TEAM -III

A Threat_Intelligence_Club

Part I-Executive summary

Overview

Effective cybersecurity implementation in an organization requires a methodical strategy that addresses numerous security facets. By taking the following actions, businesses may strengthen their cybersecurity posture and better safeguard their assets and sensitive data against the always changing threat landscape. The steps to successfully integrate cybersecurity at every organization are as follows:

- Introduction: Describe the importance of cybersecurity in contemporary organizations, focusing on the requirement to defend delicate data and systems against online assaults.
- Risk Assessment: To find potential threats and vulnerabilities unique to the organisation, conduct a thorough risk assessment. The basis for efficient cybersecurity measures is laid up in this stage.
- Cybersecurity Policy Development: Clearly state the organization's commitment to security in a document outlining its clear and thorough cybersecurity policy. Standards and laws specific to the industry should be followed by this policy.
- Employee Training and Awareness: All staff members should receive regular cybersecurity training to learn about security best practices. Encourage a culture of security awareness among staff, and make sure they are aware of reporting procedures.
- Access Control and Authentication: Apply strict access controls by abiding by the least privilege principle. For essential systems, use multi-factor authentication (MFA) to increase security.

- Network Security: Install firewalls, id/p systems, and keep network hardware and software up to date. Limit the attack surface by segmenting the network to segregate sensitive data and vital systems.

- Data Protection and Encryption: To prevent unauthorised access, encrypt sensitive data both in transit and at rest. Establish data backup and recovery protocols and implement data loss prevention (DLP) technologies.

- Incident Response Planning: Make a thorough incident response plan (IRP) that specifies what should be done in the case of a security breach. To make sure the IRP is successful, test it frequently with tabletop exercises.

- Vendor and Third-Party Risk Management: To reduce supply chain risks, evaluate the cybersecurity procedures used by suppliers and third-party vendors. Establish contractual requirements for vendors to adhere to cybersecurity standards and carry out routine inspections and monitoring.

- Continuous Monitoring and Auditing: To continuously monitor network activity, install security information and event management (SIEM) systems. To find and fix flaws, conduct frequent security audits and vulnerability assessments.

- Compliance and Regulations: Become knowledgeable about the rules and procedures for compliance that apply to your sector. Make that the company complies with data protection rules, and set up procedures for reporting violations and dealing with them.

- Budget Allocation and Resource Planning: Set aside enough money and resources, including staff, equipment, and training, for cybersecurity activities. Obtain steadfast support from the executive team and other stakeholders.

- Employee Incident Reporting: Encourage your staff to immediately report any suspicious activities or incidents. Establish a safe and private reporting system and give precise instructions on what counts as an occurrence.

IP address of https://aiactr.ac.in/ 202.66.174.169

2. Team Members Involved in Vulnerability Assessment

S.No	Name	Designation	Mobile Number

1	Ms. Neha Sharma	Assistant Professor	9999673426 neha.sharma1@bharatividyapeeth.edu
2.	Ms. Kajal Kaul	Assistant Professor	8826105961 kajal.kaul@bharatividyapeeth.edu
3.	Ms. Nisha Malhotra	Assistant Professor	9899995540 nisha.malhotra@bharatividyapeeth.edu
4.	Mr. Mohit Dayal	Assistant Professor	9999954597 mohit.dayal@bharatividyapeeth.edu

3. List of Vulnerable Parameter, location discovered

S.No	Name of the Vulnerability	Reference CWE
1	Broken Access Control	CWE 285- Improper Authorization
2	Cryptographic Failures	CWE-916: Use of Password Hash 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: Users may access unauthorised data or carry out actions they shouldn't within a web application, according to the OWASP security category known as Broken Access Control. It's when the application improperly enforces who can access what, to put it another way.

BUSINESS IMPACT:

Data Breaches: Poor access control can result in data breaches, which can expose private data and perhaps violate privacy laws (such as GDPR and HIPAA), incurring fines and harming an organization's reputation.

Unauthorised Actions: Users may take steps they aren't supposed to, such changing or deleting important data, which can cause business interruptions and financial losses.

Legal repercussions: Violations of access control restrictions may give rise to legal action as well as financial penalties.

Loss of Trust: Customer relationships and commercial partnerships may suffer if customers and partners lose faith in the company's capacity to protect their data.

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

OWASP CATEGORY : A02 2021 Cryptographic Failures

DESCRIPTION: In the OWASP category, "Cryptographic Failures" describes security flaws where cryptographic methods and algorithms are applied incorrectly within a web application, creating vulnerabilities.In the OWASP category, "Cryptographic Failures" describes security problems caused by weak or erroneous implementation of cryptographic methods and algorithms in a web application abilities.

BUSINESS IMPACT: By accepting an incoming password, computing its hash, and then comparing it to the previously saved hash, authentication is accomplished in this approach. An attacker is always able to brute force hashes offline once they have obtained saved password hashes. The only way a defender can sluggish offline attacks is by using hash algorithms that are as resource-intensive as feasible.

3. CWE: CWE 564: SQL Injection: Hibernate

OWASP CATEGORY: A03 2021 Injection

DESCRIPTION: Malicious code or SQL queries can be injected into a web application's Hibernate queries using a security flaw known as "injection using Hibernate," which could allow for unauthorised access to or manipulation of a database.

BUSINESS IMPACT: In order to acquire critical business or personally identifiable information (PII), hackers use SQL injection attacks, which ultimately exposes more sensitive data. Attackers can retrieve and modify data using SQL injection, putting the sensitive firm data kept on the SQL server at risk of exposure. Privacy of Users Is Vulnerable: Private user information, including credit card details, may be exposed by an attack, depending on the data kept on the SQL server.

4. CWE: CWE 653: Improper Isolation or Compartmentalization

OWASP CATEGORY : A04 2021 Insecure Design

DESCRIPTION: According to the OWASP definition, insecure design refers to security flaws caused by subpar web application design or architecture. It indicates that throughout the creation of the application, security issues were not sufficiently taken into account.

BUSINESS IMPACT: Risks associated with insecure system setup emerge from weaknesses in the security configuration and hardening of the many systems used in the pipeline (such as SCM, CI, and the artefact repository), which frequently presents "shooting fish in a barrel" for intruders attempting to gain a foothold in the environment.

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

OWASP CATEGORY : A05 2021 Security Misconfiguration

DESCRIPTION: In the OWASP classification, security misconfiguration refers to the incorrect installation or configuration of security mechanisms within an online application, server, or cloud service. It frequently takes place when security elements are neglected during deployment or when default settings are not altered.

BUSINESS IMPACT: Attackers can access networks, systems, and data without authorization thanks to security configuration errors, which can seriously harm your company's finances and reputation.

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

OWASP CATEGORY : A06 2021 Vulnerable and Outdated Components

DESCRIPTION: Vulnerable and Outdated Components in the OWASP category refer to security vulnerabilities that arise from the use of outdated or vulnerable software components (such as libraries or frameworks) within a web application.

BUSINESS IMPACT:

Security Breaches: Attackers can exploit known vulnerabilities in these components to compromise the application, leading to data breaches, unauthorized access, and potential legal and financial repercussions.

Operational Disruption: Security incidents resulting from vulnerable components can disrupt operations, causing downtime and financial losses.

Legal Consequences: Non-compliance with data protection laws due to data breaches can result in legal actions, regulatory fines, and damage to the organization's reputation.

Reputation Damage: Customers and stakeholders may lose trust in the organization if they discover that outdated or vulnerable components were used, affecting the organization's reputation.

