TEAM -I

A TrustDefender

Part I-Executive summary

Overview

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

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

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

IP address of mac.du.ac.in 15.206.132.167

2. Team Members Involved in vulnerability Assessment

S.No	Name	Designation	Mobile Number
1	Ms Neha Sabharwal	Assistant Professor	9873257419 nehasabharwal@its.edu.in
2	Ms Bharti Aggarwal	Assistant Professor	9871066460 Bharti_goel2003@yahoo.com
3	Ms Suman Singh	Assistant Professor	9953301020 suman_singh@iitmipu.ac.in
4	Dr. Vippan Raj Dutt	Professor	9810297809 Vippan.dutt@gmail.com

2. 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 With Insufficient 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 HTTPS Session Without 'Secure' Attribute
6	Vulnerable and Outdated Components	CWE-1395: Dependency on Vulnerable Third-Party Component
7	Identification and Authentication Failures	CWE-521: Weak Password Requirements
8	Software and Data Integrity Failures	CWE-565C: Reliance on Cookies without Validation and Integrity Checkin
9	Security Logging and Monitoring Failures	CWE-532: Insertion of Sensitive Information into Log File
10	Server Side Request Forger	CWE-918:Server Side Request Forgery

1. CWE: CWE 285- Improper Authorization

OWASP CATEGORY : A01 2021 Broken Access Control

DESCRIPTION: When an actor tries to get to a resource or carry out an action, the product either fails to execute an authorization check or does so erroneously.

BUSINESS IMPACT: Authorization is the process of determining whether a user with a certain identity can access a particular resource based on the user's rights and the permissions or other use-control requirements that pertain to the resource. When security checks are not carried out consistently, or at all, users gain access to data or can perform actions that they shouldn't be able to. Numerous problems, including information leaks, denial-of-service attacks, and arbitrary code execution, could occur from this.

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

OWASP CATEGORY: A02 2021 Cryptographic Failures

DESCRIPTION: The device creates a password hash, however, it does not use a scheme that would require enough computing effort to render password-cracking assaults impractical or expensive.

BUSINESS IMPACT: In this method, authentication is carried out by authenticating a newly generated password, computing its hash, and then comparing it to the previously saved hash. Once an attacker has gained saved password hashes, they will always be able to brute force hashes offline. A defender can only slow down offline attacks by employing hash algorithms that are as resource-intensive as is practical.

3. CWE: CWE 564: SQL Injection: Hibernate

OWASP CATEGORY : A03 2021 Injection

DESCRIPTION: A flexible SQL statement created with user-controlled data can be modified or arbitrary SQL commands can be executed by an attacker by using Hibernate for executing the statement.

BUSINESS IMPACT: Hackers employ SQL injection attacks to obtain crucial corporate or personally identifiable information (PII), which ultimately exposes additional sensitive data. Criminals can use SQL injection to retrieve and modify data, placing the private company information stored on the SQL server at danger of disclosure. Users' Privacy Is Vulnerable Based on the data stored on the SQL server, private user information, including credit card numbers, may be revealed via an attack.

4. CWE: CWE 653: Improper Isolation or Compartmentalization

OWASP CATEGORY : A04 2021 Insecure Design

DESCRIPTION: The product goes against accepted guidelines for secure design. This may result in the introduction of weaknesses or facilitate the introduction of associated weaknesses by developers during implementation. Fixing design flaws can be resource-intensive because coding is built around design.

BUSINESS IMPACT: Weaknesses in the security configurations and the hardening of the numerous systems used in the pipeline (like SCM, CI, and the artefact repository), which frequently presents "low-hanging fruits" for attackers trying to gain a foothold in the environment, are what lead to the dangers associated with insecure system setup.

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

OWASP CATEGORY : A05 2021 Security Misconfiguration

DESCRIPTION: Because the Secure property for critical cookies in HTTPS connections is not set, the user agent might transfer those cookies over an HTTP session in plaintext.

BUSINESS IMPACT: Security setup mistakes allow attackers to access networks, systems, and data without authorization, seriously harming your organization's revenue and reputation...

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

OWASP CATEGORY : A06 2021 Vulnerable and Outdated Components

DESCRIPTION: The product is dependent on an external element that contains one or more sufficiently big or complicated third-party products that utilise libraries, parts, or other third-party intellectual property as part of their functionality.

BUSINESS IMPACT: A complete operating system might be obtained from a third party for some hardware components. These parts, whether open source or closed source, might include weaknesses that the general public is aware of and that enemies could utilise to compromise the product with more flaws. Dependency-Check, a System Composition Study (SCA) tool, looks for vulnerabilities in dependencies that have been made publicly known. By determining whether a certain dependant has a common platform enumeration (CPE) identity, it is able to do this.

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.

BUSINESS IMPACT: Authentication systems usually rely on a secret that is memorised (sometimes referred to as a password) to provide an assurance of identification for a system user. This password must be sufficiently complex and challenging for an adversary to decipher. The specific requirements for how challenging the password must be depend on the type of system that needs to be protected. The selection and implementation of the appropriate password requirements are essential to the system's success.

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

OWASP CATEGORY : A08 2021 Software and Data Integrity Failures

DESCRIPTION: When carrying out security-critical actions, the product depends on the existence or values of cookies, but it does not properly verify that the setting is appropriate for the connected user. Attackers can quickly alter cookies by implementing client-side code outside of the browser or within the browser itself. Insufficient validation and integrity checking of cookies can make it possible for attackers to subvert authentication, carry out injection attacks like SQL injection and cross-site scripting, or otherwise change inputs in unanticipated ways

BUSINESS IMPACT: This issue may be the root cause of a lot of web application issues. When examining URL parameters, a developer can presume that an attacker can't change cookies. Because of this, the application might not execute fundamental input validation, making it susceptible to dangers like cross-site scripting (CSS), SQL injection, price manipulation, and others.

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

OWASP CATEGORY: A09 2021 Security Logging and Monitoring Failures

DESCRIPTION: While recording all information may be useful during the development process, it's crucial to select the right logging settings before a product is released to prevent unintentional exposure of confidential user records and system information to possible attackers. **BUSINESS IMPACT:** Log file entries may include delicate information that could betray personal user information or give an attacker vital information.

10. CWE: CWE-918 Server Side Request Forgery

OWASP CATEGORY : A10 2021 - Server Side Request Forgery

DESCRIPTION: The web server gets a URL or a request of a similar nature from an upstream component and obtains its contents, but it does not adequately verify that the request for information is being sent to the intended recipient.

BUSINESS IMPACT: A successful SSRF attack may result in unauthorised activity or access to data within the company, either on the application in question or on any back-end computer systems that the programme can communicate with.

Stage : 2 Report

NESSUS Vulnerability Report

Overview

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

Nessus is a popular vulnerability assessment tool that is widely used by cybersecurity professionals and organizations to identify and address security weaknesses in their networks, systems, and applications. Here are some of the key uses of Nessus:

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

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

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

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

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

Security Awareness and Training: By generating detailed vulnerability reports, Nessus helps security teams and IT personnel gain insights into the security posture of their systems. This information can be used to improve security awareness and training programs.

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

Penetration Testing Support: Nessus can complement manual penetration testing efforts by providing an initial overview of potentialvulnerabilities 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 : : https://mac.du.ac.in/ Target IP : 15.206.132.167

S. No.	Vulnerability name	Severity	Plugin	Description	Solution	Business Impact	Port
1	***SSL Anonymous Cipher Suites Supported***	Medium	31705	The remote host supports the use of anonymous SSL 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. Note: This is considerably easier to exploit if the attacker is on the same physical network.	Reconfigure the affected application if possible to avoid use of weak ciphers.	Enabling anonymous SSL ciphers on a remote host may provide a convenient means of encrypting traffic without the complexities of SSL certificate management, but it comes at a substantial security cost. The absence of host identity verification leaves the service susceptible to potentially devastating man-in-the-middle attacks, where malicious actors can intercept and eavesdrop on encrypted communications. This not only jeopardizes data confidentiality and integrity but also exposes the business to regulatory compliance issues, reputation damage, and potential financial liabilities, making it imperative for organizations to prioritize robust SSL/TLS configurations with proper authentication mechanisms to safeguard their	21 / tcp

						assets and customer trust.	
2		Medium		The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below : - First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.	There are three separate ways in which the chain of trust might break, which makes it impossible to trust the server's X.509 certificate. First off, the certificate chain may not start with a trustworthy authority because it may have an unusual self-signed certificate at the top of the chain or it may lack intermediate certificates		21 / tcp

				- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates. - Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize. If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the	that would have connected it to a trusted authority. Second, certificates in the chain may be invalid at the time of scanning if they have 'notBefore' dates earlier than their scan dates or 'notAfter' dates later than their scan dates. Last but not least, the certificate chain can include a signature that contradicts the information in the certificate or that cannot be checked because the signing algorithm is unsupported or unrecognized. Any break in this trust chain for public hosts in production		

	SSL Certificate Cannot Be Trusted	m	51192	web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.	makes it more difficult to authenticate the web server.		

