**Title of the project:** Addressing Data Integrity and Untrusted Search Path Vulnerabilities for Airline Websites.

## Overview

The project seeks to diminish CWE-426 vulnerabilities within the airline industry's web applications. CWE-426 depends on the insecure configuration management, guiding attackers to leverage poor validation of search paths at runtime to execute malicious code; this has serious associated risks, ranging from unauthorized data access to privilege escalation, finally resulting in an operational disruption. This project involves detailed research into the vulnerability assessment, coupled with corresponding proactive mitigation strategies that can be implemented to set up safeguards for airline websites against such vulnerabilities. This way, the project contributes to cyber resilience within the context of the airline industry by entrenching secure configuration practices, rigorous input validation, and frequent security audits in the protection of critical systems and passenger data.

The "Addressing Data Integrity and Untrusted Search Path Vulnerabilities for Airline Websites" project is one we believe to be quite important, targeted at a particular kind of cyber security threat that could have a high impact on the airline industry. This CWE-426-classified untrusted search path vulnerability brings about critical danger in probably letting attackers break into vital systems and obtain sensitive data that may distort airline operations. This approach in detecting, analyzing, and mitigating these vulnerabilities is in itself commendable for the resilience of airline websites against such threats. The project applies state-of-the-art security measures through deep vulnerability assessments and proposes effective mitigation strategies for identified risks, guaranteeing passenger data safety and operational continuity, and it considerably contributes to general cybersecurity practices within the airline industry. The proactive stance is such that, with a world

that's increasingly digital and connected, threats to cybersecurity just keep on evolving.

**Team Name - Phantom Hacker**

**List of teammates**

| **S.no** | **Name** | **College** | **Contact** |
|---|---|---|---|
| 1 | Dr. Pooja chaturvedi | Nirma University | pooja.chaturvedi@nirmauni.ac.in |
| 2 | Dr. Aparna Kumari | Nirma University | aparna.kumari@nirmauni.ac.in- |
| 3. | Prof. Deepika Bishnoi | Nirma University | deepika.bishnoi@nirmauni.ac.in |
| 4. | Prof. Sanjana | JG University | jayswalsanjana785@gmail.com |

**List of Vulnerability Table**

| **S.no** | **Vulnerability Name** | **CWE - No** |
|---|---|---|
| 1 | Insufficient Verification of Data Authenticity | CWE-345 |
| 2 | Missing Support for Integrity Check | CWE-353 |
| 3 | Untrusted Search Path | CWE-426 |
| 4 | Download of Code Without Integrity Check | CWE-494 |

| | | |
|---|---|---|
| 5 | Deserialization of Untrusted Data | CWE-502 |
| 6 | Reliance on Cookies without Validation and Integrity Checking | CWE-565 |
| 7 | Reliance on Cookies without Validation and Integrity Checking in a Security Decision | CWE-784 |
| 8 | Inclusion of Functionality from Untrusted Control Sphere | CWE-829 |
| 9 | Inclusion of Web Functionality from an Untrusted Source | CWE-830 |
| 10 | Improperly Controlled Modification of Dynamically-Determined Object Attributes | CWE-915 |

**A detailed report on "Software and Data Integrity Failures - *(1354)*" vulnerabilities.**

**REPORT:-**

**Vulnerability Name:- Insufficient Verification of Data Authenticity**

**CWE : -** CWE-345

**OWASP/SANSCategory:- A08:2021**

**Description:-**This vulnerability does not let application/product to sufficiently verify the origin or authenticity of data, in a way that causes it to accept invalid data.

**Business Impact**: An attacker who controls user input or is able to influence network connectivity can perform a variety of actions and gain access to

potentially sensitive information or event execute arbitrary code on a vulnerable system.

**Arbitrary Code Execution:** This is a vulnerability that enables attackers to execute malicious code in the affected system.

**Privilege Escalation:** Depending on how files within the search path are configured and their permissions, privilege escalation may well occur.

**Data Corruption:** Malicious code run through the untrusted search path could result in data sensitive in nature being revealed or critical files being overwritten.

**Service Disruption:** An exploit of this vulnerability may result in service disruption or downtime, thus impacting the normal running of business operations.

**Vulnerability Name:- Missing Support for Integrity Check**

**CWE : - *353***

**OWASP/SANSCategory:- A08:2021**

**Description:-**If integrity check values or "checksums" are omitted from a protocol, there is no way of determining if data has been corrupted in transmission. The lack of checksum functionality in a protocol removes the first application-level check of data that can be used. The end-to-end philosophy of checks states that integrity checks should be performed at the lowest level that they can be completely implemented. Excluding further sanity checks and input validation performed by applications, the protocol's checksum is the most important level of checksum, since it can be performed

more completely than at any previous level and takes into account entire messages, as opposed to single packets.

**Business Impact**: A lack of data integrity exposes businesses and consumers to numerous risks – from falsified or incomplete patient records to unauthorized financial account changes and transactions, such as denying access to the real owner of the monies or moving it around to fund terrorist activities. Unfortunately, the extent of some data breaches only becomes evident after customers have experienced the negative consequences attached to such breaches.

**Vulnerability Name:- Untrusted Search Path**

**CWE : -426**

**OWASP/SANSCategory:- A08:2021**

**Description:-**The product searches for critical resources using an externally-supplied search path that can point to resources that are not under the product's direct control.

**Business Impact**: Attackers can exploit an untrusted search path vulnerability by modifying the environment variable or configuration file to point to a directory controlled by the attacker. This allows the attacker to execute malicious code or install malware on the system, potentially leading to a compromise of sensitive data or complete control over the affected system.

**Vulnerability Name:- Download of Code Without Integrity Check**

**CWE : -494**

**OWASP/SANSCategory:- A08:2021**

**Description:-**The product downloads source code or an executable from a remote location and executes the code without sufficiently verifying the origin and integrity of the code.

**Business Impact**: Code from untrusted sources can introduce malware, which can compromise sensitive data, disrupt operations, and require extensive remediation efforts. Unverified code might contain security vulnerabilities or backdoors that attackers can exploit, leading to unauthorized access or control over systems. Malicious code can lock down critical business systems and demand ransom payments for their release, leading to significant financial losses and operational disruption.

**Vulnerability Name:- Deserialization of Untrusted Data**

**CWE : -502**

**OWASP/SANSCategory:- A08:2021**

**Description:-**The product deserializes untrusted data without sufficiently verifying that the resulting data will be valid.