To mitigate risks associated with vulnerable and outdated components, organizations should establish a process for tracking and updating components, use software composition analysis tools, and regularly apply patches and updates to eliminate known vulnerabilities.

7. CWE: CWE 521-Weak Password Requirements

OWASP CATEGORY : A07 2021 Identification and Authentication Failures

DESCRIPTION In the OWASP category, "Identification and Authentication Failures," security issues are those in which identity and authentication processes are improperly implemented, allowing unauthorized access to systems or data.

BUSINESS IMPACT: In order to give an assertion of identity for a system user, authentication systems frequently depend on a secret that is memorized (also known as a password). It is crucial that this password be sufficiently complicated and difficult for an enemy to guess. The sort of system that needs to be protected determines the precise requirements for how difficult a password needs to be. The effectiveness of the authentication system depends on choosing the right password requirements and putting them into practices

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

OWASP CATEGORY: A08 2021 Software and Data Integrity Failures

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

scripting, and alter inputs in unanticipated ways.

BUSINESS IMPACT: Numerous forms of flaws in online applications may have this issue as their root cause. While presuming that attackers cannot modify cookies, a developer may carry out proper validation against URL parameters. This could allow for cross-site scripting, SQL injection, price tampering, and other attacks by allowing the program to ignore simple input validation.

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

OWASP CATEGORY: A09 2021 Security Logging and Monitoring Failures

DESCRIPTION: Security Logging and Monitoring Failures problems occur when an application lacks adequate logging and monitoring capabilities, making it challenging to identify and address security occurrences.

BUSINESS IMPACT:

Undetected Attacks: Without adequate logging and monitoring, security incidents may go unnoticed, allowing attackers to persist within the system and potentially lead to data breaches or further compromise.

Delayed Incident Response: A lack of real-time monitoring can result in delayed incident response, which may exacerbate the impact of a security breach and increase the associated costs.

Compliance Violations: Insufficient logging and monitoring can lead to non-compliance with industry regulations and data protection laws, resulting in legal consequences and fines.

Reputation Damage: Security incidents that could have been prevented or mitigated with proper logging and monitoring can harm an organization's

reputation, eroding trust among customers and partners.

To mitigate security logging and monitoring failures, organizations should implement robust logging practices, set up real-time monitoring, and establish clear incident response procedures. These measures help detect and respond to security threats more effectively, reducing potential damage.

10. CWE: CWE-918 Server Side Request Forgery

OWASP CATEGORY : A10 2021 - Server Side Request Forgery

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

BUSINESS IMPACT: The web server retrieves the contents of a URL or a request of a similar sort after receiving it from an upstream component, but it does not sufficiently confirm that the request is being sent to the correct person.

Stage : 2 Report

NESSUS Vulnerability Report

Overview

Performing a vulnerability assessment for a college website is crucial to identify and address potential security weaknesses that could be exploited by attackers. Maintaining a strong defence against possible attacks requires regular monitoring and development in the security process. Additionally, it is advisable to ask for help from certified cybersecurity experts if you lack the knowledge to carry out a full inspection. Check sure the website is safe and functions properly on a variety of platforms and browsers. Record each vulnerability that has been found, along with its significance and possible effects. Determine the criticality of the fixes, prioritise them, and assist the college's IT staff or web developers in the corrective action procedure. Record each vulnerability that has been found, along with its significance and possible effects. Determine the criticality of the fixes, prioritise them, and assist the college's IT staff or web developers in the corrective action procedure.

Cybersecurity experts and organisations frequently use Nessus, a well-known vulnerability assessment tool, to find and fix security flaws in their

networks, systems, and applications. Nessus is mostly used for the following purposes:

Vulnerability Scanning: Nessus is mostly used for automatically scanning for vulnerabilities. To find known vulnerabilities and misconfigurations, it examines networks, servers, endpoints, and applications. This aids businesses in prioritising their security efforts and identifying potential avenues of entry for attackers.

Patch Management: The scan findings produced by Nessus reveal information on uninstalled patches and operating system updates. This ensures that urgent security fixes are applied swiftly, helping to maintain an up-to-date and safe IT environment.

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: Web applications can be scanned by Nessus to find flaws like SQL injection, cross-site scripting (XSS), and other problems that could leave them vulnerable to assaults.

Network Inventory and Asset Management: Nessus can offer useful details about the systems and devices connected to the network, helping to keep an accurate inventory and comprehend the attack surface of the network.

Security Awareness and Training: Nessus assists security teams and IT employees in understanding the security posture of their systems by producing thorough vulnerability reports. Programmes for

increasing security awareness and training can benefit from this material.

Risk Assessment: Nessus categorises detected vulnerabilities into severity levels, assisting organisations in prioritising their efforts by concentrating on high-risk vulnerabilities first.

Penetration Testing Support: By giving a preliminary overview of potential vulnerabilities prior to more thorough manual testing, Nessus can support manual penetration testing efforts.

Cloud Infrastructure Security: Cloud infrastructure is now being used by many businesses. Nessus can evaluate cloud environments and find vulnerabilities or misconfigurations that could compromise the security of cloud-based services.

Continuous Monitoring: Utilising continuous monitoring techniques with Nessus enables businesses to review their security posture on a frequent basis and spot changes that could lead to new vulnerabilities.

Threat Intelligence Integration: Nessus may be connected with threat intelligence feeds to compare scan results with acknowledged threats and exploits, giving users a more complete picture of the risks they may be exposed to.

Nessus is a great tool for finding existing vulnerabilities and configuration errors; it should be used as a part of a thorough security plan that also includes continuing security awareness campaigns, threat hunting, and routine manual assessments to address emerging and zero-day threats.

Target WebSite : NSUT East campus (Formerly AIACT&R) website : https://mait.ac.in/ Target IP : 202.66.174.169

S. No.	Vulnerability name	Severity	Plugin	Description	Solution	Business Impact	Port
1	HTTP Methods Allowed (per directory)	Info	48204	The remote host is running the Apache HTTP Server, an open source web server. It was possible to read the version number from the banner.	The solution is not yet available.	A remote attacker could use this flaw to cause httpd to use an excessive amount of memory and CPU time via HTTP requests with a specially-crafted Range header. This could be used in a denial of service attack.	80 / tcp / www
2	HTTP Server Type and Version	Info	49704	Nessus gathered HREF links to external sites by crawling the remote web server.	The solution is not yet available.	HTTPS redirects may be putting your visitors at risk. This is classed as a medium-risk vulnerability.	80 / tcp / www
3	HyperText Transfer Protocol (HTTP) Information	Info	84502	The remote HTTPS server is not enforcing HTTP Strict Transport Security (HSTS). HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protection.	The solution is not yet available.	A flaw was found in the way the Apache HTTP Server handled Range HTTP headers. A remote attacker could use this flaw to cause httpd to use an excessive amount of memory and CPU time via HTTP requests with a specially-crafted Range header. This could be used in	80 / tcp / www

						a denial of service attack.	
4.	HyperText Transfer Protocol (HTTP) Redirect Information	Info	43111	By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.	Analyze the redirect(s) to verify that this is valid operation for your web server and/or applicatio n.	The largest impacts tend to be net- work latency and simultaneous plugin checks	80 / tcp / www
5.	Nessus SYN scanner	Info	10107	The following HTTP methods are considered insecure: PUT, DELETE, CONNECT, TRACE, HEAD Many frameworks and languages treat 'HEAD' as a 'GET' request, albeit one without any body in the response. If a security constraint was set on 'GET' requests such that only 'authenticatedUsers' could access GET requests for a particular servlet or resource, it would be bypassed for the 'HEAD' version. This allowed unauthorized blind submission of any privileged GET request.	Protect your target with an IP filter.	Use fully qualified domain name (FQDN) objects in firewall policy rules to filter incoming or outgoing traffic from or to specific domains.	80 / tcp / www 443/tcp /www

