**TEAM -I**

**A trustworthy Defender**

# 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.Thestepstoimplementcybersecurityeffectivelyateveryorganizationinclude:

* 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 toidentifypotentialcybersecuritythreats and vulnerabilities specific to the organization. Prioritize risks based on their potential impact and likelihood of occurrence. Implement risk mitigation measures and create a risk management plan to address identified vulnerabilities.
* Train all employees on cybersecurity best practices and the role they play in safeguarding the organization's information. Educate them about phishing,social engineering, password hygiene, and other common attack vectors to promote a security-conscious culture.
* Implement strong access control measures to ensure that only authorized personnel can access sensitive data and critical systems. Utilize multi-factor authentication(MFA)foranextralayerofsecurity.
* Deploy firewalls, intrusion detection/prevention systems (IDS/IPS), and secure gatewaystomonitorandcontrolnetworktraffic
* Installantivirussoftware,endpointprotectiontools,andhost-basedfirewallson all devices to defend against malware and other threats at the device level.
* Installantivirussoftware,endpointprotectiontools,andhost-basedfirewallson all devices to defend against malware and other threats at the device level.
* Encrypt sensitive data both at restandintransittopreventunauthorizedaccess and ensure data confidentiality.
* Establish a systematic process to apply security patches and updates promptly to all software, operating systems, and firmware to address known vulnerabilities.
* Develop a well-defined incident response plan (IRP) to handle cybersecurity incidents effectively. The plan should include clear guidelines on identifying, reporting, containing, eradicating, and recovering from security incidents.
* Conduct regular internal and external security audits and assessments to evaluate the organization's security posture and identify potential weaknesses or gaps.
* Monitoring and Logging: Implement centralized logging and real-timemonitoringofnetworkandsystemactivitiestodetectandrespondtosuspicious activities promptly.
* Establish clear channels for reporting security incidents and communicatingwith stakeholders, including employees, customers, partners, and regulatory authorities.

**IPaddressofhttps://www.npci.org.in/103.14.162.209**

1. **TeamMembersInvolvedinvulnerabilityAssessment**

|  |  |  |  |
| --- | --- | --- | --- |
| **S.No** | **Name** | **Designation** | **MobileNumber** |
| 1 | A. Veluisamy | Assistant Professor | 9043215401  Krishnaprakash.ads@sonatech.ac.in |

|  |  |  |  |
| --- | --- | --- | --- |
| 2 | Santhosh Kumar C | Assistant Professor | 9786610478  [santhoshkumar.it@sonatech.ac.in](mailto:santhoshkumar.it@sonatech.ac.in) |
| 3 | David Samuel Azariya S | Assistant Professor | 9843790325 david@sonatech.ac.in |

1. **ListofVulnerableParameter,locationdiscovered**

|  |  |  |
| --- | --- | --- |
| **S.No** | **NameoftheVulnerability** | **ReferenceCWE** |
| 1 | BrokenAccessControl | CWE285-ImproperAuthorization |
| 2 | CryptographicFailures | CWE-916: Use of Password Hash With Insufficient Computational Effort |
| 3 | Injection | CWE-564:SQLInjection:Hibernate |
| 4 | InsecureDesign | CWE-653:ImproperIsolationor Compartmentalization |
| 5 | SecurityMisconfiguration | CWE-614:[Sensitive Cookie in HTTPSSession Without 'Secure' Attribute](https://cwe.mitre.org/data/definitions/614.html) |
| 6 | Vulnerable and Outdated Components | CWE-1395:DependencyonVulnerable Third-Party Component |
| 7 | Identification and AuthenticationFailures | CWE-521:WeakPasswordRequirements |
| 8 | SoftwareandDataIntegrity Failures | CWE-565C:RelianceonCookieswithout Validation and Integrity Checkin |
| 9 | Security Logging and Monitoring Failures | CWE-532:[Insertion of Sensitive Informationinto Log File](https://cwe.mitre.org/data/definitions/532.html) |
| 10 | ServerSideRequestForgery | CWE-918:ServerSideRequestForgery |

1. **CWE: CWE 285- Improper Authorization**

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

**DESCRIPTION:** The product does not perform or incorrectly performs an authorizationcheckwhenanactorattemptstoaccessaresourceorperform an action.

**BUSINESS IMPACT:** Assuming a user with a given identity, authorizationis the process of determining whether that user can access a given resource, based on the user's privileges and any permissions or other access-control specifications that apply to the resource. When accesscontrol checks are not applied consistently - ornotatall-usersareableto access data or perform actions that they should not be allowed toperform. This can lead to a widerangeofproblems,includinginformationexposures, denial of service, and arbitrary code execution.

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

**OWASP CATEGORY : A02 2021 Cryptographic Failures**

**DESCRIPTION:** The productgeneratesahashforapassword,butitusesa scheme that does not provide a sufficient level of computational effort that would make password cracking attacks infeasible or expensive.

**BUSINESS IMPACT:** In this design, authentication involves accepting an incoming password, computing its hash, and comparing it to the stored hash. After an attacker has acquired stored password hashes, they are always able to brute force hashes offline. As a defender, it is only possible to slow down offline attacks by selecting hash algorithms that are as resource intensive as possible.

# CWE:CWE564:SQLInjection:Hibernate OWASP CATEGORY : A03 2021 Injection

**DESCRIPTION:**Using Hibernate to execute a dynamic SQL statement built with user-controlled input can allow an attacker to modify the statement's meaning or to execute arbitrary SQL commands.

**BUSINESS IMPACT:** Hackers use SQL injection attacks toaccesssensitive business or personally identifiable information (PII), which ultimately increases sensitive data exposure. Using SQL injection, attackers can retrieve and alter data, which risks exposing sensitivecompanydatastored on the SQL server. Compromise Users' Privacy: Depending on the data stored on the SQL server, an attack can expose private user data, such as credit card numbers.

# 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:** Insecure system configuration risks stem from flaws in the security settings, configuration and hardening of the differentsystems across the pipeline (e.g. SCM, CI, Artifact repository), often resulting in “low hanging fruits” for attackers looking to expand their foothold in the environment.

# CWE: CWE 614-[Sensitive Cookie in HTTPS Session Without'Secure' Attribute](https://cwe.mitre.org/data/definitions/614.html)

**OWASP CATEGORY : A05 2021 Security Misconfiguration**

**DESCRIPTION:** The Secure attribute for sensitive cookies in HTTPS sessions is not set, which could cause the user agenttosendthosecookies in plaintext over an HTTP session.

**BUSINESS IMPACT:** Security misconfigurations allow attackers to gain unauthorized access to networks, systems and data, which in turn cancause significant monetary and reputational damage to your organization.

# CWE: CWE 1395: Dependency on Vulnerable Third-Party Component

**OWASP CATEGORY : A06 2021 Vulnerable and OutdatedComponents**

**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.

**BUSINESSIMPACT:**Anentireoperatingsystemmightbefroma third-party supplier in some hardware products. Whether open or closed source, these components may contain publicly known vulnerabilities that could be exploited by adversaries to compromise the product with more known vulnerabilities. Dependency-Check is a Software Composition Analysis (SCA) tool that attempts to detect publiclydisclosedvulnerabilities contained within a project's dependencies. It does this by determining if there is a Common Platform Enumeration (CPE) identifier for a given dependency.

