Title of the project :- Study of Top 10 OWASP vulnerabilities

Overview :-

When managing a website, it’s important to stay on top of the most critical security risks and vulnerabilities. The OWASP Top 10 is a great starting point to bring awareness to the biggest threats to websites in 2021.

OWASP stands for the Open Web Application Security Project, an online community that produces articles, methodologies, documentation, tools, and technologies in the field of web application security.

The OWASP Top 10 is a research-based document that raises awareness among developers, organizations, and security professionals on the most critical security risks facing web applications. The latest is the OWASP Top 10 vulnerabilities 2021, released in September 2021 after a 4-year gap. The OWASP Top 10 list is based on community research and provides data on common vulnerabilities and exploits.

Even more importantly, the OWASP Top 10 describes each category of application security risks, shows developers how to avoid them in the first place, and provides best practices for remediating them if they already exist.

List of teammates–

S.no	**name**	**collage**	**contact**
1	**Ankitkumar Rajeshkumar Thakkar**	**Institute of Technology, Nirma University**	**ankit.thakkar@nirmauni.ac.in**

List of Vulnerability Table –

S.no	**Vulnerability Name**	**CWE - No**
1	**Broken Access Control**	*CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')*
2	**Cryptographic Failures**	CWE-261 Weak Encoding for Password
3	**Injection**	*CWE-20: Improper Input Validation*
4	**Insecure Design**	CWE-266: Incorrect Privilege Assignment
5	**Security Misconfiguration**	CWE-260: Password in Configuration File
6	**Vulnerable and Outdated Components**	CWE-1104 Use of Unmaintained Third Party Components
7	**Identification and Authentication Failures**	CWE-259 Use of Hard-coded Password
8	**Software and Data Integrity Failures**	CWE-353: Missing Support for Integrity Check
9	**Security Logging and Monitoring Failures**	CWE-223: Omission of Security-relevant Information
10	**Server-Side Request Forgery**	CWE-918: Server-Side Request Forgery (SSRF)

REPORT:-

Vulnerability Name:- Broken Access Control

CWE : - *CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')*

OWASP/SANS Category:- A01:2021

Description:- The product uses external input to construct a pathname that is intended to identify a file or directory that is located underneath a restricted parent directory, but the product does not properly neutralize special elements within the pathname that can cause the pathname to resolve to a location that is outside of the restricted directory.

Business Impact:- Data is an important entity in digital communication. Exposure of sensitive information to an unauthorized user leads to data privacy issues and it severely affect the business.

Vulnerability Name:- Cryptographic Failures

CWE : - CWE-261 Weak Encoding for Password

OWASP/SANS Category:- A02:2021

Description:- Obscuring a password with a trivial encoding does not protect the password.
Business Impact:- Password is one of the credentials for providing authentication for the underlying system. Failure to protect password leads to unauthorized access to system(s) and further sensitive information.

Vulnerability Name:- Injection

CWE : - *CWE-20: Improper Input Validation*

OWASP/SANS Category:- A03:2021

Description:- The product receives input or data, but it does not validate or incorrectly validates that the input has the properties that are required to process the data safely and correctly.

Business Impact:- Improper input validation could lead to unauthorized access to the system that may contain sensitive information.

Vulnerability Name:- Insecure Design

CWE : - CWE-266: Incorrect Privilege Assignment

OWASP/SANS Category:- A04:2021

Description:- A product incorrectly assigns a privilege to a particular actor, creating an unintended sphere of control for that actor.

Business Impact:- Escalated privileged to an actor provides access control to data and/or system leads to unauthorized access to data and/or system increases attack surface.

Vulnerability Name:- Security Misconfiguration

CWE : - CWE-260: Password in Configuration File

OWASP/SANS Category:- A05:2021

Description:- The product stores a password in a configuration file that might be accessible to actors who do not know the password.

Business Impact:- This can result in compromise of the system for which the password is used. An attacker could gain access to this file and learn the stored password or worse yet, change the password to one of their choosing and make the system unavailable to legitimate users.

Vulnerability Name:- Vulnerable and Outdated Components

CWE : - CWE-1104 Use of Unmaintained Third Party Components

OWASP/SANS Category:- A06:2021

Description:- The product relies on third-party components that are not actively supported or maintained by the original developer or a trusted proxy for the original developer.

Business Impact:- Reliance on components that are no longer maintained can make it difficult or impossible to fix significant bugs, vulnerabilities, or quality issues. In effect, unmaintained code can become obsolete. This issue makes it more difficult to maintain the product, which indirectly affects security by making it more difficult or time-consuming to find and/or fix vulnerabilities. It also might make it easier to introduce vulnerabilities that could leads to attacks.