Stage 3 Report

Achieving Proactive Cybersecurity with SOC and SIEM Integration

- **Soc**

Soc
An organization's entire IT infrastructure is monitored round-the-clock by a team of IT security experts known as a security operations centre (SOC), also known as an information security operations centre (ISOC), in order to identify cybersecurity events in real time and respond to them as quickly and effectively as possible.
Additionally, a SOC chooses, manages, and maintains the cybersecurity tools used by the company. It also continuously assesses threat information to identify ways to strengthen the security posture of the company.
An organization's security practises, procedures, and response to security incidents are unified and coordinated by a SOC, which is the main advantage of

running one in-house or outsourcing it. This usually leads to better security policies and preventative measures, quicker threat detection, and quicker, more effective, and more affordable responses to security problems. Additionally, a SOC can increase customer confidence and streamline and strengthen an organization's adherence to local, national, and international privacy requirements.

- 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 cybersecurity. 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 by utilising a variety of security measures, such as firewalls, SIEM (Security Information and Event Management) solutions, intrusion detection systems (IDS), and threat intelligence feeds.

Alert Triage and Analysis:

Evaluating and sorting security alerts produced by monitoring tools according to their importance and potential impact.
Identifying a false positive or a real security situation from an alert.

Incident Investigation and Response:

The SOC team undertakes a careful investigation to determine the type and scope of the attack if an alert is determined to be a real security incident.
To ascertain the cause and effects of the occurrence, evidence must be gathered, log data must be examined, and digital forensics must be carried out.
Launch the incident response procedure, which can comprise isolating impacted 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:

The SOC team concentrates on returning affected systems and services to normal operation once the danger has been eliminated. After putting remedial measures in place to deal with the incident's underlying cause and stop similar assaults in the future.

Post-Incident Analysis and Lessons Learned:

Conducting a complete post-mortem investigation of the incident to determine how it occurred, what impact it had, and what responses were made.
Identifying areas where the organization's incident response and security posture could be improved.
Updating security processes and policies in light of the incident's lessons.

Threat Intelligence and Proactive Measures:

To keep ahead of new threats and well-known attack patterns, threat intelligence is being integrated into the SOC workflow.
Continually look for indications of potential threats and weaknesses to help prevent them from developing into serious security events.

Continuous Monitoring and Improvement:

The SOC cycle is a continuous process that involves continual security measure monitoring, analysis, and improvement to accommodate the changing threat landscape.
The SOC team may effectively identify, address, and recover from security incidents by adhering to this cycle, which reduces the impact of cyber attacks on the organization's assets and data.

- SIEM

SIEM, which stands for Security Information and Event Management, is a comprehensive cybersecurity technology and approach that helps organizations collect, correlate, analyze, and respond to security-related data and events across their IT infrastructure. SIEM systems are designed to provide a centralized and real-time view of an organization's security posture, enabling better threat detection, incident response, and compliance management.

No matter how big or small an organization may be, it is crucial to take proactive measures to monitor and mitigate IT security risks. Enterprises can gain from SIEM systems in a number of ways, and they have become a key part of optimizing security procedures.

Real-time threat recognition

Centralised compliance audits and reporting across the whole corporate infrastructure is made possible by SIEM solutions. While adhering to stringent compliance reporting rules, advanced automation speeds the gathering and analysis of system logs and security incidents.

AI-driven automation

As IT teams manage enterprise security, next-generation SIEM solutions interface with potent security orchestration, automation, and response (SOAR) technologies, saving time and resources. These technologies can handle sophisticated threat identification and incident response protocols in a great deal less time than physical teams because they use deep machine learning that automatically learns from network behaviour.

Improved organizational efficiency

SIEM can be a key factor in increasing interdepartmental efficiencies because of the enhanced visibility of IT infrastructures it offers. Teams can communicate and work together effectively while responding to threats and security issues thanks to a common dashboard, which offers a uniform view of system data, warnings, and notifications.

Detecting advanced and unknown threats

SIEM can be a key factor in increasing interdepartmental efficiencies because of the enhanced visibility of IT infrastructures it offers. Teams can communicate and work together effectively while responding to threats and security issues thanks to a common dashboard, which offers a uniform view of system data, warnings, and notifications.

Phishing - Phishing is the practise of sending communications that seem to be sent from a reliable source in order to steal sensitive corporate data, user information, login passwords, or money.

Ransomware - Malware known as ransomware encrypts a victim's data or device and threatens to keep it encrypted or worse unless the victim pays the attacker a ransom.

Distributed denial of service (DDoS) attacks - Attacks known as distributed denial of service (DDoS) attacks bombard networks and systems with uncontrollable volumes of traffic from a distributed botnet of devices, rendering servers and websites inoperable.

Data exfiltration – Data exfiltration is the manual or automated theft of data from a computer or other device via malware..

Conducting forensic investigations

When a security issue happens, SIEM solutions are excellent for performing computer forensic investigations. Organisations can effectively gather and analyse log data from all of their digital assets with SIEM systems. They can do this to reproduce previous occurrences, analyse current ones, look into

questionable behaviour, and put in place better security procedures.

Assessing and reporting on compliance

For many organizations, compliance auditing and reporting is a crucial yet difficult duty. By offering real-time audits and on-demand reporting of regulatory compliance whenever necessary, SIEM solutions significantly cut the resource expenditures necessary to manage this process.

Monitoring Users and Applications

Organizations require the level of visibility required to minimise network hazards from outside the conventional network perimeter as remote workforces, SaaS apps, and BYOD (bring your own device) rules gain popularity. SIEM systems monitor all network activity across all users, devices, and apps, greatly enhancing infrastructure transparency and identifying threats regardless of the location at which digital assets and services are accessed.

Five Predictions For The Future Of SIEM

1. Usage-based pricing schemes will prevail. These solutions allow teams to pay only for the data throughput and processing they really need each month. This pattern makes use of cloud infrastructure platforms like AWS and GCP and makes service usage predictable. Security teams won't be under as much pressure to use less data going forward.

2. Building analysis tools on top of a global SIEM data platform is likely to be the next step in the decoupling of SIEM systems, which has already begun with SOAR coming from SIEM and other extract, transform, and load (ETL) tools. By concentrating on particular industries, tool-building organisations may create the most reliable, superior-quality, and scalable software.

3. As decoupling progresses, security firms will form solid alliances to offer a sophisticated integration and accelerate time-to-value. These collaborations should advance the security sector, promote mutual business growth through client referrals, and guarantee the best user experience for security personnel.

4. Due to the availability of cloud services, the cost and complexity of a SIEM will continue to decline, making it possible for smaller and more inexperienced security teams to become productive even faster. Data onboarding, analysis, and alerting integrations are not simple with legacy SIEMs because it might take teams more than six months to get started.
The quality and ease of use of next-generation SIEMs can increase, allowing security teams to work fast and concentrate on the important tasks. This tendency will continue to cut down on startup time, which is essential for a company's profitability and the effectiveness of its security team.

5. More firms will keep receiving funding to deal with the many issues that come

with maintaining high security. The amount of venture capital funding is at an all-time high, and security breaches are still a problem for businesses of all kinds, including the massive, highly developed Fortune 1000 enterprises.
A market where there is healthy competition will not be dominated by one enterprise. Security teams have the flexibility and freedom to switch to different platforms as they see fit thanks to this competition. The conflict will then centre on usability, functionality, and flexibility.

