

TEAM -I

Vulnerability Security

Part I-Executive summary

Overview

Actualizing cyber security in an organization includes a comprehensive and proactive approach to ensure its computerized resources, information, and framework from cyber dangers. The steps to actualize cyber security viably at each organization incorporate:

- Develop a clear and well-defined cyber security arrangement and methodology that adjust with the organization's commerce goals and hazard resilience.
- Conduct a exhaustive hazard appraisal to distinguish potential cybersecurity dangers and vulnerabilities specific to the organization. Prioritize dangers based on their potential affect and probability of event. Execute chance moderation measures and make a chance administration arrange to address identified vulnerabilities.
- Prepare all representatives on cyber security best hones and the part they play in defending the organization's data. Teach them around phishing, social designing, watchword cleanliness, and other common assault vectors to advance a security-conscious culture.
- Implement solid get to control measures to guarantee that as it were authorized staff can get to delicate information and basic frameworks. Utilize multi-factor verification (MFA) for an additional layer of security.
- Convey firewalls,interruption detection/prevention frameworks (ids/ips),and secure doors to screen and control arrange traffic .
- Install antivirus computer program, endpoint security apparatuses, and host-based

firewalls on all gadgets to guard against malware and other dangers at the gadget level.

- Introduce antivirus program, endpoint security instruments, and host-based firewalls on all gadgets to protect against malware and other dangers at the gadget level.
- Scramble touchy information both at rest and in travel to avoid unauthorized get to and guarantee information confidentiality.
- Establish a orderly handle to apply security patches and overhauls instantly to all computer program, working frameworks, and firmware to address known vulnerabilities.
- Develop a well-defined occurrence reaction arrange (IRP) to handle cybersecurity occurrences successfully. The arrange ought to incorporate clear rules on distinguishing, announcing, containing, killing, and recuperating from security episodes.
- Conduct customary inner and outside security reviews and appraisals to assess the organization's security pose and distinguish potential shortcomings or crevices.
- Monitoring and Logging: Actualize centralized logging and real-time checking of organize and framework exercises to distinguish and react to suspicious exercises instantly.
- Establish clear channels for announcing security occurrences and communicating with partners, counting representatives, clients, accomplices, and administrative specialists.

IP address of <https://www.mha.gov.in/en> 184.25.56.133

2. Team Members Involved in vulnerability Assessment

S.No	Name	Designation	Mobile Number
1	Dr.Ritika Malik	Assistant Professor	9650757675 ritika.malik@bharativedyapeeth.edu

2	Mr.Nripesh Kumar Nrip	Assistant Professor	9405278721 nripesh.nrip@bharativedyapeeth.edu
3	Dr. Megha Sehgal	Assistant Professor	9654236872 megha.sehgal@bharativedyapeeth.edu

3. List of Vulnerable Parameter, location discovered

S.No	Name of the Vulnerability	Reference CWE
1	Broken Access Control	CWE 285- Improper Authorization
2	Cryptographic Failures	CWE-916: Use of Password Hash 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 Forgery	CWE-918:Server Side Request Forgery

1. CWE: CWE 285- Improper Authorization

OWASP CATEGORY: A01 2021 Broken Access Control

DESCRIPTION: The product does not perform or incorrectly performs an authorization check when an actor attempts to access a resource or perform an action.

BUSINESS IMPACT: Accepting a client with a given character, authorization is the method of deciding whether that client can get to a given asset, based on the user's benefits and any authorizations or other access-control determinations that apply to the asset. When get to control checks are not connected reliably - or not at all - clients are able to get to information or perform activities that they ought to not be allowed to perform. This will lead to a wide extend of issues, counting data exposures, dissent of benefit, and self-assertive code execution.

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

OWASP CATEGORY: A02 2021 Cryptographic Failures

DESCRIPTION: The product generates a hash for a password, but it uses a scheme that does not provide a sufficient level of computational effort that would make password cracking attacks infeasible or expensive.

BUSINESS IMPACT: In this plan, verification includes tolerating an approaching watchword, computing its hash, and comparing it to the put away hash. After an assailant has obtained put away watchword hashes, they are continuously able to brute drive hashes offline. As a shield, it is as it was conceivable to moderate down offline assaults by selecting hash calculations that are as asset seriously as conceivable.

3. CWE: CWE 564: SQL Injection: 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: Programmers utilize SQL infusion assaults to get to delicate trade or actually identifiable data (PII), which eventually increments delicate information introduction. Utilizing SQL infusion, aggressors can recover and modify information, which dangers uncovering delicate company information put away on the SQL server. Compromise Users' Protection: Depending on the information put away on the SQL server, an assault can uncover private client information, such as credit card numbers.

4. CWE: CWE 653: Improper Isolation or Compartmentalization

OWASP CATEGORY: A04 2021 Insecure Design

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

BUSINESS IMPACT: Uncertain framework arrangement dangers stem from blemishes within the security settings, setup and solidifying of the distinctive frameworks over the pipeline (e.g. SCM, CI, Artifact store), frequently coming about in “low hanging fruits” for aggressors looking to expand their toehold within the environment.

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

OWASP CATEGORY: A05 2021 Security Misconfiguration

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

BUSINESS IMPACT: Security misconfigurations permit assailants to pick up unauthorized get to systems, frameworks and information, which in turn can cause noteworthy money related and reputational harm to your organization.

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

OWASP CATEGORY: A06 2021 Vulnerable and Outdated Components

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

BUSINESS IMPACT: A complete working framework may be from a third-party provider in a few equipment items. Whether open or closed source, these components may contain freely known vulnerabilities that might be abused by foes to compromise the item with more known vulnerabilities. Dependency-Check could be a Computer program Composition Investigation (SCA) device that endeavors to identify freely uncovered vulnerabilities contained inside a project's conditions. It does this by deciding in the event that there's a Common Stage Identification (CPE) identifier for a given reliance.