Vulnerability Name:- Identification and Authentication Failures

CWE : - CWE-259 Use of Hard-coded Password

OWASP/SANS Category:- A07:2021

Description:- The product contains a hard-coded password, which it uses for its own inbound authentication or for outbound communication to external components.

Business Impact:- A hard-coded password typically leads to a significant authentication failure that can be difficult for the system administrator to detect. Once detected, it can be difficult to fix, so the administrator may be forced into disabling the product entirely. In addition, if hard-coded password is accessible to an attacker that could lead to control over the device. Moreover, the system will be unavailable to the owner if password is changed by the attacker.

Vulnerability Name:- Software and Data Integrity Failures

CWE : - CWE-353: Missing Support for Integrity Check

OWASP/SANS Category:- A08:2021

Description:- The product uses a transmission protocol that does not include a mechanism for verifying the integrity of the data during transmission, such as a checksum.

Business Impact:- Data integrity is an important aspect of cyber security. Failure to have data integrity check during data transit and at rest does not provide guarantee about the correctness of the data.

Vulnerability Name:- Security Logging and Monitoring Failures

CWE : - CWE-223: Omission of Security-relevant Information

OWASP/SANS Category:- A09:2021

Description:- The product does not record or display information that would be important for identifying the source or nature of an attack, or determining if an action is safe.

Business Impact:- Omission of security-relevant information leads to failure to identify nature of an attack that could disallow to take appropriate counter measures to prevent similar attacks in future results in to such systems remains vulnerable to the same and/or similar attacks.

Vulnerability Name:- Server-Side Request Forgery

CWE: CWE-918: Server-Side Request Forgery (SSRF)

OWASP/SANS Category:- A10:2021

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:- SSRF will lead to servicing requests from unauthorized users and could provide sensitive information to them.

Stage 2

Overview :-

Nessus is a platform developed by Tenable that scans for security vulnerabilities in devices, applications, operating systems, cloud services and other network resources.

Originally launched as an open source tool in 1998, its enterprise edition became a commercial product in 2005. Nessus now encompasses several products that automate point-in-time vulnerability assessments of a network's attack surface, with the goal of enabling enterprise IT teams to stay ahead of cyber attackers by proactively identifying and fixing vulnerabilities as the tool discovers them, rather than after attackers exploit them.

Nessus identifies software flaws, missing patches, malware, denial-of-service vulnerabilities, default passwords and misconfiguration errors, among other potential flaws. When Nessus discovers vulnerabilities, it issues an alert that IT teams can then investigate and determine what -- if any -- further action is required.

Key features of Nessus

Nessus is known for its vast plugin database. These plugins are dynamically and automatically compiled in the tool to improve its scan performance and reduce the time required to assess, research and remediate vulnerabilities. Plugins can be customized to create specific checks unique to an organization's application ecosystem.

Target website — kgr.ac.in

Target ip address:- 184.168.115.31

List of vulnerability —

s.no	**Vulnerability name**	**Severity**	**plugins**
1	*Apache Server ETag Header Information Disclosure*	Medium	88098
2	Apache HTTP Server Version	Info	48204
3	SMTP Service Cleartext Login Permitted	Low	54582
4	SMTP Authentication Methods	Info	54580
5	SSL Certificate 'commonName' Mismatch	Info	54510
6	*SSL Cipher Suites Supported*	Info	21643
7	SSL Perfect Forward Secrecy Cipher Suites Supported	Info	57041
8	SSL Certificate Information	Info	10863
9	SSL Cipher Block Chaining Cipher Suites Supported	Info	70544
10	SSL Certificate Signed Using Weak Hashing Algorithm (Known CA)	Info	95631

11	SSL Root Certification Authority Certificate Information	Info	94761
12	SSL / TLS Versions Supported	Info	56984
13	SSL/TLS Recommended Cipher Suites	Info	156899
14	TLS Version 1.2 Protocol Detection	Info	136318
15	TLS Version 1.3 Protocol Detection	Info	138330
16	HyperText Transfer Protocol (HTTP) Information	Info	24260
17	HTTP Methods Allowed (per directory)	Info	43111

REPORT:-

Vulnerability Name:- *Apache Server ETag Header Information Disclosure*

severity : - Medium

Plugin:- 88098

Port :- 80 / tcp / www

Description:- The remote web server is affected by an information disclosure vulnerability due to the ETag header providing sensitive information that could aid an attacker, such as the inode number of requested files.

solution:- Modify the HTTP ETag header of the web server to not include file inodes in the ETag header calculation.