3	SSL Self-Signed Certificate [redacted]	MEDIUM	57582	The 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. 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.	Purchase or generate a proper SSL certificate for this service	The X.509 certificate chain for this service lacks the endorsement of a recognized certificate authority, rendering SSL usage ineffective. In the case of a public host in a production environment, this deficiency opens the door for potential man-in-the-middle attacks, as the absence of trusted certification allows anyone to intercept and compromise the connection with the remote host. It's important to note that this plugin does not assess certificate chains ending in certificates signed by unrecognized authorities, emphasizing the critical need for robust certificate validation to ensure secure and trusted communications.	21 / tcp
4		LOW	153953	The remote SSH server is configured to allow key exchange	Contact the vendor or consult product documentat	according to the IETF draft Key Exchange (KEX) Method Updates and	22 / tcp / ssh

				algorithms which are considered weak. This is based on the IETF draft document Key Exchange (KEX) Method Updates and Recommendations for Secure Shell (SSH) draft-ietf-curdle-ssh-kex-sha2-20. Section 4 lists guidance on key exchange algorithms that SHOULD NOT and MUST NOT be enabled. This includes: diffie-hellman-group-exchange-sha1 diffie-hellman-group1-sha1 gss-gex-sha1-* gss-group1-sha1-* gss-group14-sha1-* rsa1024-sha1 Note that this plugin only checks for the options of the SSH server, and it does not check for vulnerable software versions.	ion to disable the weak algorithms.	Recommendations for Secure Shell (SSH), which is categorized as weak. Section 4 of the document describes key exchange algorithms that are strongly discouraged or expressly forbidden, and it describes this non-compliant arrangement. These unreliable algorithms include rsa1024-sha1, diffie-hellman-group-exchange-sha1, gss-gex-sha1, gss-group1-sha1, gss-group14-sha1-*, and diffie-hellman-group-sha1. It's important to note that this plugin solely evaluates the SSH server's settings and does not look for outdated software versions, highlighting the necessity of immediately patching poor key exchange methods to strengthen SSH security.	

	SSH Weak Key Exchange Algorithms Enabled							

5		Low	70658	The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext. Note that this plugin only checks for the options of the SSH server and does not check for vulnerable software versions.	Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption.	Configuring the SSH server to support Cipher Block Chaining (CBC) encryption has a significant negative impact on corporate operations because it presents a security flaw that could allow unauthorized access to sensitive data that has been encrypted. Attackers may be able to extract plaintext from encrypted messages using known security flaws in CBC mode, endangering the confidentiality and integrity of vital corporate data. Malicious actors may use this vulnerability to access systems and data without authorization, resulting in data breaches, problems with legal and regulatory compliance, and harm to the organization's reputation. In order to maintain the greatest levels of data security and safeguard the company from these threats, it is essential to quickly correct flaws in the SSH server configuration and use more	22 / tcp / ssh

	SSH Server CBC Mode Ciphers Enabled					secure encryption techniques.	
6	***SSL/TLS Recommended Cipher Suites***	info	156899	The remote host has open SSL/TLS ports which advertise discouraged cipher suites. It is recommended to only enable support for the following cipher suites: TLSv1.3: - 0x13,0x01 TLS13_AES_128_GCM_SHA256 - 0x13,0x02 TLS13_AES_256_GCM_SHA384 - 0x13,0x03 TLS13_CHACHA20_POLY1305_SHA256 TLSv1.2: - 0xC0,0x2B ECDHE-ECDSA-AES128-GCM-SHA256 - 0xC0,0x2F ECDHE-RSA-AES128-GCM-SHA256 - 0xC0,0x2C ECDHE-ECDSA-AES256-GCM-SHA384 - 0xC0,0x30 ECDHE-RSA-AES256-GCM-	Only enable support for recommened cipher suites.	The business impact of having open SSL/TLS ports that advertise discouraged cipher suites can be significant. It poses a potential security risk to the organization as it may allow for weaker encryption algorithms that are susceptible to attacks. This configuration could undermine the confidentiality and integrity of data transmitted over these ports, leading to data breaches, compromised customer information, and legal consequences in terms of regulatory non-compliance. Furthermore, it might erode customer trust if they become aware of the security	21 / tcp

				SHA384 - 0xCC,0xA9 ECDHE-ECDSA-CHACHA20-POLY1305 - 0xCC,0xA8 ECDHE-RSA-CHACHA20-POLY1305 - 0x00,0x9E DHE-RSA-AES128-GCM-SHA256 - 0x00,0x9F DHE-RSA-AES256-GCM-SHA384 This is the recommended configuration for the vast majority of services, as it is highly secure and compatible with nearly every client released in the last five (or more) years.		weaknesses, potentially resulting in a loss of business and reputation damage. Therefore, it is advisable to follow the recommended cipher suite configuration to ensure a high level of security, compatibility, and protection against emerging threats, thus safeguarding the organization's data and reputation.	
7	Nessus SYN scanner	Info	11219	This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target. Note that SYN	Protect your target with an IP filter.	The ability of this SYN 'half-open' port scanner to quickly assess the accessibility of network services has a significant impact on business operations. While	21 / tcp

				scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.		this can be beneficial for efficiency, it can also put a strain on less resilient firewalls and possibly lead to unclosed connections on the remote target if network conditions are unfavorable.	
8	***DNS Server Detection***	info	11002	The remote service is a Domain Name System (DNS) server, which provides a mapping between hostnames and IP addresses.	Disable this service if it is not needed or restrict access to internal hosts only if the service is available externally.	The fact that the remote service is a Domain Name System (DNS) server has a substantial influence on company because DNS is essential for maintaining the dependability and accessibility of online services. It is crucial for converting understandable hostnames into computer-readable IP addresses, making it easier to browse websites, send	53 / tcp / dns

						emails, and perform other crucial internet operations. Any interruption or compromise of the DNS service may result in communication problems, website outages, and even serious financial loss. Furthermore, it is crucial to protect DNS servers from malicious assaults such as DNS hijacking, cache poisoning, and other threats that could result in data breaches and harm to one's reputation. Consequently, upkeep of a strong and secure DNS infrastructure is essential for business continuity and protecting the company's online visibility.	

9	SSL Certificate Chain Contains Certificates Expiring Soon	info	83298	The remote host has an SSL certificate chain with one or more SSL certificates that are going to expire soon. Failure to renew these certificates before the expiration date may result in denial of service for users.	Renew any soon to expire SSL certificates.	The remote host's SSL certificate chain, which contains certificates that are about to expire, has a substantial negative impact on company since it puts users at risk of service interruption and possible service denial. Web browsers and other clients may reject SSL/TLS connections if these certificates are not promptly reissued before they expire. If this happens, the services may become unavailable and customers may experience inconvenience. In addition to causing service interruptions, it can harm the company's reputation, lose customers, and cause financial losses if crucial web processes are impacted. In order to maintain a high level of customer satisfaction and continuous service availability,	21 / tcp

						proactive certificate management and renewal are essential.	

10		info	10185	The remote host is running a server that understands the Post Office Protocol (POP), used by email clients to retrieve messages from a server, possibly across a network link.	Disable this service if you do not use it.	Given that POP is essential to email communication within enterprises, the remote host's operation of a server that supports it will have a substantial impact on business operations. Any disruptions or problems with the POP server can prevent email access, which may result in communication delays, missed opportunities, and decreased staff productivity. POP allows email clients to retrieve messages from a server. Reliable and effective email communication is essential for internal collaboration, client relations, and overall operational efficiency in a corporate setting. Maintaining seamless email services and upholding the organization's capacity to carry	110 / tcp

	POP ServerPOP Server Detection					out daily operations successfully and professionally depend on the POP server's continued reliable functioning.	