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: Confirmation components regularly depend on a memorized mystery (moreover known as a watchword) to supply an attestation of character for a client of a framework. It is subsequently critical that this secret word be of adequate complexity and illogical for a foe to figure. The particular necessities around how complex a secret word ought to be depends on the sort of framework being secured. Selecting the right watchword prerequisites and upholding them through execution are basic to the in general victory of the confirmation component.

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

OWASP CATEGORY: A08 2021 Software and Data Integrity Failures

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

BUSINESS IMPACT: This issue can be essential to numerous sorts of shortcomings in web applications. A engineer may perform appropriate approval against URL parameters whereas expecting that assailants cannot adjust treats. As a result, the program might skip fundamental input approval to empower cross-site scripting, SQL infusion, cost altering, and other assaults.

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

OWASP CATEGORY: A09 2021 Security Logging and Monitoring Failures

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

BUSINESS IMPACT: Data composed to log records can be of a touchy nature and grant profitable direction to an aggressor or uncover delicate client data.

10. CWE: CWE-918 Server Side Request Forgery

OWASP CATEGORY: A10 2021 - Server Side Request Forgery

DESCRIPTION: The web server receives a URL or similar request from an upstream component and retrieves the contents of this URL, but it does not sufficiently ensure that the request is being sent to the expected destination.

BUSINESS IMPACT: A fruitful SSRF assault can frequently result in unauthorized activities or get to information inside the organization, either within the helpless application itself or on other back-end frameworks that the application can communicate with.

Stage: 2 Reports

NESSUS Vulnerability

ReportOverview

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Target website: www.gdgoenka.com

Target IP address: - 3.108.65.60

List of vulnerability

S.no	Vulnerability name	Severity	Plugins	Port	Description	Solution	Business Impact
------	--------------------	----------	---------	------	-------------	----------	-----------------

1.	Service Detection	info	22964	443 / tcp / www	Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.	Apply regular vulnerability scans and patches to address service detection vulnerabilities.	Service Detection vulnerabilities can expose systems to unauthorized access, data breaches, and service disruptions.
2	Nessus SYN scanner	info	11219	443 / tcp / www	This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.	Protect your target with an IP filter.	Nessus SYN scanner enhances security by identifying network vulnerabilities, reducing cyber risks.
3	TRACK Methods Allowed	Mixed	11213	443 / tcp / www	The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server	Disable these HTTP methods. Refer to the plugin output for more information.	TRACK Methods Allowed can enable web server information leakage, risking sensitive data exposure.

					connections.		
4	PHP Version Detection	Info	48243	443 / tcp / www	Nessus was able to determine the version of PHP available on the remote web server.	Upgrade PHP to the latest secure version and disable version disclosure.	helps secure web applications, preventing vulnerabilities and data breaches.
5	HTTP Server Type and Version	Info	10107	80 / tcp / www	This plugin attempts to determine the type and the version of the remote web server.	Disable version disclosure and apply regular security patches.	Exposing HTTP server type/version can aid attackers, increasing security risks.
6	Apache Banner Linux Distribution Disclosure	Info	18261	NA	Nessus was able to extract the banner of the Apache web server and determine which Linux distribution the remote host is running.	If you do not wish to display this information, edit 'httpd.conf' and set the directive 'ServerTokens Prod' and restart Apache.	provide attackers with information useful for targeted attacks or exploitation.

7	HTTP Methods Allowed	Info	43111	80 / tcp / www	By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.	can lead to security misconfigurations and potential attacks.	Configure server to limit HTTP methods, blocking unauthorized or dangerous requests.
8	TRACE Methods Allowed	Mixed	11213	443 / tcp / www	The remote web server supports the TRACE and/or TRACE methods. TRACE and TRACE are HTTP methods that are used to debug web server connections.	Disable these HTTP methods. Refer to the plugin output for more information.	Can expose sensitive information, enabling potential security breaches.
9	TCP/IP Timestamps Supported	Info	25220	NA	The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can	Disable TCP/IP Timestamps or use firewall rules to block related attacks.	can be exploited to launch timestamp- based attacks, compromising security.

					sometimes be computed.		
10	TLS Versions Supported	Info	56984	NA	This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.	Upgrade TLS to the latest secure version and disable vulnerable protocols.	can expose sensitive data, risking security breaches and compliance violations.