Business Impact::- The said vulnerability could lead to exposure of sensitive information to an attacker that results into data privacy and confidentiality issues.

Vulnerability Name:- *Apache HTTP Server Version*

severity : - Info

Plugin:- 48204

Port :- 80 / tcp / www

Description:- 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.

solution:- Apache HTTP Server should be updated to the latest version, if not updated.

Business Impact::- The existing Apache HTTP Server may have vulnerability that could be exploited by an attacker to perform attacks.

Vulnerability Name:- *SMTP Service Cleartext Login Permitted*

severity : - Low

Plugin:- 54582

Port :- 587 / tcp / smtp

Description:- The remote host is running an SMTP server that advertises that it allows cleartext logins over unencrypted connections. An attacker may be able to uncover user names and passwords by sniffing traffic to the server if a less secure authentication mechanism (i.e. LOGIN or PLAIN) is used.

solution:- Configure the service to support less secure authentication mechanisms only over an encrypted channel.

Business Impact::- Cleartext login information can be intercept by an attacker to obtain credentials. Further, the credentials to be used by the attacker to get sensitive information.

Vulnerability Name:- *SMTP Authentication Methods*

severity : - Info

Plugin:- 54580

Port :- 587 / tcp / smtp

Description:- The remote SMTP server advertises that it supports authentication.

solution:- Review the list of methods and whether they're available over an encrypted channel.

Business Impact::- The authentication methods advertised by SMTP server could be exploited to find vulnerabilities by an attacker which could be utilized to perform attacks.

Vulnerability Name:- *SSL Certificate 'commonName' Mismatch*

severity : - Info

Plugin:- 45410

Port :- 443 / tcp, 465 / tcp / smtp, 2083 / tcp / www

Description:- The service running on the remote host presents an SSL certificate for which the 'commonName' (CN) attribute does not match the hostname on which the service listens.

solution:- If the machine has several names, make sure that users connect to the service through the DNS hostname that matches the common name in the certificate.

Business Impact::- Personal information at risk from man-in-the-middle attacks. Reduction in trust as the site becomes insecure.

Vulnerability Name:- *SSL Cipher Suites Supported*

severity : - Info

Plugin:- 21643

Port :- 465 / tcp / smtp

Description:- This plugin detects which SSL ciphers are supported by the remote service for encrypting communications.

solution:- Disable weak cipher suits.

Business Impact::- Use of weak cipher suits give attackers to opportunity to break weak cipher.

Vulnerability Name:- *SSL Perfect Forward Secrecy Cipher Suites Supported*

severity : - Info

Plugin:- 57041

Port :- 443 / tcp

Description:- The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

solution:-

Business Impact::- Perfect forward secrecy is valuable against attackers who may be able to achieve READ access, but not WRITE access. In other words, an attacker who can undertake cryptanalysis of the underlying ciphers being used and modify the way the session key generator functions may be responsible for failed forward secrecy.

Vulnerability Name:- *SSL Certificate Information*

severity : - Info

Plugin:- 10863

Port :- 443 / tcp, 2083 / tcp / www

Description:- This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

solution:-

Business Impact::- If website is not secure, users data/information will be at risk.

Vulnerability Name:- SSL Cipher Block Chaining Cipher Suites Supported

severity : - Info

Plugin:- 70544

Port :- 443 / tcp

Description:- The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.

solution:-

Business Impact::- Improper p**adding could lead to CBC/ECB vulnerable.**

Vulnerability Name:- *SSL Certificate Signed Using Weak Hashing Algorithm (Known CA)*

severity : - Info

Plugin:- 95631

Port :- 443 / tcp

Description:- The remote service uses a known CA certificate in the SSL certificate chain that has been signed using a cryptographically weak hashing algorithm (e.g., MD2, MD4, MD5, or SHA1). These signature algorithms are known to be vulnerable to collision attacks (CVE-2004-2761, for example). An attacker can exploit this to generate another certificate with the same digital signature, allowing the attacker to masquerade as the affected service.

Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire after January 1, 2017 as vulnerable. This is in accordance with Google's gradual sunsetting of the SHA-1 cryptographic hash algorithm.

Note that this plugin will only fire on root certificates that are known certificate authorities as listed in Tenable Community Knowledge Article 000001752. That is what differentiates this plugin from plugin 35291, which will fire on any certificate, not just known certificate authority root certificates.

Known certificate authority root certificates are inherently trusted and so any potential issues with the signature, including it being signed using a weak hashing algorithm, are not considered security issues.

solution:- Contact the Certificate Authority to have the certificate reissued.

