Stage 3

Report

Prepared by	**Dr.Sumaiya Thaseen,** **Associate Professor,** **School of Computer Engineering and Information Systems,** **Vellore Institute of Technology, Vellore, Tamil Nadu** **isumaiyathaseen@vit.ac.in**

SIEM Log Management

SIEM software solutions collect log data from multiple sources, such as applications and network hardware, and aggregate it into a centralized platform. They can perform correlation and real-time analytics to alert teams to indicators of compromise (IoCs), such as failed login attempts, letting them respond faster and more effectively to ongoing attacks.

3.1 Security Operations Center (SOC)

The foundational technology of a SOC is a SIEM, which aggregates device, application logs, and events from security tools from across the entire organization. The SIEM uses correlation and statistical models to identify events that might constitute a security incident, alert SOC staff about them, and provide contextual information to assist investigation. A SIEM functions as a “single pane of glass” which enables the SOC to monitor enterprise systems.

While SOCs are undergoing transformation and assuming additional roles, their core activity remains incident response. The SOC is the organizational unit that is expected to detect, contain, and mitigate cyber attacks against the organization. The people responsible for incident response are Tier 1, Tier 2 and Tier 3 analysts, and the software they primarily rely on is the SOC’s Security Information and Event Management (SIEM) system.

The SOC team chooses the log sources based on usage patterns, their impact on threat detection, coverage, auditing requirements, and adaptability to the organization’s log management platform.

3.2 SOC – Cycle

There are four main stages in SOC Cycle as shown in figure 1.

1. **Preparation**

   This process involves identifying, integrating, and processing relevant data sources for the SOC's tasks. It includes determining which assets need protection, identifying relevant logs, and establishing methods for collecting and processing these logs. Additionally, it involves identifying and integrating external data sources, such as threat intelligence.

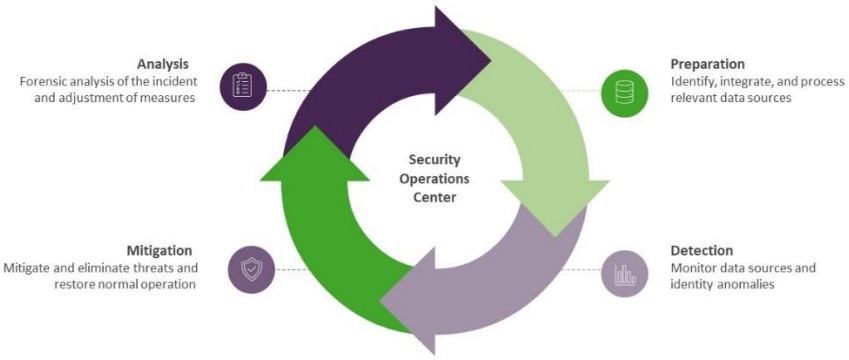

Figure 1: SOC Cycle

2. **Detection**

   Activities in this step are considered the core function of the SOC.

   They revolve around answering key questions using the data prepared in the previous step such as determining desired and undesired activities, assessing the organization's exposure to threats, identifying indicators of a potential attack in the data, and distinguishing whether a suspicious event constitutes a security incident.

3. **Mitigation**

   When a specific incident is identified during the detection phase, this process activity comes into play. Its purpose is to efficiently mitigate and eliminate the threat. Additionally, the SOC focuses on restoring operational capability to minimize the impact on ongoing operations.

4. **Analysis**

   After an incident has been remediated, and operational capability has been restored, the SOC supports the analysis of the incident. This analysis helps prepare defenses and detection mechanisms to address any potential recurrence of the threat.

3.3 SIEM

SIEM tools combine the capabilities of Security Event Management (SEM), Security Information Management (SIM), and Security Event Correlation (SEC) into one solution. Log management refers to the entire process teams use to handle logs generated by the various applications in their IT environment.

Log management can be broken down into a series of independent subprocesses. It usually starts with collecting log data from a data source. The logs are then aggregated into a central location where they can be analyzed. In some cases, log data also needs to be transformed. This means that log data must be reorganized or decomposed to conform to the format standards used by the organization or to make them easier to parse. Logs can then be centrally analyzed or visualized.