Stage 3 Report

Achieving Proactive Cyber security with SOC and SIEM Integration

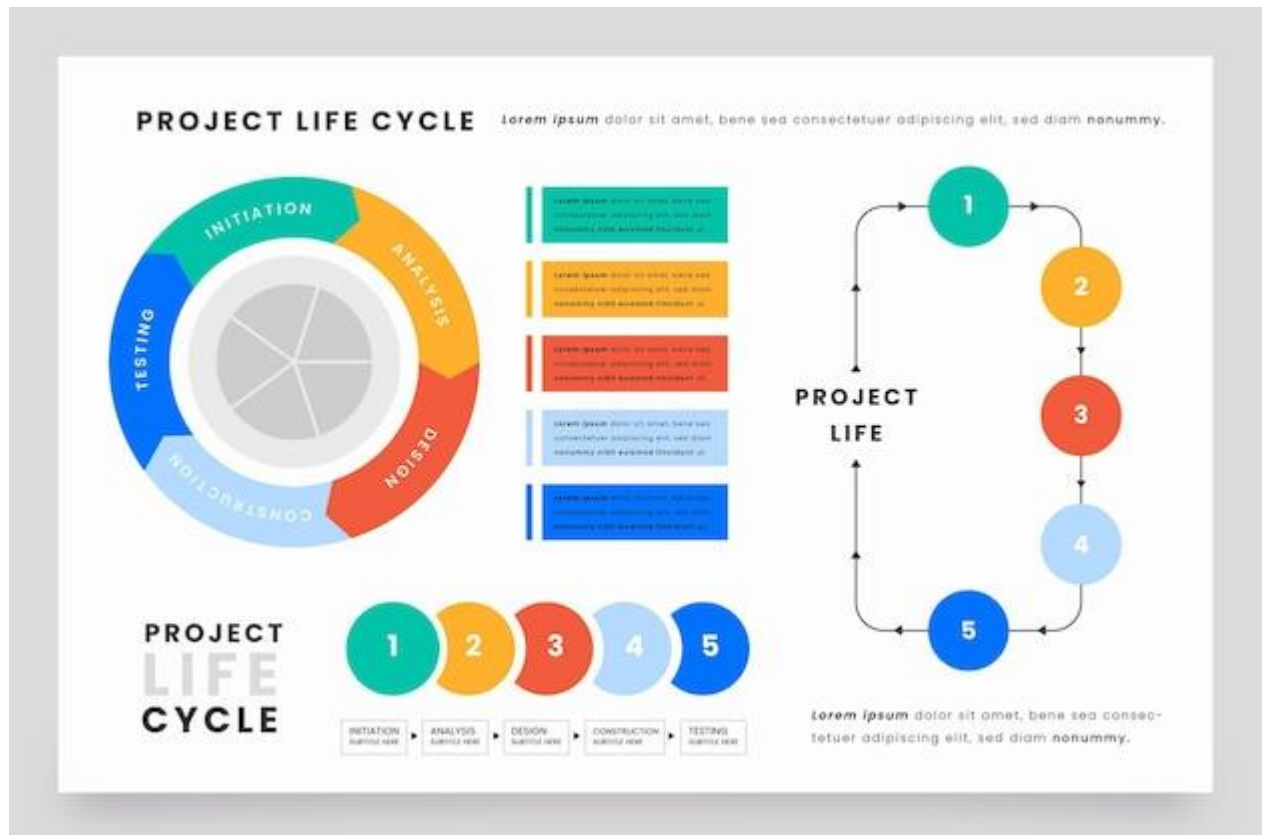
- SOC

SOC is essential for ongoing network, system, and application monitoring within a company. Potential security problems, such as malware infections, data breaches, and unauthorized access attempts, can be detected and handled by this system. Time is crucial when a security event arises. SOC teams are prepared to react quickly and efficiently to security breaches in order to limit and minimize harm. SOC doesn't just respond to occurrences; it also proactively finds infrastructure gaps and vulnerabilities. Companies may improve their security posture and put precautionary measures in place in the future thanks to this proactive strategy. Security analysts are continuously alert and prepared to respond to new threats at all times because to SOC's round-the-clock monitoring.

- SOC - cycle

The SOC cycle, often referred to as the SOC lifespan or SOC workflow, is an ongoing

process that specifies the essential processes required in maintaining a company's cyber security. From threat identification to incident response and recovery, it includes all of these processes. The following steps commonly make up the SOC cycle:



Threat Detection and Monitoring:

Network, systems, and application activity are continuously monitored for any security threats and irregularities. Utilizing a variety of security tools, such as firewalls, SIEM (Security Information and Event Management) solutions, intrusion detection systems (IDS), and threat intelligence feeds.

Alert Triage and Analysis:

Evaluating and ranking security alarms sent by monitoring tools in accordance with their seriousness and possible significance. Figuring out if an alert represents a true security issue or a false positive.

Incident Investigation and Response:

If an alert is determined to be a real security incident, the SOC team launches a careful investigation to determine the type and scope of the assault.

Assembling information, reviewing log data, and carrying out digital forensics to identify the cause and effects of the occurrence. Starting the incident response procedure, this can include isolating affected systems, containing the threat, and averting future harm.

Incident

Containment

and

Eradication:

Taking urgent steps to stop the incident's propagation throughout the organization's network and to control it. To return the afflicted systems to a secure state, the malicious components must be eliminated.

Recovery and Remediation:

After the risk is killed, the SOC group centers on reestablishing influenced frameworks and administrations to typical operation.

Actualizing remediation measures to address the root cause of the occurrence and anticipate comparative assaults within the future.

Post-Incident Analysis and Lessons Learned:

Conducting a intensive autopsy investigation of the occurrence to get it how it happened, what was the affect, and what steps were taken to reply.

Identifying areas of change within the organization's security pose and occurrence reaction methods.

Upgrading security arrangements and strategies based on the lessons learned from the occurrence.

Threat Intelligence and Proactive Measures:

Joining risk insights into the SOC workflow to remain ahead of rising dangers and known assault designs.

Proactively chasing for signs of potential dangers and vulnerabilities some time recently they lead to full-fledged security occurrences.

Continuous Monitoring and Improvement:

The SOC cycle may be a persistent prepare, with progressing observing, examination, and enhancement of security measures to adjust to the advancing risk scene.

By taking after this cycle, the SOC group can viably identify, react to, and recuperate from security episodes, minimizing the effect of cyber dangers on the organization's resources and information.

- **SIEM**

SIEM Security data and occasion management, or SIEM, could be a security arrangement that makes a difference organizations recognize and address potential security dangers and vulnerabilities some time recently they have a chance to disturb trade operations.