Business Impact::- Use of weak hashing algorithm can be exploited by attackers to generate another digital certificate with the same digital signature.

Vulnerability Name:- *SSL Root Certification Authority Certificate Information*

severity : - Info

Plugin:- 94761

Port :- 443 / tcp

Description:- The remote service uses an SSL certificate chain that contains a self-signed root Certification Authority certificate at the top of the chain.

solution:- Ensure that use of this root Certification Authority certificate complies with your organization's acceptable use and security policies.

Business Impact::- It can impact websites and users.

Vulnerability Name:- *SSL / TLS Versions Supported*
severity : - Info

Plugin:- 56984

Port :- 443 / tcp

Description:- This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.

solution:- Use latest version for TLS/SSL.

Business Impact::- The system could be vulnerable if latest version of TLS/SSL is not being used.

Vulnerability Name:- *SSL/TLS Recommended Cipher Suites*

severity : - Info

Plugin:- 156899

Port :- 443 / tcp

Description:- The remote host has open SSL/TLS ports which advertise discouraged cipher suites. It is recommended to only enable support for the following cipher suites:

TLSv1.3:

-	0x13,0x01	TLS13_AES_128_GCM_SHA256
-	0x13,0x02	TLS13_AES_256_GCM_SHA384
-	0x13,0x03	TLS13_CHACHA20_POLY1305_SHA256

TLSv1.2:

-	0xC0,0x2B	ECDHE-ECDSA-AES128-GCM-SHA256
-	0xC0,0x2F	ECDHE-RSA-AES128-GCM-SHA256
-	0xC0,0x2C	ECDHE-ECDSA-AES256-GCM-SHA384
-	0xC0,0x30	ECDHE-RSA-AES256-GCM-SHA384
-	0xCC,0xA9	ECDHE-ECDSA-CHACHA20-POLY1305
-	0xCC,0xA8	ECDHE-RSA-CHACHA20-POLY1305

This is the recommended configuration for the vast majority of services, as it is highly secure and compatible with nearly every client released in the last five (or more) years.

solution:- Only enable support for recommened cipher suites.

Business Impact::- Use of weak cipher suits could lead to security issues.

Vulnerability Name:- *TLS Version 1.2 Protocol Detection*

severity : - Info

Plugin:- 136318

Port :- 443 / tcp

Description:- The remote service accepts connections encrypted using TLS 1.2.

solution:- Use latest TLS version supported by the system

Business Impact::- This protocol has significant vulnerabilities, most of which affect TLS v1. 2 and older versions, could be exploited by attackers.

Vulnerability Name:- *TLS Version 1.3 Protocol Detection*

severity : - Info

Plugin:- 138330

Port :- 465 / tcp / smtp

Description:- The remote service accepts connections encrypted using TLS 1.3.

solution:- PQC algorithms should be adopted in TLS.

Business Impact::- The security of the TLS Handshake as defined in TLS 1.2 or TLS 1.3 is affected by the quantum threat.

Vulnerability Name:- *HyperText Transfer Protocol (HTTP) Information*

severity : - Info

Plugin:- 24260

Port :- 80 / tcp / www

Description:- This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive is enabled, etc...

This test is informational only and does not denote any security problem.

solution:-

Business Impact::-

Vulnerability Name:- *HTTP Methods Allowed (per directory)*

severity : - Info

Plugin:- 43111

Port :- 80 / tcp / www

Description:- By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.

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.

As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes' in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.

Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

solution:- NA

Business Impact::- NA

Stage 3

Report

Tittle :- Study of SOC and SIEM

Below are side headings we need to write at least a paragraph for each what we understood from each topic:-