Stage 3 Report

Achieving Proactive Cybersecurity with SOC and SIEM Integration

- **Security Operations Center (SOC)**

A centralized department within a company called a Security Operations Center (SOC) is crucial for tracking down, identifying, evaluating, and responding to security problems in real time. Its main goal is to continuously monitor and evaluate security events in order to protect the company's digital assets, such as networks, apps, and data. To proactively detect potential threats, risks, and suspicious behaviors, the SOC makes use of a combination of cutting-edge technologies, knowledgeable cyber security experts, and strong processes. These can include malware infestations and unauthorized access attempts. These can include malware infestations and unauthorized access attempts. Rapid incident response is made possible by the SOC's proactive strategy, which also lessens the potential effects of security breaches. To provide a comprehensive and successful cyber security strategy that is in line with the company's tolerance for risk and business objectives, SOCs frequently integrate intelligence on threats and work in conjunction with other teams. In conclusion, an organized SOC is an essential part of contemporary cyber security efforts, operating as a buffer against the constantly changing panorama of cyber threats.

- **SOC – cycle**

The Security Operations Center (SOC) operates in a continuous cycle to ensure effective security monitoring, incident detection, response, and ongoing improvement. This cycle is crucial for maintaining a proactive and adaptive cyber security posture. The SOC cycle typically involves the following stages:

- **Monitor and Collect Data:** The cycle begins with continuous monitoring of network traffic, system logs, and various security devices such as firewalls, intrusion detection systems (IDS), and endpoint protection systems. Data is collected from these sources to establish a baseline and detect anomalies or potential security incidents.
- **Detect and Analyze Anomalies:** Security analysts analyze the collected data to identify anomalies and potential security threats. This involves correlating events, investigating suspicious activities, and determining the severity and credibility of potential threats.
- **Alert and Prioritize Incidents:** Based on their impact and seriousness, possible threats and incidents are categorized. Lower-priority issues are treated in accordance with the specified incident response processes, whereas high-priority occurrences are escalated for prompt action..
- **Incident Response and Mitigation:** Security teams respond to identified incidents by containing the threat, eradicating malicious elements, and restoring affected systems to normal operation. Incident response actions may involve isolating affected systems, gathering evidence, and collaborating with other departments or external partners.
- **Investigation and Root Cause Analysis:** After containing and mitigating the incident, a thorough investigation is conducted to determine the root cause and extent of the incident. This includes analyzing attack vectors, identifying vulnerabilities, and understanding the tactics, techniques, and procedures (TTPs) used by threat actors.
- **Lessons Learned and Knowledge Enhancement:** Post-incident, the SOC team reviews the incident handling process to identify strengths and weaknesses. Lessons learned are documented to enhance incident response procedures and strengthen security controls. Knowledge gained from each incident enriches the team's capabilities for future threat detection and response.
- **Adapt and Improve Security Measures:** Based on lessons learned and insights gained, the SOC team works on refining security measures. This may involve updating detection rules, fine-tuning monitoring systems, implementing additional security controls, or providing additional training to staff to enhance the overall security posture.

- **Continuous Monitoring and Iteration:** The SOC cycle is continuous, with the team persistently monitoring the environment, staying updated on emerging threats, adapting security measures, and refining incident response procedures. This iterative process ensures that the organization is constantly evolving and effectively addressing the dynamic threat landscape.

By following this cycle, the SOC maintains a proactive and resilient security posture, crucial for safeguarding an organization's assets and data against evolving cyber threats.

- **Security Information and Event Management (SIEM)**

A Security Information and Event Management (SIEM) system is a powerful and sophisticated technology used by organizations to centralize, aggregate, and analyze security-related data from various sources within their IT infrastructure. This includes logs, events, and alerts from network devices, servers, applications, and security solutions like firewalls and intrusion detection systems (IDS). The SIEM platform correlates this data, applying advanced analytics and machine learning algorithms to identify patterns, anomalies, and potential security incidents. By consolidating and contextualizing diverse data, SIEM helps security teams gain actionable insights into security events, enabling them to detect and respond to threats in real-time or near real-time.

SIEM facilitates incident investigation and forensics by providing a comprehensive view of security events and their relationship to one another. It aids in compliance management by assisting organizations in meeting regulatory requirements for data security and reporting. SIEM solutions play a crucial role in enhancing an organization's security posture by streamlining incident response, improving operational efficiency, and enabling proactive threat hunting. Overall, SIEM systems are fundamental tools for modern cybersecurity, helping organizations manage and fortify their defenses against a continuously evolving threat landscape.

SIEM (Security Information and Event Management) solutions offer a multitude of benefits to enterprises, making them a vital component in the realm of cybersecurity by optimizing security workflows. Here are some key ways in which SIEM solutions provide substantial advantages to organizations:

- **Centralized Security Monitoring:**

SIEM solutions aggregate and centralize security data from various sources into a single platform. This centralized approach allows security teams to monitor the organization's entire IT environment from a unified interface, simplifying monitoring and enhancing efficiency.

- **Real-time Threat Detection and Alerts:**

SIEM systems analyze security events and data in real-time, enabling swift detection of potential threats or security incidents. Automated alerts and notifications are generated, allowing security teams to respond promptly and mitigate risks, reducing the potential impact of cyber-attacks.

- **Advanced Threat Detection and Correlation:**

SIEM platforms employ sophisticated correlation and analytics capabilities to detect complex threats. By correlating disparate events and applying advanced algorithms, SIEM can identify patterns and anomalies that may go unnoticed by traditional security tools.

- **Improved Incident Response and Investigation:**

SIEM solutions facilitate a structured incident response process by providing detailed information about security incidents. Security teams can quickly investigate incidents, identify the root cause, understand the attack vector, and take appropriate actions to prevent future occurrences.

- **Compliance and Reporting:**

For organizations subject to regulatory compliance requirements, SIEM solutions simplify compliance management by automating data collection and reporting. They generate compliance reports, ensuring that the organization adheres to industry-specific regulations and standards.

- **Efficient Log Management and Retention:**

SIEM systems help manage and retain logs efficiently, providing a comprehensive audit trail of security events. This capability is crucial for forensic analysis, incident investigations, and meeting legal and regulatory requirements for data retention.

- **Optimized Resource Utilization:**

SIEM solutions optimize resource utilization by reducing false positives and allowing security teams to focus on genuine threats. This efficiency ensures that security resources are directed where they are needed most, improving overall productivity and cost-effectiveness.

- **Threat Intelligence Integration:**

SIEM platforms can integrate threat intelligence feeds, enriching the analysis of security events with up-to-date information about known threats and vulnerabilities. This integration enhances threat detection and provides a broader context for incident analysis.

- **Scalability and Flexibility:**

SIEM solutions are designed to scale with the organization's growth. They can handle an increasing volume of data and adapt to evolving security requirements, ensuring continued effectiveness as the organization expands or modifies its IT infrastructure.

- **Future of SIEM**

  Predicting the future of Security Information and Event Management (SIEM) involves anticipating trends based on current advancements, emerging technologies, and evolving cybersecurity needs. Here are five predictions for the future of SIEM:

  - **Integration with Extended Detection and Response (XDR) Platforms:**

  SIEM is expected to integrate more seamlessly with Extended Detection and Response (XDR) platforms. XDR platforms provide a broader view of security events by integrating data from multiple sources, including endpoint, network, and cloud. The integration of SIEM with XDR will enhance threat detection and response capabilities by leveraging AI and machine learning to correlate and analyze a wider range of security data.

  - **Enhanced Automation and Orchestration:**

  Future SIEM solutions will increasingly leverage automation and orchestration to handle routine and repetitive security tasks. Automation will help in rapidly responding to known threats, while orchestration will streamline incident response workflows, enabling faster and more coordinated actions during security incidents.

  - **Advanced Behavioral Analytics and AI-driven Insights:**

  SIEM will employ more advanced behavioral analytics and AI-driven insights to detect subtle and sophisticated cyber threats. Machine learning algorithms will help identify abnormal patterns of behavior within the network, endpoints, and applications, allowing for the early detection of anomalies that might signify a security breach.

