could take

teams more than six months to get started, which means data onboarding, analysis and alerting integrations are non-trivial.

Next-gen SIEMs can improve quality and simplicity, enabling security teams to move quickly and focus on the work that matters. This trend will continue to reduce startup time, which is critical for a business's bottom line and a security team's efficiency.

5. More startups will continue to be funded to address the multifaceted challenges of upholding strong security. Venture funding is at an all-time high, and security breaches continue to be an issue for organizations of all sizes — including the large, sophisticated Fortune 1000 companies.

Healthy competition means that not a single company will own a majority of the market share. This competition gives security teams optionality and the freedom to move to other platforms as they see fit. Then, the battle will become about ease of use, capabilities and flexibility.

- **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.

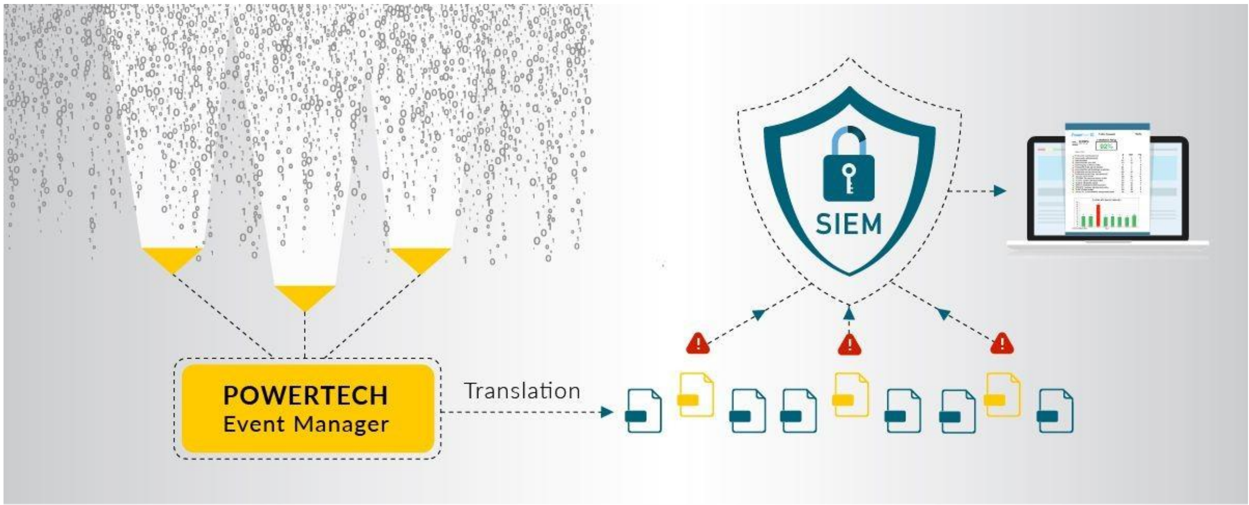
Foster knowledge sharing and best practices from incident investigations and analysis within the organization.

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.

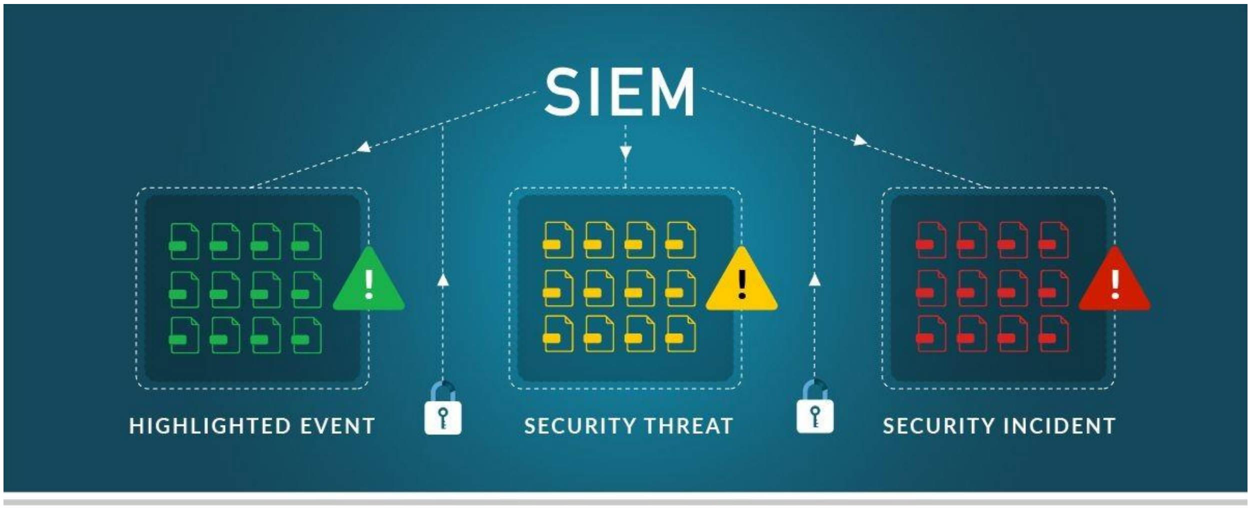
As a syslog server incessantly pings with every security notification, security teams can feel as though they are drowning in a sea of security warnings. Without a SIEM, it’s difficult to know which events are truly critical and which can be ignored. However, when a SIEM has been implemented, security 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.