# CWE:CWE 521-[WeakPassword Requirements](https://cwe.mitre.org/data/definitions/521.html)

**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 mechanisms often rely on a memorized secret (also known as a password) to provide an assertion of identity for a user of a system. It is therefore important that thispassword be of sufficient complexity and impractical for an adversary to guess. The specific requirements aroundhowcomplexapasswordneedstobedepends on the type of system being protected. Selecting the correct password requirements and enforcing them throughimplementationarecriticaltothe overall success of the authentication mechanism.

# CWE:CWE-565CRelianceonCookieswithoutValidationand Integrity Checkin

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

**DESCRIPTION: T**he product relies on the existence or values of cookies whenperformingsecurity-criticaloperations,butitdoesnotproperlyensure that the setting is valid for the associated user.Attackers can easily modify cookies, within the browser or by implementing theclient-sidecodeoutside of the browser. Reliance on cookies without detailedvalidationandintegrity 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:** This problem can be primary to many types of weaknesses in web applications.Adevelopermayperformpropervalidation against URL parameters while assuming that attackers cannot modify cookies. As a result,theprogrammightskipbasicinputvalidationtoenable cross-site scripting, SQL injection, price tampering, and other attacks.

# 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:** Information written to log files can be of a sensitive nature and give valuable guidance to an attacker or expose sensitive user information.

# 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 ofthisURL,butitdoesnot sufficiently ensure that the request is being sent to the expected destination.

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

**Stage:2 Report**

**NESSUSVulnerabilityReport 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 theirseverityandpotentialimpact.Prioritizefixes based on criticality and help the college's IT team or web developers with the remediation process. Document all identified vulnerabilities, along with their severity and potential impact. Prioritize fixes based on criticality and help the college's IT team or web developers with the remediation process.

Nessusisapopularvulnerabilityassessmenttoolthatiswidelyusedby

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 identifygapsandachieve 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 tothe 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 gaininsightsintothesecuritypostureoftheirsystems.This

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

**Risk Assessment:** Nessus assigns severity levels to identified vulnerabilities,helpingorganizationsprioritizetheireffortsbyfocusing on high-risk vulnerabilities first.

**Penetration Testing Support:** Nessus can complement manual penetration testing efforts by providinganinitialoverviewofpotential 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 andzero-day threats.

**TargetWebSite:** en.Wikipedia.org **Target IP : 198.35. 26.96**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **S.**  **No.** | **Vulnera bility name** | **Severi ty** | **Plugi n** | **Description** | **Solution** | **Business Impact** | **Port** |
| 1 | SSL  Medium Strength Cipher Suites Supporte d (SWEET3 2) | High | 42873 | The remote host supports the use of SSL ciphers that offer  mediumstrength encryption.  Nessus regards mediumstrength as any  encryption that useskeylengths | Reconfigur e the  affected application if possible  to avoid  use of  medium strength ciphers. | Successful  brute-forcingof weak ciphers canresultina malicious actor decryptingdata containing sensitive information, potentially leading to a | 208  7,20  83,2  096 |
|  |  |  |  | atleast64bits |  | complete |  |
|  |  |  |  | and less than |  | compromise of |  |
|  |  |  |  | 112bits,orelse |  | confidentiality |  |
|  |  |  |  | that uses the |  | andintegrity. |  |
|  |  |  |  | 3DESencryption |  | The extent of |  |
|  |  |  |  | suite. |  | damageisreally only limitedto |  |
|  |  |  |  |  |  | the value of |  |
|  |  |  |  |  |  | compromised |  |
|  |  |  |  |  |  | data and the |  |
|  |  |  |  |  |  | imagination of |  |
|  |  |  |  |  |  | theattacker. |  |
| 2 |  | Mediu |  | The remote | Enable | theattackercan | 208 |
| TLS  Version 1.0  Protocol Detection | m | 10474  3 | service accepts connections encrypted using TLS1.0.TLS1.0  hasa number of cryptographic | support for TLS1.2  and 1.3, anddisable support for TLS 1. | exploit a  vulnerability in the implementation ofCBC(cipher block chaining) | 7,20  83,2  096 |
|  |  |  |  | design flaws. |  | inTLS1.0.This |  |
|  |  |  |  | Modern |  | enables the |  |
|  |  |  |  | implementations |  | attacker to |  |
|  |  |  |  | of TLS 1.0 |  | decrypt the |  |
|  |  |  |  | mitigate these |  | encrypted data |  |
|  |  |  |  | problems, but |  | between two |  |
|  |  |  |  | newer versions |  | users/systems |  |
|  |  |  |  | ofTLSlike1.2 |  | byinjectingthe |  |
|  |  |  |  | and 1.3 are |  | crafted packets |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  | designedagainst theseflawsand shouldbeused whenever possible. |  | into TLS  streams using MITM  techniques. |  |
| 3 |  | Mediu | 15728 | Theremotehost | Only | vulnerable to | 208 |
| TLS  Version | m | 8 | has open  SSL/TLS ports | enable supportfor | downgrade attacks since | 7,20  83,2 |
|  | 1.1  Protocol |  |  | which advertise discouraged | recommen dedcipher | they rely on SHA-1hashfor | 096 |
|  | Deprecat |  |  | ciphersuites. | suites. | theintegrityof |  |
|  | ed |  |  | LikeTLSv1.3: |  | exchanged messages.Even |  |
|  |  |  |  | - 0x13,0x01 |  | authentication |  |
|  |  |  |  | TLS13\_AES\_128 |  | of handshakes |  |
|  |  |  |  | \_GCM\_SHA256 |  | is done based |  |
|  |  |  |  |  |  | onSHA-1,which |  |
|  |  |  |  |  |  | makesiteasier |  |
|  |  |  |  |  |  | foranattacker |  |
|  |  |  |  |  |  | to impersonate |  |
|  |  |  |  |  |  | a server for |  |
|  |  |  |  |  |  | MITMattacks. |  |
| 4 |  | Low | 48204 | Theremotehost | Disable | A flaw was | 443 |
|  | 48204 |  |  | is running the | theseHTTP | found in the |  |
|  | Apache |  |  | Apache HTTP | methods. | waytheApache |  |
|  | HTTP |  |  | Server,anopen | Refer to | HTTP Server |  |
|  | Server |  |  | source web | the plugin | handled Range |  |
|  | Version |  |  | server. It was | output for | HTTPheaders.A |  |
|  |  |  |  | possibletoread | more | remoteattacker |  |
|  |  |  |  | the version | information | could use this |  |
|  |  |  |  | numberfromthe banner. | . | flaw to cause httpdtousean |  |
|  |  |  |  |  |  | excessive |  |
|  |  |  |  |  |  | amount of |  |
|  |  |  |  |  |  | memory and |  |
|  |  |  |  |  |  | CPU time via |  |
|  |  |  |  |  |  | HTTP requests |  |
|  |  |  |  |  |  | with a |  |
|  |  |  |  |  |  | specially-crafted |  |
|  |  |  |  |  |  | Range header. |  |
|  |  |  |  |  |  | This could be |  |
|  |  |  |  |  |  | usedinadenial |  |
|  |  |  |  |  |  | of service |  |
|  |  |  |  |  |  | attack. |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 5 |  | Low | 16660 | Report Fully |  | Use fully | NA |
|  | Asset |  | 2 | QualifiedDomain | qualifieddomain |  |
|  | Attribute: |  |  | Name (FQDN) | name (FQDN) |  |
|  | Fully |  |  | for the remote | objects in |  |
|  | Qualified |  |  | host. | firewall policy |  |
|  | Domain |  |  |  | rules to filter |  |
|  | Name |  |  |  | incoming or |  |
|  | (FQDN) |  |  |  | outgoing traffic |  |
|  |  |  |  |  | from or to |  |
|  |  |  |  |  | specific |  |
|  |  |  |  |  | domains. |  |
| 6 | DNS  server | Low | 72779 | Nessuswasable toobtainversion |  | NSattackscan enable threat | 53 |
|  | detection |  |  | information by | actors to take |  |
|  |  |  |  | sendingaspecial | down servers, |  |
|  |  |  |  | TXTrecordquery | stealdata,lead |  |
|  |  |  |  | to the remote | users to |  |
|  |  |  |  | host. | fraudulentsites, |  |
|  |  |  |  |  | and perform |  |
|  |  |  |  |  | Distributed |  |
|  |  |  |  |  | Denial of |  |
|  |  |  |  |  | Service(DDoS) |  |
|  |  |  |  |  | attacks. |  |
| 7 | DNS | Low | 10028 | Theremotehost isrunningBIND | It is  possibleto | BIND DNS  reveals the | 53 |
|  | Server |  |  | oranotherDNS | hide the | versionnumber |  |
|  | BIND |  |  | server that | version | when queried |  |
|  | version |  |  | reports its | number of | for a certain |  |
|  | Directive |  |  | version number | BIND by | TXT record. |  |
|  | Remote |  |  | whenitreceives | using the | software |  |
|  | Version |  |  | aspecialrequest | 'version' | administrator |  |
|  | Detection |  |  | for the text | directivein | will configure |  |
|  |  |  |  | 'version.bind' in | the | the DNS |  |
|  |  |  |  | the domain | 'options' | softwaretolog, |  |
|  |  |  |  | 'chaos'. | section in | ataminimum, |  |
|  |  |  |  |  | named.con | success and |  |
|  |  |  |  |  | f. | failureevents |  |
| 8 | HSTS | Low | 11002 | The remote | Configure | HTTPSredirects | 208 |
| missing from |  |  | HTTPSserveris not enforcing | theremote webserver | maybeputting yourvisitorsat | 7 |
|  | HTTPS |  |  | HTTP Strict | to use | risk. This is |  |
|  | server |  |  | Transport | HSTS. | classed as a |  |
|  |  |  |  | Security(HSTS). |  | medium-risk |  |
|  |  |  |  | HSTS is an |  | vulnerability. |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  | optional |  | nawareusercan |  |
| responseheader | navigate by |
| that can be | mistaketothe |
| configured on | unencrypted |
| the server to | version of the |
| instruct the | webapplication |
| browsertoonly | oracceptinvalid |
| communicatevia | certificates.This |
| HTTPS.Thelack | leads to |
| of HSTS allows | sensitive data |
| downgrade | being sent |
| attacks, | unencrypted |
| SSL-stripping | overthewire |
| man-in-the-midd |  |
| le attacks, and |  |
| weakens |  |
| cookie-hijacking |  |
| protections. |  |
| 9 | Web applicatio | low | 10066  9 | Theremoteweb application sets | Each cookie | Since tracking cookies are | 208  7,20 |
|  | nCookies |  |  | various cookies | should be | usedtogather | 83 |
|  | are |  |  | throughout a | carefully | information |  |
|  | expired |  |  | user's | reviewed | about you |  |
|  | unauthenticated | to | without your |  |
|  |  |  |  | and | determine | authorization, |  |
|  |  |  |  | authenticated | if it | theypresenta |  |
|  |  |  |  | session. | contains | real threat to |  |
|  |  |  |  | However,Nessus | sensitive | your online |  |
|  |  |  |  | has detected | dataoris | privacy. |  |
|  |  |  |  | thatoneormore | reliedupon | Tracking cookies |  |
|  |  |  |  | of the cookies | for a | like third-party |  |
|  |  |  |  | havean'Expires' | security | cookies aren't |  |
|  |  |  |  | attributethatis | decision. | usedto enhance |  |
|  |  |  |  | setwithapast |  | yourexperience |  |
|  |  |  |  | date or time, | If needed, | but rather to |  |
|  |  |  |  | meaning that | set an | keep track of |  |
|  |  |  |  | these cookies | expiration | your activity |  |
|  |  |  |  | willberemoved | dateinthe | across certain |  |
|  |  |  |  | bythe browser. | future so | websites. |  |
|  |  |  |  |  | the cookie |  |  |
|  |  |  |  |  | willpersist |  |  |
|  |  |  |  |  | or remove |  |  |
|  |  |  |  |  | theExpires |  |  |
|  |  |  |  |  | cookie |  |  |
|  |  |  |  |  | attribute |  |  |
|  |  |  |  |  | altogether |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  | to convert the cookie to a  session cookie. |  |  |
| 10 | Nessus | Low | 11219 | Thispluginisa | Protect | The largest | 21,2 |
|  | SYN  Scanner |  |  | SYN 'half-open' portscanner.It | yourtarget withanIP | impactstendto be net- work | 2 |
|  |  |  |  | shall be | filter. | latency and |  |
|  |  |  |  | reasonablyquick |  | simultaneous |  |
|  |  |  |  | even against a firewalled target |  | pluginchecks. |  |