  - **Focus on Cloud-native SIEM Solutions:**

  As organizations continue to adopt cloud technologies and workloads, SIEM solutions will become increasingly cloud-native. Cloud-native SIEM will provide better scalability, flexibility, and agility to adapt to dynamic and distributed cloud environments. Additionally, these solutions will offer enhanced visibility into cloud-related threats and security events.

  - **Integration of Threat Intelligence and Threat Hunting Capabilities:**

  Future SIEM platforms will enhance threat intelligence integration and incorporate proactive threat hunting capabilities. This integration will enable organizations to harness threat intelligence feeds to stay updated on emerging threats and use threat hunting techniques to proactively search for potential threats within their environment.

- **Siem Cycle**

The Security Information and Event Management (SIEM) cycle outlines the systematic process involved in managing security information and events using a SIEM solution. This cycle ensures that security operations are effective, well-coordinated, and continuously improving. Here are the key stages of the SIEM cycle:

- **Data Collection and Aggregation:**

The SIEM cycle begins with collecting security-related data from various sources within the organization's IT infrastructure. This includes logs, events, alerts, and other relevant information generated by network devices, applications, servers, and security solutions. The collected data is then aggregated into a centralized SIEM platform.

- **Normalization and Parsing:**

Once the data is aggregated, it undergoes normalization and parsing processes to ensure a standardized format. This step is crucial for consistent analysis and correlation of events from diverse sources, aligning them into a common structure that the SIEM system can interpret.

- **Event Correlation and Analysis:**

In this stage, the SIEM solution correlates and analyzes the normalized data to detect patterns, anomalies, and potential security incidents. Sophisticated algorithms and correlation rules are applied to identify events that may indicate a security threat or violation of security policies.

- **Alert Generation and Prioritization:**

Based on the correlation and analysis, the SIEM system generates alerts or notifications for security incidents or events that require attention. Alerts are prioritized based on predefined rules, severity levels, or the potential impact on the organization's security.

- **Incident Handling and Response**:

When alerts are generated, the security team initiates incident handling and response procedures. This involves investigating the incident, determining its scope and impact, containing the incident to prevent further damage, and implementing appropriate measures to mitigate the threat.

- **Forensic Investigation and Reporting:**

After an incident is contained, the SIEM solution supports forensic investigation by providing a comprehensive view of the incident details, including timelines, affected systems, and actions taken. This information is crucial for generating incident reports and documenting lessons learned.

- **Knowledge and Rule Base Enhancement:**

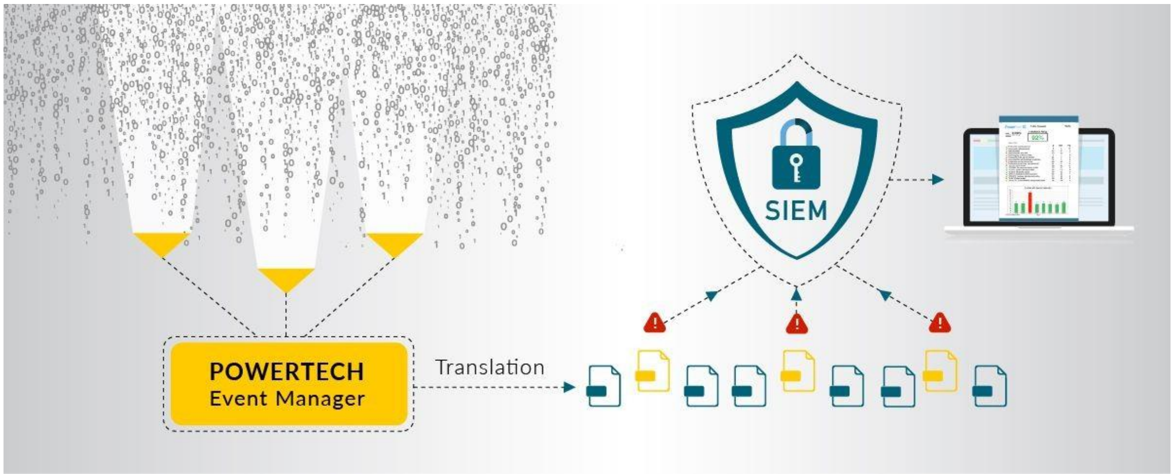
Post-incident, the SIEM system undergoes knowledge and rule base enhancement. Security teams review incident response procedures, correlation rules, and alerting mechanisms to incorporate lessons learned and improve the SIEM's detection and response capabilities.

- **Continuous Monitoring and Fine-tuning:**

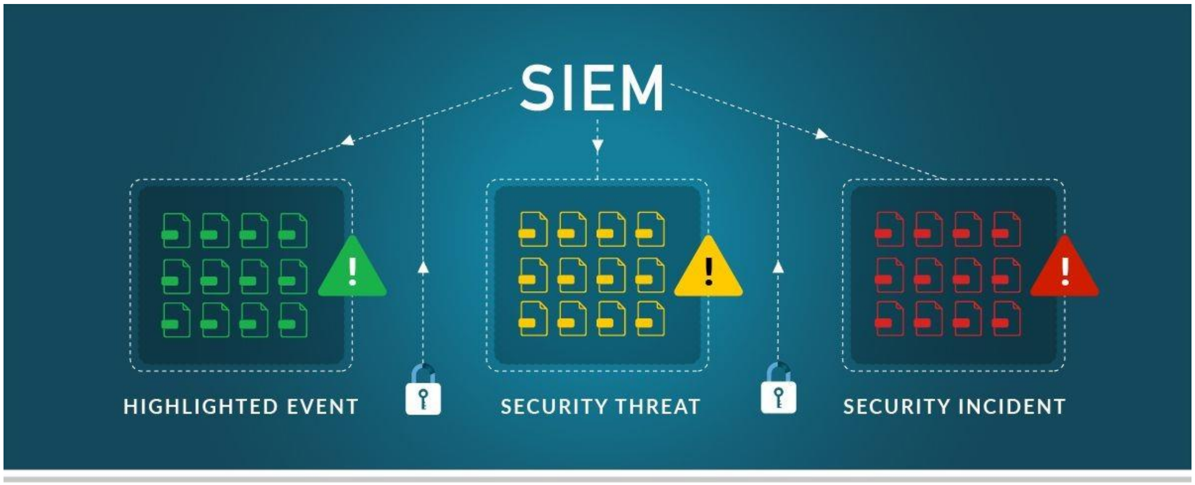
The SIEM cycle is continuous, with the system continuously monitoring security events, adapting to evolving threats, and fine-tuning its rules, alerts, and response mechanisms. This iterative process ensures that the SIEM solution remains effective and up-to-date in the ever-changing cybersecurity landscape.