- Siem Cycle

A Security Information and Event Management (SIEM) system's lifespan consists of a number of interconnected stages that guarantee the successful deployment, use, and upkeep of the SIEM solution. The following stages typically make up the SIEM life cycle:

Planning and Assessment:
Define the goals and parameters of the SIEM deployment while taking the organization's security needs and compliance objectives into account.
Assess the security infrastructure, data sources, and log management procedures in detail to find any holes and suggest changes.
Create a thorough deployment strategy for the SIEM solution that addresses resource allocation, timing, and roles.

Design and Architecture:

Design the SIEM architecture based on the needs and data sources of the organisation, taking into account elements like scalability, redundancy, and performance.
Choose the optimum deployment strategy (on-premises, cloud-based, hybrid) depending on the requirements and available resources of the organisation.
Plan how data sources will be integrated into the SIEM, making sure that all pertinent security events are gathered and analysed centrally.

Data Collection and Integration:
To collect logs and events from diverse sources, including firewalls, network devices, servers, applications, and endpoints, use data collectors and agents.
To make analysis and correlation more effective, normalise and enrich the collected data.
To include data streams from security devices and other sources into the SIEM platform, configure connections and parsers.
Event Analysis and Correlation:Create and refine correlation rules and use cases to find malicious behaviour and security threat patterns.
Correlate and analyse events in real-time.
Increase the SIEM's capacity to identify new threats and well-known attack vectors by using threat intelligence feeds.

Incident Detection and Response:

In response to generated alerts, look into any security occurrences.
To evaluate the extent and effect of identified security occurrences, conduct a thorough analysis.
Start incident response procedures, such as containment, elimination, and recovery.

Forensics and Investigation:

To comprehend the causes of incidents and the tactics utilised by attackers, perform a thorough forensics examination.
Save and record evidence for conceivable legal or regulatory needs.

Reporting and Compliance:

Generate and present security reports and dashboards for various stakeholders, including IT management, executives, auditors, and regulatory authorities.
Ensure compliance with relevant industry standards and regulations by monitoring and reporting on security events and incidents.

Continuous Monitoring and Maintenance:

Continuously monitor the SIEM infrastructure and adjust the configuration as needed to maintain optimal performance.
Regularly update correlation rules, threat intelligence feeds, and other components to keep the SIEM effective against evolving threats.
Conduct periodic reviews and assessments of the SIEM's performance and effectiveness to identify areas for improvement.
Training and Knowledge Transfer:
Train SOC personnel and IT staff on the effective use of the SIEM solution.
Foster knowledge sharing and best practices from incident investigations and analysis within the organization.
The SIEM lifecycle is a continuous and iterative process, with each phase building upon the insights and experiences gained from previous stages. This approach ensures that the SIEM solution remains relevant, efficient, and effective in helping organizations detect and respond to security threats.
Security teams may feel as though they are drowning in a sea of security warnings as a syslog server persistently pings with each security notification. It can be challenging to determine which events should be paid attention to and which can be ignored without a SIEM. Security personnel, however, have a far clearer picture of the security of their environment once a SIEM has been established. There may not actually be any threats, or there may be numerous occurrences taking place that are simply not yet having an impact on performance.

SOC plays a crucial role in continuously monitoring an organization's network, systems, and applications. It can detect and respond to potential security incidents, including malware infections, data breaches, and unauthorized access attempts. When a security incident occurs, time is of the essence. SOC teams are trained to respond swiftly and effectively to contain and mitigate the damage caused by security breaches. SOC doesn't

merely react to incidents; it proactively identifies vulnerabilities and weaknesses in the organization's infrastructure. This proactive approach enables companies to strengthen their security posture and implement measures to prevent future attacks. SOC provides 24/7 monitoring, ensuring that security analysts are constantly vigilant and ready to respond to emerging threats, regardless of the time of day. SOC is a critical component of a robust cybersecurity strategy. It empowers organizations to detect, respond to, and prevent cyber threats, safeguarding sensitive data, maintaining business continuity, and preserving the organization's reputation in an increasingly interconnected and threat-prone digital landscape. SOC acts as the central hub for incident coordination and communication. It facilitates collaboration among various teams, such as IT, legal, communications, and executive management, ensuring a cohesive and efficient response to security incidents.

- **SOC - cycle**

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

Threat Detection and Monitoring:

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

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

Alert Triage and Analysis:

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

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

Incident Investigation and Response:

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

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

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

Incident Containment and Eradication:

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

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

Recovery and Remediation:

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

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

Post-Incident Analysis and Lessons Learned:

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

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

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

Threat Intelligence and Proactive Measures:

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

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

Continuous Monitoring and Improvement:

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

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

- **SIEM**

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

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

Real-time threat recognition

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

AI-driven automation

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

Improved organizational efficiency

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

Detecting advanced and unknown threats

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

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

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

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

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

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

Conducting forensic investigations

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

Assessing and reporting on compliance

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

Monitoring Users and Applications

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

Five Predictions For The Future Of SIEM

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

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

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

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

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

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

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

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

- **Siem Cycle**

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

Planning and Assessment:

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

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

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

Design and Architecture:

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

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

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

Data Collection and Integration:

Implement data collectors and agents to gather logs and events from various sources, such as firewalls, network devices, servers, applications, and endpoints.

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

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

Event Correlation and Analysis:

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

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

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

Incident Detection and Response:

Respond to generated alerts by investigating potential security incidents.

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

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

Forensics and Investigation:

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

Preserve and document evidence for potential legal or regulatory purposes.

Reporting and Compliance:

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

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

Continuous Monitoring and Maintenance:

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

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

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

Training and Knowledge Transfer:

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

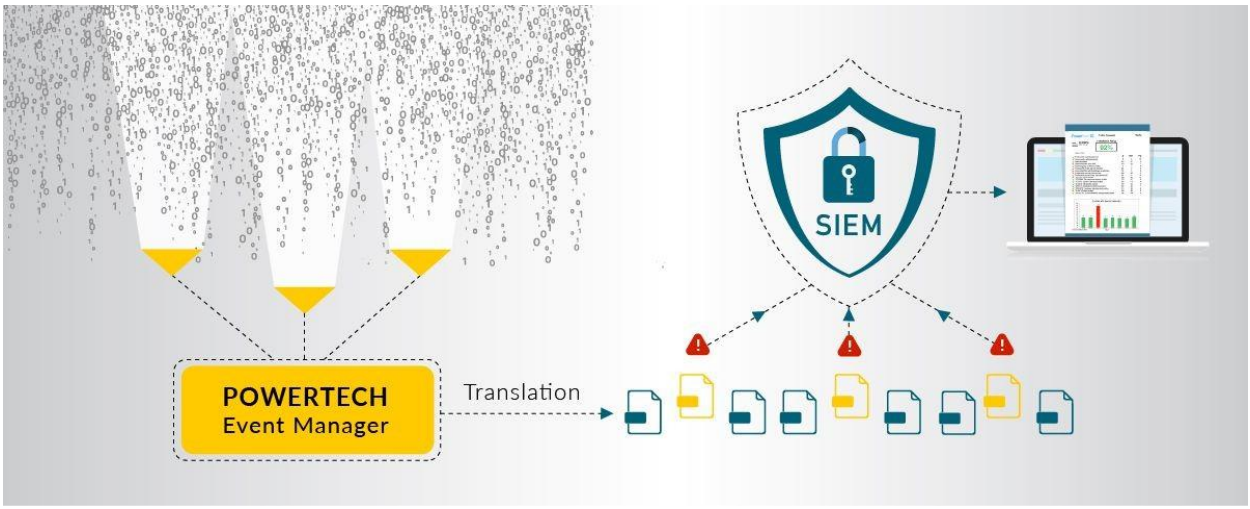
Foster knowledge sharing and best practices from incident investigations and analysis within the organization.