Threat Detection

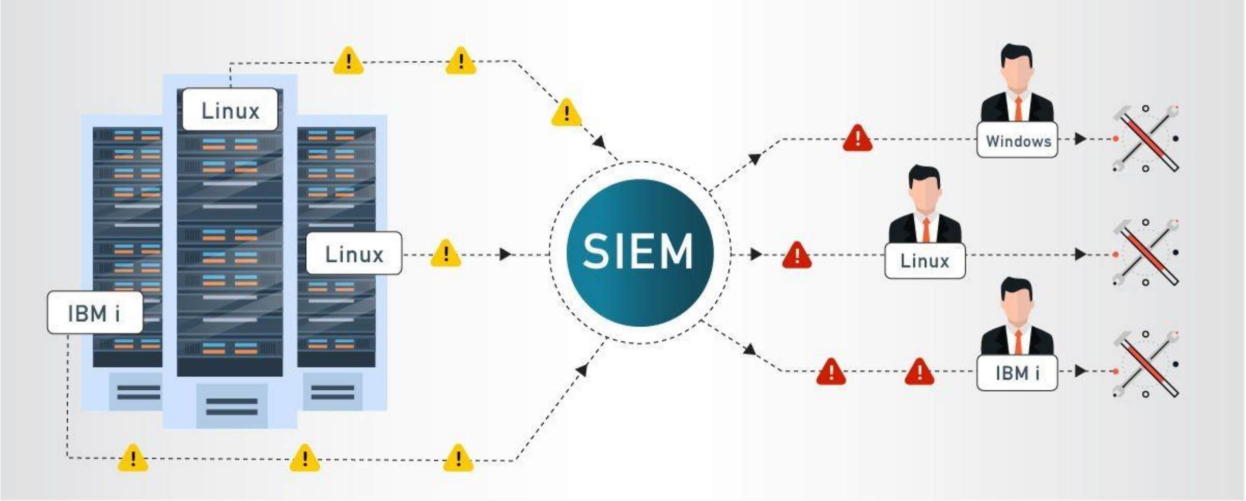
Translation



Prioritization

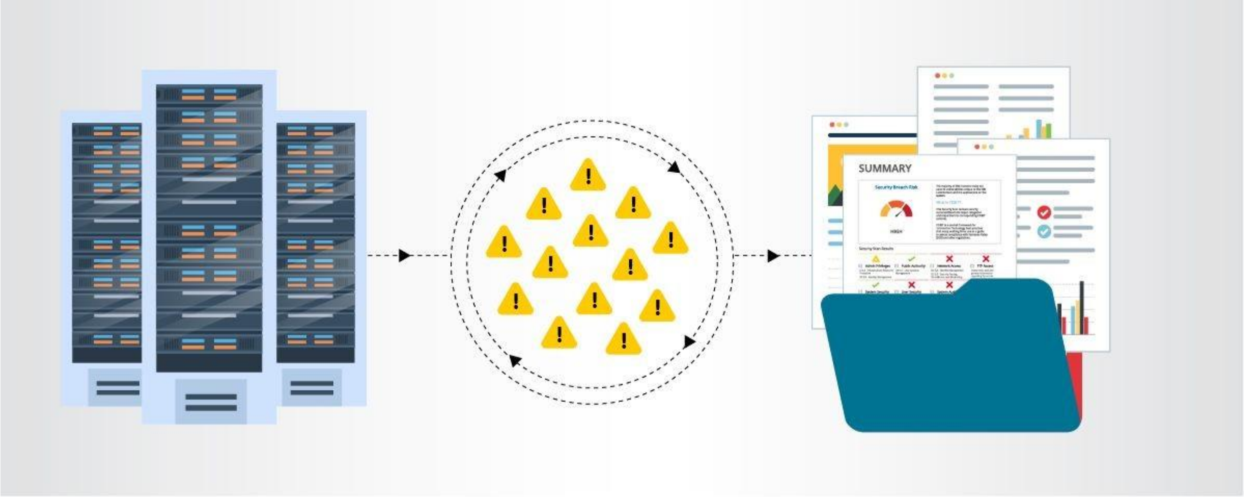

SIEM
HIGHLIGHTED EVENT
SECURITY THREAT
SECURITY INCIDENT

Escalation


Linux
Linux
IBM i
SIEM
Windows
Linux
IBM i

Analysis

Compliance



- **MISP**

MISP, Malware Information Sharing Platform and Threat Sharing, core functionalities are:

An efficient IOC and indicators database, allowing to store technical and non-technical information about malware samples, incidents, attackers and intelligence.

Features of MISP, the open source threat sharing platform

A threat intelligence platform for sharing, storing and correlating Indicators of Compromise of targeted attacks, threat intelligence, financial fraud information, vulnerability information or even counter-terrorism information. Discover how MISP is used today in multiple organisations. Not only to store, share, collaborate on cyber security indicators, malware analysis, but also to use the IoCs and information to detect and prevent attacks, frauds or threats against ICT infrastructures, organisations or people.

An efficient IoC and indicators database allowing to store technical and non-technical information about malware samples, incidents, attackers and intelligence.

Automatic correlation finding relationships between attributes and indicators from malware, attacks campaigns or analysis. Correlation engine includes correlation between attributes and more advanced correlations like Fuzzy hashing correlation (e.g. ssdeep) or CIDR block matching. Correlation can be also enabled or event disabled per attribute.

A flexible data model where complex objects can be expressed and linked together to express threat intelligence, incidents or connected elements.

Built-in sharing functionality to ease data sharing using different models of distributions. MISP can synchronize automatically events and attributes among different MISP. Advanced filtering functionalities can be used to meet each organization sharing policy including a flexible sharing group capacity and an attribute level distribution mechanism.