Threat Detection

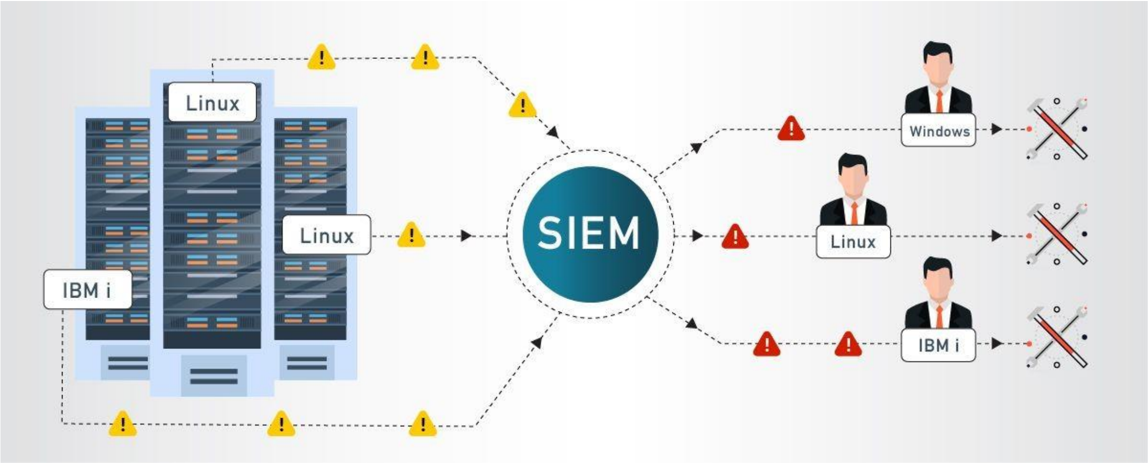
Translation



Prioritization

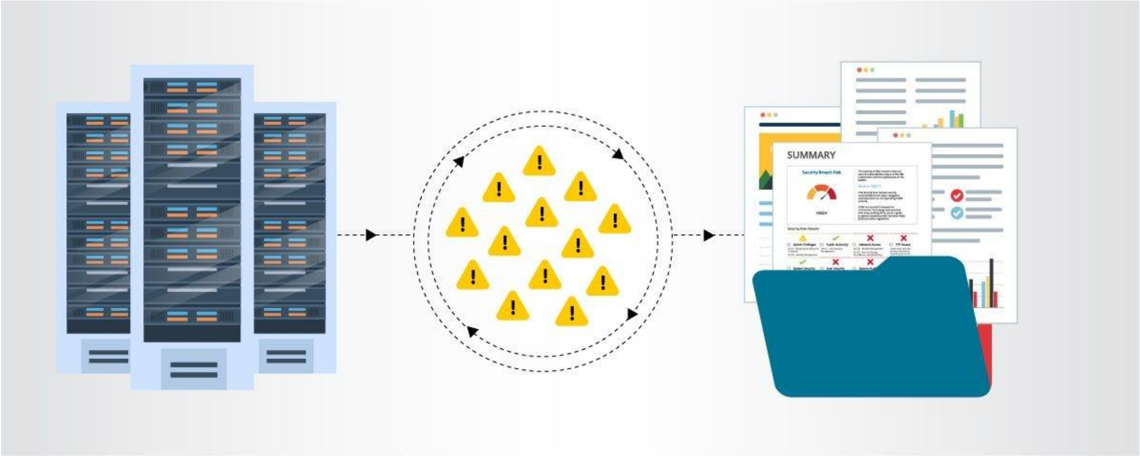


Escalation



Analysis

Compliance



- **Malware Information Sharing Platform (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 MISPuser-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

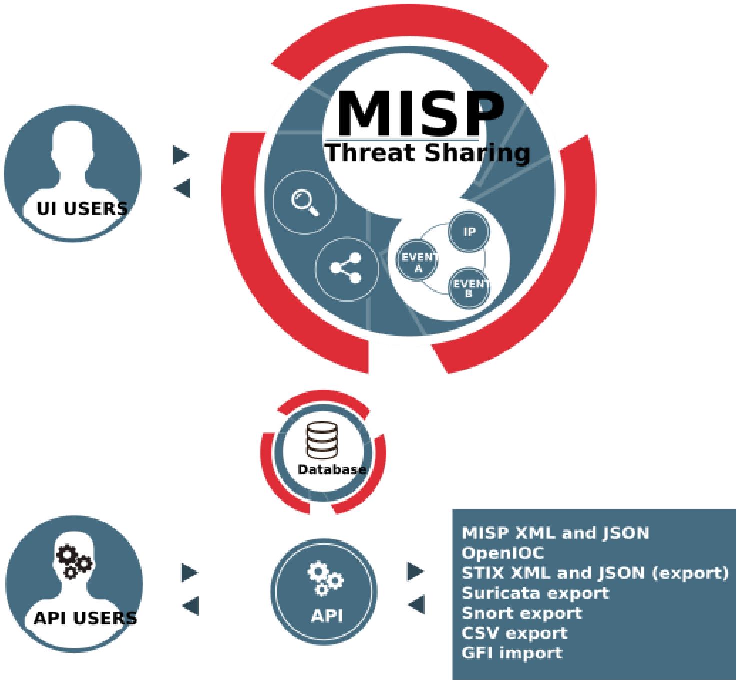
Data you store is immediately available to your colleagues and partners. Store the event id in your ticketing system or be informed by the signed and encrypted email notifications.

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.

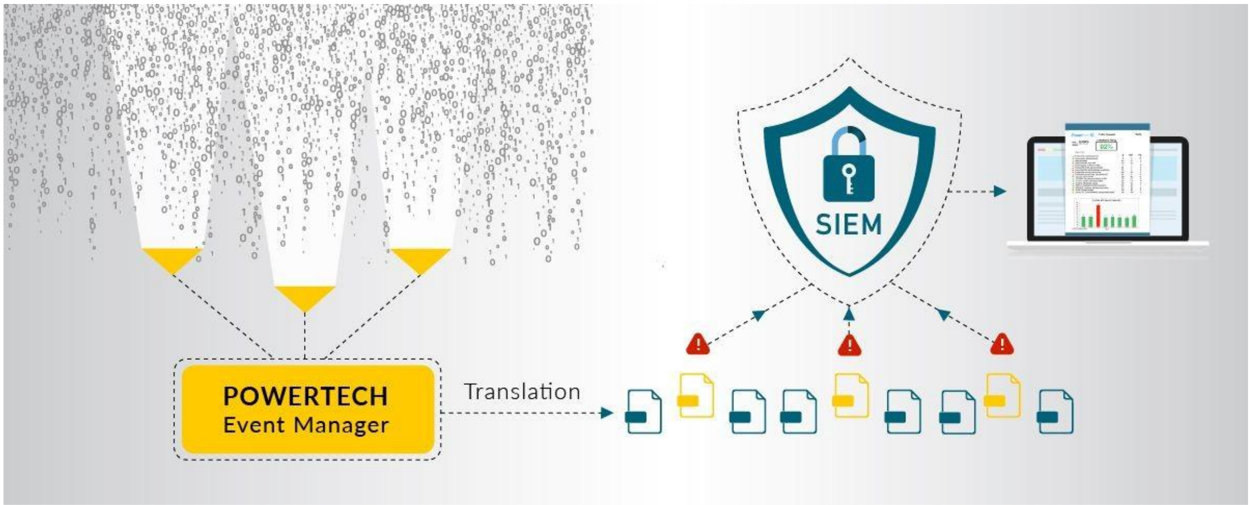
Collaborative sharing of analysis and correlation

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.