**Business Impact**:Untrusted data can be manipulated to execute arbitrary code during deserialization, allowing attackers to take control of the system. Deserialization vulnerabilities can be exploited to access sensitive information, leading to data breaches and loss of confidential data.

**Vulnerability Name:- Reliance on Cookies without Validation and Integrity Checking**

**CWE : -565**

**OWASP/SANSCategory:- A08:2021**

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

**Business Impact**: Without validation and integrity checking, cookies can be intercepted and manipulated, allowing attackers to hijack user sessions and gain unauthorized access to user accounts and sensitive information.

**Vulnerability Name:- Reliance on Cookies without Validation and Integrity Checking in a Security Decision**

**CWE : -784**

**OWASP/SANSCategory:- A08:2021**

**Description:-**The product uses a protection mechanism that relies on the existence or values of a cookie, but it does not properly ensure that the cookie is valid for the associated user. Attackers can easily modify cookies, within the browser or by implementing the client-side code outside of the browser. Attackers can bypass protection mechanisms such as authorization and authentication by modifying the cookie to contain an expected value.

**Business Impact**:Reliance on cookies without validation and integrity checking in airline websites can lead to serious security vulnerabilities, such as session hijacking and unauthorized access. This can result in the theft of sensitive customer information, including personal data and payment details,

causing significant financial losses and legal repercussions. Additionally, the breach of customer trust can damage the airline's reputation, leading to decreased customer loyalty and a loss of market share. Operational disruptions and the need for extensive security overhauls further add to the financial and resource burden on the airline.

**Vulnerability Name:- Inclusion of Functionality from Untrusted Control Sphere**

**CWE : -829**

**OWASP/SANSCategory:- A08:2021**

**Description:-**The product imports, requires, or includes executable functionality (such as a library) from a source that is outside of the intended control sphere. When including third-party functionality, such as a web widget, library, or other source of functionality, the product must effectively trust that functionality. Without sufficient protection mechanisms, the functionality could be malicious in nature (either by coming from an untrusted source, being spoofed, or being modified in transit from a trusted source). The functionality might also contain its own weaknesses, or grant access to additional functionality and state information that should be kept private to the base system, such as system state information, sensitive application data, or the DOM of a web application.

This might lead to many different consequences depending on the included functionality, but some examples include injection of malware, information exposure by granting excessive privileges or permissions to the untrusted functionality, DOM-based XSS vulnerabilities, stealing user's cookies, or open redirect to malware (CWE-601).

**Business Impact**:Improperly controlled modification of dynamically-determined object attributes can lead to severe security vulnerabilities, allowing attackers to manipulate critical data and application behavior. This can result in unauthorized access to sensitive information, financial fraud, and disruption of services. The consequences include loss of customer trust, significant financial costs associated with breach mitigation and legal penalties, and potential operational downtime. Such vulnerabilities also expose the company to reputational damage, adversely affecting competitive positioning and long-term business sustainability.

**Vulnerability Name:- Inclusion of Web Functionality from an Untrusted Source**

**CWE : -830**

**OWASP/SANSCategory:- A08:2021**

**Description:-**The product includes web functionality (such as a web widget) from another domain, which causes it to operate within the domain of the product, potentially granting total access and control of the product to the untrusted source.

**Business Impact**:Inclusion of web functionality from an untrusted source can lead to significant security breaches, resulting in data theft, malware infections, and severe reputational damage. This undermines customer trust, causes financial losses through mitigation costs and regulatory fines, and disrupts airline operations, ultimately impacting market competitiveness and long-term revenue.

**Vulnerability Name:- Improperly Controlled Modification of Dynamically-Determined Object Attributes**

**CWE : -915**

**OWASP/SANSCategory:- A08:2021**

**Description:-**The product receives input from an upstream component that specifies multiple attributes, properties, or fields that are to be initialized or updated in an object, but it does not properly control which attributes can be modified.

**Business Impact**: The product searches for critical resources using an externally-supplied search path that can point to resources that are not under the product's direct control.

**Example:**

This code prints all of the running processes belonging to the current user “test” in programming language PHP

```
//assume getCurrentUser() returns a username that is
guaranteed to be alphanumeric (avoiding CWE-78)
$userName = getCurrentUser();
$command = 'ps aux | grep ' . $userName;
system($command);
```

If invoked by an unauthorized web user, it is providing a web page of potentially sensitive information on the underlying system, such as command-line arguments (CWE-497). This program is also potentially vulnerable to a PATH based attack (CWE-426), as an attacker may be able to create malicious versions of the ps or grep commands. While the program does not explicitly raise privileges to run the system commands, the PHP interpreter may by default be running with higher privileges than users.

**References**


- [REF-207] John Viega and Gary McGraw. "Building Secure Software: How to Avoid Security Problems the Right Way". Chapter 12, "Trust Management and Input Validation." Pages 317-320. 1st Edition. Addison-Wesley. 2002.

- [REF-18] Secure Software, Inc.. "The CLASP Application Security Process". 2005. <https://cwe.mitre.org/documents/sources/TheCLASPApplicationSecurityProcess.pdf>.

- [REF-62] Mark Dowd, John McDonald and Justin Schuh. "The Art of Software Security Assessment". Chapter 10, Process Attributes, page 603. 1st Edition. Addison Wesley. 2006.

- [REF-176] Michael Howard and David LeBlanc. "Writing Secure Code". Chapter 8, "Canonical Representation Issues." Page 229. 1st Edition. Microsoft Press. 2001-11-13.

- [REF-7] Michael Howard and David LeBlanc. "Writing Secure Code". Chapter 11, "Don't Trust the PATH - Use Full Path Names" Page 385. 2nd Edition. Microsoft Press. 2002-12-04. <https://www.microsoftpressstore.com/store/writing-secure-code-9780735617223>.

# Stage 2

**Overview :-**

- Nessus Professional, the industry's most widely deployed vulnerability assessment solution helps you reduce your organization's attack surface and ensure compliance. Nessus features high-speed asset discovery, configuration auditing, target profiling, malware detection, sensitive data discovery and more. Nessus supports more technologies than competitive solutions, scanning operating systems, network devices, next generation firewalls, hypervisors, databases, web servers and critical infrastructure for vulnerabilities, threats and compliance violations. With the world's largest continuously updated library of vulnerability and configuration checks, and the support of Tenable's expert vulnerability research team, Nessus sets the standard for vulnerability scanning speed and accuracy.