**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 bysecuritybreaches.SOCdoesn'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 vigilantandreadytorespond to emerging threats, regardless of the time of day. SOC is a critical component of a robust cybersecuritystrategy.Itempowersorganizationsto 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 facilitatescollaborationamongvariousteams,suchasIT, 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'scybersecurity.Itencompasses 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 asintrusiondetectionsystems (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 securityincidentorafalse positive.

# Incident Investigation and Response:

Ifan 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.

Removingthemaliciouselementsanderadicatingthethreattorestore the affected systems to a secure state.

# Recovery and Remediation:

Afterthethreatiseradicated,theSOCteamfocusesonrestoring affected systems and services to normal operation.

Implementing remediation measures to address the root cause ofthe 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 workflowtostayaheadof 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)](https://www.ibm.com/topics/artificial-intelligence) to automate many of the manualprocessesassociatedwiththreatdetectionand[incidentresponse](https://www.ibm.com/topics/incident-response).

BenefitsRegardless 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 [securityorchestration, automation and response (SOAR)](https://www.ibm.com/topics/security-orchestration-automation-response) 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 ofITenvironmentsthatitprovides, SIEM can be an essential driver ofimprovinginterdepartmentalefficiencies. 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](https://www.ibm.com/topics/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 threatintelligencefeedsandAItechnology,SIEMsolutionscanhelpsecurity teams respond more effectively to a wide range of cyberattacks including:

[Insider threats](https://www.ibm.com/topics/insider-threats) - security vulnerabilities or attacks that originatefrom individuals with authorized access to company networks and digital assets.

[Phishing](https://www.ibm.com/topics/phishing) - messages that appeartobesentbyatrustedsender,often used to steal user data, login credentials, financial information, or other sensitive business information.

[Ransomware](https://www.ibm.com/topics/ransomware) - [malware](https://www.ibm.com/topics/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](https://www.ibm.com/topics/ddos) - attacks that bombard networks and systems with unmanageable levels of traffic from adistributed network of hijacked devices (botnet), degrading performance of websites and servers until they are unusable.

[Data exfiltration](https://www.ibm.com/topics/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](https://www.ibm.com/topics/computer-forensics) 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 andchallenging task formanyorganizations.SIEMsolutionsdramaticallyreduce 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)](https://www.ibm.com/products/maas360/byod) policies, organizations need the level of visibility necessary to mitigate network risks from outside the traditional networkperimeter.SIEMsolutionstrackallnetworkactivityacrossallusers, devices, and applications, significantly improving transparency across the entire infrastructure anddetectingthreatsregardlessofwheredigitalassets 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 decouplingofSIEMplatforms—whichhasalreadystartedwith SOARcomingfromSIEM 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.