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

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

Threat Detection

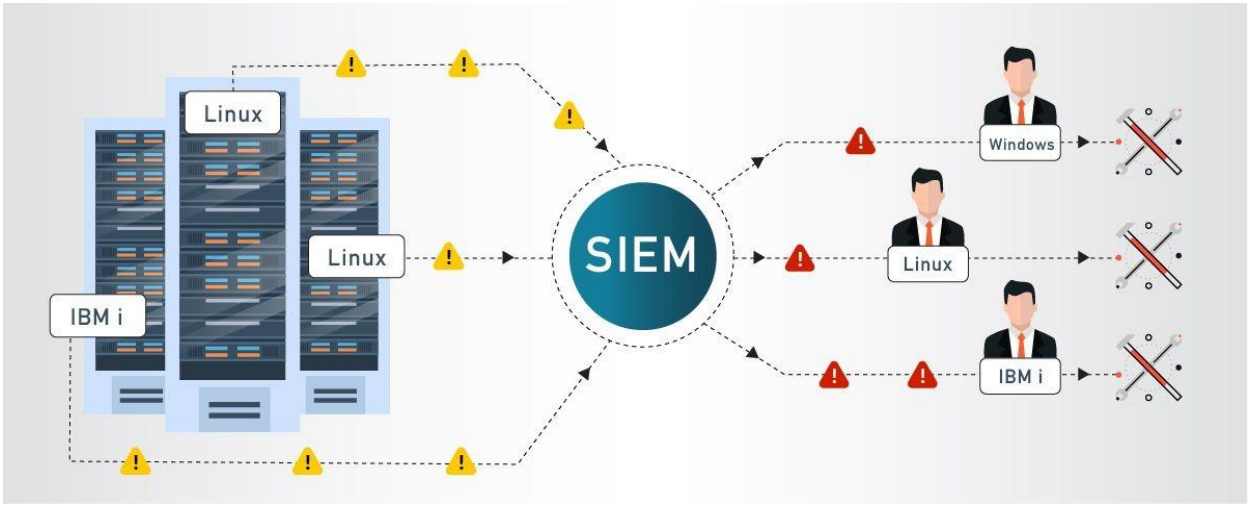
Translation



Prioritization

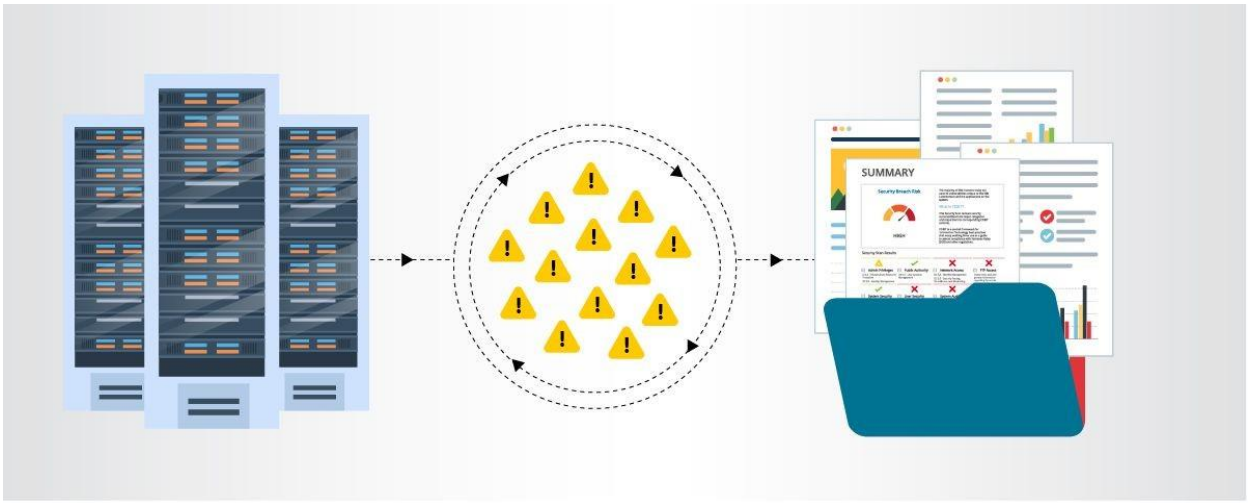

SIEM
HIGHLIGHTED EVENT
SECURITY THREAT
SECURITY INCIDENT

Escalation


Linux
Linux
IBM i
SIEM
Windows
Linux
IBM i

Analysis

Compliance



- **MISP**

The fundamental features of MISP, or Malware Information Sharing Platform and Threat Sharing, are:

a useful IOC and indicators database that may hold both technical and non-technical data regarding malware samples, incidents, attackers, and intelligence.

Features of MISP, the open source threat sharing platform

A threat intelligence platform that allows users to exchange, store, and correlate threat intelligence, financial fraud, vulnerability, and counter-terrorism information as well as indicators of compromise from targeted attacks. Find out how MISP is currently being used by various organisations. The IoCs and information are used to not only store, share, and collaborate on malware research and cyber security indicators, but also to identify and stop attacks on ICT infrastructures, businesses, or individuals.

An effective database of IoC and indications that can store both technical and non-technical data regarding malware samples, incidents, attackers, and intelligence.
Finding correlations between characteristics and indications automatically using data from malware, attack campaigns, or analysis. The correlation engine offers correlation between attributes as well as more complex correlations like CIDR block matching or fuzzy hashing correlation (e.g., ssdeep). the correlation.

Built-in sharing capabilities to make it easier to share data using various distribution methods. MISP allows for the automated synchronisation of events and properties between MISP. Each organization's sharing policy can be met using advanced filtering functionalities, such as a variable sharing group capacity and an attribute level distribution process.
End users can create, edit, and collaborate on events, attributes, and indications using a simple user interface. a graphical user interface that allows for easy switching between events and correlations. a capability for creating and viewing associations between objects in an event graph

This approach of light collaboration on events and attributes lets MISP users sugges t updates or changes to characteristics or indications.
Data sharing involves automatically synchronising and exchanging information with third parties and trust groups via MISP.

Feed import is a flexible tool for importing and integrating MISP feeds, OSINT feeds , and third-party threat intelligence.
There are numerous preset feeds included with the normal MISP installation.
Sharing delegation: This simple pseudo-
anonymous technique enables the publication of events and indicators to be moved to another entity.

Through a comprehensive API, MISP can be integrated with your own products.
MISP comes with PyMISP, a flexible Python library that may be used to retrieve, mo dify, or update events attributes, handle malware samples, or look for attributes

Flexible taxonomy for categorising and labelling events in accordance with your own categorization systems or pre-existing taxonomies.
Intelligence vocabularies called MISP galaxy and bundled with existingthreat actors, malware, RAT, ransomware or MITRE ATT&CK which can be easily linked with events in MISP.
Expansion modules in Python to expand MISP with your own services or activate already available misp-modules. Sighting support to get observations from organizations concerning shared indicators and attributes.