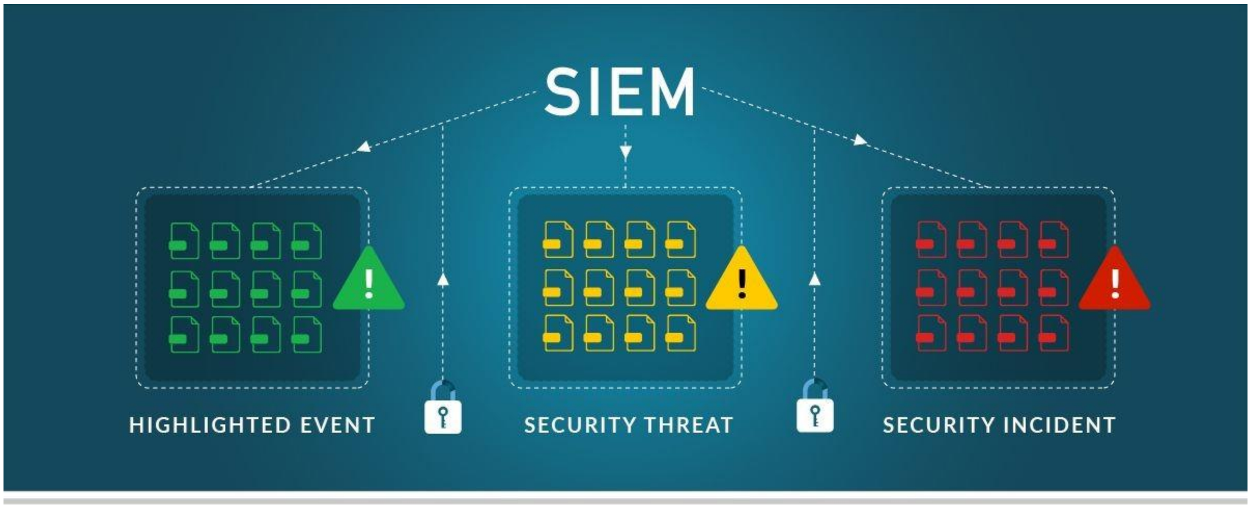


Threat Detection

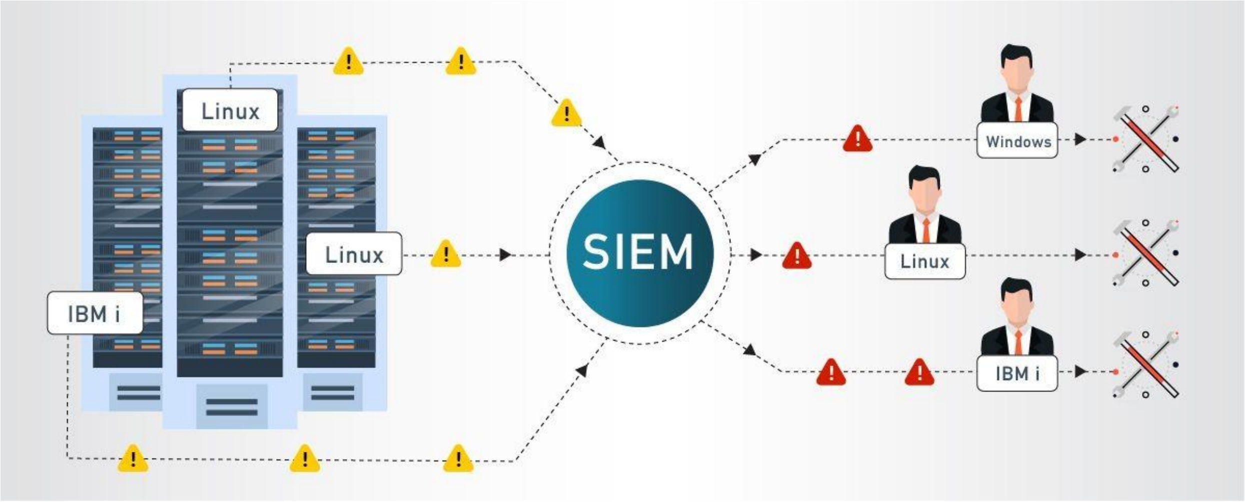
Translation



Prioritization

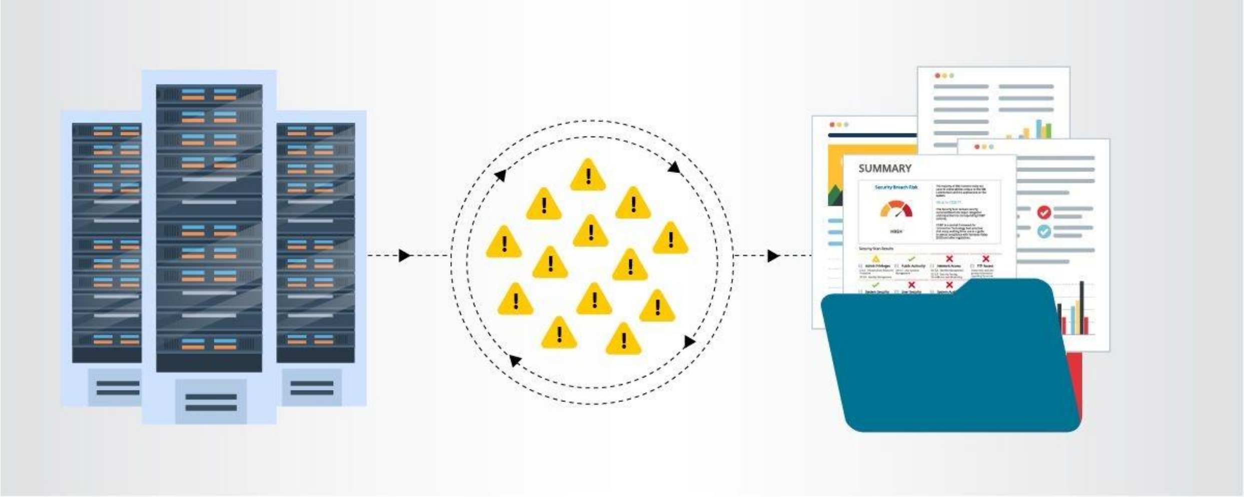


Escalation



Analysis

Compliance



- **MISP**

MISP, Malware Information Sharing Platform and Threat Sharing, corefunctionalities 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. Notonly 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. Correlationcan 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 differentmodels 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 lists to help the analysts contribute events and attributes.

storing data in a structured format (allowing automated use of the database for various purposes) with extensive support of cyber security indicators along with ud 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 usersto 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 withPyMISP 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 toyour 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 existingthreat 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

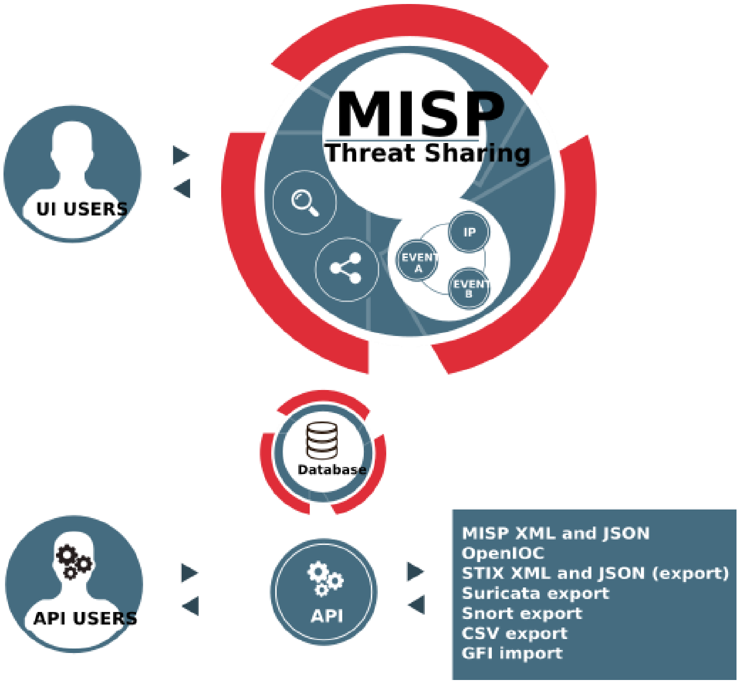
Data you store is immediately available to your colleagues and partners. Store the event id in your ticketing system or be informed by the signed and encrypted email notifications.

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 orcustom 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 inpossession 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 acolleague had already worked on another, similar, threat? Or that an external report has already been made? When new data is added MISP willimmediately 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**

  Institute of technology
  My college has 3 labs and total of around 300 systems for networking.

- **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:

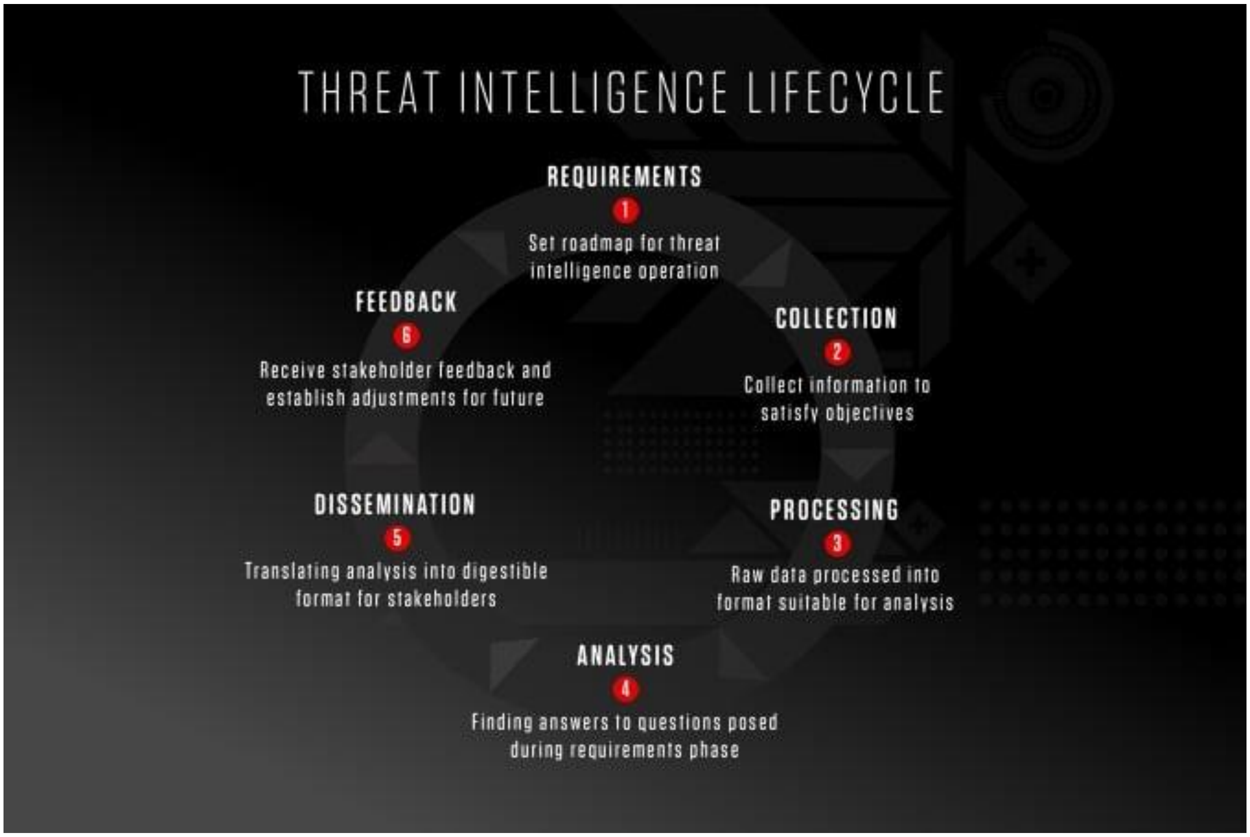
- Continuously monitor the SOC's performance and effectiveness in detecting and responding to security incidents.
- Generate regular reports and metrics to measure the SOC's performance and communicate its value to stakeholders.