- Key Benefits :
  • Reduce the attack surface: Prevents attacks by identifying vulnerabilities that need to be addressed
  • Comprehensive: Meets the widest range of compliance and regulatory standards
  • Scalable: Start with a Nessus Professional single user license and move to Nessus Manager or Tenable.io as your vulnerability management needs increase
  • Constantly updated: New content continually being added by the Tenable research team
  • Highly accurate scanning with low false positives
  • Scalable to hundreds-of-thousands of systems
  • Easy deployment and maintenance
  • Low cost to administer and operate


**Figure 1.**

Discovery: Accurate, high-speed asset discovery • Scanning: Vulnerability scanning (including IPv4/IPv6/hybrid networks) o Un-credentialed vulnerability discovery o Credentialed scanning for system hardening and missing patches o Meets PCI DSS requirements for internal vulnerability scanning.

Coverage: Broad asset coverage and profiling o Network devices: firewalls/routers/switches (Juniper, Check Point, Cisco, Palo Alto Networks), printers, storage o Offline configuration auditing of network devices

**Target website:- Make my trip**

**Target ip address:- 3.33.210.219**

**List of vulnerability**

| s.no | Vulnerability name | Severity | plugins |
|---|---|---|---|
| **1** | Insufficient Verification of Data Authenticity | high | 190360 |
| **2** | Missing Support for Integrity Check | high | 119811 |
| **3** | Untrusted Search Path | high | 35674 |
| **4** | Download of Code Without Integrity Check | high | 502037 |
| **5** | Deserialization of Untrusted Data | critical | 173829 |
| **6** | Reliance on Cookies without Validation and Integrity Checking | high | 33929 |
| **7** | Reliance on Cookies without Validation and Integrity Checking in a Security Decision | high | 54887 |
| **8** | Inclusion of Functionality from Untrusted Control Sphere | critical | 500630 |
| **9** | Inclusion of Web Functionality from an Untrusted Source | high | 11850 |
| **10** | Improperly Controlled Modification of Dynamically-Determined Object Attributes | high | 98024 |

**REPORT:-**

**Vulnerability Name:-** Insufficient Verification of Data Authenticity

**Severity : - High**

**Plugin:- 190360**

**Description:-**

**Solution:- The only way to protect application against this weakness is to perform additional checks on data authenticity. When developing the application consider all possible input data sources and use unique tokens to validate user input, always verify client and server identity.**

**Business Impact**::- An attacker who controls user input or is able to influence network connectivity can perform a variety of actions and gain access to potentially sensitive information or even execute arbitrary code on vulnerable systems.

**Vulnerability Name:-** Missing Support for Integrity Check

**Severity : - High**

**Plugin:- 119811**

**Description:- If integrity check values or "checksums" are omitted from a protocol, there is no way of determining if data has been corrupted in transmission. The lack of checksum functionality in a protocol removes the first application-level check of data that can be used. The end-to-end**

**philosophy of checks states that integrity checks should be performed at the lowest level that they can be completely implemented. Excluding further sanity checks and input validation performed by applications, the protocol's checksum is the most important level of checksum, since it can be performed more completely than at any previous level and takes into account entire messages, as opposed to single packets.**

**Solution:-**

**Add an appropriately sized checksum to the protocol, ensuring that data received may be simply validated before it is parsed and used.**

**Ensure that the checksums present in the protocol design are properly implemented and added to each message before it is sent.**

**Business Impact**::- An attacker who controls user input or is able to influence network connectivity can perform a variety of actions and gain access to potentially sensitive information or event execute arbitrary code on vulnerable system.

**Vulnerability Name:-** Untrusted Search Path

**Severity : - High**

**Plugin:- 35674**

**Description:-**

**Solution:- The only way to protect application against this weakness is to perform additional checks on data authenticity. When developing the application consider all possible input data sources and use unique tokens to validate user input, always verify client and server identity.**

**Business Impact**::- An attacker who controls user input or is able to influence network connectivity can perform a variety of actions and gain access to potentially sensitive information or event execute arbitrary code on vulnerable system.

**Vulnerability Name:-** Download of Code Without Integrity Check

**Severity : - High**

**Plugin:- 502037**

**Description:-**

**Solution:- The only way to protect application against this weakness is to perform additional checks on data authenticity. When developing the application consider all possible input data sources and use unique tokens to validate user input, always verify client and server identity.**

**Business Impact**::- An attacker who controls user input or is able to influence network connectivity can perform a variety of actions and gain access to potentially sensitive information or event execute arbitrary code on vulnerable system.

**Vulnerability Name:-** Deserialization of Untrusted Data

**Severity : -** critical

**Plugin:- 173829**

**Description:-**

**Solution:- The only way to protect application against this weakness is to perform additional checks on data authenticity. When developing the application consider all possible input data sources and use unique tokens to validate user input, always verify client and server identity.**

**Business Impact**::- An attacker who controls user input or is able to influence network connectivity can perform a variety of actions and gain access to potentially sensitive information or event execute arbitrary code on vulnerable system.

**Vulnerability Name:-** Reliance on Cookies without Validation and Integrity Checking

**Severity : - High**

**Plugin:- 33929**

**Description:-**

**Solution:- The only way to protect application against this weakness is to perform additional checks on data authenticity. When developing the application consider all possible input data sources and use unique tokens to validate user input, always verify client and server identity.**

**Business Impact**::- An attacker who controls user input or is able to influence network connectivity can perform a variety of actions and gain access to potentially sensitive information or event execute arbitrary code on vulnerable system.

**Vulnerability Name:-** Reliance on Cookies without Validation and Integrity Checking in a Security Decision

**Severity : - High**

**Plugin:- 54887**

**Description:-**

**Solution:- The only way to protect application against this weakness is to perform additional checks on data authenticity. When developing the application consider all possible input data sources and use unique tokens to validate user input, always verify client and server identity.**

**Business Impact**::- An attacker who controls user input or is able to influence network connectivity can perform a variety of actions and gain access to potentially sensitive information or event execute arbitrary code on vulnerable system.

**Vulnerability Name:-** Inclusion of Functionality from Untrusted Control Sphere

**Severity : -** critical

**Plugin:- 500630**

**Description:-**

**Solution:- The only way to protect application against this weakness is to perform additional checks on data authenticity. When developing the application consider all possible input data sources and use unique tokens to validate user input, always verify client and server identity.**

**Business Impact**::- An attacker who controls user input or is able to influence network connectivity can perform a variety of actions and gain access to potentially sensitive information or event execute arbitrary code on vulnerable system.

