TEAM -VI

Techiee Demons

Part I-Executive summary

Overview

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

- Create a cybersecurity policy and plan that is precise and well-defined and that is in line with the goals and risk tolerance of the firm.
- To find potential cybersecurity risks and vulnerabilities specific to the organization, do a thorough risk assessment. Put risks in order of importance depending on their potential impact and propensity to arise. To address identified vulnerabilities, implement risk mitigation measures and develop a risk management strategy.
- All staff members should receive training on cybersecurity best practices and their role in protecting the organization's data. To encourage a security-conscious culture, teach them about phishing, social engineering, password hygiene, and other typical attack vectors.
- Put in place stringent access control procedures to guarantee that only vetted individuals have access to sensitive information and vital systems. Use multi-factor authentication (MFA) to provide an additional security layer.
- Implement secure gateways, intrusion detection/prevention systems (IDS/IPS), and firewalls to track and manage network traffic.
- To guard against malware and other threats at the device level, install host-based firewalls, endpoint protection programs, and antivirus software on all devices.
- To guard against malware and other threats at the device level, install host-based firewalls, endpoint protection programs, and antivirus software on all devices.
- Encrypt sensitive data while it is in transit and at rest to protect privacy and prevent unauthorized access.
- Create a methodical procedure for immediately installing security patches and updates to

all software, operating systems, and firmware to fix known vulnerabilities.

- To address cybersecurity issues successfully, create a well-defined incident response plan (IRP). Clear instructions on recognizing, reporting, containing, eradicating, and recovering should be included in the strategy.
- Carry out routine internal and external security audits and assessments to analyze the organization's security posture and spot any holes or potential vulnerabilities.
- Monitoring and logging: To quickly identify and react to suspicious activities, implement centralized logging and real-time monitoring of network and system activity.
- Create distinct routes for informing stakeholders, including as staff members, clients, business partners, and regulatory agencies, about security events.

IP address of irctc.com 103.116.163.23

2. Team Members Involved in vulnerability Assessment

S.No	**Name**	**Designation**	**Mobile Number**
1	Mr. V. Shiyam	Assistant Professor	8072543162 shiyamv@ksrct.ac.im
2	Suryansh porwal	Network Engineer	9258430874 suryansh@bvicam.in
3	Raghunath patil	Computer Programmer	8010233511 raghunath.patil@bharatividyapeeth.edu

3. List of Vulnerable Parameter, location discovered

S. No	Name of the Vulnerability	Reference CWE
1	Broken Access Control	CWE-377: Insecure Temporary File
2	Cryptographic Failures	CWE-338: Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG)
3	Injection	CWE-471: Modification of Assumed-Immutable Data (MAID)
4	Insecure Design	CWE-646: Reliance on File Name or Extension of Externally-Supplied File
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-287: Improper Authentication
8	Software and Data Integrity Failures	CWE-915: Improperly Controlled Modification of Dynamically-Determined Object Attributes
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-377: Insecure Temporary File

OWASP CATEGORY: A01 2021 Broken Access Control

DESCRIPTION: Application and system data may be subject to attack if temporary files are created and used in an unsafe manner.

BUSINESS IMPACT: To mitigate these business impacts, organizations should implement strong data security practices, including secure handling of temporary files. This may involve encrypting sensitive data, setting appropriate access controls, regularly auditing and monitoring file systems, and educating employees about security best practices. Additionally, having an incident response plan in place can help minimize the damage in case of a security breach related to temporary files.

Here are some of the key business impacts of insecure temporary files:

- ❖ Data Breaches
- ❖ Legal and Regulatory Consequences
- ❖ Reputation Damage
- ❖ Financial Loss
- ❖ Operational Disruption:
- ❖ Loss of Intellectual Property
- ❖ Compliance Challenges
- ❖ Customer and Employee Trust
- ❖ Resource Drain

2. CWE-338: Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG)

OWASP CATEGORY: A02 2021 Cryptographic Failures

DESCRIPTION: Pseudo-random number generators (PRNGs) are frequently not made for encryption. For algorithms that require random numbers, a mediocre source of randomness could occasionally be adequate or even preferred. Weak generators often consume less processing power and/or do not use the system's limited supply of valuable entropy sources. Even though these PRNGs may have some extremely helpful properties, these same qualities might also be utilized to compromise the encryption.

BUSINESS IMPACT: Employing robust, cryptographically secure PRNGs for all security-critical applications, such as key generation, encryption, and secure token generation, will help enterprises reduce these negative effects on their bottom line. To find and fix problems in cryptographic implementations, routine security audits and vulnerability assessments should be carried out. Keeping up with industry best practices and adhering to pertinent security standards and laws are also crucial for lowering the danger posed by shoddy PRNGs.