An intuitive user-interface for end-users to create, update and collaborate on events and attributes/indicators. A graphical interface to navigate seamlessly between events and their correlations. An event graph functionality to create and view relationships between objects and attributes. Advanced filtering functionalities and warning list to help the analysts to contribute events and attributes.

storing data in a structured format (allowing automated use of the database for various purposes) with an extensive support of cyber security indicators along fraud indicators as in the financial sector.

export: generating IDS (Suricata, Snort and Bro are supported by default), OpenIOC, plain text, CSV, MISP XML or JSON output to integrate with other systems (network IDS, host IDS, custom tools

import: bulk-import, batch-import, free-text import, import from OpenIOC, GFI sandbox, ThreatConnect CSV or MISP format.

Flexible free text import tool to ease the integration of unstructured reports into MISP.

A gentle system to collaborate on events and attributes allowing MISP users to propose changes or updates to attributes/indicators.

Data-sharing: automatically exchange and synchronization with other parties and trust-groups using MISP.

Feed import: flexible tool to import and integrate MISP feed and any threatintel or OSINT feed from third parties. Many default feeds are included in standard MISP installation.

Delegating of sharing: allows a simple pseudo-anonymous mechanism to delegate publication of event/indicators to another organization.

Flexible API to integrate MISP with your own solutions. MISP is bundled with PyMISP which is a flexible Python Library to fetch, add or update events attributes, handle malware samples or search for attributes.

Adjustable taxonomy to classify and tag events following your own classification schemes or existing taxonomies. The taxonomy can be local to your MISP but also shareable among MISP instances. MISP comes with a default set of well-known taxonomies and classification schemes to support standard classification as used by ENISA, Europol, DHS, CSIRTs or many other organizations.

Intelligence vocabularies called MISP galaxy and bundled with existing threat actors, malware, RAT, ransomware or MITRE ATT&CK which can be easily linked with events in MISP.

Expansion modules in Python to expand MISP with your own services or activate already available misp-modules.

sighting support to get observations from organizations concerning shared indicators and attributes. Sighting can be contributed via MISP user-interface, API as MISP document or STIX sighting documents. Starting with MISP 2.4.66, Sighting has been extended to support false-negative sighting or expiration sighting.

STIX support: export data in the STIX format (XML and JSON) including export/import in STIX 2.0 format.

integrated encryption and signing of the notifications via PGP and/or S/MIME depending on the user preferences.

Real-time publish-subscribe channel within MISP to automatically get all changes (e.g. new events, indicators, sightings or tagging) in ZMQ (e.g. misp-dashboard) or Kafka.

Sharing with humans

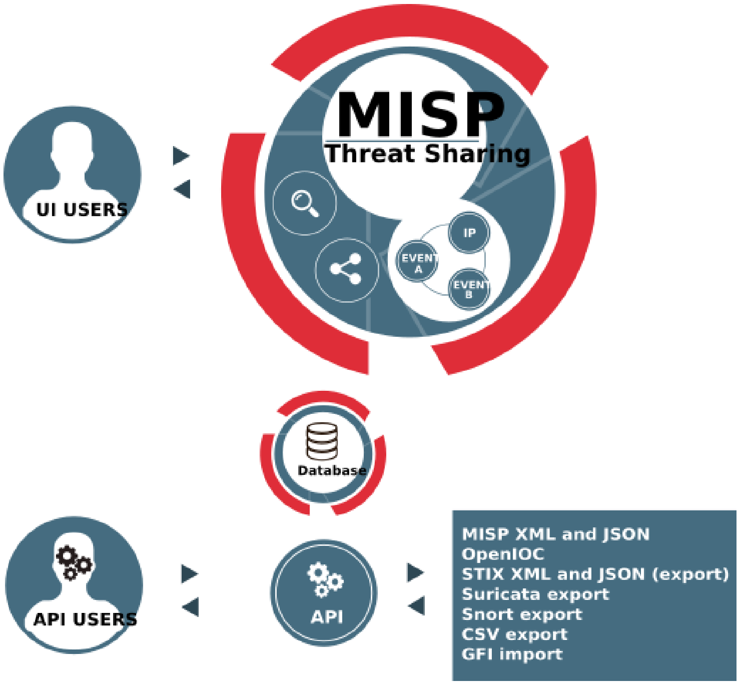
Data you store is immediately available to your colleagues and partners. Store the event id in your ticketing system or be informed by the signed and encrypted email notifications.

Sharing with machines

By generating Snort/Suricata/Bro/Zeek IDS rules, STIX, OpenIOC, text or csv exports MISP allows you to automatically import data in your detection systems resulting in better and faster detection of intrusions. Importing data can also be done in various ways: free-text import, OpenIOC, batch import, sandbox result import or using the preconfigured or custom templates. If you run MISP internally, data can also be uploaded and downloaded automagically from and to externally hosted MISP instances. Thanks to this automation and the effort of others you are now in possession of valuable indicators of compromise with no additional work.

Collaborative sharing of analysis and correlation

How often has your team analyzed to realize at the end that a colleague had already worked on another, similar, threat? Or that an external report has already been made? When new data is added MISP will immediately show relations with other observables and indicators. This results in more efficient analysis, but also allows you to have a better picture of the TTPs, related campaigns and attribution.



- **Your college network information**

  Tagore Engineering College

  A total of 5 labs and approximately 200 systems are available.