**Vulnerability Name:-** Inclusion of Web Functionality from an Untrusted Source

**Severity : - High**

**Plugin:- 11850**

**Description:-**

**Solution:- The only way to protect application against this weakness is to perform additional checks on data authenticity. When developing the application consider all possible input data sources and use unique tokens to validate user input, always verify client and server identity.**

**Business Impact**::- An attacker who controls user input or is able to influence network connectivity can perform a variety of actions and gain access to potentially sensitive information or event execute arbitrary code on vulnerable system.

**Vulnerability Name:-** Improperly Controlled Modification of Dynamically-Determined Object Attributes

**Severity : - High**

**Plugin:- 98024**

**Description:-**

**Solution:- The only way to protect application against this weakness is to perform additional checks on data authenticity. When developing the application consider all possible input data sources and use unique tokens to validate user input, always verify client and server identity.**

**Business Impact**::- An attacker who controls user input or is able to influence network connectivity can perform a variety of actions and gain access to potentially sensitive information or event execute arbitrary code on vulnerable system.

**References:**


1 https://www.youtube.com/watch?v=x87gbgQD4eg&ab_channel=JonGood

2 https://www.youtube.com/watch?v=35a0VhzIO2Y&ab_channel=KtechHub

3https://www.youtube.com/watch?v=gK0xw69yJLA&ab_channel=O-LineSecurity

# Stage 3-Report

# Tittle : The Impact of SoC on Modern Cyber Security Practices

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 refers to the centralized facility within an organization in cybersecurity that is tasked with the continuous monitoring, detection, response, and mitigation of cyber threats and incidents within the institution. It serves as the corporate hub of security operations, bringing together fully and cohesively trained personnel, defined processes, and advanced technologies with the aim of protecting information assets of the organization while ensuring compliance with the set regulatory provisions.
  The SOC works 24/7 and thus provides an organization with constant vigil over its digital structure. This is an operation of concern that has to be done continuously, considering that cyber threats could emanate any time in respect to the identification and effective action towards the same in case. A SOC team generally comprises security analysts—security alert reviewers and investigators—and incident responders managing and mitigating security breaches, while others involve SOC managers in charge of operations and strategy, and threat hunters—those involved in looking for the hiders, invisible threats missed by automated systems.The SOC has implemented a raft of technologies aimed at enhancing its monitoring capabilities and detection. SIEM systems collect all data sources, such as network devices, servers, applications, and analyze them to find any sort of suspicious activity. IDPS helps in identifying and blocking potential intrusions. Endpoint Detection and Response (EDR) tools monitor endpoints, such as computers and mobile devices, for signs of malicious activity.

- **SOC cycle:**
  SOCs have a structured set of processes that are carried out to ensure that security is maintained. These processes are typically categorised into the following phases:

1. **Monitoring:** SOC monitoring is crucial in preventing cyberattacks. With the help of advanced tools and technologies, the team keeps an eye on the organisation's network,

looking for any signs of malicious activity. This 24/7 SOC service ensures that potential threats are detected in realtime, minimising the damage they can cause.

2. **Threat Detection:** Using tools like Security Information and Event Management (SIEM) systems, SOC teams examine large amounts of information to detect potential threats. It involves correlating events across different sources to identify patterns indicative of a cyberattack.
3. **Incident Response:** The team jumps into action once a threat is detected and follows a predefined set of procedures to contain, remove, and restore the affected systems. This process is crucial to ensure that the impact of a security incident is minimised.
4. **Threat Hunting:** Instead of waiting for automated tools to detect threats, SOC monitoring teams proactively search for signs of malicious activity within their networks. It ensures that even the most sophisticated threats, which might evade traditional detection methods, are identified.
5. **Reporting:** Transparency is key in cybersecurity. SOC reporting involves creating detailed logs and reports of all the activities within the network. These reports are crucial for audits, compliance, and understanding the organisation's security posture.
6. **Continuous Improvement:** SOC processes are continuously reviewed and updated to counter new threats. Regular training sessions, workshops, and simulations are conducted to ensure the team is always prepared.

Figure 1: Soc cycle

**MISP (Malware Information Sharing Platform & Threat Sharing)**

The Malware Information Sharing Platform & Threat Sharing (MISP) is an opensource threat intelligence platform designed to improve the sharing of structured threat information. MISP enables organizations to share, store, and correlate indicators of compromise (IoCs) of targeted attacks, malware, and other threats. By fostering

collaboration and information sharing, MISP helps organizations enhance their situational awareness and improve their defensive capabilities.

Key Features of MISP

1. Threat Data Collection and Sharing: MISP allows organizations to collect, store, and share threat intelligence data with trusted partners, including indicators of compromise (IoCs), threat actors, TTPs (Tactics, Techniques, and Procedures), and more.

2. Data Correlation and Analysis: MISP provides powerful data correlation capabilities, enabling organizations to link related events, identify patterns, and gain insights into emerging threats.

3. Collaborative Environment: MISP facilitates collaboration among multiple organizations, allowing them to share threat intelligence in a structured and standardized format. This collaboration helps in building a comprehensive view of the threat landscape.

4. Automation and Integration: MISP supports automation through REST APIs, which allows for seamless integration with other security tools such as SIEMs, IDS/IPS, and endpoint protection systems. This automation helps in the timely sharing and updating of threat information.

5. Granular Access Control: MISP offers granular access control mechanisms to ensure that sensitive threat information is shared only with authorized entities. Organizations can define sharing groups and access levels to manage who can see and contribute to the threat data.

6. Customizable Dashboards and Reports: MISP provides customizable dashboards and reporting capabilities to visualize threat data, track trends, and generate actionable intelligence.

Understanding How MISP Works

1. Data Ingestion: Organizations can ingest threat intelligence data into MISP from various sources, including manual input, automated feeds, and integration with other security tools.

2. Data Structuring and Enrichment: MISP structures the ingested data using a standardized format, such as the MISP data model. It enriches the data with additional context and metadata to enhance its usefulness.

3. Correlation and Analysis: MISP correlates the ingested data to identify relationships between different threat indicators and events. This correlation helps in understanding the broader threat landscape and detecting potential security incidents.

4. Sharing and Collaboration: Organizations can share the enriched and correlated threat intelligence data with trusted partners and communities. MISP ensures that shared data is structured and standardized, facilitating effective collaboration.