Here are the key business impacts of using a weak PRNG:

- Security Breaches
- Data Vulnerability
- Loss of Customer Trust
- Regulatory Compliance Issues
- Financial Loss
- Operational Disruption
- Intellectual Property Risks

3. CWE: CWE-471: Modification of Assumed-Immutable Data (MAID)

OWASP CATEGORY: A03 2021 Injection

DESCRIPTION: A presumed-immutable ingredient is not adequately shielded from assault by the product. When an input is so essential to the operation of the program that it shouldn't be altered in any way but is, this happens. When they are not, some resources, such as cookies, hidden form fields in web applications, and reverse DNS lookups, are frequently considered to be immutable.

BUSINESS IMPACT: Modification of Assumed-Immutable Data (MAID) is the term used to describe the unlawful changing of data that was once believed to be immutable or unchangeable. Because it compromises data integrity and can result in a number of problems, this can have substantial and broad-reaching business effects.

Here are some of the main effects of MAID on business.

- Data Integrity Compromised
- Operational Disruption
- Financial Loss
- Legal and Regulatory Consequences
- Reputation Damage
- Loss of Competitive Advantage
- Security Vulnerabilities
- Compliance Challenges
- Investigation and Remediation Costs

4. CWE: CWE-646: Reliance on File Name or Extension of Externally-Supplied File

OWASP CATEGORY: A04 2021 Insecure Design

DESCRIPTION: The server has a security feature that works on the presumption that any URI that is requested through HTTP GET won't result in the associated resource's state changing. Since certain apps permit GET to edit state, this may allow attackers to get around intended access limitations and launch resource modification and deletion attacks.

BUSINESS IMPACT: Software vulnerability is defined by the Common Weakness Enumeration (CWE) entry 646, "Reliance on File Name or Extension of Externally-Supplied File," where a program or system depends on the file name or file extension provided by a user or external source to decide on security measures or to identify the type of the file. Because it puts the company at risk for numerous security breaches, this flaw might have a big impact on the company's operations.

Here are some of the key business impacts of MAID

- Security Breaches
- Data Loss or Corruption
- Malware Propagation
- Financial Loss
- Reputation Damage
- Legal and Regulatory Consequences
- Operational Disruption
- Loss of Competitive Advantage

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

OWASP CATEGORY : A05 2021 Security Misconfiguration

DESCRIPTION: The user agent could communicate sensitive cookies over an HTTP session in plaintext if the Secure attribute for such cookies in HTTPS sessions is not specified.

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

To mitigate the business impact of sensitive cookies used without the 'Secure' attribute, organizations should:

- Set the 'Secure' Attribute
- Implement HTTP Strict Transport Security (HSTS
- Regularly Test for Vulnerabilities
- Educate Developers and Staff
- Monitor and Log Security Events
- Have an Incident Response Plan

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

OWASP CATEGORY: A06 2021 Vulnerable and Outdated Components

DESCRIPTION: The product is dependent on a third-party component that includes one or more big or complicated enough products and that utilise libraries, modules, or other intellectual property created by parties other than the product's developer for some of their functioning.

BUSINESS IMPACT: In some hardware items, a full operating system may come from a third-party source. Whether open source or closed source, these components could include flaws that are known to the public and might be used by adversaries to compromise the product with further flaws. A Software Composition Analysis (SCA) tool called Dependency-Check seeks to identify vulnerabilities in dependencies that have been made publicly known. It accomplishes this by figuring out whether a certain dependent has a Common Platform Enumeration (CPE) identity.

To mitigate the business impact of dependency on vulnerable third-party components, organizations should take the following steps:

- Continuous Monitoring
- Patch Management
- Risk Assessment
- Security Assessments
- Security Contracts
- Incident Response Plan

7. CWE: CWE-287: Improper Authentication

OWASP CATEGORY: A07 2021 Identification and Authentication Failures

DESCRIPTION: The product does not prove or does not properly verify that an actor is who they say they are when they claim to have a certain identification.

BUSINESS IMPACT: Improper authentication refers to a security weakness where an application or system fails to adequately verify the identity of a user or entity trying to access its resources. This vulnerability can have significant business impacts, as it opens the door to unauthorized access, data breaches, and other security risks.

Here are the key business impacts of improper authentication:

- Unauthorized Access
- Data Breaches
- Financial Loss
- Legal and Regulatory Consequences
- Reputation Damage
- Operational Disruption

8. CWE: CWE-915: Improperly Controlled Modification of Dynamically-Determined Object Attributes

OWASP CATEGORY: A08 2021 Software and Data Integrity Failures

DESCRIPTION: The product gets data from an upstream component that lists various characteristics, properties, or fields that need to be initialized or updated in an object, but it is unable to correctly regulate which fields can be changed. Vulnerability might result from properties that were unexpectedly changed if they were only meant to be used internally by the object. Language-specific methods that enable it, such bulk assignment, autobinding, or object injection, are occasionally aware of this flaw.

BUSINESS IMPACT: A software flaw or vulnerability known as "Improperly Controlled Modification of Dynamically-Determinate Object Attributes" occurs when a program permits changes to an object's characteristics or properties depending on dynamically determined input, such as user-provided data or outside input. Due to its potential to cause security concerns, data corruption, and operational challenges, this vulnerability might have a substantial negative impact.