- **How you think you deploy soc in your college**

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

Assessment and Requirements Gathering:

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

Build a Skilled Team:

- Recruit or assign skilled security professionals to form the SOC team.
- 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 feeds.

Integration and Data Collection:

- Integrate security tools and systems with the SIEM to centralize log 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 SOC activities, including incident handling, response protocols, escalation procedures, and communication guidelines.
- Implement incident categorization and prioritization mechanisms.

Implement Monitoring and Alerting:

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

Incident Response and Escalation:

- Develop a formal incident response plan that outlines the steps to be taken in the event of a security incident.
- Define roles and responsibilities for incident handling, and establish a clear escalation path for severe incidents.

Training and Skill Development:

- Provide comprehensive training to the SOC team on the use of security 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 attack scenarios 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.

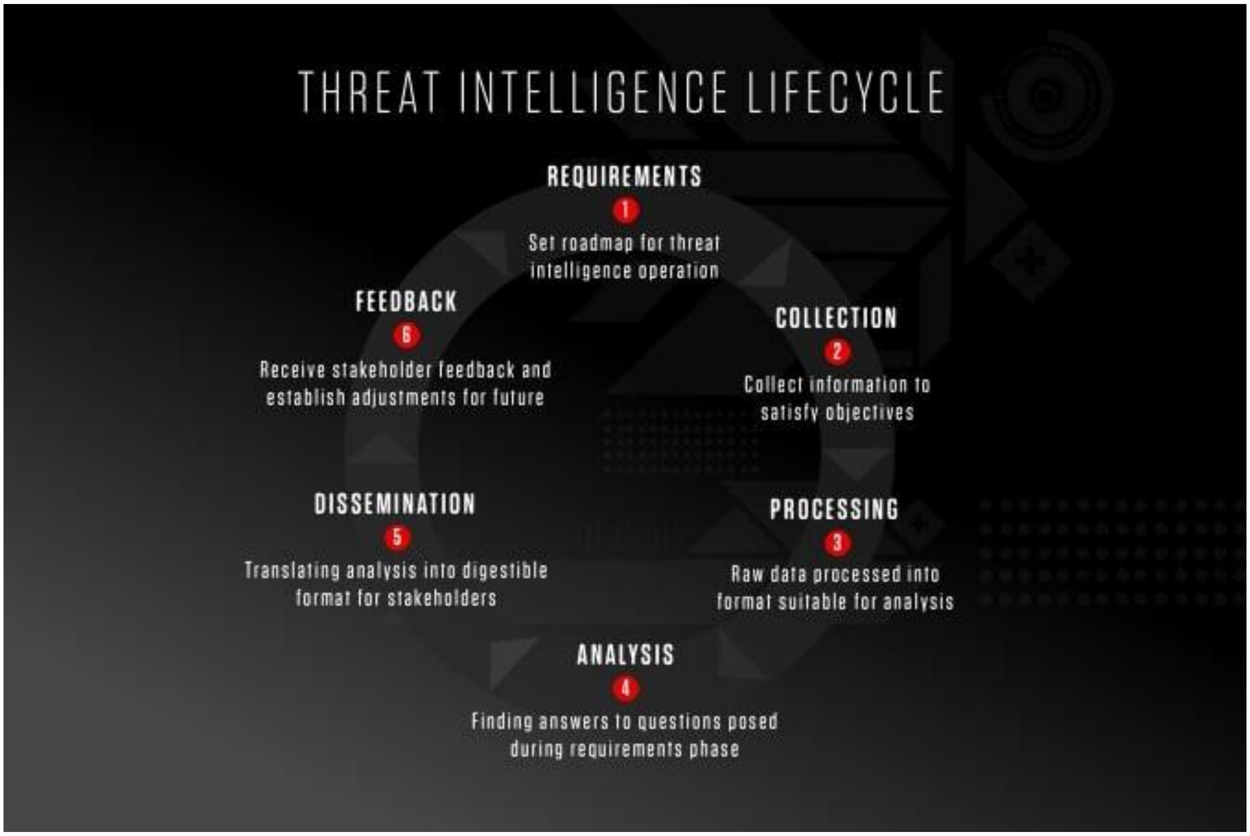
- Generate regular reports and metrics to measure the SOC's performance and communicate its value to stakeholders.

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 is data that is collected, processed, and analyzed to understand a threat actor’s motives, targets, and attack behaviors. Threat intelligence enables us to make faster, more informed, data-backed security decisions and change their behavior from reactive to proactive in the fight against threat actors.



THREAT INTELLIGENCE LIFECYCLE

REQUIREMENTS
1
Set roadmap for threat intelligence operation

COLLECTION
2
Collect information to satisfy objectives

PROCESSING
3
Raw data processed into format suitable for analysis

ANALYSIS
4
Finding answers to questions posed during requirements phase

DISSEMINATION
5
Translating analysis into digestible format for stakeholders

FEEDBACK
6
Receive stakeholder feedback and establish adjustments for future

Threat intelligence is important for the following reasons:

- sheds light on the unknown, enabling security teams to make better decisions
- empowers cyber security stakeholders by revealing adversarial motives and their tactics, techniques, and procedures (TTPs)
- helps security professionals better understand the threat actor's decision-making process
- empowers business stakeholders, such as executive boards, CISOs, CIOs and CTOs; to invest wisely, mitigate risk, become more efficient and make faster decisions

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

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

- **Incident response**

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 be further 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.