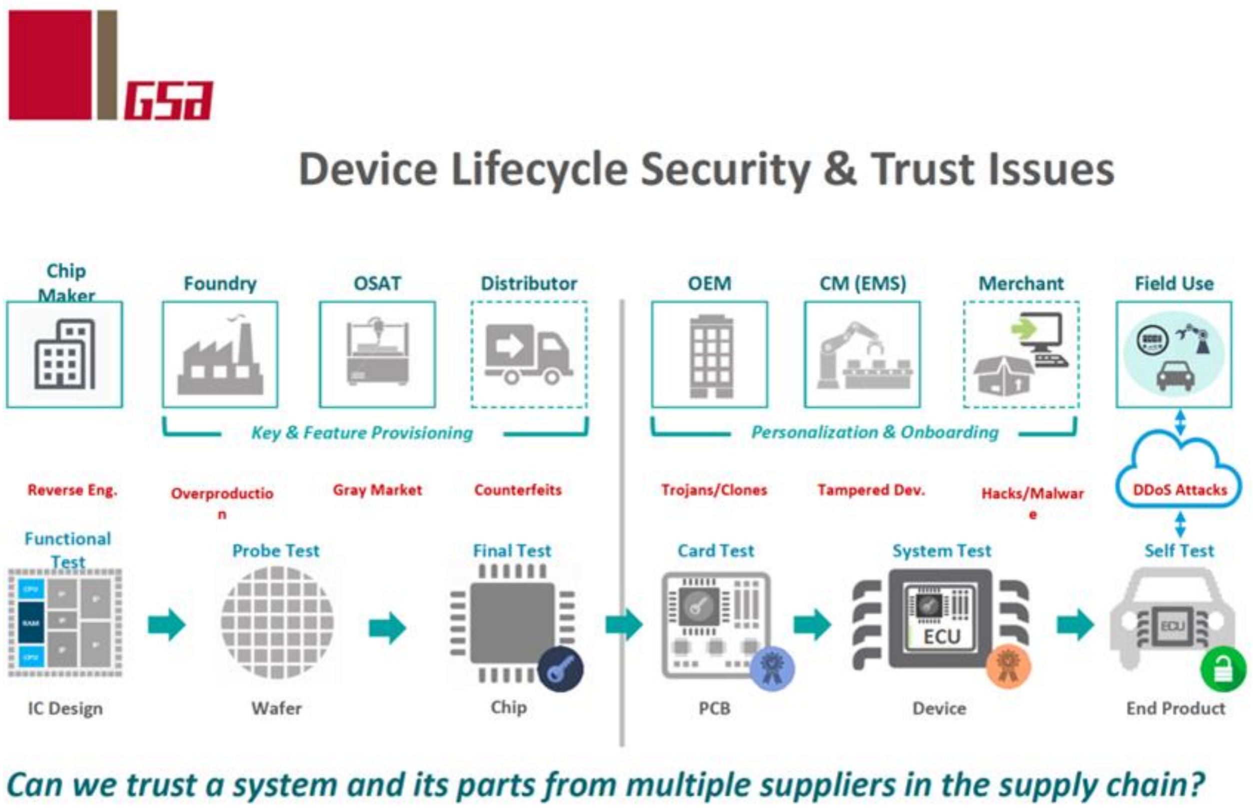
- **SOC: A security operations center (SOC) improves an organization's threat detection, response and prevention capabilities by unifying and coordinating all cybersecurity technologies and operations.**

- **A SOC—usually pronounced "sock" and sometimes called an information security operations center, or ISOC—is an in-house or outsourced team of IT security professionals dedicated to monitoring an organization's entire IT infrastructure 24x7. Its mission is to detect, analyze and respond to security incidents in real-time. This orchestration of cybersecurity functions allows the SOC team to maintain vigilance over the organization's networks, systems and applications and ensures a proactive defense posture against cyber threats.**

  The SOC also selects, operates and maintains the organization's cybersecurity technologies and continually analyzes threat data to find ways to improve the organization's security posture.

  When not on premises, a SOC is often part of outsourced managed security services (MSS) offered by a managed security service provider (MSSP). The chief benefit of operating or outsourcing a SOC is that it unifies and coordinates an organization's security system, including its security tools, practices and response to security incidents. This usually results in improved preventative measures and security policies, faster threat detection, and faster, more effective and more cost-effective response to security threats. A SOC can also improve customer confidence, and simplify and strengthen an organization's compliance with industry, national and global privacy regulations.

- **SOC – cycle:**



Device Lifecycle Security & Trust Issues

Chip Maker
Foundry
OSAT
Distributor
OEM
CM (EMS)
Merchant
Field Use

Key & Feature Provisioning
Personalization & Onboarding

Reverse Eng.
Overproductio n
Gray Market
Counterfeits
Trojans/Clones
Tampered Dev.
Hacks/Malwar e
DDoS Attacks