Here are some of the key business impacts associated with CWE-915:

- Data Corruption
- Security Vulnerabilities
- Unauthorized Access
- Operational Disruption
- Financial Loss

9. CWE: CWE-532: Insertion of Sensitive Information into Log File

OWASP CATEGORY: A09 2021 Security Logging and Monitoring Failures

DESCRIPTION: While recording all information may be useful during the development process, it's crucial to select the right logging settings before a product is released to prevent unintentional exposure of critical user data and system information to possible attackers.

BUSINESS IMPACT: Sensitive data being added to log files can have a big impact on organization since it puts security, privacy, and compliance at risk. Log files are frequently used to keep track of system occurrences and troubleshoot problems, but when sensitive information is unintentionally logged, it can cause a number of complications.

To mitigate the business impact of sensitive information insertion into log files, organizations should adopt the following best practices:

- Data Redaction
- Log Management
- Access Controls
- Regular Auditing
- Data Classification
- Security Awareness
- Incident Response Plan

10. CWE: CWE-918 Server Side Request Forgery

OWASP CATEGORY: A10 2021 - Server Side Request Forgery

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

BUSINESS IMPACT: Server-Side Request Forgery (SSRF) vulnerabilities can have significant business impact and consequences if they are successfully exploited. These impacts can vary depending on the specific context and the extent of the SSRF attack, but some common business-related consequences include:

- Data Breaches
- Loss of Customer Trust
- Reputation Damage
- Financial Loss
- Regulatory Compliance Issues
- Operational Disruption
- Intellectual Property Theft
- Legal Consequences
- Resource Consumption

Stage : 2 Report

NESSUS Vulnerability Report

Overview

A Nessus Vulnerability Report is a detailed document generated by Nessus, a popular vulnerability scanning tool developed by Tenable Network Security. The report provides comprehensive information about the vulnerabilities and security issues discovered during a vulnerability scan of a target system or network. These reports are valuable for IT and security professionals as they help identify weaknesses that could potentially be exploited by malicious actors. Below, I'll outline the typical contents and sections you might find in a Nessus Vulnerability Report:

1. **Executive Summary:** This section provides a high-level overview of the scan results. It typically includes a summary of the number of vulnerabilities found, their severity levels, and a brief description of the potential risks.

2. **Introduction:** This section provides background information about the scan, including the target system or network, the scan date, and the scanning tool used (Nessus).

3. **Vulnerability Summary:** Here, you'll find a breakdown of the vulnerabilities discovered during the scan, organized by severity levels (e.g., critical, high, medium, low). Each vulnerability is typically listed with its name, severity rating, and a brief description.

4. **Detailed Vulnerability Findings:** This is the most extensive part of the report. It provides in-depth information about each vulnerability, including:

- Vulnerability ID and name

- Severity rating (CVSS score)

- Description of the vulnerability

- Recommendations for remediation or mitigation

- References to external resources or advisories

- Technical details about the vulnerability, including affected systems, ports, and services

5. **Vulnerability Compliance:** This section may contain information about compliance checks against specific security standards or regulations (e.g., CIS benchmarks, PCI DSS). It shows whether the target system is compliant or non-compliant with these standards and provides recommendations for achieving compliance.

6. **Host Information:** Details about the target hosts, including their IP addresses, hostnames, operating systems, and open ports, are usually included in this section.

7. **Remediation Actions:** This section provides actionable recommendations for addressing the identified vulnerabilities. It often includes step-by-step instructions on how to mitigate or fix the issues, along with references or links to additional resources.

8. **Appendices:** Additional information, such as a glossary of terms, references to vulnerability databases (e.g., CVE IDs), or supplementary data, may be included in the appendices.

9. **Charts and Graphs:** Some Nessus reports include visual elements, such as charts and graphs, to help stakeholders quickly understand the distribution of vulnerabilities by severity or type.

10. **Customization:** Nessus allows for some level of report customization. Users can often tailor the report's content, format, and style to meet their specific needs or compliance requirements.

Nessus Vulnerability Reports are valuable tools for organizations to assess and prioritize their cybersecurity efforts. They provide a detailed roadmap for addressing security weaknesses and improving overall security posture. Security teams can use the information in these reports to remediate vulnerabilities, reduce risk, and enhance the resilience of their systems and networks.