API as MISP document or STIX sighting documents. Starting with MISP 2.4.66, Sighting has been extended to support false-negative sighting or expiration sighting.

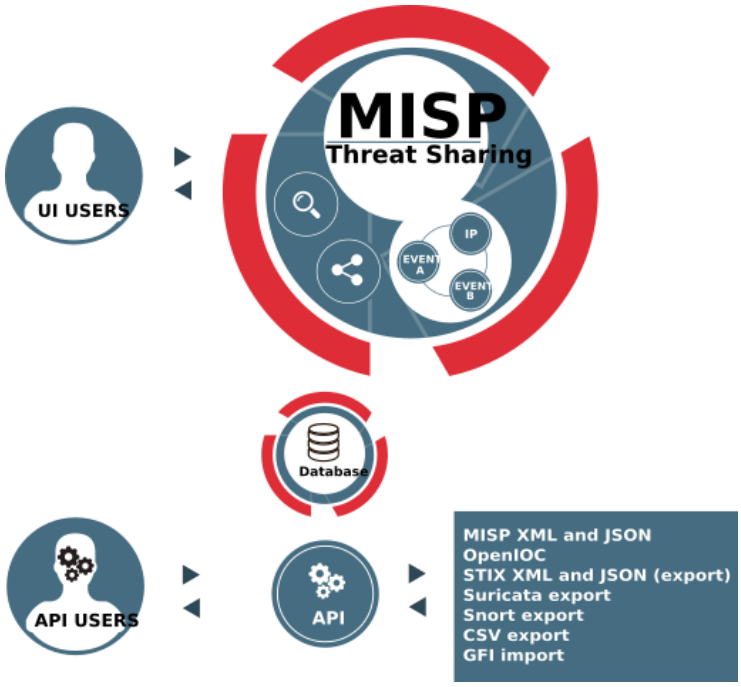
Support for STIX includes exporting and importing data in STIX 2.0 format (XML and JSON).

Integrated PGP and/or S/MIME encryption and signature of the alerts, depending on the user's preferences.

A real-time publish-subscribe channel in MISP can be used to automatically receive any changes (such as new events, indicators, sightings, or tags) in ZMQ (such as the misp-dashboard) or Kafka.

Cooperating with people

The information you store is instantly accessible to your partners and coworkers. Keep the event ID in your ticketing system or receive notifications via signed and encrypted email.



- **Your college network information**

  Bharati Vidyapeeth's College of Engineering

  A total of 12 labs and approximately 520 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 unknown, enabling security teams to make better decisions
- empowers cyber security stakeholders by revealing adversarial motives and their tactics, techniques, and procedures (TTPs)
- helps security professionals better understand the threat actor's decision-making process
- empowers business stakeholders, such as executive boards, CISOs, CIOs and CTOs; to invest wisely, mitigate risk, become more efficient and make faster decisions

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

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

- **Incident response**

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

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

Who Handles Incident Responses?

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

Six Steps for Effective Incident Response

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

What is the NIST incident response model?

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

Preparation - Organizations should take the necessary steps to be prepared for a cybersecurity incident when one occurs.

Detection and analysis - The cybersecurity response team is responsible for detecting and analyzing incidents to determine how to proceed and who needs to be notified.

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

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

- **Qradar & understanding about tool**

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

the QRadar architecture.

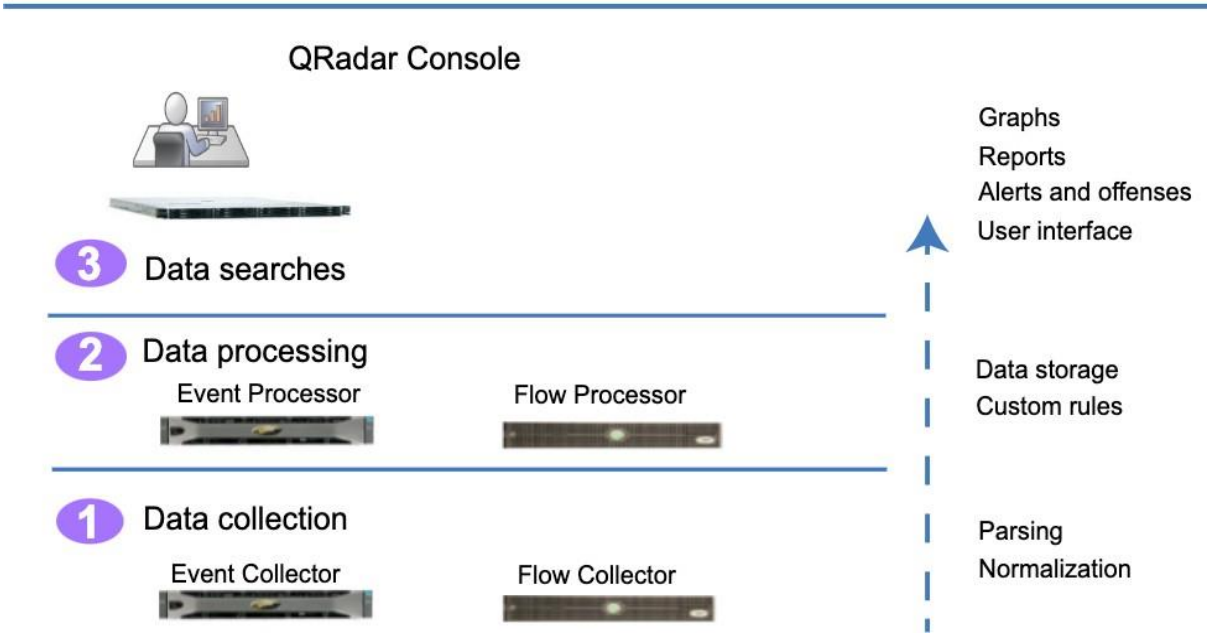


Figure 1. QRadar architecture

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

Data collection

Data collection is the first layer, where data such as events or flows is collected from your network. The All-in-One appliance can be used to collect the data directly from your network or you can use collectors such as QRadar Event Collectors or QRadar QFlow Collectors to collect event or flow data. The data is parsed and normalized before it passed to the processing layer. When the raw data is parsed, it is normalized to present it in a structured and usable format.

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

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

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

Data processing

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

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

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

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

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

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

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

Data searches

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

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

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

QRadar components

Use IBM QRadar components to scale a QRadar deployment, and to manage data collection and processing in distributed networks.

QRadar maximum EPS certification methodology

IBM QRadar appliances are certified to support a certain maximum events per second (EPS) rate. Maximum EPS depends on the type of data that is processed, system configuration, and system load.

QRadar events and flows

The core functions of IBM QRadar SIEM are managing network security by monitoring flows and events.

Conclusion

Stage 1 :- what you understand from Web application testing .