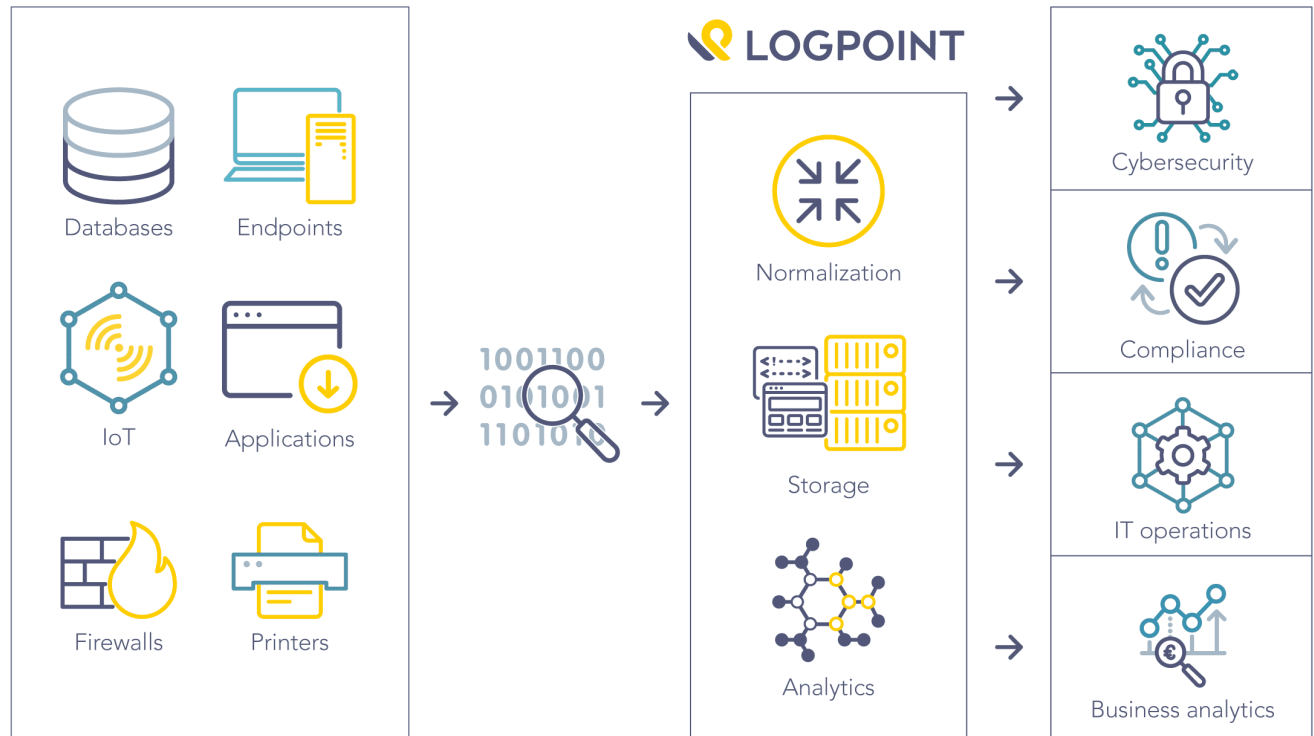
What is SIEM?

SIEM (often pronounced "sim") stands for security information and event management, a type of cybersecurity solution that collects and converges data from different parts of your IT environment for the intent of security monitoring.



Blumira

SIEM at a glance



SIEM frameworks offer assistance venture security groups identify client behavior peculiarities and utilize manufactured insights (AI) to mechanize numerous of the manual forms related with danger discovery and occurrence reaction.

Benefits Notwithstanding of how expansive or little an organization may be, taking proactive steps to screen for and moderate IT security dangers is fundamental. SIEM arrangements advantage undertakings in a assortment of ways and have ended up a critical component in streamlining security workflows.

Real-time threat recognition

SIEM arrangements empower centralized compliance reviewing and detailing over a complete commerce framework. Progressed mechanization streamlines the collection and examination of framework logs and security occasions to decrease inner asset utilization whereas assembly strict compliance announcing benchmarks.

AI-driven automation

Today's next-gen SIEM courses of action facilitated with viable security coordination, mechanization and response (Take off) systems, saving time and resources for IT bunches as they manage exchange security. Utilizing significant machine learning that actually learns from organize behavior, these courses of action can handle complex hazard recognizable verification and event response traditions in basically less time than physical bunches.

Improved organizational efficiency

Since of the made strides deceivability of IT situations that it gives, SIEM can be an basic driver of progressing relationship efficiencies. A central dashboard gives a bound together see of framework information, alarms and notices, empowering groups to communicate and collaborate proficiently when reacting to dangers and security episodes.

Detecting advanced and unknown threats

Considering how rapidly the cyber security scene changes, organizations ought to be able to depend on arrangements that can distinguish and react to both known and obscure security dangers. Utilizing coordinates danger insights bolsters and AI innovation, SIEM arrangements can offer assistance security groups react more viably to a wide extend of cyberattacks counting:

Insider dangers - security vulnerabilities or assaults that begin from people with authorized get to to company systems and advanced resources.

Phishing - messages that show up to be sent by a trusted sender, regularly utilized to take client information, login accreditations, monetary data, or other touchy trade data.

Ransom ware - Malware that locks a victim's information or gadget and debilitates to keep it locked—or worse—unless the casualty pays a emancipate to the assailant.

Disseminated dissent of benefit (DDoS) assaults - assaults that assault systems and frameworks with unmanageable levels of activity from a dispersed arrange of captured gadgets (botnet), debasing execution of websites and servers until they are unusable.

Information exfiltration – robbery of information from a computer or other gadget, conducted physically, or naturally utilizing malware.

Conducting forensic investigations

SIEM arrangements are perfect for conducting computer scientific examinations once a security occurrence happens. SIEM arrangements permit organizations to effectively collect and analyze log information from all of their advanced resources in one put. This gives them the capacity to reproduce past episodes or analyze modern ones to examine suspicious movement and execute more viable security forms.