Target Website : K.S.Rangasamy College Of Technology : ksrct.ac.in

Target IP: 172.67.129.34

S. No.	Vulnerability name	Severity	Plugin	Description	Solution	BusinessImpact	Port
1	**SSL Medium Strength Cipher Suites Supporte d (SWEET32)**	**High**	**42873**	**The usage of SSL ciphers that provide medium strength encryption is supported by the remote host.** **Any encryption that employs the 3DES encryption suite or at least key lengths of at least 64 bits but not more than 112 bits is considered medium strength by Nessus.**	**To prevent using medium strength ciphers, if at all feasible, reconfigure the concerned application.**	**A hostile actor may be able to decode data containing sensitive information by successful brute-forcing of weak ciphers, potentially resulting in a total breach of confidentiality and integrity. The worth of the compromised data and the attacker's creativity are basically the only factors that can restrict the degree of the harm.**	2087,2083,2096
2	**HTTP Server Type and Version**	**Info**	**10107**	**This plugin attempts to determine the type and the version of the remote web server.**	**N/A**	**An attacker might use the disclosed information to harvest specific security vulnerabilities for the version identified. Configure your web server to prevent information leakage from the SERVER header of its HTTP response.**	**8880,443,2083,2096**

3	**Hypertext Transfer Protocol (HTTP) Information**	Info	**24260**	This test gives some information about the remote HTTP protocol - the version used whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...	Update status of HTTP method and active the pipeline	An attacker might exploit particular security flaws for the detected version using the information that has been released. Configure your web server to stop data from leaking from the HTTP response's SERVER header.	80,443,2052
4	**Device Type**	Info	**54615**	Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).	N/A	Maybe have possibility to misconnection match while printing g or any actions	N/A
5	**Nessus SYN Scanner**	Info	**11219**	SYN 'half-open' port scanning is what this plugin does. Even when used against a target protected by a firewall, it must be rather rapid.	Use an IP filter to shield your target.	The largest impacts tend to be net- work latency and simultaneous plugin checks.	22
6	**Common Platform Enumeration (CPE)**	info	**45590**	By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and	N/A	Common Platform Enumeration (CPE) is a standardized method for naming and identifying software and hardware platforms, making it	N/A

				software products found on a host. available for the product, this plugin computes the best possible CPE based on the information available from the scan.		easier for organizations to manage their IT assets and assess their cyber security posture	
7	**Open Port Re-check**	**Info**	**10919**	One of several ports that were previously open are now closed or unresponsive. There are several possible reasons for this - The scan may have caused a service to freeze or stop running. - Administrator may have stopped a particular service during the scanning process.	Steps to resolve this issue include : - Increase checks_read_timeout and/or reduce max_checks. - Disable any IPS during the Nessus scan	**Regularly re-checking open ports helps identify potential security vulnerabilities and weaknesses in your network. By discovering and addressing these issues proactively, businesses can enhance their overall security posture and reduce the risk of cyber attacks and data breaches.**	

The SOC and Security Information and Event Management (SIEM)

a. 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. A strong cyber security strategy must include SOC. In an increasingly linked and risk-prone digital environment, it equips enterprises to recognize, address, and avoid cyber risks, protecting sensitive data, ensuring business continuity, and protecting the organization's brand. SOC serves as the primary coordination and communication center for incidents. It makes it easier for different teams to collaborate, including those in IT, law, communications, and executive management, enabling a coordinated and effective response to security issues.

b. 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 cyber security. 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.

c. SIEM

SIEM A security system called security information and event management, or SIEM, assists organizations in identifying and addressing possible security threats and vulnerabilities before they have a chance to impair daily operations. Enterprise security teams can leverage SIEM systems to identify user behavior anomalies and automate a number of the manual procedures involved in threat detection and incident response using artificial intelligence (AI).

Benefits No matter how big or small an organization may be, it is crucial to take proactive measures to monitor for 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

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.

Ransom ware - 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.

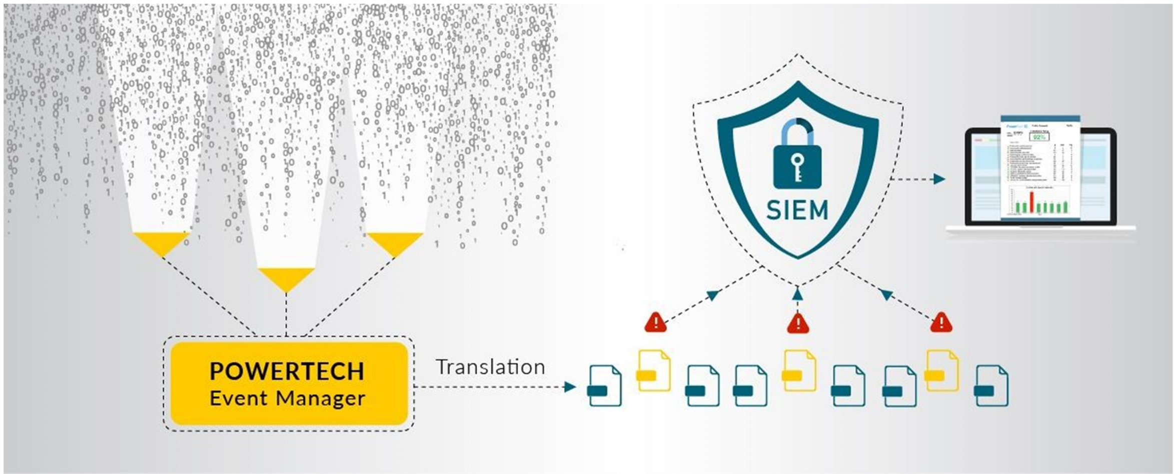
Foster knowledge sharing and best practices from incident investigations and analysis within the organization.