1. As decoupling continues to occur, security companies will create strongpartnershipstoprovideanelegantintegrationand 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.
2. The cost and complexity of aSIEMwillcontinuetobereduced(per the availability of cloud services), enabling smaller and newer security teamstogetuptospeedevenquicker.WithlegacySIEMs,itcouldtake

teams more than six months to get started, which means dataonboarding, 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 continuetoreducestartuptime,whichiscriticalforabusiness'sbottomline and a security team's efficiency.

1. More startups will continue to be funded to address the multifaceted challenges of upholding strong security. Venture funding is at an [all-time high](https://news.crunchbase.com/news/global-vc-funding-h1-2021-monthly-recap/), 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 InformationandEventManagement(SIEM) system involves several interconnected stages that ensure the effective implementation, operation, and maintenance of the SIEM solution. TheSIEM 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.

Conductathoroughassessmentoftheexistingsecurityinfrastructure, data sources, and log managementpracticestoidentifygapsandnecessary 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 eventsfrom 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.

EventCorrelationandAnalysis:

Developandfine-tunecorrelationrulesandusecasestoidentify 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 feedstoenhancetheSIEM'sabilitytodetect emerging threats and known attack vectors.

Incident Detection and Response:

Respond to generated alerts by investigating potential security incidents.

Performdetailedanalysistodeterminethescopeandimpactof identified security events.

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

ForensicsandInvestigation:

Conductin-depthforensicsanalysistounderstand the root cause of incidents and the methods used by attackers.

Preserve and document evidence for potential legal or regulatory purposes.

ReportingandCompliance:

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 correlationrules,threatintelligencefeeds,andother components to keep the SIEM effective against evolving threats.

Conduct periodic reviews and assessments oftheSIEM'sperformance and effectiveness to identify areas for improvement.

TrainingandKnowledgeTransfer:

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.

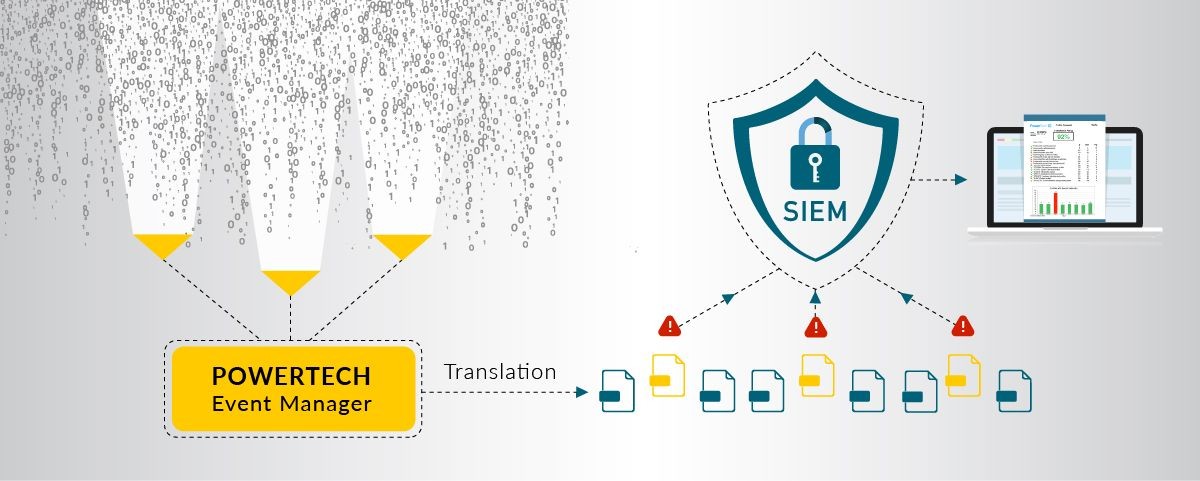
The SIEM lifecycle is a continuous and iterative process, with each phase building upon the insights and experiences gained from previous stages. This approach ensures that the SIEM solution remains relevant, efficient, and effective in helping organizations detect and respond to security threats.

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](https://www.coresecurity.com/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.

ThreatDetection



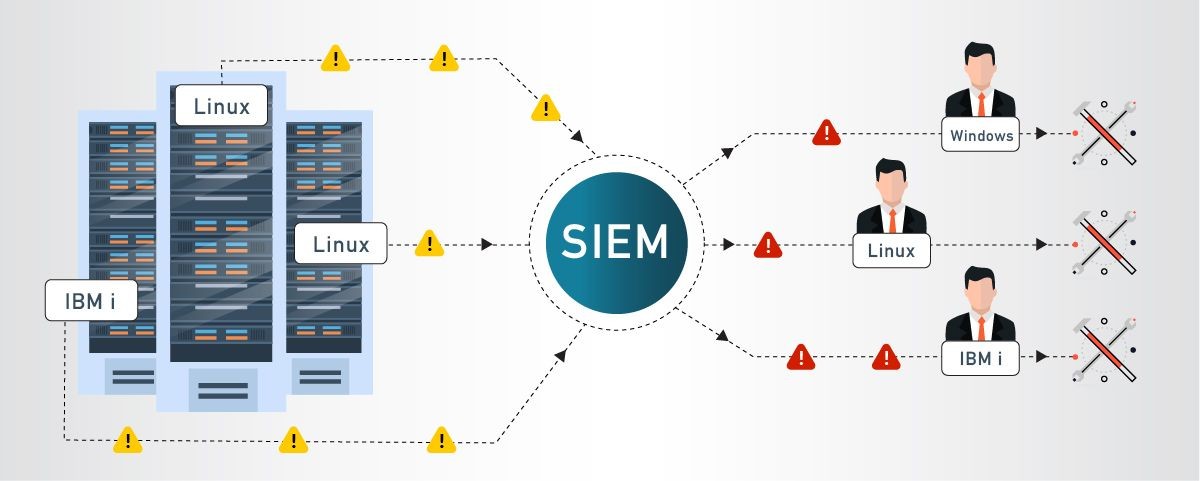
Translation



Prioritization



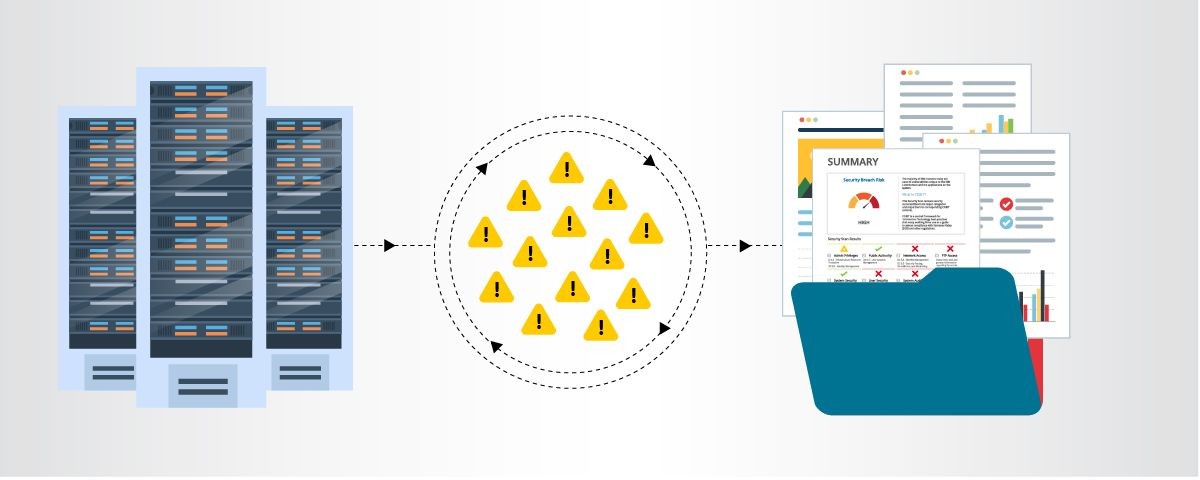
Escalation



Analysis



Compliance



# MISP

MISP, Malware Information Sharing Platform andThreatSharing,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 isusedtodayinmultipleorganisations.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 advancedcorrelationslike Fuzzy hashing correlation(e.g.ssdeep)orCIDRblockmatching.Correlation can be also enabled or event disabled per attribute.