Surveying and detailing on compliance

Compliance inspecting and announcing is both a fundamental and challenging errand for numerous organizations. SIEM arrangements drastically decrease the asset uses required to oversee this prepare by giving real-time reviews and on-demand announcing of administrative compliance at whatever point required.

Monitoring Users and Applications

With the rise in notoriety of farther workforces, SaaS applications and BYOD (bring your possess gadget) approaches, organizations require the level of deceivability vital to relieve organize dangers from exterior the conventional arrange edge. SIEM arrangements track all organize action over all clients, gadgets, and applications, essentially progressing straightforwardness over the complete foundation and recognizing dangers notwithstanding of where computerized resources and administrations are being gotten to.

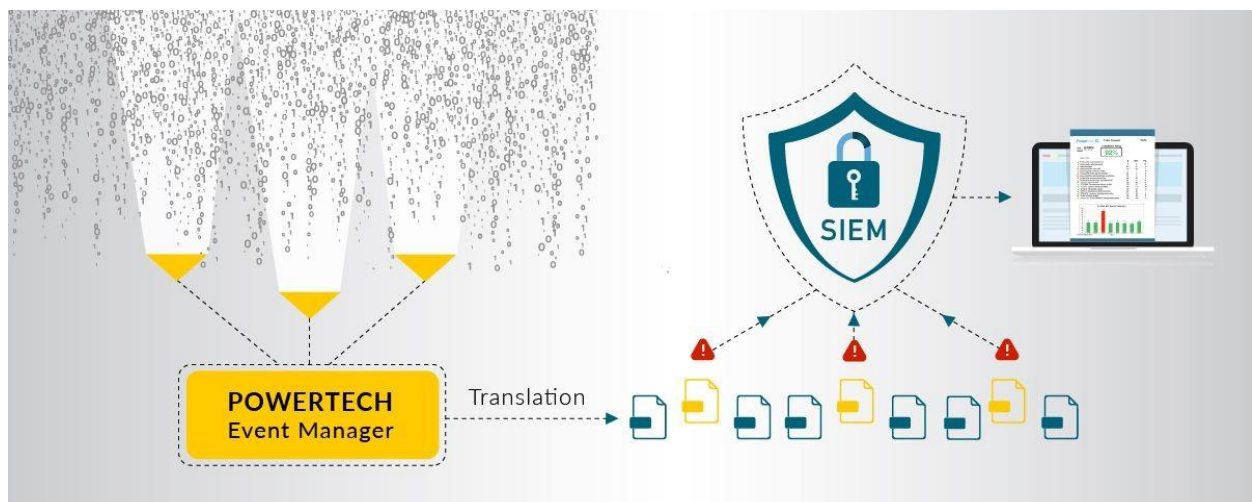


TOP 5 FEATURES TO LOOK FOR IN SIEM SOLUTIONS





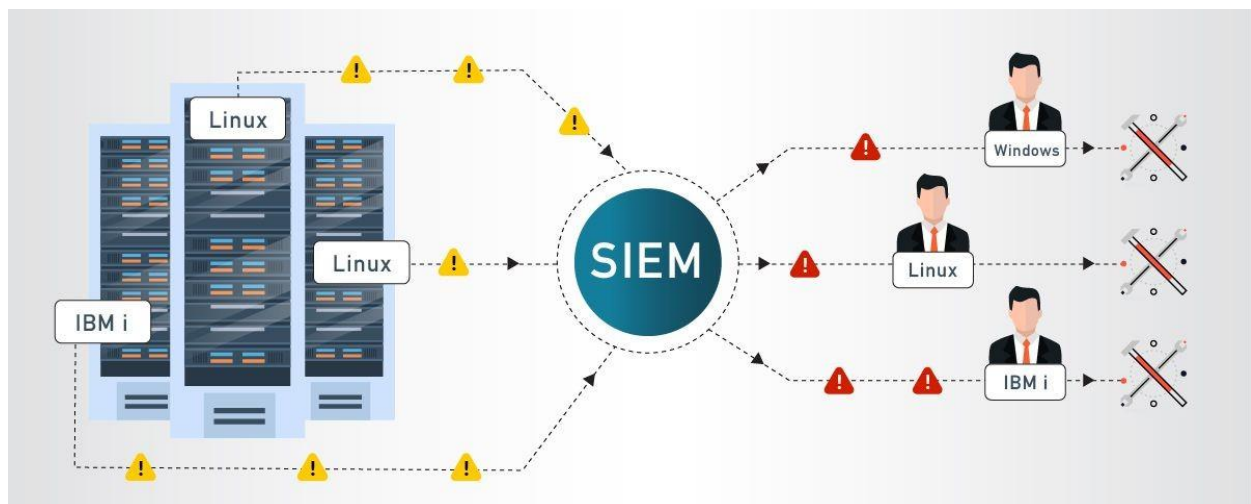
Translation



Prioritization



Escalation



Analysis



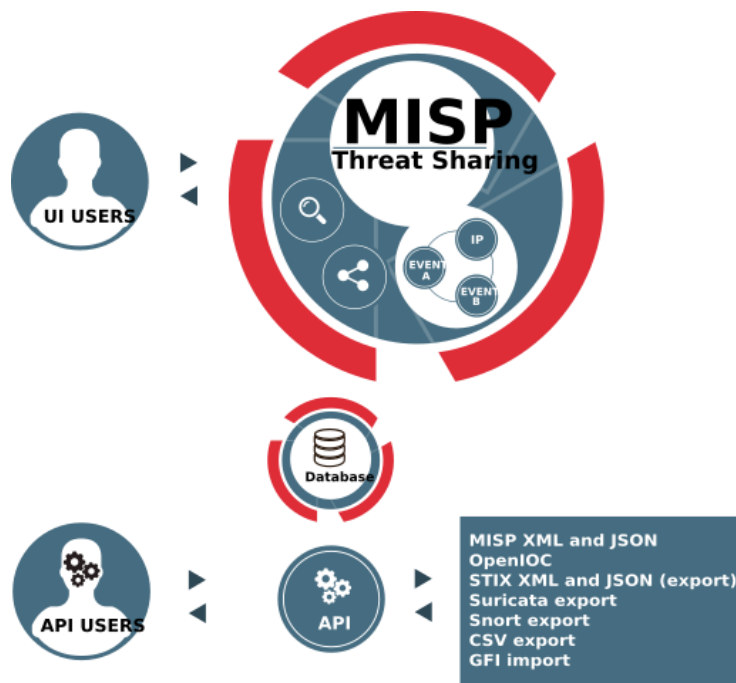
Compliance



- **MISP**

MISP, Malware Data Sharing Stage and Risk Sharing, center functionalities are:

An productive IOC and pointers database, permitting to store specialized and non-technical data approximately malware tests, occurrences, assailants and insights.



- **Your college network information**

Bharati Vidyapeeth Deemed to be University, Institute of Management and Research, New Delhi

A total of 3 labs and approximately 400 approx. systems are available.

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

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

Assessment and Requirements Gathering:

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

Budget and Resource Allocation:

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

Build a Skilled Team:

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

Infrastructure and Technology Setup:

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

Integration and Data Collection:

- Integrate security tools and systems with the SIEM to centralize log and event

data collection.

- Ensure that critical data sources, such as firewalls, servers, network devices, and applications, are sending logs to the SIEM.

Establish Processes and Procedures:

- Define standard operating procedures (SOPs) for various SOC activities, including incident handling, response protocols, escalation procedures, and communication guidelines.
- Implement incident categorization and prioritization mechanisms.

Implement Monitoring and Alerting:

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

Incident Response and Escalation:

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

Training and Skill Development:

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