5. Automation and Integration: MISP's APIs enable integration with other security tools and automation of threat intelligence workflows. This integration ensures that threat data is continuously updated and available for analysis and response.

**Benefits of Using MISP**

- Enhanced Threat Intelligence: MISP improves the quality and relevance of threat intelligence by enabling the sharing and correlation of data from multiple sources.
- Improved Situational Awareness: By leveraging shared threat intelligence, organizations gain a comprehensive view of the threat landscape, improving their situational awareness.
- Proactive Defense: MISP helps organizations move from a reactive to a proactive security posture by providing timely and actionable threat intelligence.
- Community Collaboration: MISP fosters a collaborative environment where organizations can share knowledge and insights, collectively enhancing their defensive capabilities.
- CostEffective Solution: As an opensource platform, MISP offers a costeffective solution for threat intelligence sharing and management, reducing the need for expensive proprietary tools.

MISP is a powerful tool for enhancing threat intelligence and improving cybersecurity defenses through collaboration and data sharing. By enabling organizations to collect, share, and analyze threat data in a structured and standardized manner, MISP helps build a comprehensive view of the threat landscape and supports proactive defense strategies. Integrating MISP into an organization's security operations can significantly enhance its ability to detect, understand, and respond to emerging threats.

- **Your college network information:**

The Department of Computer Science and Engineering (CSE) at our college maintains a robust network infrastructure consisting of 50 nodes and 500 endpoints. This extensive network supports a wide range of academic and research activities, necessitating a strong

focus on cybersecurity. To ensure the security and integrity of this network, our college employs a Security Operations Center (SOC).

The SOC is instrumental in monitoring and protecting our network. It continuously scans for vulnerabilities, manages security incidents, and enforces security policies. By leveraging advanced threat intelligence and providing user awareness training, the SOC helps safeguard our network against potential cyber threats, ensuring a secure and resilient computing environment for students, faculty, and staff.

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

Deploying a Security Operations Center (SOC) in a college involves a series of strategic steps to ensure comprehensive protection for the network. Here is the StepbyStep SOC Deployment in a College

1. Assessment and Planning

- Network Assessment: Conduct a thorough assessment of the current network infrastructure, identifying critical assets, potential vulnerabilities, and existing security measures.
- Requirements Gathering: Determine the specific requirements for the SOC, including the types of threats to be monitored, compliance needs, and operational goals.
- Budget and Resources: Define the budget and allocate resources, including personnel, technology, and training.

2. Infrastructure Setup

- Hardware and Software: Procure and set up the necessary hardware (servers, workstations, network devices) and software (SIEM, threat intelligence platforms, log management tools).
- Physical Location: Designate a secure physical space for the SOC, ensuring it has the necessary facilities and access controls.

3. Staffing and Training

- Hiring Experts: Recruit skilled cybersecurity professionals, including SOC analysts, incident responders, and threat hunters.
- Training Programs: Implement ongoing training programs to keep the SOC team updated on the latest threats and security practices.
-

4. Implementation of Security Tools

- SIEM (Security Information and Event Management): Deploy SIEM solutions to collect, analyze, and correlate security event data from across the network.
- Threat Intelligence: Integrate threat intelligence feeds to provide realtime information on emerging threats and vulnerabilities.
- Endpoint Protection: Install and configure endpoint protection solutions on all 500 endpoints to detect and respond to malware and other threats.
-

5. Monitoring and Incident Response

- 24/7 Monitoring: Establish continuous monitoring of network activity to detect anomalies and potential security incidents.
- Incident Response Plan: Develop and implement a detailed incident response plan, outlining the steps to be taken in the event of a security breach.
- Regular Drills: Conduct regular incident response drills to ensure the team is prepared for realworld scenarios.
-

6. Policy and Compliance

- Security Policies: Create and enforce comprehensive security policies covering data protection, access controls, and acceptable use of network resources.
- Compliance: Ensure the SOC meets all relevant regulatory and compliance requirements, such as GDPR, FERPA, and other educationspecific guidelines.
-

7. Continuous Improvement

- Regular Audits: Perform regular security audits and vulnerability assessments to identify and address weaknesses.
- Feedback Loop: Establish a feedback loop to learn from incidents and continuously improve SOC processes and technologies.

Deploying a SOC in a college setting involves careful planning, strategic implementation of technologies, and continuous monitoring and improvement. By following these steps, the college can create a robust defense against cyber threats, ensuring the security and integrity of its network infrastructure.

# Threat intelligence:

Threat Intelligence is a Security Operations Center function related to gathering, processing, and using all the information available on current and future cyber threats. It gives organizations an indepth understanding of threats and enables preparation for attacks, thus enhancing the general security posture.

**Key Aspects of Threat Intelligence:**

- **Information Gathering:** This is the act of sourcing data from various sources, then:
- **OSINT:** Information in the public domain, such as news articles and blog posts, and social media.
- **Technical Intelligence:** Sensors, logs, monitoring tools—source of indicators of compromise (IoCs): IP addresses, domain names, file hashes, etc.
- **HUMINT:** Information received from human sources; for example, security researchers, informants.
- **Dark Web Intelligence:** This comes from darkweb forums, marketplaces, and other underground sources that play host to cybercriminal activities.

- Analysis is an examination and interpretation of the collected data to come up with patterns, trends, and actionable insight. This includes:
- **Correlation:** Relating independent pieces of data to estimate related threats and attack vectors.
- **Contextualization:** Know the context within which threats are acting—such as their intents, capabilities, and tactics.
- **Prioritization:** Based on the severity of threats and possibility of attacks, prioritization is necessary for efforts to respond.
- **Information Sharing:** The analyzed threat intelligence is shared with the following stakeholders in an organization:
- **SOC Team:** Security analysts and incident responders need information to be better placed while detecting and mitigating threats effectively.
- **IT and Security Teams:** That consists of the dissemination of information to broader IT and security teams in order to enhance defenses and apply preventive measures within their works.
- **Executive Leadership:** Ensure that top leadership is aware of major threats and their potential impact on the organization.

# Incident response:

The incident response steps that organizations need to take have been summarized in a sixstep plan by the SANS Institute.
Every phase of the sixstep plan needs to be followed in sequence, as each builds upon the previous phase.