A flexible data model where complex [objects](https://www.misp-project.org/objects.html) can be expressed and [linked together](https://www.misp-project.org/objects.html#_relationships) 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 functionalitytocreateandviewrelationshipsbetweenobjectsand

attributes. Advanced filtering functionalities and [warning list](https://github.com/MISP/misp-warninglists) 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](https://www.misp-project.org/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 easetheintegrationofunstructuredreports into MISP.

A gentle systemtocollaborateoneventsandattributesallowingMISPusers 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](https://www.misp-project.org/feeds/) and any threatintel or OSINT feed from third parties. Many [default feeds](https://www.misp-project.org/feeds/) areincluded in standard MISP installation.

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

FlexibleAPItointegrateMISPwithyourownsolutions.MISPisbundledwith [PyMISP](https://github.com/MISP/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[existingtaxonomies](https://github.com/MISP/misp-taxonomies).Thetaxonomycanbelocalto your MISP but also shareable among MISP instances. MISP comes with a default set of well-known [taxonomies and classification schemes](https://www.misp-project.org/taxonomies.html) to support standard classification as used by ENISA, Europol, DHS, CSIRTs or many other organizations.

Intelligence vocabulariescalledMISPgalaxyandbundledwithexisting [threat actors, malware, RAT, ransomware or MITRE ATT&CK](https://www.misp-project.org/galaxy.html) which can be easily linked with events in MISP.

E[xpansion modules](https://misp.github.io/misp-modules/) in Python to expand MISP with your own services or activate already available [misp-modules](https://github.com/MISP/misp-modules).

sighting support to get observations from organizations concerning sharedindicatorsandattributes.Sighting[canbecontributed](https://www.circl.lu/doc/misp/automation/index.html#sightings-api)viaMISP

user-interface, API as MISP document or STIXsightingdocuments.Starting with MISP 2.4.66, [Sighting has been extended](https://www.misp-project.org/2017/02/16/Sighting-The-Next-Level.html) 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](https://github.com/MISP/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 bythe 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, batchimport,sandboxresultimportorusingthepreconfiguredor customtemplates. If you run MISP internally, data can also be uploaded and downloaded automagically from and to externally hosted MISP instances. Thankstothisautomationandtheeffortofothersyouarenowin possession of valuable indicators of compromise with no additional work.

Collaborativesharingofanalysisandcorrelation

Howoftenhasyourteamanalyzedtorealizeattheendthata colleaguehadalreadyworkedonanother,similar,threat?Orthatan

externalreporthasalreadybeenmade?WhennewdataisaddedMISPwill immediately show relations with other observables and indicators. This results in more efficient analysis, but also allows you to have a better

pictureoftheTTPs,relatedcampaignsandattribution.



# Your college network information

TagoreEngineeringCollege

Atotal of 5labs and approximately200 systems are available.

# How you think you deploy soc in your college

DeployingaSecurityOperationsCenter(SOC)inanorganizationinvolves carefulplanning,resourceallocation,andastructuredapproach.Hereare the key steps to deploy a SOC:

AssessmentandRequirements Gathering:

* + Conductathoroughassessmentoftheorganization'scurrent cybersecurity posture, including existing security measures, tools, and processes.
  + Identifythespecificsecuritychallenges,risks,andcompliance requirements that a SOC will address.
  + DefinethegoalsandobjectivesoftheSOCdeploymenttoalign with the organization's overall security strategy.

BudgetandResource Allocation:

* + Determinethebudgetandresourcerequirementsfor establishing and maintaining the SOC.
  + Allocatepersonnel,hardware,software,andothernecessary resources to support the SOC operations.

Build a Skilled Team:

* + RecruitorassignskilledsecurityprofessionalstoformtheSOC team.
  + Theteamshouldincludesecurityanalysts,incidentresponders, threat hunters, and SOC management personnel.

InfrastructureandTechnologySetup:

* + EstablishthephysicalorvirtualinfrastructurefortheSOC, including servers, network equipment, and storage.
  + Deploy the required security technologies, such as SIEM, intrusiondetectionandpreventionsystems(IDS/IPS),firewalls, endpoint protection, and threat intelligence feeds.

IntegrationandDataCollection:

* + IntegratesecuritytoolsandsystemswiththeSIEMtocentralize log and event data collection.
  + Ensurethatcriticaldatasources,suchasfirewalls,servers, network devices, and applications, are sending logs to the SIEM.

Establish Processes and Procedures:

* + Definestandardoperatingprocedures(SOPs)forvariousSOC activities, including incident handling, response protocols,

escalation procedures, and communication guidelines.

* + Implementincidentcategorizationandprioritization mechanisms.

Implement Monitoring and Alerting:

* + ConfiguretheSIEMtogeneratereal-timealertsbasedon predefined correlation rules and security use cases.
  + Fine-tunealertingthresholdstominimizefalsepositivesand focus on critical alerts.

IncidentResponseand Escalation:

* + Developaformalincidentresponseplanthatoutlinesthesteps to be taken in the event of a security incident.
  + Definerolesandresponsibilitiesforincidenthandling,and establish a clear escalation path for severe incidents.

TrainingandSkillDevelopment:

* + ProvidecomprehensivetrainingtotheSOCteamontheuseof security tools, incident analysis, threat hunting, and incident response best practices.
  + Keeptheteamupdatedonthelatestcybersecuritytrends, attack techniques, and relevant certifications.

TestingandContinuousImprovement:

* Conductregulartabletopexercisesandsimulatedcyberattack scenarios to test the SOC team's response capabilities.
* UsetheinsightsgainedfromtestingtoimproveandrefinetheSOC's processes and procedures.

Monitoring and Reporting:

* ContinuouslymonitortheSOC'sperformanceandeffectivenessin detecting and responding to security incidents.
* GenerateregularreportsandmetricstomeasuretheSOC's performance and communicate its value to stakeholders.

IntegrationwithITandBusinessFunctions:

* FostercollaborationbetweentheSOCandotherITandbusinessunits to ensure a coordinated approach to security.
* Engagewithexecutivemanagementandboardmemberstogain support and buy-in for SOC initiatives
* Deploying a SOC isanongoingprocessthatrequiresadaptabilityand continuous improvement. Regular assessments, training, andupdates 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 tomakefaster,moreinformed,data-backedsecurity decisions and change their behavior from reactive to proactive in the fight against [threat actors](https://www.crowdstrike.com/cybersecurity-101/threat-actor/).