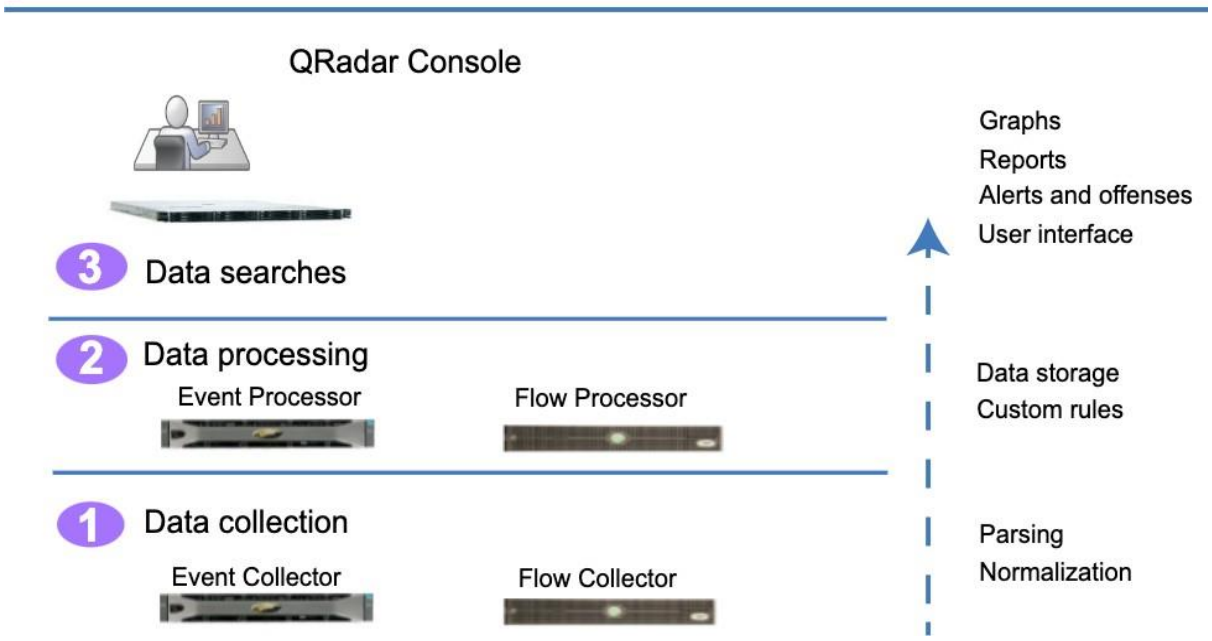


Figure 1. QRadar architecture

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:

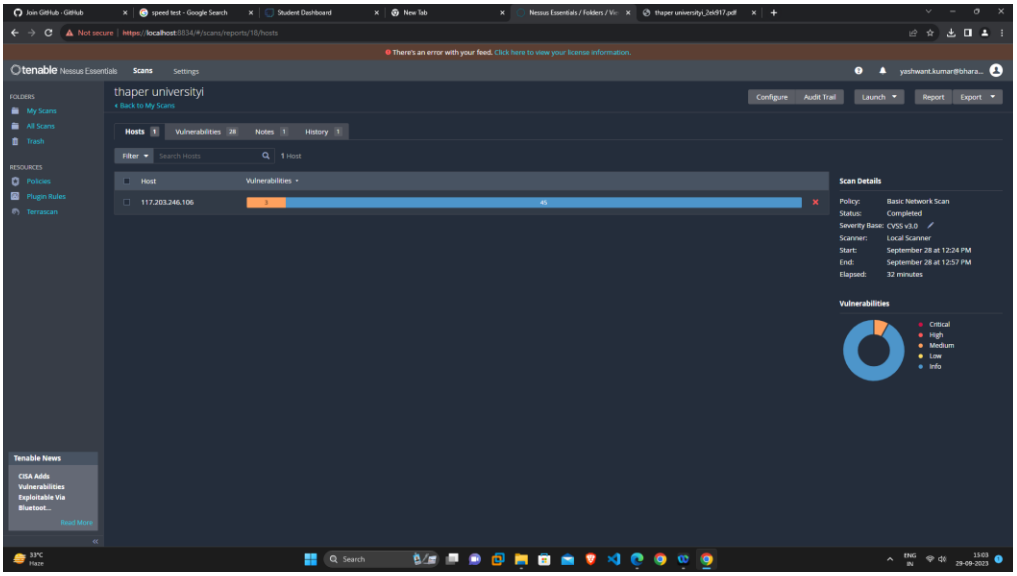
- Identification of Security Vulnerabilities
- Bug Detection and Resolution
- Validation of Functional Requirements
- Usability and User Experience Evaluation
- Performance and Load Testing Results
- Compatibility Testing Insights
- Accessibility Compliance
- Security Compliance and Risk Mitigation
-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



thaper universityi

Host	Vulnerabilities
117.203.246.106	3 45

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: September 28 at 12:24 PM
End: September 28 at 12:57 PM
Elapsed: 32 minutes

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

SOC (Security Operations Center): The primary purpose of a SOC is to monitor and defend an organization's IT infrastructure against security threats and incidents. SOC analysts use various tools and technologies to detect, analyze, and respond to security events in real-time. The expected outcomes of a well-functioning SOC include:

a. **Improved Threat Detection**: SOC analysts monitor network traffic, log data, and security alerts to identify potential threats and security incidents promptly.

b. **Faster Incident Response**: With a SOC in place, organizations can respond quickly to security incidents and mitigate the impact of breaches or attacks.

c. **Enhanced Security Posture:** A proactive SOC helps organizations implement robust security measures and continually improve their overall security posture.

d. **Reduced Downtime and Losses:** Detecting and mitigating security incidents swiftly can minimize downtime and financial losses resulting from cyber-attacks.