Functional Test
Probe Test
Final Test
Card Test
System Test
Self Test

ECU

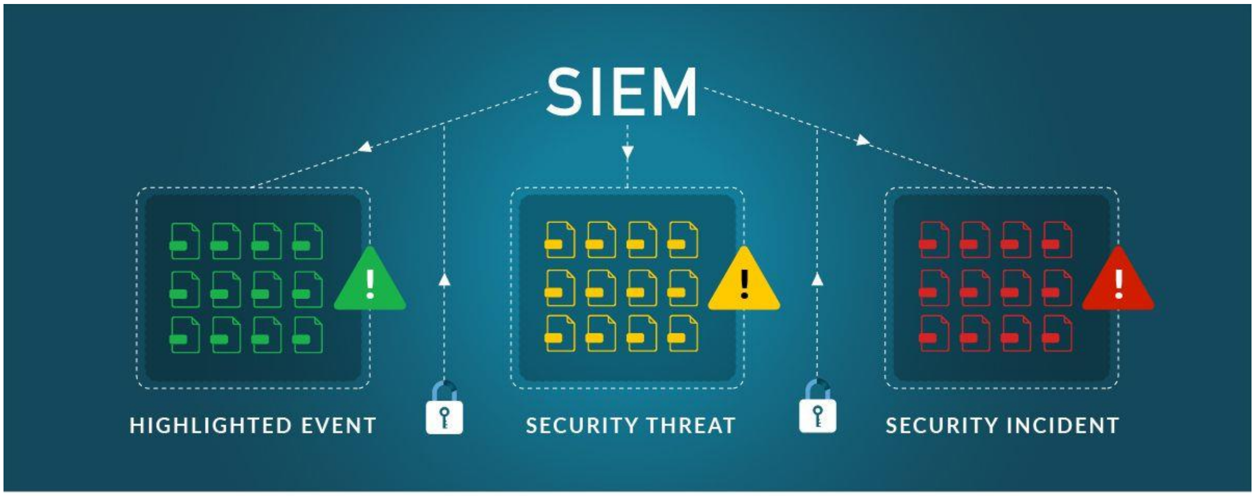
IC Design
Wafer
Chip
PCB
Device
End Product

Can we trust a system and its parts from multiple suppliers in the supply chain?

- **Siem**
- Security information and event management, 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.
- The original SIEM platforms were log management tools. They combined security information management (SIM) and security event management (SEM) functions. These platforms enabled real-time monitoring and analysis of security-related events.

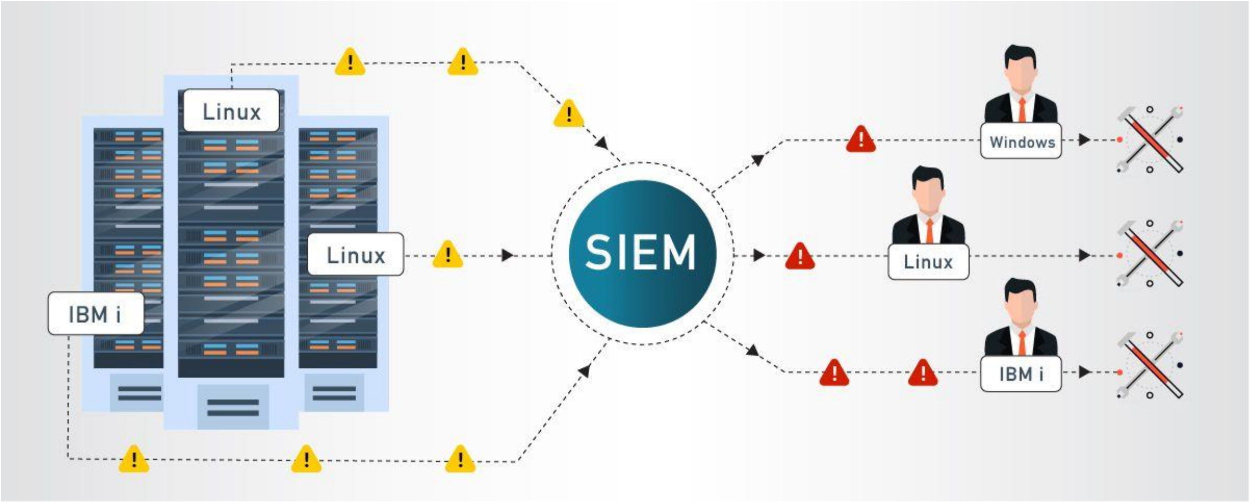
  Also, they facilitated tracking and logging of security data for compliance or auditing purposes. Gartner coined the term SIEM for the combination of SIM and SEM technologies in 2005.
- Over the years, SIEM software has evolved to incorporate user and entity behavior analytics (UEBA), as well as other advanced security analytics, AI and machine learning capabilities for identifying anomalous behaviors and indicators of advanced threats. Today SIEM has become a staple in modern-day security operation centers (SOCs) for security monitoring and compliance management use cases.