Threat intelligence is important for the following reasons:

* shedslightontheunknown,enablingsecurityteamstomakebetter decisions
* empowerscybersecuritystakeholdersbyrevealingadversarial motives and their tactics, techniques, and procedures (TTPs)
* helpssecurityprofessionalsbetterunderstandthethreatactor’s decision-making process
* empowers business stakeholders, such as executive boards, CISOs, CIOsandCTOs;toinvestwisely,mitigaterisk,becomemoreefficient and make faster decisions

Fromtoptobottom,threatintelligenceoffersuniqueadvantagestoevery member of a security team, including:

* Sec/IT Analyst
* SOC
* CSIRT
* Intel Analyst
* ExecutiveManagement

# 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 orbreach (the “incident”). Ultimately, thegoalistoeffectivelymanagetheincidentso 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](https://digitalguardian.com/blog/7-tips-building-effective-incident-response-plan) in place. This plan should define what constitutes an incidentforthecompany and provide a clear, guided process to be followedwhenanincidentoccurs. Additionally, it’s advisable to specify the teams, employees, or leaders responsible for both managing the overall incident response initiative and thosetasked with takingeach action specified inthe incident response plan.

# Who Handles Incident Responses?

Typically, incident response is conducted by an organization’s [computerincident response team (CIRT)](http://www.sans.org/reading-room/whitepapers/incident/computer-incident-response-team-641), 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](http://www.gartner.com/it-glossary/cirt-cyber-incident-response-team), 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. Preparationhelpsorganizationsdetermine howwelltheirCIRTwillbeabletorespondtoanincidentandshouldinvolve policy,responseplan/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 firewallstodetectanddetermineincidentsandtheir scope.

**Containment** - Once an incident is detected or identified, containingitisa top priority. The main purpose ofcontainmentistocontainthedamageand prevent further damage from occurring (as noted in step number two, the earlier incidentsaredetected,thesoonertheycanbecontainedtominimize damage). It’simportanttonotethatallofSANS’recommendedstepswithin the containment phase should be taken, especially to “prevent the destruction of any evidence that may be needed later for prosecution.” Thesestepsincludeshort-termcontainment,systemback-up,and long-term containment.

**Eradication** - Eradication is the phase of effective incident response that entails removing the threat andrestoringaffectedsystemstotheirprevious state, ideally while minimizing data loss. Ensuring that the proper steps have been taken to this point, including measuresthatnotonlyremovethe malicious content but also ensure that the affected systems are completely clean, are the main actions associated with eradication.

**Recovery -** Testing, monitoring, and validating systemswhileputtingthem 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 phasealsoincludesdecisionmakingintermsofthetimeand datetorestoreoperations,testingandverifyingthecompromised systems,

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

**Lessons Learned** - Lessons learned is a criticalphaseofincidentresponse 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 informationthatmayhavebeenmissedduring the incident, plus complete documentation to provideinformationforfuture 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 cansave yourcompanysubstantialtimeandmoneybyenablingyoutoregaincontrol 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](https://www.digitalguardian.com/blog/5-key-criteria-creating-incident-response-plan-practical-your-organization) 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 andrecover from cyber attacks](https://www.digitalguardian.com/blog/do%E2%80%99s-and-don%E2%80%99ts-incident-response).

Followingarethe[fivestepsor pillarsoftheincidentresponse process](https://www.digitalguardian.com/blog/five-steps-incident-response).

**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 awarenesstraining.

**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 incidentisdetected,adefinedresponseshould 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 toproceedandwho 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 sizeandcomplexity.Thefollowingdiagramshowsthelayersthatmakeup

the QRadar architecture.

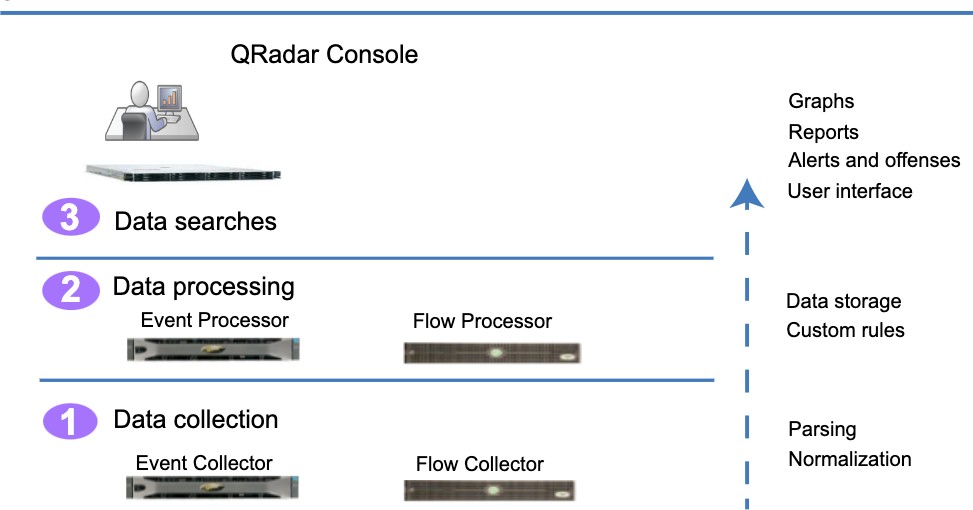


Figure1.QRadararchitecture

The QRadar architecture functions the same way regardless of the size or number of components in a deployment. Thefollowingthreelayersthatare 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 fromyournetwork.TheAll-in-Oneappliancecanbeusedtocollect the data directly from your network or you can use collectors such as QRadar Event Collectors or QRadar QFlow Collectors tocollecteventorflow 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 thatyoumightwanttologinyour device logs.

Flow data is network activity information or session information between two hosts on a network,whichQRadartranslatesintoflowrecords.QRadar translates or normalizes raw dataintoIPaddresses,ports,byteandpacket counts, andotherinformationintoflowrecords,whicheffectivelyrepresents a session between two hosts. In addition to collecting flowinformationwith 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), whichgeneratesoffensesand 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 applianceisexceeded,thenyoumight 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 Forensicscollectdifferenttypesofdata 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 networkscenariosthroughalteringconfigurations and implementing rules in your network.

Use QRadar Vulnerability Manager to scan your network and process the vulnerabilitydataormanagethevulnerabilitydatathatiscollectedfrom

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 useitforsearches,reports, alerts, and investigations.

# [QRadar components](https://www.ibm.com/docs/en/SS42VS_7.4/com.ibm.qradar.doc/c_qradar_comps2_deployment_guide.html)

Use IBMQRadarcomponentstoscaleaQRadardeployment,andtomanage data collection and processing in distributed networks.