### Step 1: Prepare

Preparation is the most crucial phase in the incident response plan, as it determines how well an organization will be able to respond in the event of an attack. It requires several key elements to have been implemented to enable the organization to handle an incident:

1. Policy: Provides a written set of principles, rules, or practices within an organization and is a crucial action that offers guidance as to whether an incident has occurred.
2. Response plan/strategy: The response plan needs to include the prioritization of incidents based on organizational impact, from minor incidents like a single workstation failing to a medium risk like a server going down, and highrisk issues like data being stolen from a department. This can help build the case for management buyin and gain resources required to handle an incident effectively.
3. Communication: Having a communication plan is vital to ensuring the entire CSIRT knows who to contact, when, and why. Not having a plan will likely delay the response time and result in the wrong people being contacted.
4. Documentation: This is a vital step in an incident response plan. Documenting the incident assists the organization in providing evidence in the event the incident is considered a criminal act. It also facilitates learning lessons for the future. Everything the CSIRT does must be documented and be able to answer any potential who, what, when, where, and why questions.
5. Team: The CSIRT needs to be comprised of people from different disciplines and departments across the organization, not just technical or security teams.
6. Access control: The CSIRT also needs to have the appropriate permissions to perform their roles. For example, having permission to access networks and systems to mitigate problems and having that permission removed when it is no longer needed.
7. Tools: Software and hardware are crucial to helping the CSIRT investigate an incident. This can range from antimalware programs and laptops to screwdrivers. All of the tools required must be contained in a "jump bag."
8. Training: Training is crucial to ensuring a team is prepared to tackle a security incident. It is recommended to have regular drills so all CSIRT members know their duties as and when an incident occurs.

### Step 2: Identify

The second phase deals with detecting and determining whether an incident has occurred. Information such as error messages and log files must be gathered from various sources, including intrusion detection systems and firewalls, to make this decision. If an incident has occurred, it should be reported as quickly as possible to give the CSIRT enough time to collect evidence and prepare for the next steps. CSIRT members also need to be notified and begin the incident response plan process.

For example, the Fortinet FortiGuard solution analyzes over 100 billion security events per day to detect and defend against the evolving threat landscape. It offers realtime threat intelligence that protects customers from new advanced threats and detects and prevents breaches as and when they happen.

### Step 3: Contain

Once a threat has been identified, the organization must limit and prevent any further damage. There are several necessary steps to help them mitigate an incident and prevent the destruction of evidence.

1. Shortterm containment: This aims to limit the damage as quickly as possible. It can be as simple as isolating infected machines to taking down production servers and routing all traffic to failover servers.
2. System backup: Forensic software must capture an image of affected systems as they were during the incident to preserve evidence and understand how they were compromised.
3. Longterm containment: This step sees the affected systems temporarily fixed to ensure they can continue to be used while rebuilding clean systems. The primary focus is for accounts or backdoors left by attackers to be removed and security patches to be installed.

### Step 4: Eradicate

This phase sees the removal and restoration of systems affected by the security incident. As in all phases of the plan, documentation is crucial to determining the cost of manhours, resources, and overall impact of the attack. The organization also must ensure that malicious content has been removed from affected systems and systems have been thoroughly cleaned to prevent the risk of reinfection.

The eradication phase is also crucial to helping businesses improve their defenses and fix vulnerabilities based on the lessons they learned to make sure their systems do not get compromised again.

### Step 5: Recover

This phase helps organizations carefully bring affected systems back into the production environment and ensures another incident does not occur. Systems must be tested, monitored, and validated as they move back into production so they are not reinfected by malware or compromised. Important decisions here include:

1. The time and date that operations are restored. System operators and owners must make the final decision based on the CSIRT's advice
2. How to test and verify that compromised systems are clean and fully functional
3. The duration that abnormal behaviors are monitored
4. Tools used to test, monitor, and validate system behavior

### Step 6: Learn

It is vital for organizations to review their incident response and adapt their approach for future attacks. All documentation that was not completed during the incident now needs to be compiled, along with additional information that may benefit future incidents.

The report must provide a playbyplay review of what happened throughout the entire incident. This will help the CSIRT improve its performance, learn from the events that occurred, and provide reference materials for future events. The report can also be used as training material for new employees and to guide any drills that teams hold.

After an event, a lessons learned meeting should take place as soon as possible. Your report should cover:

1. When the problem was first detected, how, and by whom
2. The root cause of the incident
3. How the problem was contained and eradicated
4. Actions performed throughout the recovery process
5. Areas where the CSIRT was effective and areas for improvement
6. Suggestions and discussion around how to improve the CSIRT


Figure 2: Incident Response

# QRadar & Understanding the Tool

-
- Introduction to QRadar
- IBM QRadar is a comprehensive Security Information and Event Management (SIEM) solution designed to help organizations detect, understand, and respond to security threats. It integrates realtime correlation and behavioral anomaly detection to provide a holistic view of the network security landscape. QRadar collects and analyzes log data from various sources, such as network devices, endpoints, and applications, to identify suspicious activities and potential security breaches.
-
- Key Features of QRadar
- 1. Log Management: QRadar efficiently collects, parses, and stores log data from diverse sources, ensuring that all relevant security information is available for analysis and compliance reporting.
-