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.

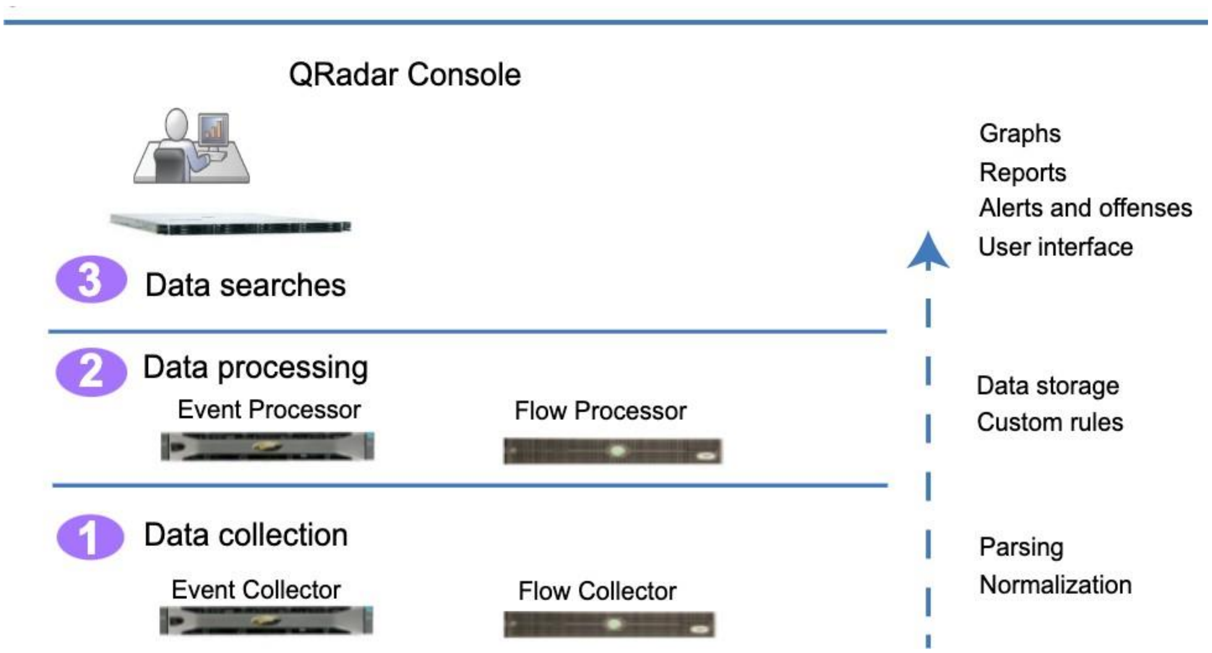


Figure 1. QRadar architecture

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 fromother 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:

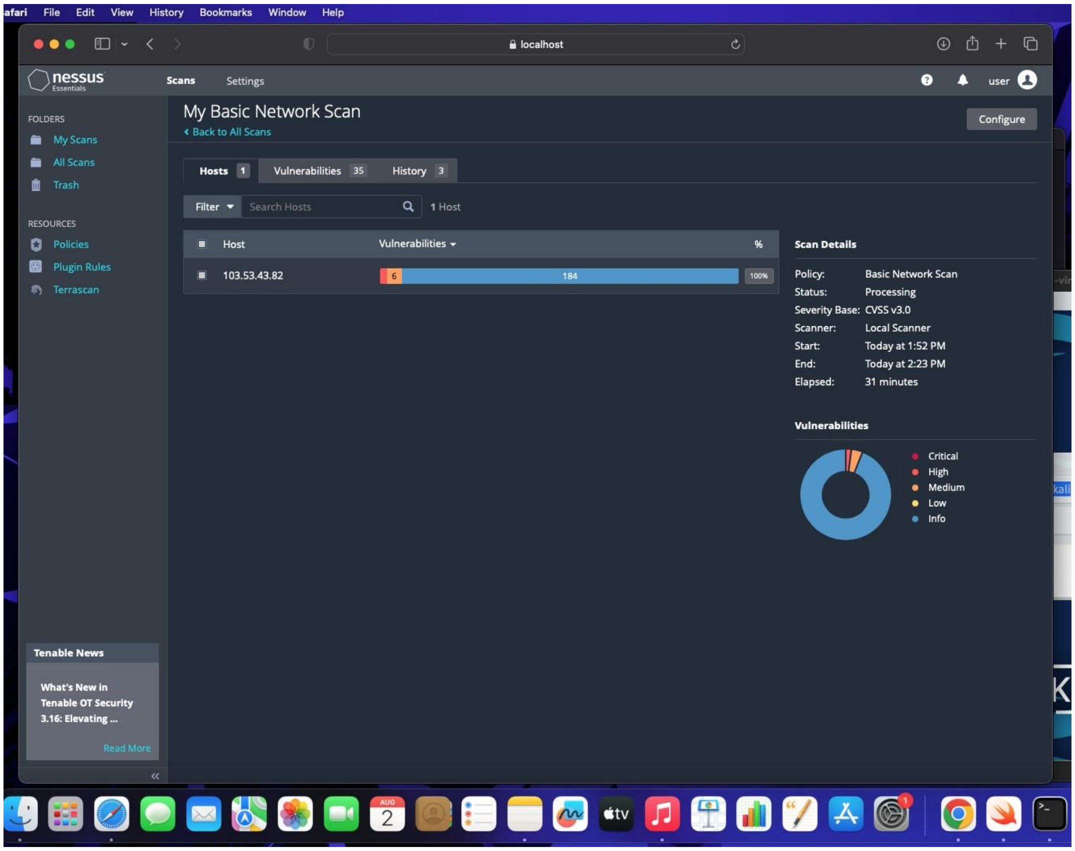
- Identification of Security Vulnerabilities
- Bug Detection and Resolution
- Validation of Functional Requirements
- Usability and User Experience Evaluation
- Performance and Load Testing Results
- Compatibility Testing Insights
- Accessibility Compliance
- Security Compliance and Risk Mitigation
-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



My Basic Network Scan

‹ Back to All Scans

1 Host

Host	Vulnerabilities	%
103.53.43.82	6 184	100%

Scan Details

Policy: Basic Network Scan
Status: Processing
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 1:52 PM
End: Today at 2:23 PM
Elapsed: 31 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