# [QRadar maximum EPS certification methodology](https://www.ibm.com/docs/en/SS42VS_7.4/com.ibm.qradar.doc/c_qradar_max_EPS_cert_meth.html)

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](https://www.ibm.com/docs/en/SS42VS_7.4/com.ibm.qradar.doc/c_qradar_deploy_event_and_flow_pipeline.html)

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 impacttheapplication'sperformanceanduserexperience. The specific outcomes of web application testing include:

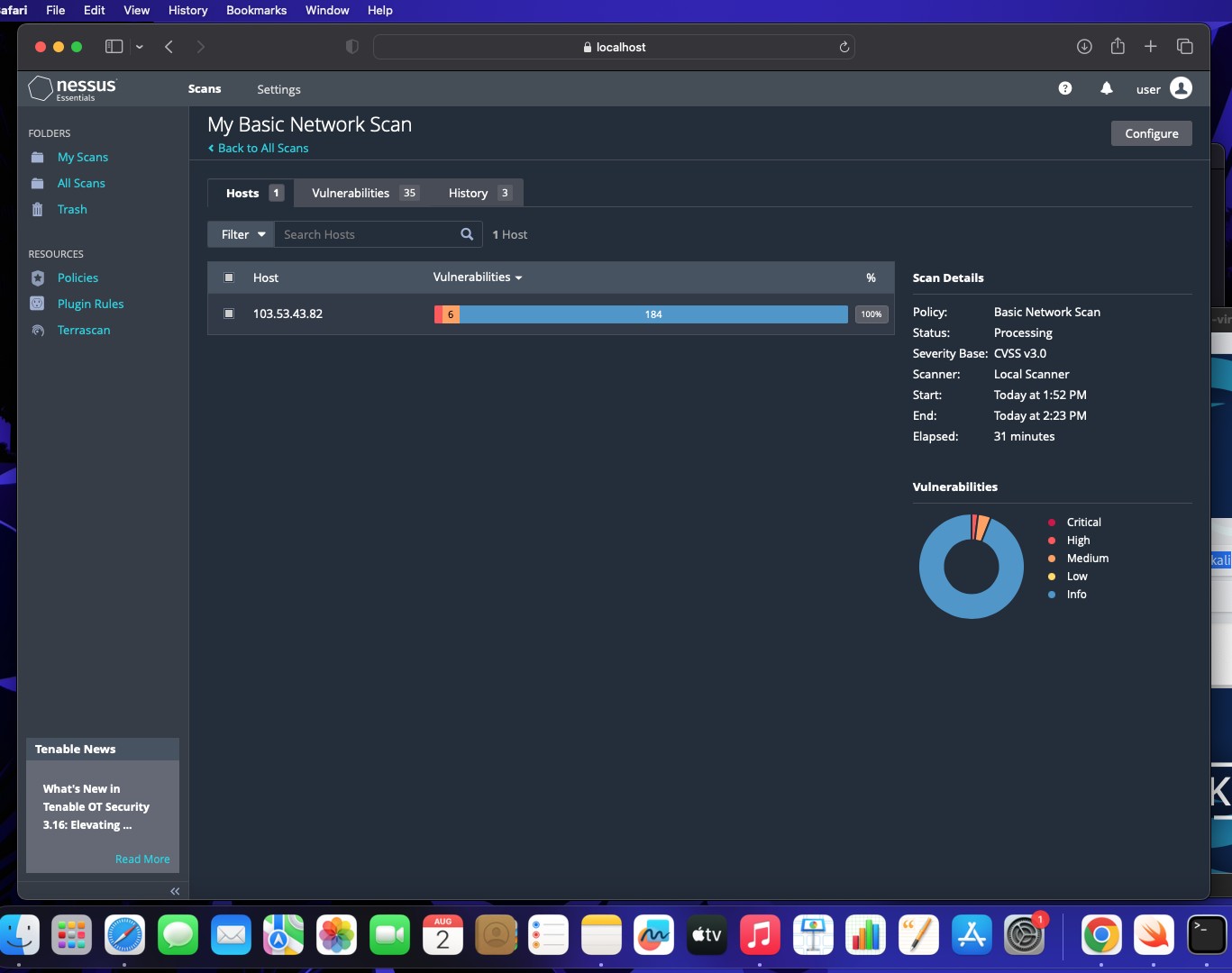
* IdentificationofSecurity Vulnerabilities
* Bug Detection and Resolution
* ValidationofFunctionalRequirements
* Usabilityand UserExperience Evaluation
* PerformanceandLoadTestingResults
* CompatibilityTestingInsights
* Accessibility Compliance
* SecurityCompliance andRisk Mitigation
* Optimization Recommendations
* EnhancedQualityAssurance
* Increased Customer Confidence
* CompliancewithRegulatory 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.



# 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:

* 1. **Improved Threat Detection**: SOC analysts monitornetworktraffic,log data, and security alerts to identify potential threats and security incidents promptly.
  2. **Faster Incident Response**: With a SOC in place, organizations can respond quickly to security incidentsandmitigatetheimpactofbreachesor attacks.
  3. **Enhanced Security Posture:** A proactive SOC helps organizations implement robust security measures and continually improve their overall security posture.
  4. **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:

1. **Centralized Log Management:** SIEM aggregates log datafromdiverse sources, making it easier for analysts to access and analyze information from a single dashboard.
2. **EarlyThreatDetection:**SIEMtoolscanidentifypatternsandanomalies in the data, enabling early detection of security incidents and potential breaches.
3. **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.
4. **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, offeringavisualrepresentationofsecurity-relateddataand insights. The expected outcomes of using QRadar and its dashboardinclude:

1. **Real-TimeVisibility:**TheQRadardashboardprovidesreal-timevisibility into security events and incidents,enablinganalyststorespondpromptlyto emerging threats.
2. **CustomizableVisualizations:**Analystscancustomizethedashboardto displayrelevantinformation,suchastopthreats,networktraffic,orsecurity incidents.
3. **ThreatIntelligenceIntegration:**QRadarintegrateswithvariousthreat intelligence feeds, enhancing its ability to detect and respond to advanced threats.
4. **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, changinguserexpectations,andtheneedtoensuresecurity 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 thesechangesandcontinuouslyupgrade 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 responsetothechangingcybersecuritylandscapeandtechnological

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 :-

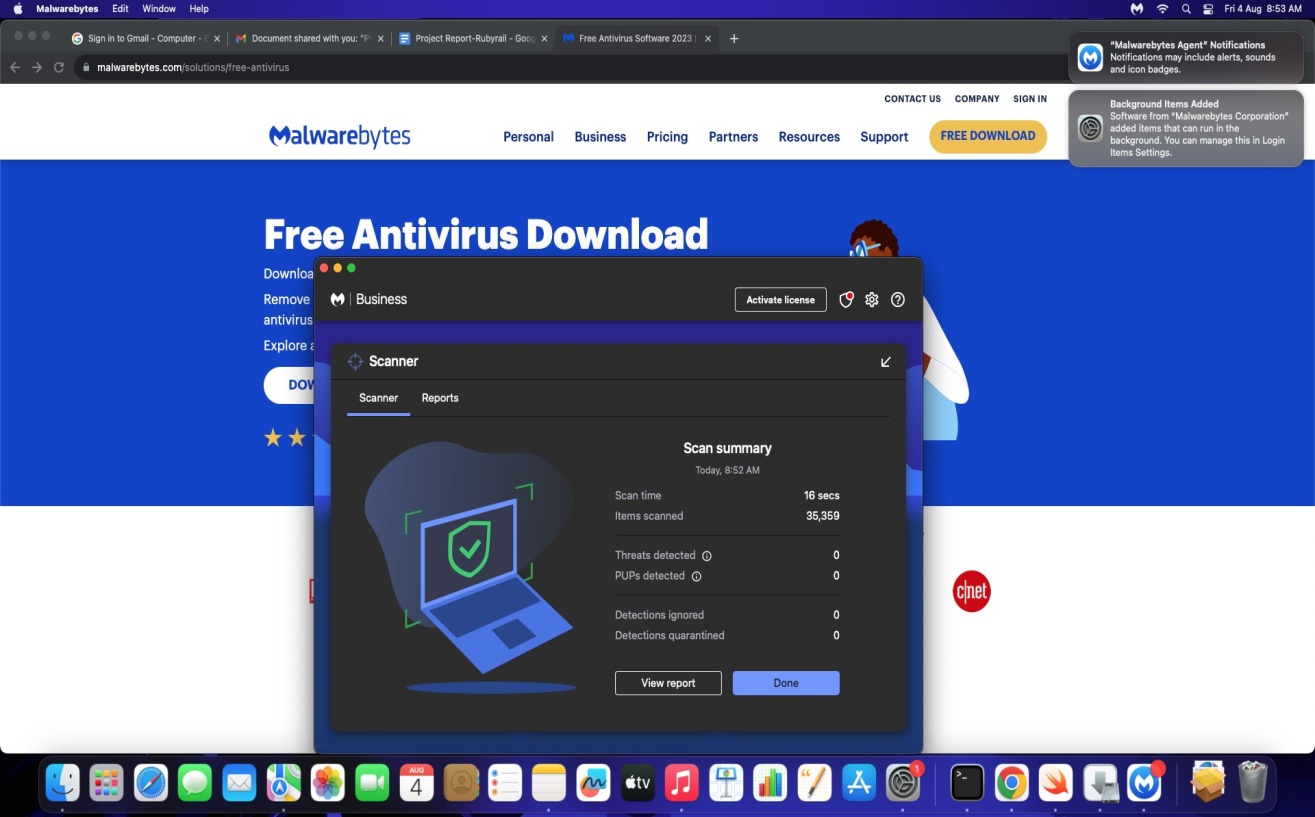
Nessus, cybermap.kaspersky.com, thehackersone.com, chaptgpt, wepik.com (AI image editor), Gamma (AI based PPT), OWASP top 10 vulnerabilities(2021), thehackersnews.com, CWE, exploitDB, virtual box, live websites-bugcrowd, nslookup.io, OSINT framework, mitre framework, IBM fix central, QRadar Installation,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