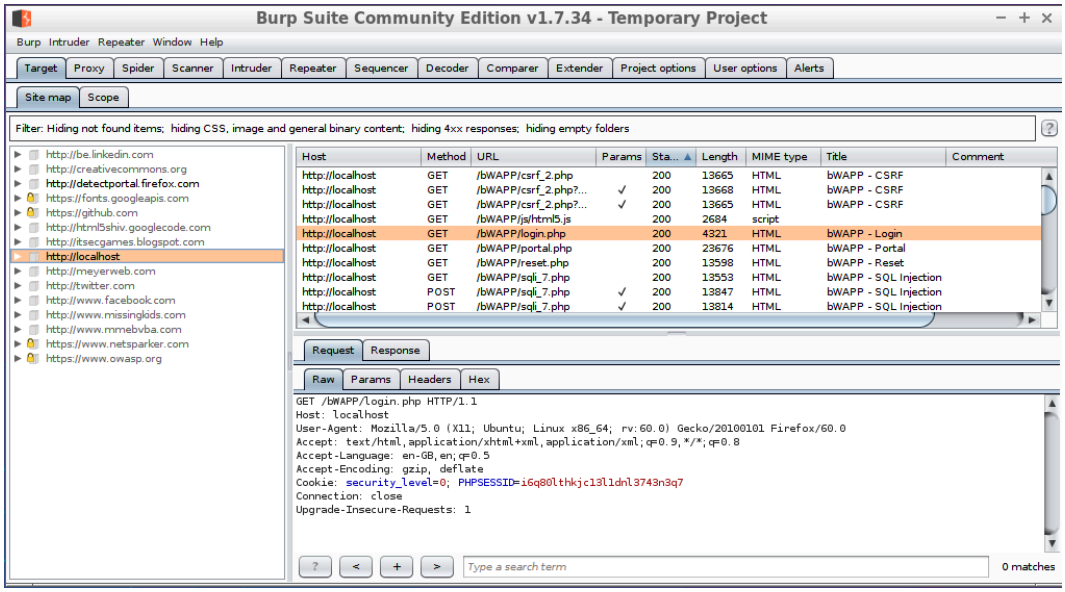
- 2. Realtime Monitoring and Alerting: The tool provides realtime monitoring of network activities and generates alerts for suspicious behaviors or policy violations, enabling swift response to potential threats.
-
- 3. Advanced Threat Detection: QRadar employs sophisticated analytics, including machine learning and behavioral analysis, to detect advanced threats such as insider threats, APTs (Advanced Persistent Threats), and zeroday attacks.
-
- 4. Incident Response: Integrated incident response capabilities allow security teams to investigate, contain, and remediate incidents effectively. QRadar provides detailed insights and forensic data to support thorough investigations.
-
- 5. Compliance Management: QRadar helps organizations meet regulatory requirements by providing comprehensive reporting and audit trails. It supports various compliance frameworks, such as GDPR, PCI DSS, and HIPAA.
-
- 6. Scalability and Flexibility: The solution can scale to accommodate the needs of small organizations to large enterprises, offering flexible deployment options, including onpremises, cloud, and hybrid environments.
-
- Understanding How QRadar Works
- 1. Data Collection: QRadar collects data from a wide range of sources, including firewalls, routers, switches, endpoints, applications, and databases. This data is normalized and enriched to provide a consistent format for analysis.
-
- 2. Parsing and Normalization: Once collected, QRadar parses the log data to extract meaningful information. It normalizes the data to ensure consistency, making it easier to correlate events across different sources.
-
- 3. Correlation and Analysis: QRadar uses correlation rules and machine learning algorithms to analyze the normalized data. It identifies patterns, anomalies, and correlations that indicate potential security incidents.
-
- 4. Alerting and Reporting: When a potential threat is detected, QRadar generates alerts and notifies the security team. It also provides detailed reports and dashboards that offer insights into the security posture and trends over time.
-
- 5. Incident Response and Forensics: QRadar facilitates incident response by providing actionable intelligence and forensic data. Security teams can drill down into the details of an incident, understand its impact, and take appropriate actions to mitigate the threat.

-
- Benefits of Using QRadar
- Comprehensive Visibility: QRadar provides a unified view of the entire network, enabling security teams to monitor and understand security events across the organization.
- Improved Threat Detection: Advanced analytics and realtime monitoring capabilities enhance the detection of complex and sophisticated threats.
- Streamlined Compliance: QRadar's robust reporting and audit capabilities help organizations streamline compliance efforts and maintain regulatory adherence.
- Efficient Incident Management: Integrated incident response tools facilitate quick and effective management of security incidents, minimizing potential damage.
-
- IBM QRadar is a powerful SIEM solution that offers comprehensive security monitoring, advanced threat detection, and efficient incident response capabilities. By providing deep insights into network activities and potential threats, QRadar helps organizations enhance their security posture, protect sensitive data, and comply with regulatory requirements. Understanding how to effectively leverage QRadar's features and functionalities is crucial for building a resilient and proactive cybersecurity strategy.
-

# Conclusion :

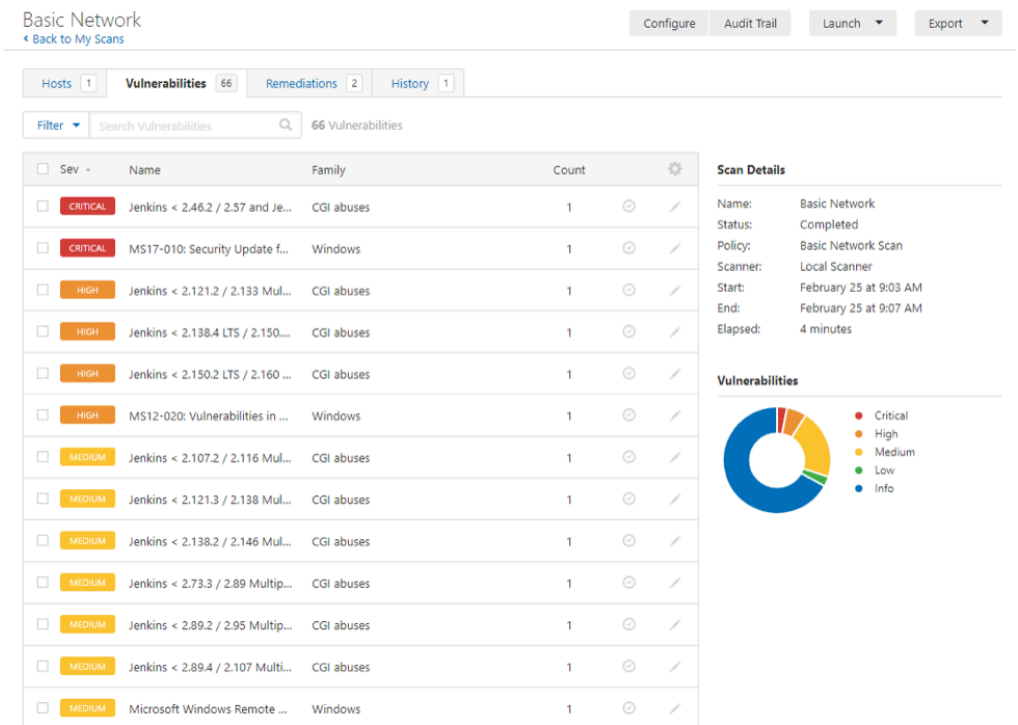
- **Stage 1 : Web Application Testing**

  Web application testing involves a series of tests to assess the security, functionality, performance, and usability of web applications. This process identifies vulnerabilities such as SQL injection, crosssite scripting (XSS), and authentication flaws. Tools like OWASP ZAP or Burp Suite are commonly used for these tests.




- **Stage 2: Nessus Report**

- The Nessus report is generated after a vulnerability scan using the Nessus tool. It provides detailed findings on security vulnerabilities within the network and systems, including a risk score, the affected components, and remediation advice. The report is divided into sections for high, medium, and lowseverity vulnerabilities, aiding in prioritization.