Testing and Continuous Improvement:

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

Monitoring and Reporting:

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

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

Integration with IT and Business Functions:

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

• **Threat intelligence**

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



Threat intelligence is important for the following reasons:

- sheds light on the obscure, empowering security groups to form superior choices
- empowers cyber security partners by uncovering ill-disposed thought processes and their strategies, procedures, and methods (TTPs)
- helps security experts superior get it the risk actor's decision-making handle
- empowers trade partners, such as official sheets, CISOs, CIOs and CTOs; to contribute admirably, moderate hazard, gotten to be more productive and make speedier choices
- From top to bottom, threat intelligence offers unique advantages to every member of a security team, including:

- Sec/IT Investigator
- SOC
- CSIRT
- Intel Examiner
- Executive Administration

- **Incident response**

Occurrence reaction may be a term utilized to portray the method by which an organization handles a information breach or cyberattack, counting the way the organization endeavors to oversee the results of the assault or breach (the “incident”). Eventually, the objective is to viably oversee the occurrence so that the harm is constrained and both recuperation time and costs, as well as collateral harm such as brand notoriety, are kept at a least.

Organizations ought to, at least, have a clear occurrence reaction arrange in put. This arrange ought to characterize what constitutes an occurrence for the company and give a clear, guided handle to be taken after when an occurrence happens. Furthermore, it’s prudent to indicate the groups, representatives, or pioneers capable for both overseeing the generally occurrence reaction activity and those entrusted with taking each activity indicated within the occurrence reaction arrange.

Who Handles Incident Responses?

Regularly, occurrence reaction is conducted by an organization’s computer occurrence reaction group (CIRT), moreover known as a cyber-occurrence reaction group. CIRTs more often than not are comprised of security and common IT staff, together with individuals of the lawful, human resources, and public relations divisions. As Gartner depicts, a CIRT may be a gather that “is capable for reacting to security breaches, infections, and other possibly disastrous episodes in ventures that confront critical security dangers. In expansion to specialized pros able of dealing with particular dangers, it ought to incorporate specialists who can direct venture administrators on fitting communication within the wake of such incidents.”