- **Siem Cycle**



A SIEM provides built-in guidance for which events need to be dealt with immediately. However, all events can be classified in a variety of ways. A SIEM is highly configurable and can indicate how serious the event is to varying degrees of specificity. For example, it may be tied to a specific regulatory framework or placed into general categories of severity, such as:

- **Highlighted Event** – An event noted only for its irregularity. May or may not need further action depending on further analysis.
- **Security Threat** – A security threat is an event that may not be posing immediate risk but should be investigated as soon as possible.
- **Security Incident** – A security threat that indicates an imminent threat, or an attack that is taking place. Requires immediate action.



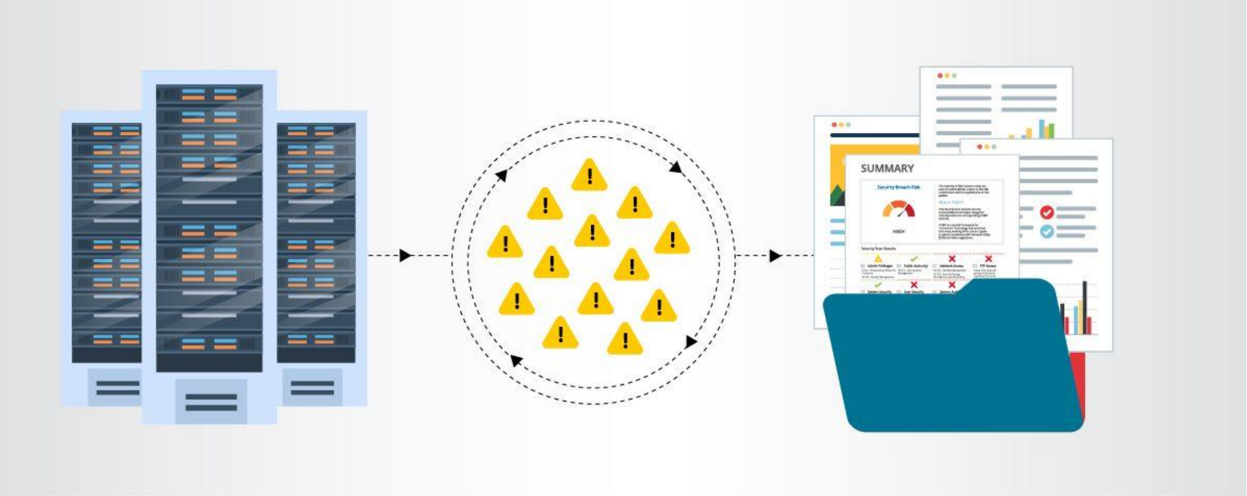
A SIEM will generate alerts and send out notifications to exactly the right security team members when a threat requires action. These real time alerts allow staff to act quickly to prevent or neutralize risks.

For example, if a SIEM sent out an alert that a virus has been detected on a Linux server, endangering sensitive data, an alert would be sent to the Linux admin who is best equipped to quarantine the server to prevent further infection until the virus is removed.

Alternately, a SIEM could launch an alert if someone was attempting to access a privileged account with multiple password guesses. A security admin or an automated response could lock out the account until additional verification was made, or security analysts made further investigations.

SIEM
SUMMARY
Security Breach Risk
HIGH
REPORT

Security teams can use a SIEM to complete a thorough examination and analysis. As discussed above, raw data is stored from an event, and a SIEM can also generate reports with varying degrees of detail that document the lifecycle of an event. Security teams can annotate these reports with notes that record their investigation, as well as recommendations on actions to take for similar events. These reports become critical documentation that demonstrates an overall picture of an organization’s cybersecurity.



Raw data flagged when a security event occurs is kept on record for a given period of time to maintain compliance for retention regulations. Reports generated by SIEMs create a complete audit trail, keeping an organization compliant with little effort.

While SIEMs provide a clear path to dealing with security threats, saving time is the biggest advantage that a SIEM solution provides. Security Teams are perpetually busy protecting their organization's data, and time spent on tasks that could be automated is time wasted. Not only that, it is time that is often desperately needed to prevent or battle harmful threats that could cost an organization time, money, and even their reputation.

MISP: MISP is an open source software solution for collecting, storing, distributing and sharing cyber security indicators and threats about cyber security incidents analysis and malware analysis. MISP is designed by and for incident analysts, security and ICT professionals or malware reversers to support their day-to-day operations to share structured information efficiently.

The objective of MISP is to foster the sharing of structured information within the security community and abroad. MISP provides functionalities to support the exchange of information but also the consumption of said information by Network Intrusion Detection Systems (NIDS), LIDS but also log analysis tools, SIEMs.

- **Your college network information**
  ISP Switch<-> Firewall <->VLAN<->Switches<->Machines
- **How you think you deploy soc in your college**
  SOC should be integrated with firewall or as a separate entity to detect and recover threats.