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.

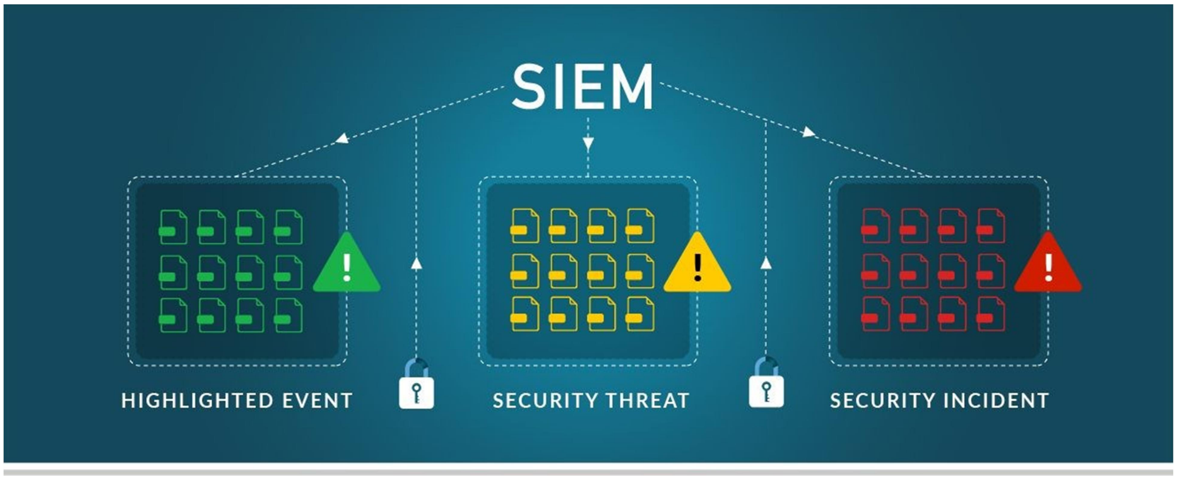
As a syslog server incessantly pings with every security notification, security teams can feel as though they are drowning in a sea of security warnings. Without a SIEM, it’s difficult to know which events are truly critical and which can be ignored. However, when a SIEM has been implemented, security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