- **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

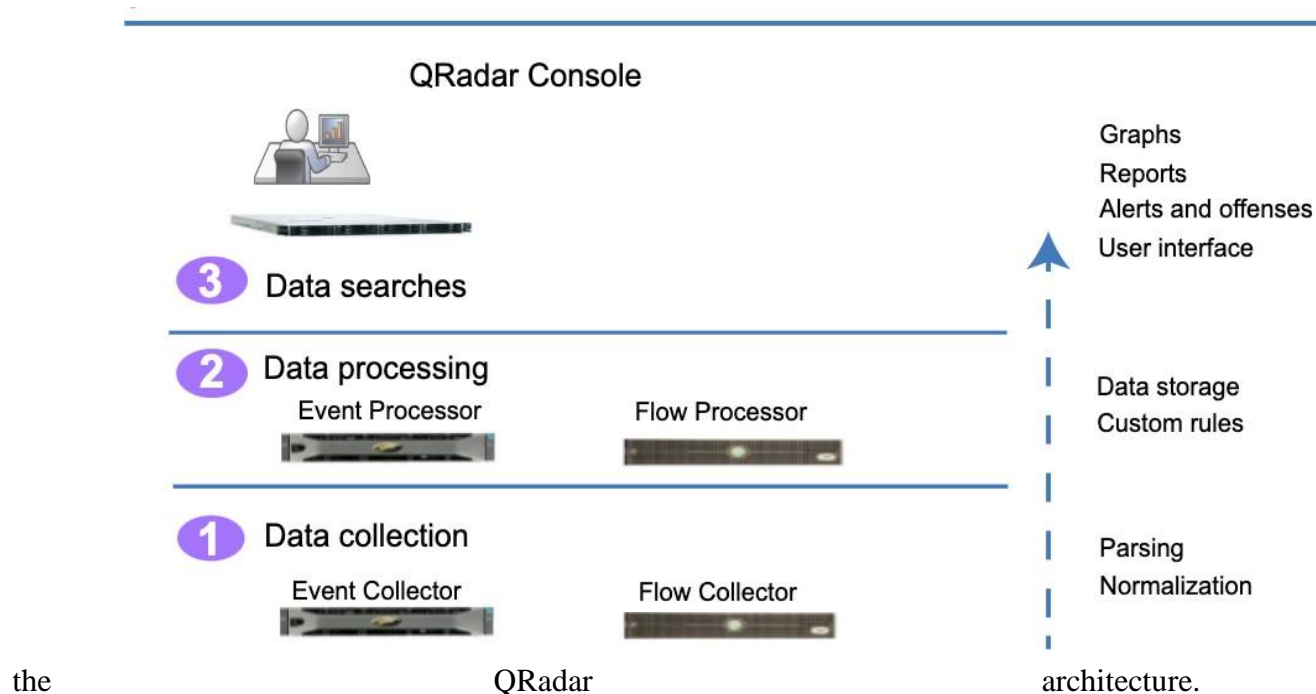


Figure 1. QRadar architecture

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 is passed to the processing layer. When the raw data is parsed, it is normalized to present it in a structured and usable format.

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

Event data represents events that occur at a point in time in the user's environment such as user logins, email, VPN connections, firewall denys, proxy connections, and any other events that you might want to log in your device logs.

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

Data processing

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

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

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

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

Use QRadar Vulnerability Manager to scan your network and process the vulnerability data or manage the vulnerability data that is collected from

other scanners such as Nessus, and Rapid7. The vulnerability data that is collected is used to identify various security risks in your network.

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

Data searches

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

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

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

QRadar components

Use IBM QRadar components to scale a QRadar deployment, and to managedata 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.

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

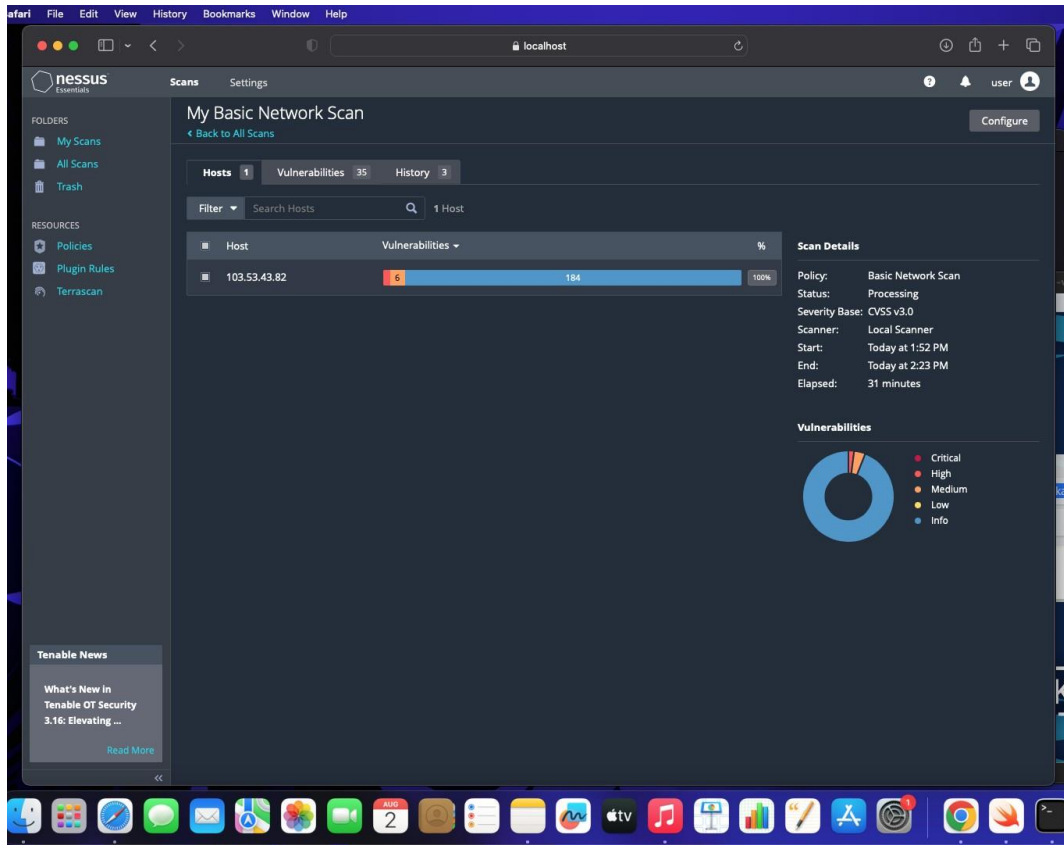
In summary, the outcome of web application testing is an enhanced, secure, and reliable web application that meets user expectations and delivers a smooth and seamless experience to its users. It provides developers and stakeholders with the confidence that the application is ready for deployment and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



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 / SIEM

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

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

Topics explored :-

Introduction to cybersecurity, Growth of cyber security, 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:-