- *Screenshot Description*: A screenshot of a Nessus scan report, showing the dashboard with an overview of vulnerabilities, a detailed list of issues, their severity, and recommendations for remediation.

- **Stage 3: SOC/SIEM/QRadar Dashboard** The SOC/SIEM/QRadar dashboard offers a comprehensive view of an organization's security status, aggregating data from various sources to monitor and analyze security events. It provides realtime alerts, visualizations of attack trends, and detailed logs for incident analysis, facilitating rapid response to security incidents.

- 

-

# Future Scope :

- Stage 1 : future scope of web application testing  The future scope of web application testing include AI and ML integration.
- Stage 2 : future scope of testing process you understood .
- Stage 3 : future scope of SOC / SEIM The scope of a security operation center (SOC) in the future is likely to continue to evolve and expand, as technology advances and the threat landscape becomes more complex. Some possible areas of focus for SOCs in the future include:
    - Advanced threat detection and response: SOCs will likely need to use more advanced methods for detecting and responding to cyber threats, such as artificial intelligence (AI) and machine learning (ML) technologies.
    - Automation and orchestration: SOCs will likely need to automate more of their processes and use orchestration tools to manage multiple security technologies and platforms.

- Cloud and multicloud security: SOCs will likely need to address security challenges related to cloud computing, including protecting data and applications in multicloud environments.
- Internet of Things (IoT) security: SOCs will likely need to address security challenges related to IoT devices, such as securing connected devices and managing the data they generate.
- Regulatory compliance: SOCs will likely need to ensure compliance with various regulations, such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA).

It's important to note that the specific scope of a SOC can vary depending on the organization and its specific needs. Additionally, new challenges and technology may arise in the future that are not currently considered.

-

# Topics explored

We explored topics in a Security Operations Center (SOC):

- Threat Intelligence Analysis: Analyzing and leveraging threat data to understand and mitigate cybersecurity risks.
- Security Incident Response: Coordinated actions and procedures to detect, analyze, and respond to cybersecurity incidents promptly.
- Intrusion Detection and Prevention: Monitoring and blocking unauthorized access attempts and malicious activities on networks and systems.
- Log Management and Analysis: Collecting, storing, and analyzing logs from various sources to detect security incidents and investigate breaches.
- Vulnerability Management: Identifying, assessing, and mitigating vulnerabilities in systems and applications to reduce the risk of exploitation.
- Security Monitoring and Alerting: Continuous monitoring of networks and systems for security threats, with realtime alerts for suspicious activities.
- Forensic Analysis: Investigating cybersecurity incidents by collecting and analyzing digital evidence to understand the scope and impact of an attack.

- Endpoint Security: Protecting individual devices (endpoints) from cybersecurity threats, including malware and unauthorized access.

- Network Traffic Analysis: Monitoring and analyzing network traffic to detect anomalies, unauthorized access, and potential threats.

- Malware Analysis: Analyzing the behavior and characteristics of malware to understand its impact and develop countermeasures.

- Compliance Monitoring and Reporting: Ensuring adherence to security policies, regulations, and standards through monitoring and reporting.

- Incident Escalation Procedures: Formalized steps and protocols for escalating security incidents to appropriate stakeholders for response and resolution.

- Security Policies and Procedures: Establishing guidelines and protocols to govern the organization's approach to cybersecurity and risk management.

- User Behavior Analytics (UBA): Monitoring and analyzing patterns of user behavior to detect insider threats and unauthorized activities.

- Threat Hunting Techniques: Proactive and iterative searching through networks and systems to detect and isolate advanced threats that evade traditional security measures.

- SIEM (Security Information and Event Management) Configuration: Configuring and managing SIEM systems to collect, correlate, and analyze security event data for proactive threat detection and response.

# Tools explored

The explored topic in a Security Operations Center (SOC) along with tools commonly used for each are mentioned here:

- Threat Intelligence Analysis
    - Tools: Threat intelligence platforms (TIPs) like ThreatConnect, Anomali, Recorded Future

- Security Incident Response

- Tools: Incident response platforms like IBM Resilient, Palo Alto Networks Cortex XSOAR (formerly Demisto), Splunk Phantom

- Intrusion Detection and Prevention
  - Tools: Intrusion detection systems (IDS) like Snort, Suricata, Cisco Firepower, intrusion prevention systems (IPS) like Cisco IPS, Palo Alto Networks PANOS

- Log Management and Analysis
  - Tools: SIEM (Security Information and Event Management) platforms like IBM QRadar, Splunk Enterprise Security, ArcSight

- Vulnerability Management
  - Tools: Vulnerability scanners like Nessus, Qualys, Rapid7 Nexpose, penetration testing tools like Metasploit, Burp Suite

- Security Monitoring and Alerting
  - Tools: SIEM platforms (mentioned above), endpoint detection and response (EDR) solutions like CrowdStrike Falcon, Carbon Black

- Forensic Analysis
  - Tools: Digital forensic tools like EnCase Forensic, Autopsy, FTK (Forensic Toolkit), memory forensics tools like Volatility

- Endpoint Security
  - Tools: Endpoint protection platforms (EPP) like Symantec Endpoint Protection, McAfee Endpoint Security, Microsoft Defender for Endpoint

- Network Traffic Analysis
  - Tools: Network traffic analysis tools like Wireshark, SolarWinds NetFlow Traffic Analyzer, PRTG Network Monitor

- Malware Analysis
  - Tools: Sandboxing tools like Cuckoo Sandbox, Hybrid Analysis, automated malware analysis tools

- Compliance Monitoring and Reporting
  - Tools: GRC (Governance, Risk, and Compliance) platforms like RSA Archer, MetricStream, ServiceNow

- Incident Escalation Procedures

    - Tools: Incident response playbooks and procedures managed within incident response platforms (mentioned above)

- Security Policies and Procedures
    - Tools: Policy management platforms like Netwrix Auditor, ManageEngine ADAudit Plus, SolarWinds Access Rights Manager

- User Behavior Analytics (UBA)
    - Tools: UBA solutions integrated with SIEM platforms or standalone products

- Threat Hunting Techniques
    - Tools: Threat hunting platforms and tools, often integrated with SIEM or EDR solutions

Each of these topics involves specific tools and technologies designed to enhance the capabilities of a SOC in detecting, responding to, and mitigating cybersecurity threats.

—THE END —