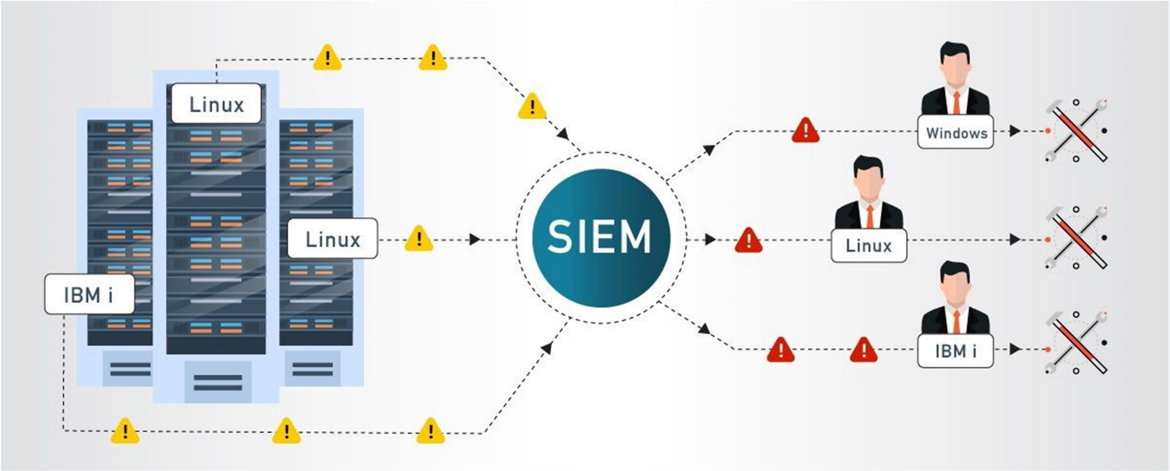
Translation



Prioritization


SIEM
HIGHLIGHTED EVENT
SECURITY THREAT
SECURITY INCIDENT

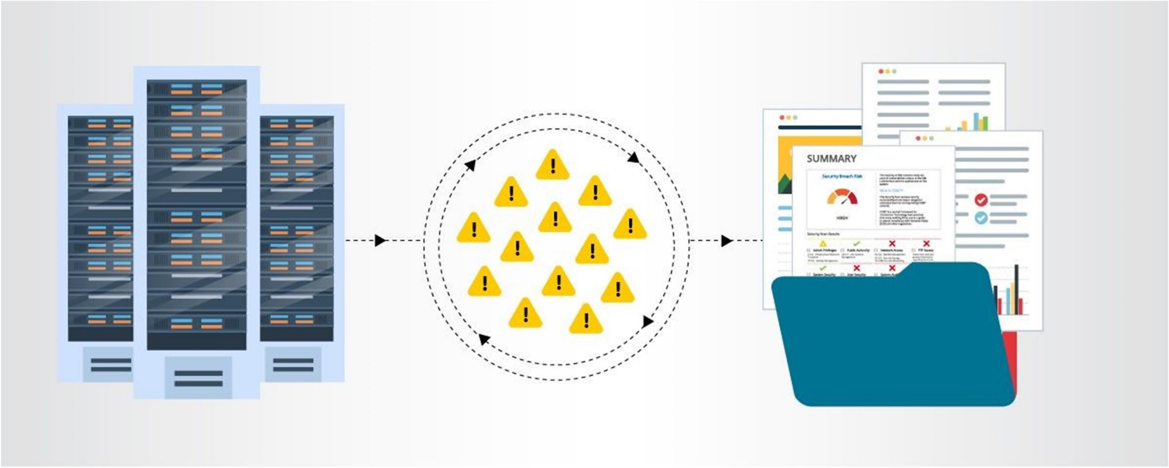
Escalation


Linux
Linux
IBM i
SIEM
Windows
Linux
IBM i

Analysis

SIEM
SUMMARY
Security Breach Risk
HIGH
REPORT

Compliance



- **MISP**

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

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

Features of MISP, the open source threat sharing platform

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Sharing with humans

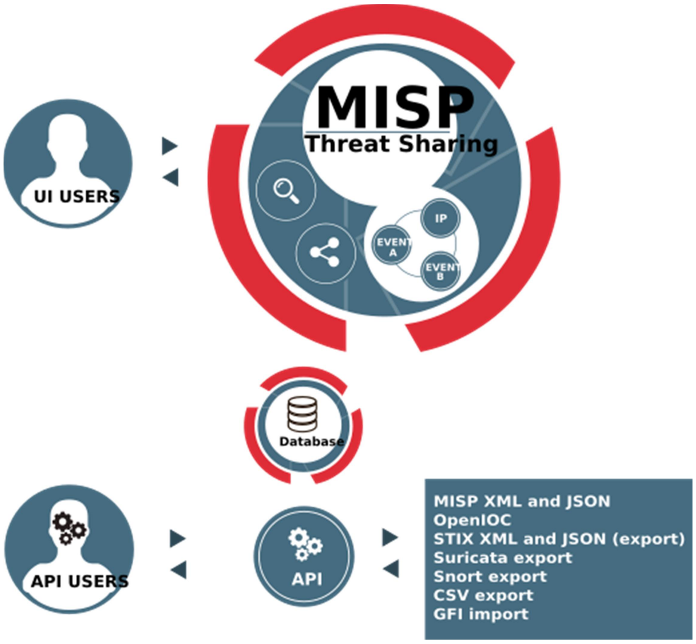
Data you store is immediately available to your colleagues and partners. Store the event id in your ticketing system or be informed by the signed and encrypted email notifications.

Sharing with machines

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

Collaborative sharing of analysis and correlation

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



- ## Your college network information

Tagore Engineering College

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

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

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

Assessment and Requirements Gathering:

Conduct a thorough assessment of the organization's currentcyber security 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 alignwith the organization's overall security strategy.

Budget and Resource Allocation:

- Determine the budget and resource requirements forestablishing 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 SOCteam.

- 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 prioritizationmechanisms.

Implement Monitoring and Alerting:

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

Incident Response and Escalation:

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

Training and Skill Development:

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

techniques, and relevant certifications.

Testing and Continuous Improvement:

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

Monitoring and Reporting:

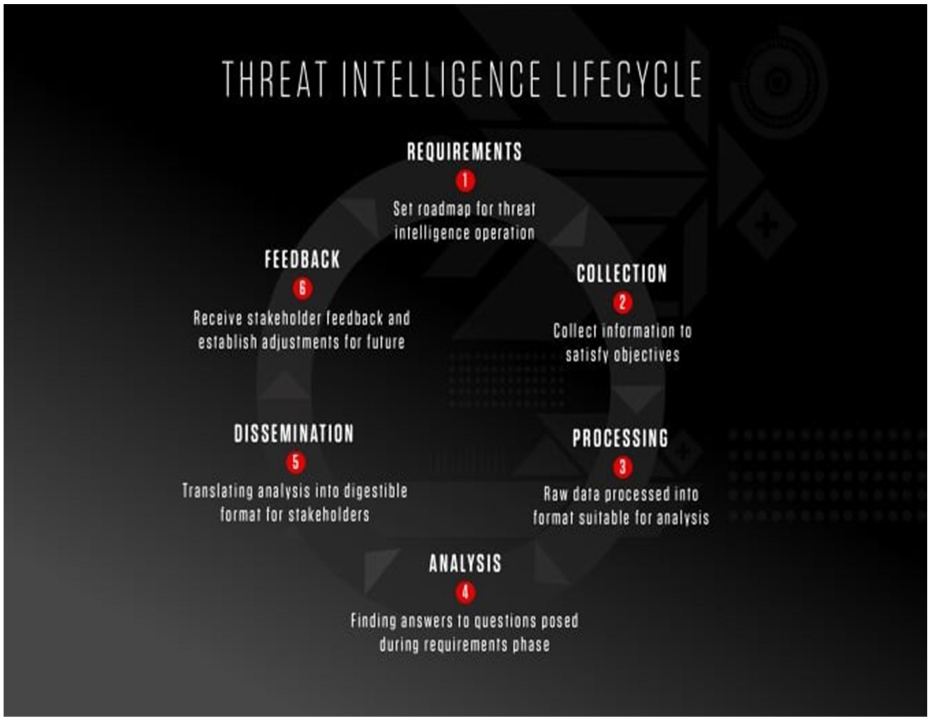
- Continuously monitor the SOC's performance and effectiveness in detecting and responding to security incidents.
- Generate regular reports and metrics to measure the SOC's performance and communicate its value to stakeholders.