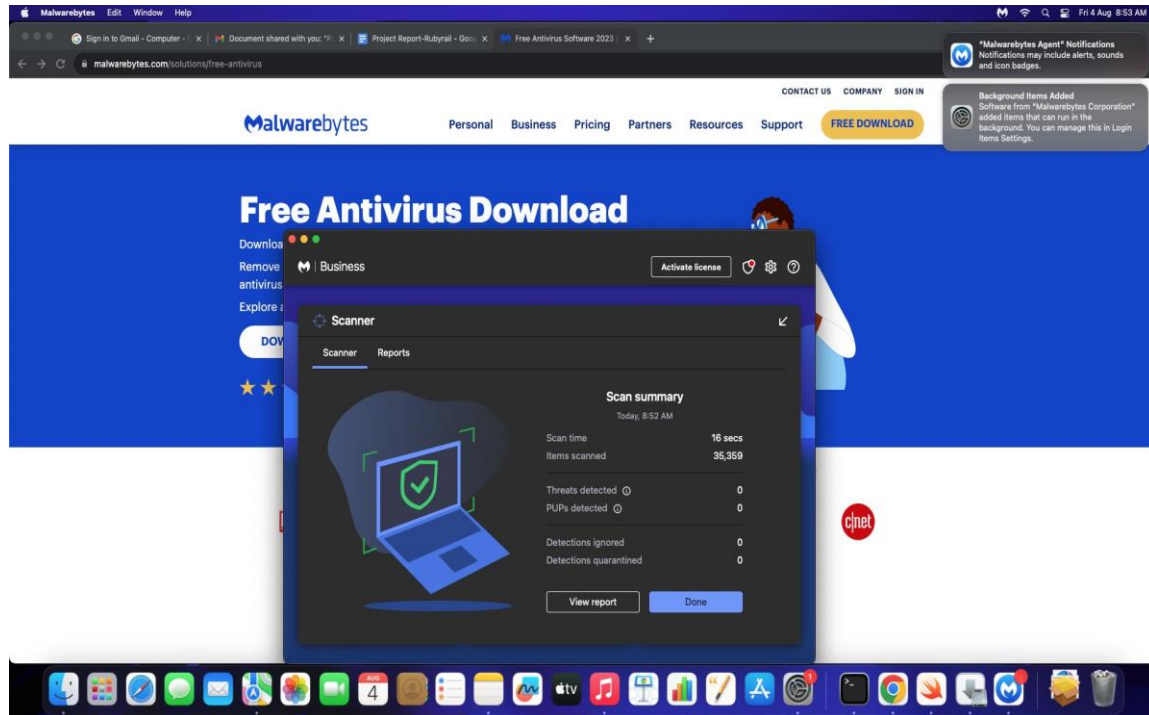
Nessus, cybermap.kaspersky.com, thehackersone.com, chaptgpt,wepik.com (AI image editor), Gamma (AI based PPT), OWASP top 10 vulnerabilities(2021), thehackersnews.com, CWE, exploitDB, virtual box, live websites-bugcrowd, nslookup.io, OSINT framework, mitre framework, IBM fix central, QRadar Installation,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

MALWAREBYTES

FREE DOWNLOADS

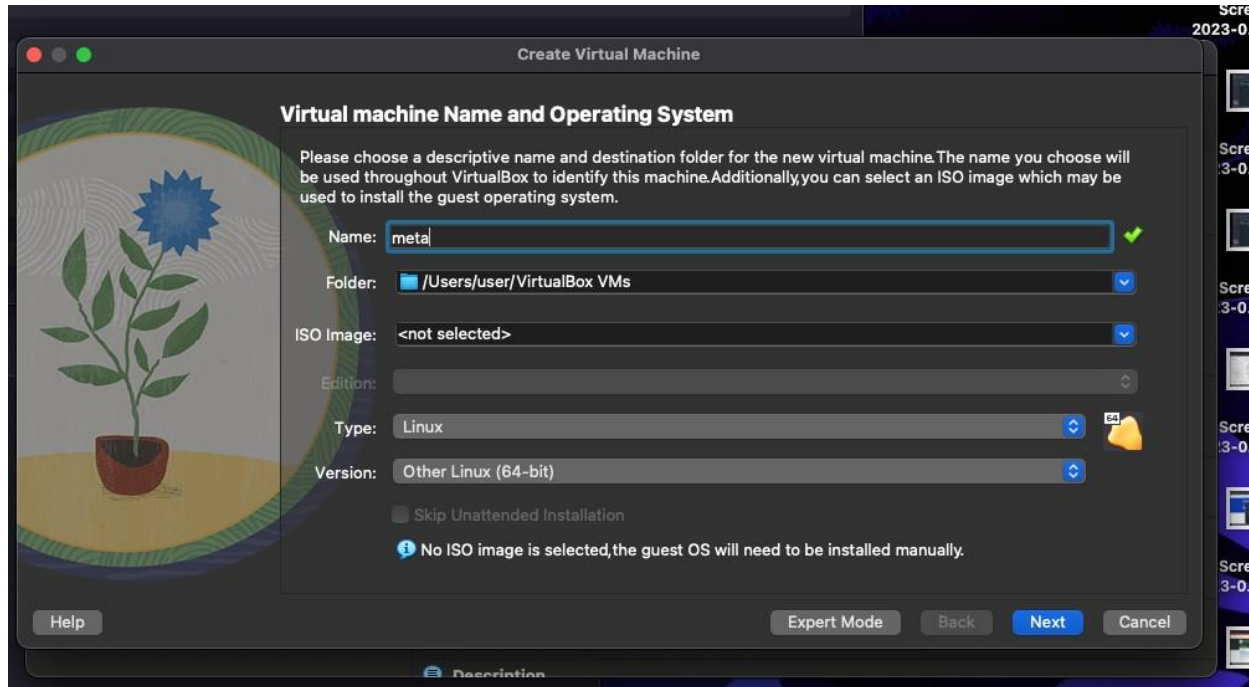
Free Antivirus Software 2023

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



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.



- 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-> metasploitable 2 vmdk

Metasploit

—(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/threctftpsvc_long_mode		2006-11-27

great No 3CTftpSvc TFTP Long Mode Buffer Overflow

4 exploit/windows/ftp/3cdaemon_ftp_user

2005-01-04

Testing Metasploit using Kali Linux

> 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