**MALWAREBYTES**

**FREE DOWNLOADS**

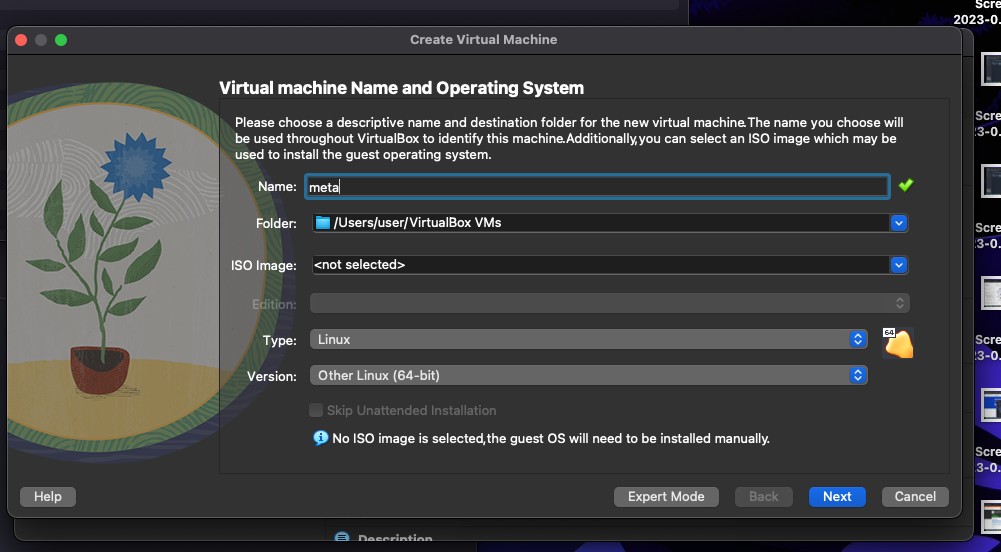
**Free Antivirus Software 2023**

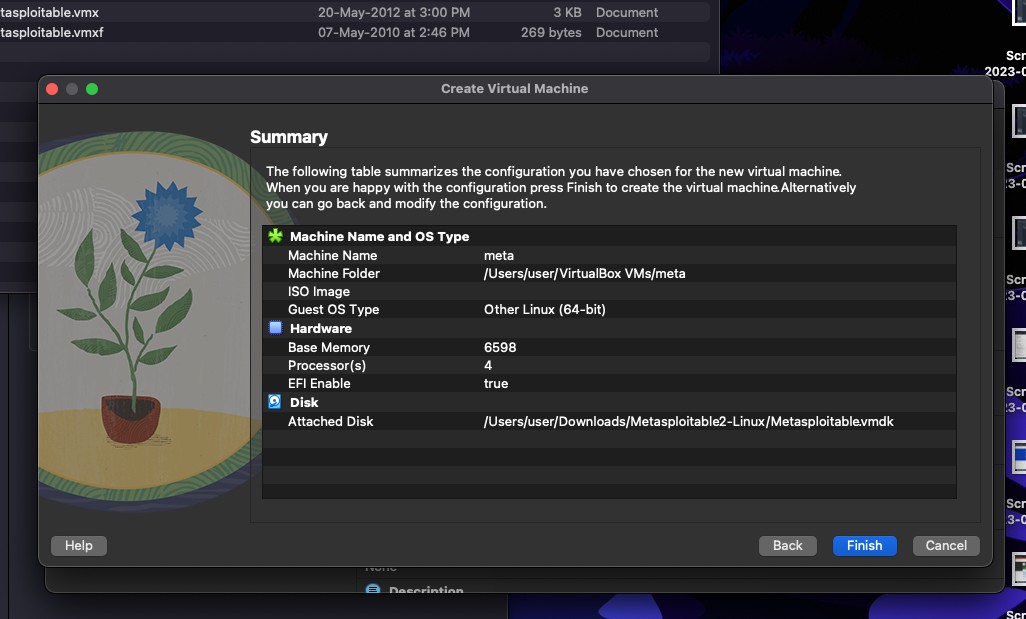
Looking for free antivirus and malware removal? Scan and remove viruses andmalwarefor free. Malwarebytes free antivirus includes multiple layers of malware-crushing tech. Our anti-malware finds and removes threats like viruses, ransomware, spyware, adware, and Trojans.



# Metasploitable2(Linux)isaframeworkwhichiscombinationNmapandexploit database.

Metasploitable is an intentionally vulnerable Linux virtual machine. This VM can be usedtoconductsecuritytraining,testsecuritytools,andpracticecommonpenetration testing techniques.





* 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**

=[metasploitv6.3.4-dev ]

+----=[2294exploits-1201auxiliary-409post ]

+----=[968payloads-45encoders-11 nops ]

+----=[9 evasion ]

Metasploit tip: View a module's description using info,ortheenhancedversioninyourbrowserwith info -d

MetasploitDocumentation:https://docs.metasploit.com/

**msf6>searchexploit**

MatchingModules

================

# Name DisclosureDateRank

CheckDescription

-

0 auxiliary/dos/http/cable\_haunt\_websocket\_dos 2020-01-07

normal No "Cablehaunt"CableModemWebSocketDoS

|  |  |  |  |
| --- | --- | --- | --- |
| 1 | exploit/linux/local/cve\_2021\_3493\_overlayfs | 2021-04-12 | |
| great | Yes 2021UbuntuOverlayfsLPE |  | |
| 2 | exploit/windows/ftp/32bitftp\_list\_reply | 2010-10-12 | good |
| No | 32bitFTPClientStackBufferOverflow |  |  |

|  |  |
| --- | --- |
| 3 exploit/windows/tftp/threectftpsvc\_long\_mode | 2006-11-27 |
| great No 3CTftpSvcTFTPLongModeBufferOverflow |  |
| 4 exploit/windows/ftp/3cdaemon\_ftp\_user | 2005-01-04 |

TestingMetaspoiltusingKalilinux

**> 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**