Integration with IT and Business Functions:

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

- ### Threat intelligence

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


THREAT INTELLIGENCE LIFECYCLE
REQUIREMENTS
1
Set roadmap for threat intelligence operation
COLLECTION
2
Collect information to satisfy objectives
PROCESSING
3
Raw data processed into format suitable for analysis
ANALYSIS
4
Finding answers to questions posed during requirements phase
DISSEMINATION
5
Translating analysis into digestible format for stakeholders
FEEDBACK
6
Receive stakeholder feedback and establish adjustments for future

Threat intelligence is important for the following reasons:

- sheds light on the unknown, enabling security teams to make better decisions
- empowers cyber security stakeholders by revealing adversarialmotives 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 recovery time and costs, as well as collateral damage such as brand reputation, are kept at a minimum.

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 crucial stage of incident response is becoming ready for a foreseeable security breach. Policy, response plan/strategy, communication, documentation, identifying the CIRT members, access control, tools, and training should all be included in preparation as it aids organizations in deciding how well their CIRT will be able to respond to an incident.

Identification - The process of identification is how accidents are discovered, ideally quickly to enable quick action and hence minimize costs and losses. In order to detect incidents and ascertain their breadth, IT personnel accumulate events from log files, monitoring tools, error messages, intrusion detection systems, and firewalls.

Containment - Containing an occurrence as soon as it is discovered or recognized is of utmost importance. The fundamental goal of containment is to stop future damage from happening while also containing the existing damage (as was mentioned in step two, the earlier incidents are discovered, the sooner they may be contained to reduce damage). It's crucial to remember that all of the containment phase recommendations from SANS should be followed, especially in order to "prevent the destruction of any evidence that may be needed later for prosecution." Long-term containment, system backup, and short-term containment are some of these steps.

Eradication - Eradication is the stage of effective incident response where the threat is eliminated and affected systems are returned to their prior state, ideally with the least amount of data loss possible.

Recovery - The key activities connected with this stage of incident response are testing, monitoring, and validating systems as they are put back into production to ensure that they are not re-infected or compromised. Making decisions about whether to resume operations, testing and verifying the compromised systems, keeping an eye out for unusual behaviors, and using tools for testing, monitoring, and validating system behavior are all part of this phase.

Lessons Learned - The phase of incident response known as lessons learned is crucial because it aids in educating and enhancing future incident response efforts. In this step, organizations can add details to their incident response plans that might have been overlooked during the occurrence as well as comprehensive documentation to help with future problems. Lessons learned reports provide a thorough analysis of the entire incident and can be utilized as training materials for new CIRT members, benchmarks for comparison, or at recap sessions.

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.

- **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.