SIEM (Security Information and Event Management): SIEM is a technology that helps collect, analyze, and correlate log data from various sources within an organization's IT environment. The main goal of SIEM is to provide a centralized platform for real-time monitoring, threat detection, and incident response. The expected outcomes of using a SIEM system are:

a. Centralized Log Management: SIEM aggregates log data from diverse sources, making it easier for analysts to access and analyze information from a single dashboard.

b. Early Threat Detection: SIEM tools can identify patterns and anomalies in the data, enabling early detection of security incidents and potential breaches.

c. Simplified Incident Investigation: SIEM allows analysts to correlate events from different sources, providing a comprehensive view of security incidents for faster and more accurate investigations.

d. Compliance and Reporting: SIEM can help organizations meet regulatory compliance requirements by generating security reports and audits.

QRadar Dashboard (IBM QRadar): QRadar is a popular SIEM solution provided by IBM. The QRadar dashboard is a critical component of the QRadar system, offering a visual representation of security-related data and insights. The expected outcomes of using QRadar and its dashboard include:

a. Real-Time Visibility: The QRadar dashboard provides real-time visibility into security events and incidents, enabling analysts to respond promptly to emerging threats.

b. Customizable Visualizations: Analysts can customize the dashboard to display relevant information, such as top threats, network traffic, or security incidents.

c. Threat Intelligence Integration: QRadar integrates with various threat intelligence feeds, enhancing its ability to detect and respond to advanced threats.

d. Incident Response Automation: The QRadar dashboard can be integrated with automation tools to streamline incident response processes.

It's important to note that the effectiveness of these security measures relies on the expertise of the security team, the quality of data collected, and the organization's commitment to maintaining a strong security posture. Continuous monitoring, analysis, and improvement are crucial for maximizing the outcomes and benefits of SOC, SIEM, and QRadar implementations.

Future Scope

Stage 1:- Future scope of web application testing

The future scope of web application testing will be shaped by technological advancements, changing user expectations, and the need to ensure security and reliability in an increasingly interconnected digital world. Testing professionals will need to adapt to these trends and continuously upgrade their skills to meet the evolving demands of web application testing.

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

The future scope of the testing process will see increased automation, integration with emerging technologies, and a focus on ensuring quality, security, and performance in the ever-evolving software landscape. Testing professionals will need to adapt to these changes and continuously upgrade their skills to stay relevant in the dynamic field of software testing

Stage 3:- future scope of SOC / SEIM

The future scope of SOC (Security Operations Center) and SIEM (Security Information and Event Management) is expected to expand and evolve in response to the changing cybersecurity landscape and technological 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 :-

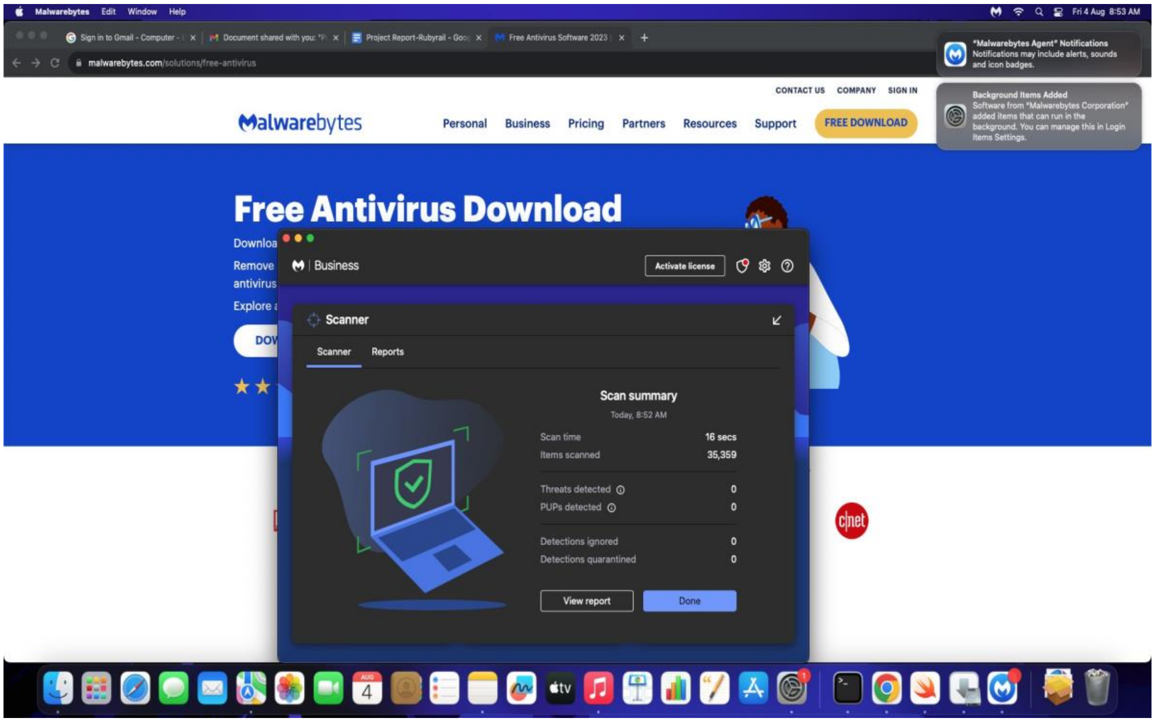
Nessus, cybermap.kaspersky.com, thehackersone.com, chapt gpt, wepik.com (AI image editor), Gamma (AI based PPT), OWASP top 10 vulnerabilities(2021), thehackersnews.com, CWE, exploitDB, virtual box, live websites-bugcrowd, nslookup.io, OSINT framework, mitre framework, IBM fix central, QRadar Installation,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

MALWAREBYTES

FREE DOWNLOADS

Free Antivirus Software 2023

Looking for free antivirus and malware removal? Scan and remove viruses and malware for free. Malwarebytes free antivirus includes multiple layers of malware-crushing tech. Our anti-malware finds and removes threats like viruses, ransomware, spyware, adware, and Trojans.