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

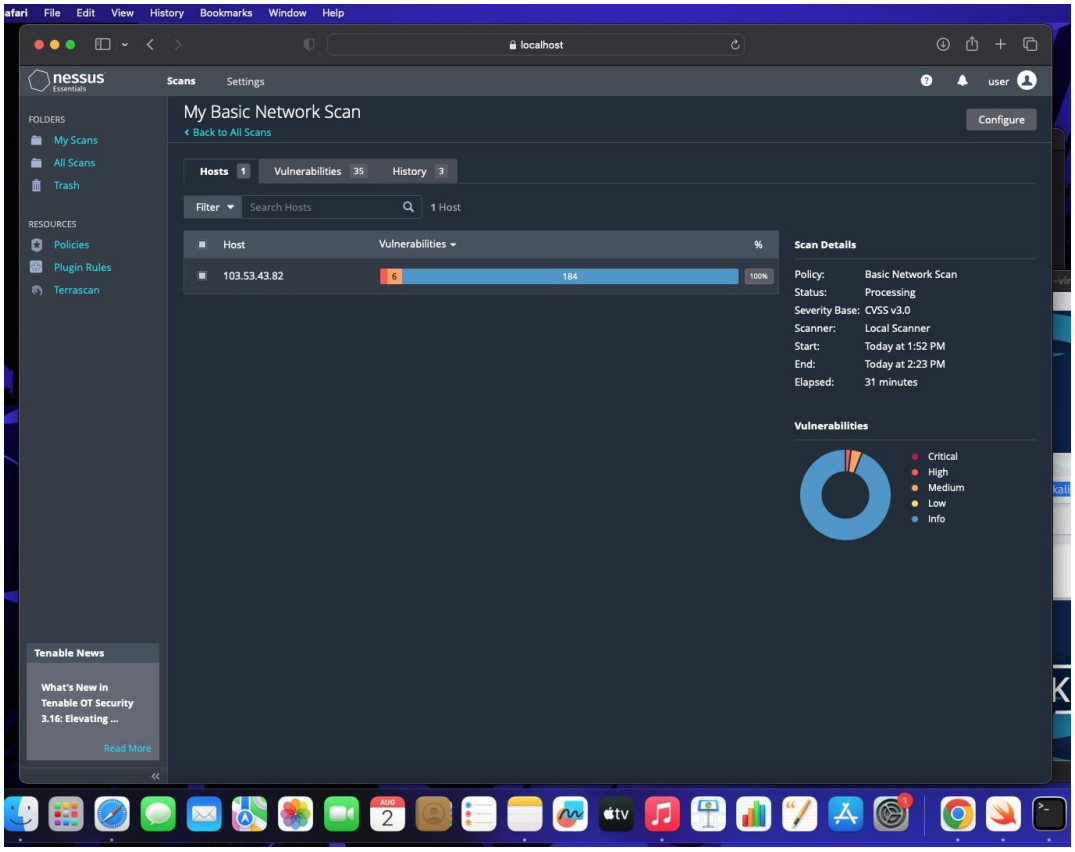
- Identification of Security Vulnerabilities
- Bug Detection and Resolution
- Validation of Functional Requirements
- Usability and User Experience Evaluation
- Performance and Load Testing Results
- Compatibility Testing Insights
- Accessibility Compliance
- Security Compliance and Risk Mitigation
- Optimization Recommendations
- Enhanced Quality Assurance
- Increased Customer Confidence
- Compliance with Regulatory Requirements

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

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

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

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



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 trends such as increasing application complexity, the shift towards microservices and APIs, mobile-first design, web accessibility testing, the integration of AI and automation, and a heightened focus on security and privacy. Web application testers will need to adapt to these changes and acquire specialized skills to ensure the quality, performance, and security of modern web applications.

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

Increased automation, integration with cutting-edge technologies, and an emphasis on guaranteeing quality, security, and performance in the ever-changing software ecosystem will all be part of the testing process's future scope. To stay relevant in the rapidly changing world of software testing, testing professionals will need to adjust to these changes and continually improve their skills.

Stage 3 :- future scope of SOC / SEIM

he future scope of SOC (Security Operations Center) and SIEM (Security Information and Event Management) can be summarized as follows:

Advanced Threat Detection: SOC and SIEM will increasingly focus on advanced threat detection, leveraging artificial intelligence (AI) and machine learning (ML) to identify sophisticated and evolving cyber threats in real-time.

Cloud Security: With the growing adoption of cloud technologies, SOC and SIEM will expand their capabilities to provide robust cloud security monitoring and threat detection for cloud-native environments.

Automation and Orchestration: SOC and SIEM tools will incorporate more automation and orchestration capabilities to streamline incident response processes, reducing response times and improving efficiency.

Zero Trust Security: The adoption of Zero Trust security models will lead to a stronger emphasis on continuous authentication and monitoring, requiring SOC and SIEM to adapt to these new security paradigms.

Integration with DevSecOps: SOC and SIEM will integrate with DevSecOps practices, ensuring that security is ingrained in the development pipeline, with security checks and monitoring at every stage.

Compliance and Reporting: SOC and SIEM will continue to assist organizations in meeting compliance requirements and providing robust reporting capabilities for auditing and regulatory purposes.

Threat Intelligence Sharing: Increased collaboration and threat intelligence sharing among organizations and industries will enhance the effectiveness of SOC and SIEM in identifying and mitigating threats.

User and Entity Behavior Analytics (UEBA): The use of UEBA within SIEM systems will expand, enabling organizations to better detect insider threats and unusual user behavior patterns.

Remote Work Security: The remote work trend will lead to a greater need for SOC and SIEM to secure distributed environments and monitor remote access to corporate networks.

Privacy and Data Protection: As data privacy regulations continue to evolve, SOC and SIEM will play a critical role in ensuring the protection of sensitive data and compliance with privacy laws.

In summary, the future scope of SOC and SIEM involves staying ahead of emerging threats, adapting to evolving technologies, and providing comprehensive security monitoring and incident response capabilities across various environments, including on-premises, cloud, and remote work settings.

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 :-

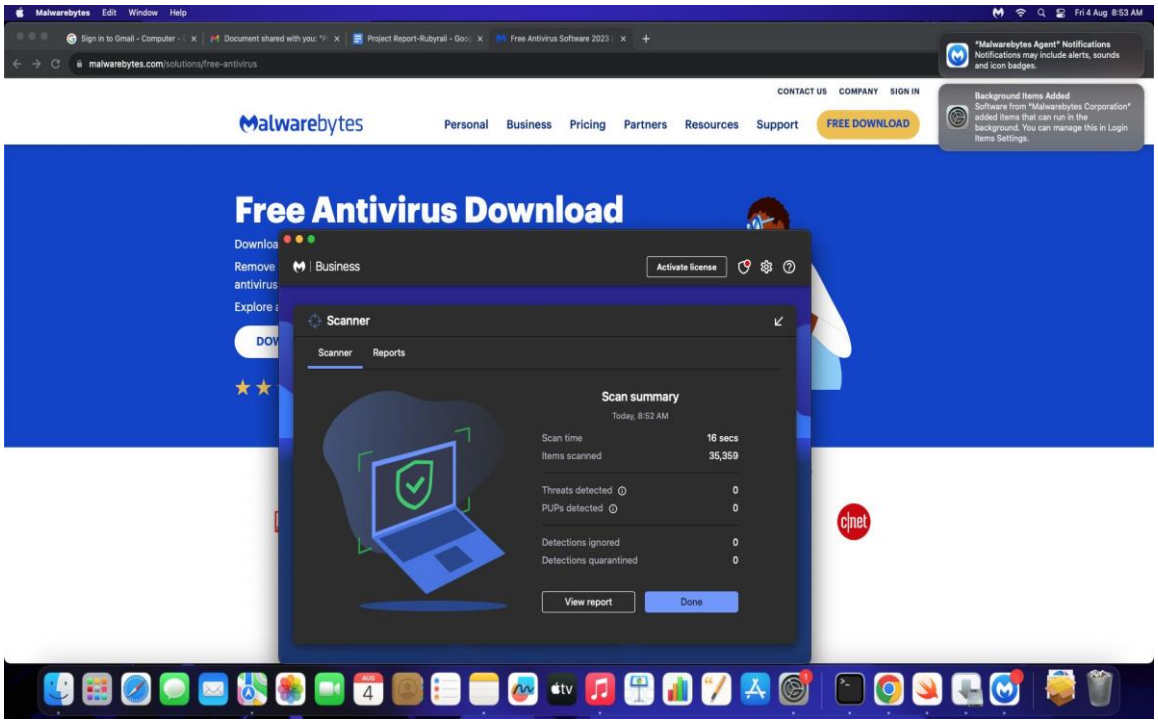
Nessus, cybermap.kaspersky.com, thehackersone.com, chaptgpt, wepik.com (AI image editor), Gamma (AI based PPT), OWASP top 10 vulnerabilities(2021), thehackersnews.com, CWE, exploitDB, virtual box, live websites-bugcrowd, nslookup.io, OSINT framework, mitre framework, IBM fix central, QRadar Installation,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