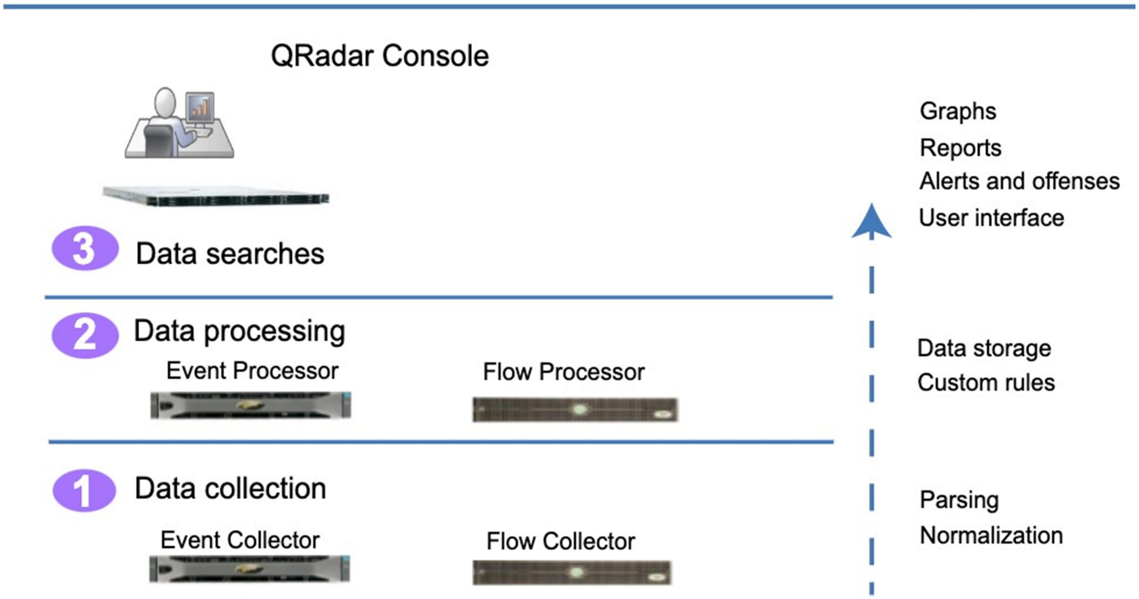


Figure 1. QRadar architecture

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:

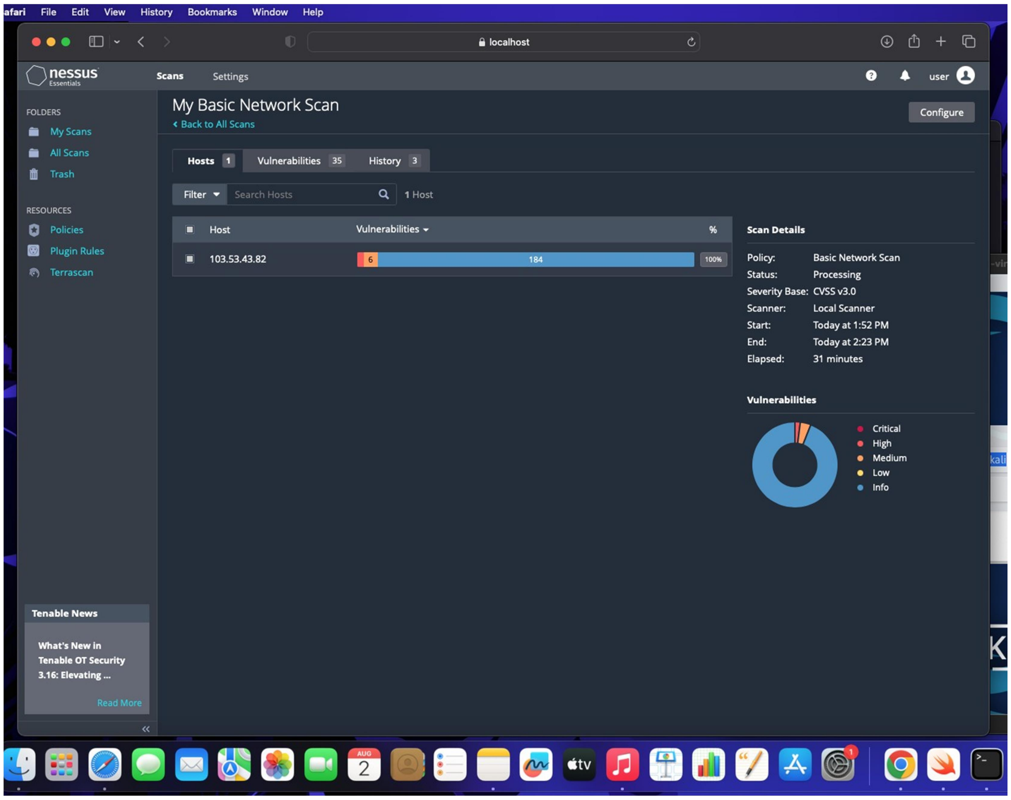
- Identification of Security Vulnerabilities
- Bug Detection and Resolution
- Validation of Functional Requirements
- Usability and User Experience Evaluation
- Performance and Load Testing Results
- Compatibility Testing Insights
- Accessibility Compliance
- Security Compliance and Risk Mitigation
-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



My Basic Network Scan

‹ Back to All Scans

Hosts 1 | Vulnerabilities 35 | History 3

1 Host

Host	Vulnerabilities	%
103.53.43.82	6 184	100%

Scan Details

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

Vulnerabilities

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.

Future Scope

Stage 1 :- Future scope of web application testing

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

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

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

Stage 3 :- future scope of SOC / SEIM

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

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

Topics explored :-

Introduction to cybersecurity, Growth of cybersecurity, Data sanity, Cloud service and cloud security, Data breach, Firewall, Antivirus, Digital ecosystem, Data protection, Types of cyber attacks, Essential terminology, Introduction to networking, Web APIs, web hooks, Web shell concepts, Vulnerability stack,OWASP top 10 applications, QRadar, SOC, SIEM

Tools explored :-

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