Malwarebytes Edit Window Help
Fri 4 Aug 8:53 AM
Sign in to Gmail - Computer
Document shared with you
Project Report-Rubyrail - Goo
Free Antivirus Software 2023
malwarebytes.com/solutions/free-antivirus
CONTACT US COMPANY SIGN IN
Malwarebytes
Personal Business Pricing Partners Resources Support FREE DOWNLOAD
Free Antivirus Download
Business
Activate license
Scanner
Scanner Reports
View report
Done

"Malwarebytes Agent" Notifications
Notifications may include alerts, sounds and icon badges.

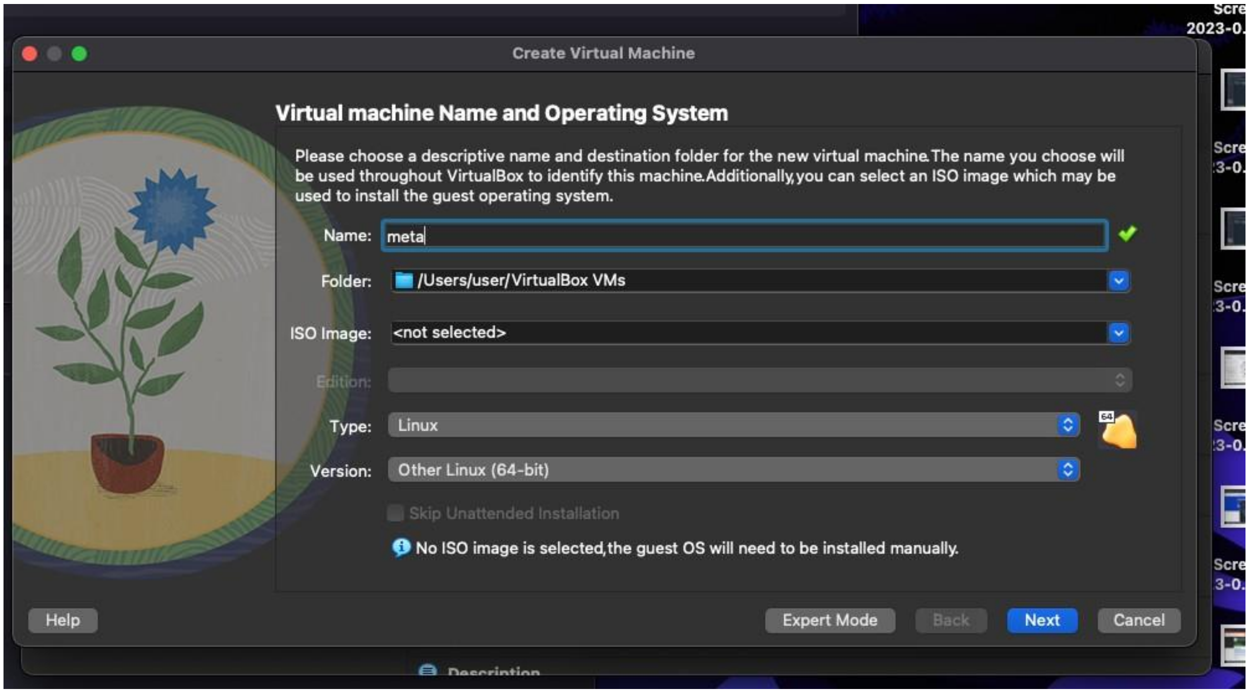
Background Items Added
Software from "Malwarebytes Corporation" added items that can run in the background. You can manage this in Login Items Settings.

Scan summary
Today, 8:52 AM

Scan time	16 secs
Items scanned	35,359
Threats detected	0
PUPs detected	0
Detections ignored	0
Detections quarantined	0

Metasploitable2 (Linux) is a framework which is combination Nmap and exploit database.

Metasploitable is an intentionally vulnerable Linux virtual machine. This VM can be used to conduct security training, test security tools, and practice common penetration testing techniques.



Virtual machine Name and Operating System

Please choose a descriptive name and destination folder for the new virtual machine. The name you choose will be used throughout VirtualBox to identify this machine. Additionally, you can select an ISO image which may be used to install the guest operating system.