MALWAREBYTES

FREE DOWNLOADS

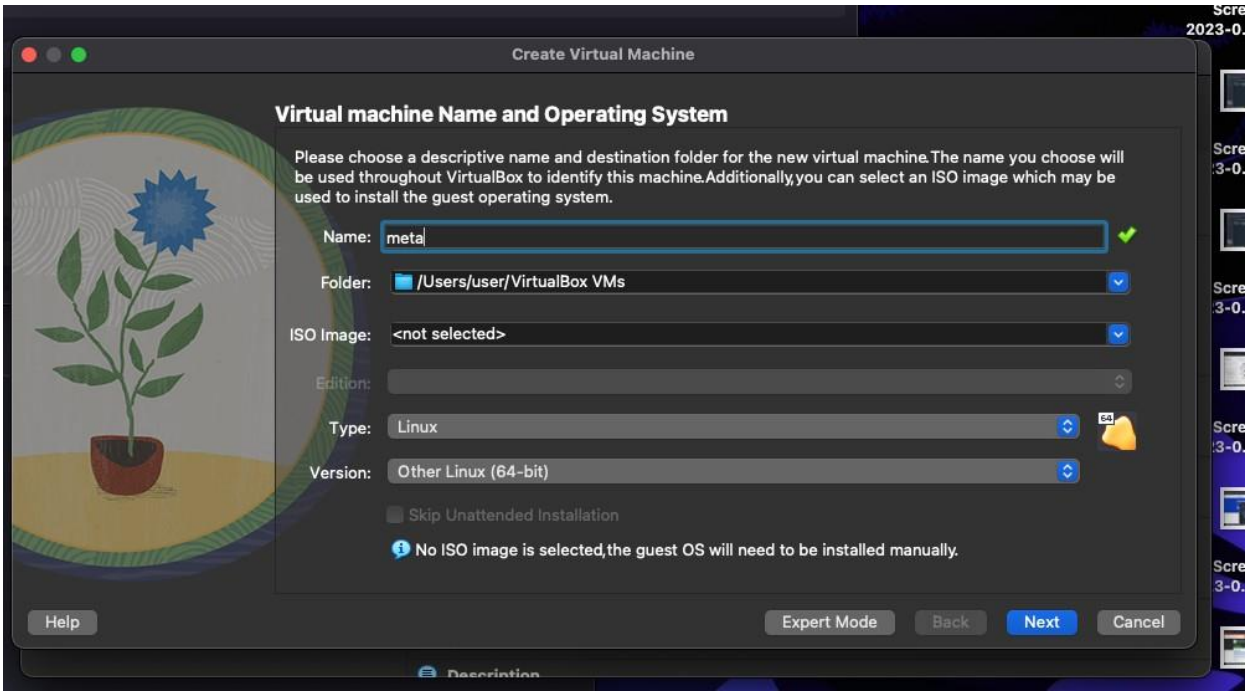
Free Antivirus Software 2023

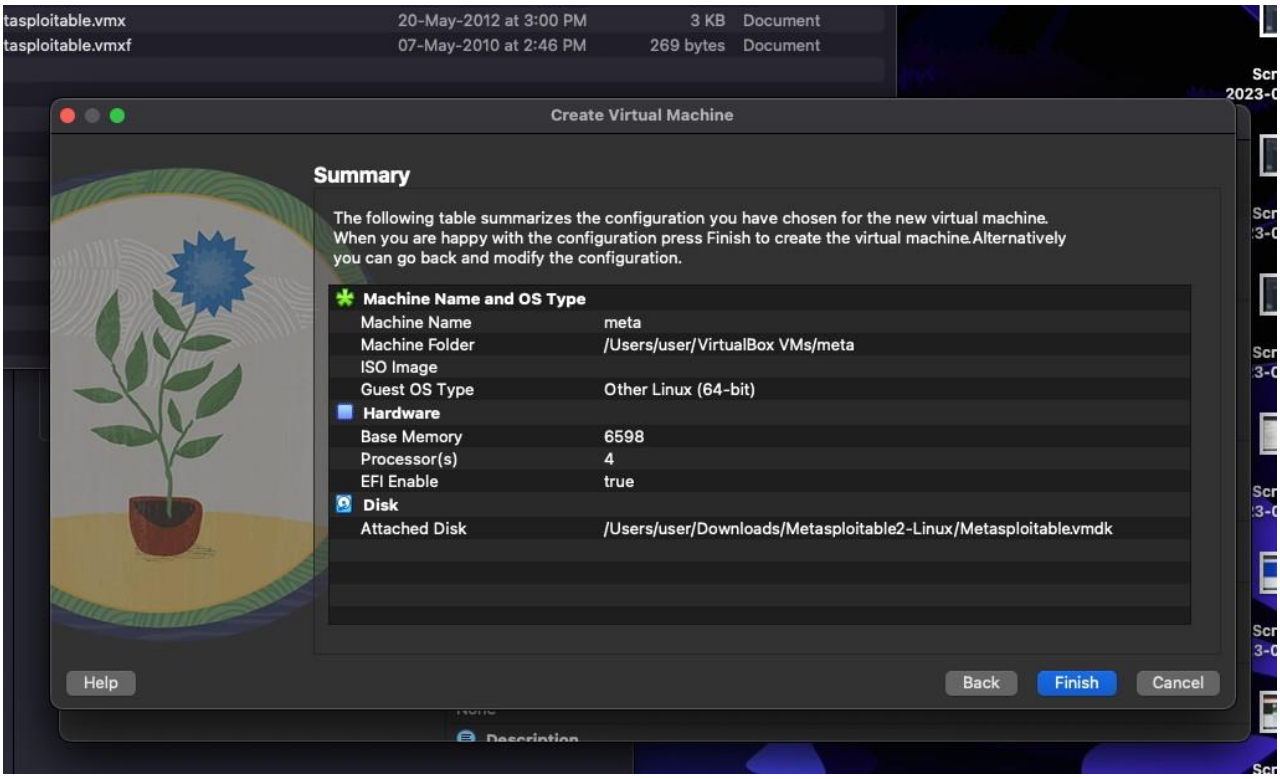
Looking for free antivirus and malware removal? Scan and remove viruses and malware for free. Malwarebytes free antivirus includes multiple layers of malware-crushing tech. Our anti-malware finds and removes threats like viruses, ransomware, spyware, adware, and Trojans.



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-> metaspoiltable 2 vmdk

Metaspoilt

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

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

msf6 > search exploit

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

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

Testing Metaspoilt using Kalilinux

> nmap -A 10.5.174.221

msfg> use auxiliary/admin/http/tomcat_ghostcat

>show options

>set RHOSTS 10.5.174.221

>run

>exploit

>search vsftp

>run

>exploit

> use modulename

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