- **Threat intelligence**

Threat Intelligence is evidence-based information about cyber attacks that cyber security experts organize and analyze. This information may include:

- Mechanisms of an attack
- How to identify that an attack is happening
- Ways different types of attacks might affect the business
- Action-oriented advice about how to defend against attacks

- **Incident response:**

Incident response (IR) is the effort to quickly identify an attack, minimize its effects, contain damage, and remediate the cause to reduce the risk of future incidents.

Almost every company has, at some level, a process for incident response. However, for those companies looking to establish a more formal process, the pertinent questions one must ask are:

1. What are the steps to activate the responsible parties involved in responding to an incident should one appear?
2. How comprehensive and specific should your response plan be?
3. Do you have enough people (and the right people) to respond appropriately?
4. What are your acceptable SLAs for responding to an incident and returning to normal operations?

- **Qradar & understanding about tool**
  IBM® QRadar® is a network security management platform that provides situational awareness and compliance support. QRadar uses a combination of flow-based network knowledge, security event correlation, and asset-based vulnerability assessment.

A great way to get started is to try out the IBM QRadar Experience Center app, which is supported on QRadar V7.3.1 or later. The app comes with several predefined security use cases that you can run to demonstrate how QRadar can help you detect security threats.
Watch QRadar in action as the simulation data is sent to QRadar from the app. After you watch the video tutorial that explains the use case, explore the corresponding QRadar content, and see how you might investigate such a threat in your own environment.

Use the app to upload and play your own logs in QRadar. Access the IBM Security Learning Academy and other resources to explore how you can use the powerful threat detection capabilities of QRadar to protect your network.

- **Log activity**
  In IBM QRadar, you can monitor and display network events in real time or perform advanced searches.
- **Network activity**
  In IBM QRadar you can investigate the communication sessions between two hosts.
- **Assets**
  IBM QRadar automatically creates asset profiles by using passive flow data and vulnerability data to discover your network servers and hosts.
- **Offenses**
  In IBM QRadar you can investigate offenses to determine the root cause of a network issue.
- **Reports**
  In IBM QRadar you can create custom reports or use default reports.
- **Data collection**
  IBM QRadar accepts information in various formats and from a wide range of devices, including security events, network traffic, and scan results.
- **QRadar rules**
  Rules perform tests on events, flows, or offenses. If all the conditions of a test are met, the rule generates a response.

- **Supported web browsers**
  For the features in IBM QRadar products to work properly, you must use a supported web browser.
- **Apps overview**
  IBM QRadar apps are created by developers. After a developer creates an app, IBM certifies and publishes it in the IBM Security App Exchange. QRadar administrators can then browse and download the apps and then install the apps into QRadar to address specific security requirements.
- **Apps that are installed by default with QRadar**
  To improve workflow, some apps that were previously only available on the IBM Security App Exchange are now installed by default.

Conclusion :-

- **Stage 1 :- what you understand from Web application testing .**
  Web application testing presents vulnerability along with severity, if present.
- **Stage 2 :- what you understand from the nessus report .**
  - **NESSUS is a web application testing tool that provides report about the different vulnerability present in the identified web application with severity, plugin needed, description of the vulnerability, solutions, if any.**
- **Stage 3 :- what you understand from SOC / SEIM / Qradar Dashboard .**

Use the Dashboard tab, which is the default view when you log in to IBM QRadar, to focus on specific areas of your network security. The workspace supports multiple dashboards on which you can display your views of network security, activity, or data that is collected.

Future Scope :-

- **Stage 1 :- future scope of web application testing**
  - **In the growing era of digital life, web application is one of the important ways to connect with different users. With increase in the usage of digital devices, internet, various tools and hardware capabilities, various types of attacks possible. Hence, web application testing will always be needed in future.**
- **Stage 2 :- future scope of testing process you understood .**
  - **The testing process that we understood as of day should be refined over the period of time by having knowledge about newer attacks and how to avoid/minimize and mitigate if needed.**
- **Stage 3 :- future scope of SOC / SEIM**

SOC and SEIM is a useful tool for identifying and recovering from vulnerability. It helps security administrator. However, the functionality of SOC/SEIM depends on the sanitized data presented to it. Hence, it is difficult to detect "ZERO DAY" attacks. Also, the knowledge that the tool has may not be accurate which could lead to increase in False Negative and False Positives that needs to be taken care.

Topics explored :-
Kali Linux, NESSUS, QRADAR, SIEM, SOC, Digital Forensics, NMAP
Tools explored :-
Kali Linux, NESSUS, QRADAR, SIEM, SOC, NMAP