Name: meta ✓

Folder: /Users/user/VirtualBox VMs

ISO Image: <not selected>

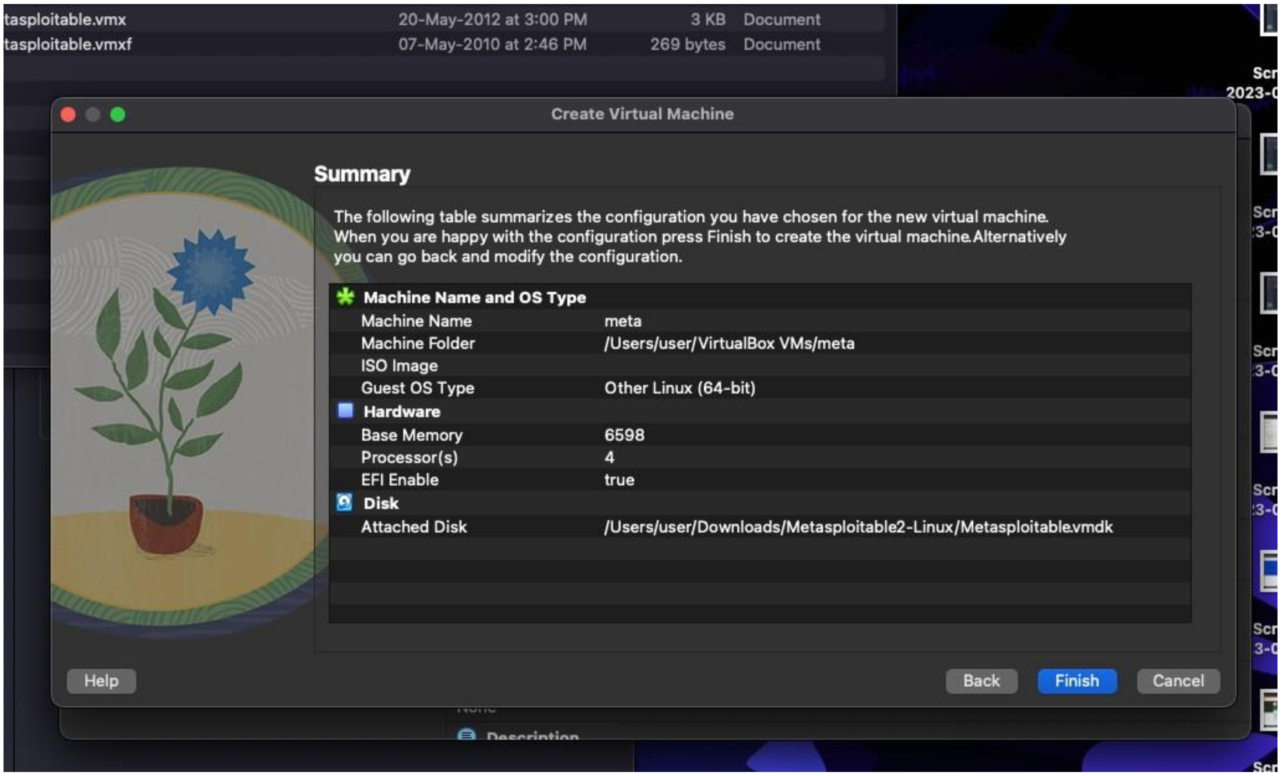
Edition:

Type: Linux

Version: Other Linux (64-bit)

□ Skip Unattended Installation

No ISO image is selected, the guest OS will need to be installed manually.


tasploitable.vmx 20-May-2012 at 3:00 PM 3 KB Document
tasploitable.vmxf 07-May-2010 at 2:46 PM 269 bytes Document
Create Virtual Machine
Help
Back
Finish
Cancel

Summary

The following table summarizes the configuration you have chosen for the new virtual machine. When you are happy with the configuration press Finish to create the virtual machine. Alternatively you can go back and modify the configuration.

Machine Name and OS Type	
Machine Name	meta
Machine Folder	/Users/user/VirtualBox VMs/meta
ISO Image	
Guest OS Type	Other Linux (64-bit)
Hardware	
Base Memory	6598
Processor(s)	4
EFI Enable	true
Disk	
Attached Disk	/Users/user/Downloads/Metasploitable2-Linux/Metasploitable.vmdk

- Base memory 6000
- Processor 4
- Enable FPT
- Use an existing hard disk file

- File folder - click add button
- Select downloads folder and metasploitable 2 linux-> metaspoiltable 2 vmdk

Metaspoilt

```
┌──(kali㉿kali)-[~]
└─$ msfconsole
       =[ metasploit v6.3.4-dev                          ]
+ -- --=[ 2294 exploits - 1201 auxiliary - 409 post       ]
+ -- --=[ 968 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: View a module's description using
info, or the enhanced version in your browser with
info -d
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search exploit

Matching Modules
================

   #     Name                                                   Disclosure Date  Rank
Check  Description
   -     ------                                                 ---------------  ----       -----  -----------
   0     auxiliary/dos/http/cable_haunt_websocket_dos                          2020-01-07
normal     No     "Cablehaunt" Cable Modem WebSocket DoS
   1     exploit/linux/local/cve_2021_3493_overlayfs                           2021-04-12
great      Yes    2021 Ubuntu Overlayfs LPE
   2     exploit/windows/ftp/32bitftp_list_reply                     2010-10-12       good
No     32bit FTP Client Stack Buffer Overflow
   3     exploit/windows/tftp/threectftpsvc_long_mode                          2006-11-27
great      No     3CTftpSvc TFTP Long Mode Buffer Overflow
   4     exploit/windows/ftp/3cdaemon_ftp_user                               2005-01-04
```

Testing Metaspoilt using Kalilinux

> nmap -A 10.5.174.221

msfg> use auxiliary/admin/http/tomcat_ghostcat

>show options

```
>set RHOSTS 10.5.174.221

>run

>exploit


>search vsftp

>run

>exploit

> use modulename

>ls - lists all files from other terminal from the given IP
```