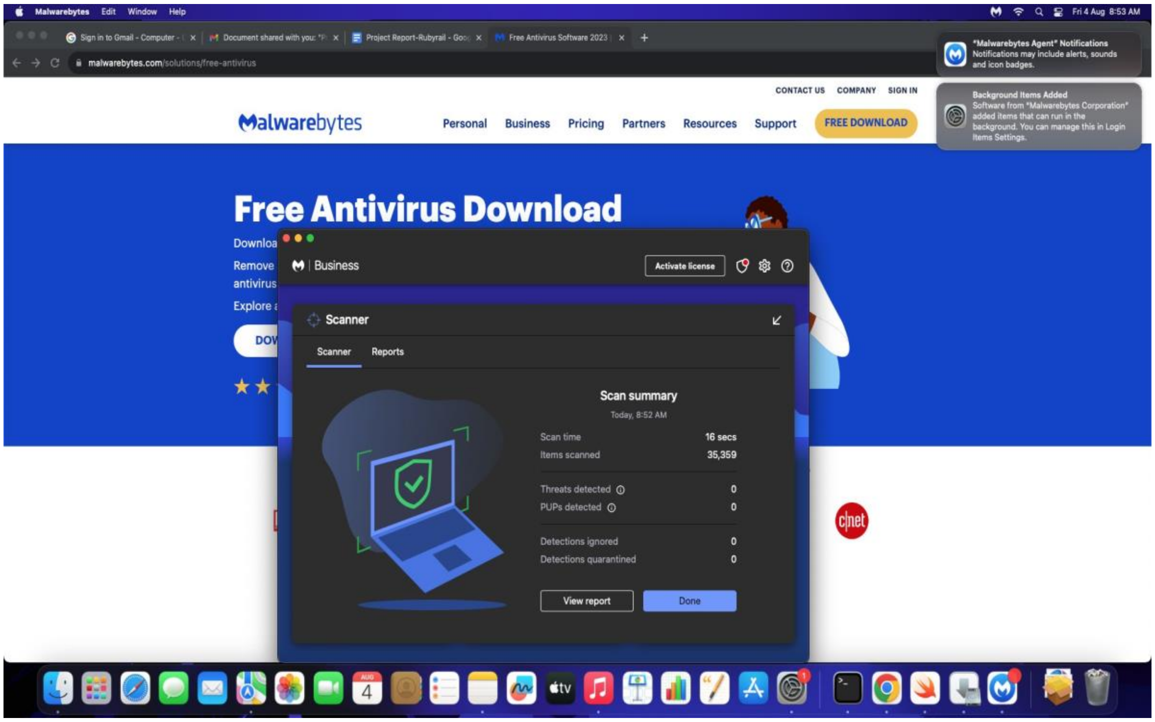
Tools explored :-

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

FREE DOWNLOADS

Free Antivirus Software 2023 - Malwarebytes

Malwarebytes free antivirus includes multiple layers of malware-crushing tech. It 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: "P
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.

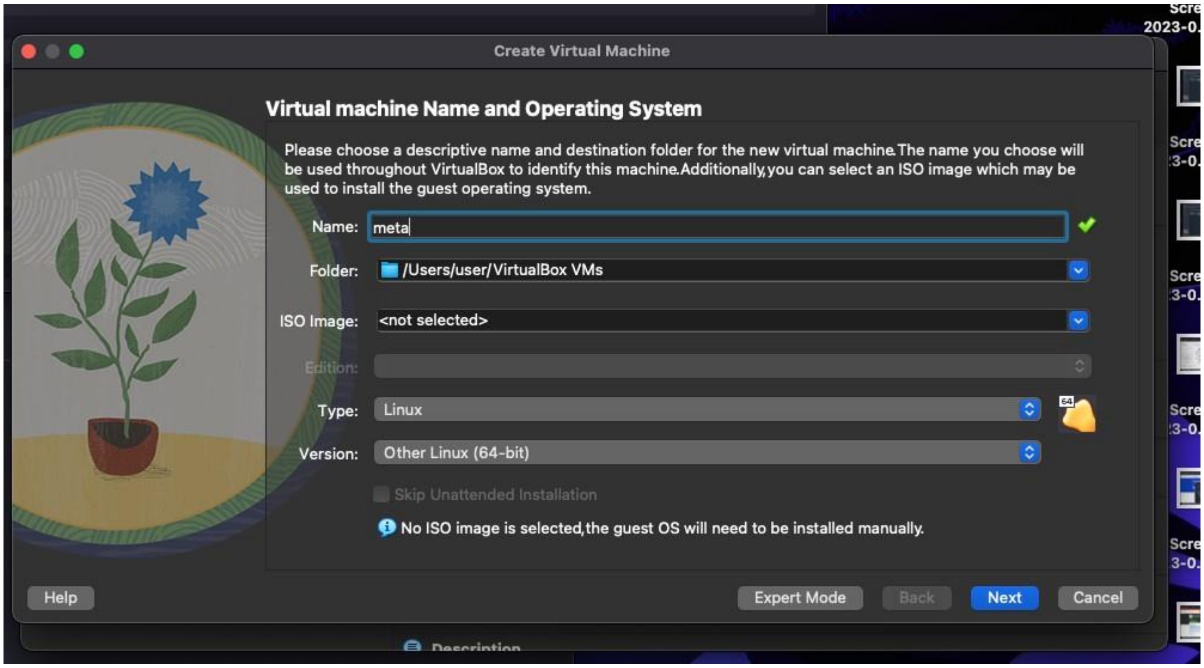
Background Items Added
Software from "Malwarebytes Corporation" added items that can run in the background. You can manage this in Login Items Settings.

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:

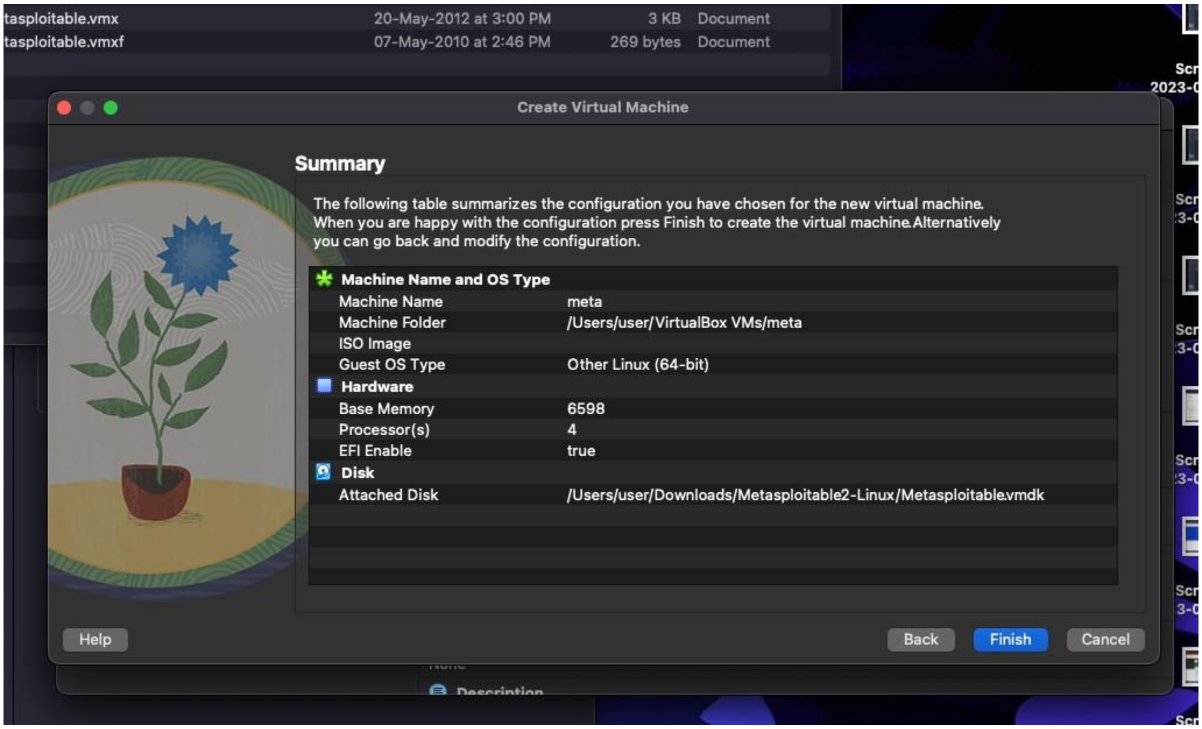
Type: Linux

Version: Other Linux (64-bit)

□ Skip Unattended Installation

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

Help
Expert Mode
Back
Next
Cancel



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

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
```