3.4 SIEM Cycle

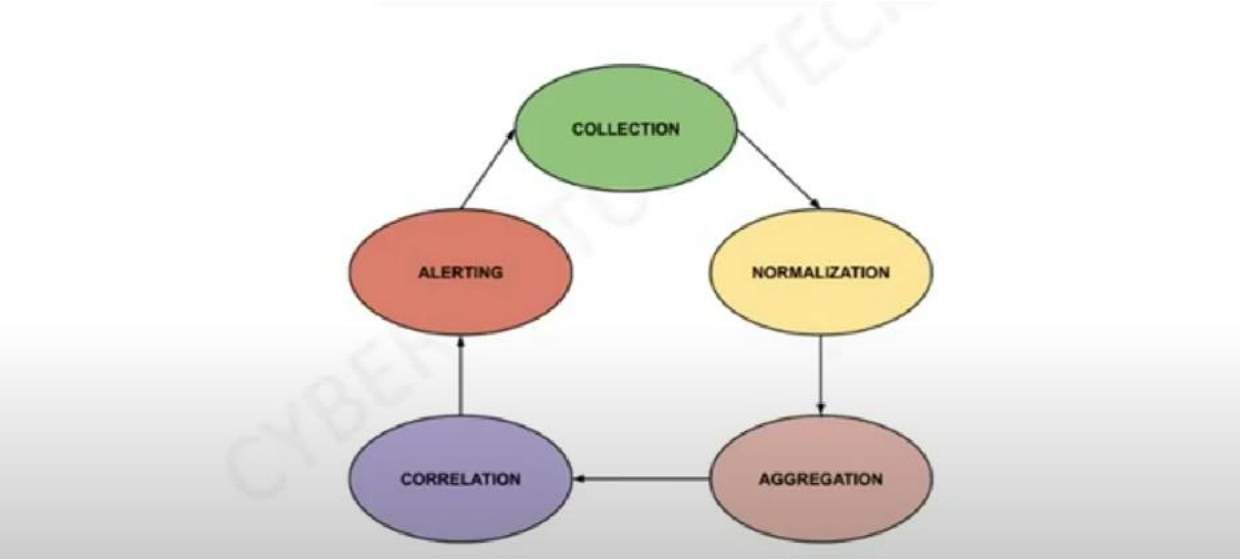

Figure 2: SIEM Cycle

The various events in SIEM are collection, normalization, aggregation, correlation, and alerting. The biggest challenge in collecting data in the context of SIEM is overcoming the variety of log formats. A SIEM system, by its very nature, will be pulling data from many layers — servers, firewalls, network routers, databases — to name just a few, each logging in a different format. Once collected, parsed and stored, the next step in SIEM systems is in charge of connecting the dots and correlating events from the different data sources. This correlation work is based on rules that are either provided by various SIEM tools, predefined for different attack scenarios, or created and fine-tuned by the analyst. A correlation rule defines a specific sequence of events that could be indicative of a breach in security. For example, a rule could be created to identify when more than x amount of requests is sent from specific IP ranges and ports within an amount of time. Once correlation rules are put in place and monitoring

dashboards built to provide a comprehensive overview of the system, the last key component of a SIEM system is how incidents are handled once identified.

Most SIEM systems support mechanisms to automatically contain and mitigate security events. For example, based on correlation rules, a SIEM system can be configured to automatically begin an internal escalation process — executing scripts that begin the process of containment and passing the ball to the correct resource in the organization by triggering an alert, opening a ticket, and so forth.

3.5 Malware Information Sharing Platform (MISP)

A threat intelligence platform as shown in figure 3 for sharing, storing and correlating Indicators of Compromise of targeted attacks, threat intelligence, financial fraud information, vulnerability information or even counter-terrorism information.

MISP is used today in multiple organisations not only to store, share, collaborate on cyber security indicators, malware analysis, but also to use the IoCs and information to detect and prevent attacks, frauds or threats against ICT infrastructures, organisations or people.

Figure 3: Snapshot of MISP

- An **efficient IoC and indicators** database allowing to store technical and non-technical information about malware samples, incidents, attackers and intelligence.
- Automatic **correlation** finding relationships between attributes and indicators from malware, attacks campaigns or analysis. Correlation engine includes correlation between attributes and more advanced correlations like Fuzzy hashing correlation (e.g. ssdeep) or CIDR block matching. Correlation can be also enabled or event disabled per attribute.
- A flexible data model where complex objects can be expressed and linked together to express threat intelligence, incidents or connected elements.
- Built-in **sharing functionality** to ease data sharing using different model of distributions. MISP can synchronize automatically events and attributes among different MISP. Advanced filtering functionalities can be used to meet each organization sharing policy including a **flexible sharing group** capacity and an attribute level distribution mechanisms.
- An **intuitive user-interface** for end-users to create, update and collaborate on events and attributes/indicators. A **graphical interface** to navigate seamlessly between events and

their correlations. An **event graph** functionality to create and view relationships between objects and attributes. Advanced filtering functionalities and warning list to help the analysts to contribute events and attributes.

- **storing data** in a structured format (allowing automated use of the database for various purposes) with an extensive support of cyber security indicators along fraud indicators as in the financial sector.
- **export**: generating IDS (Suricata, Snort and Bro are supported by default), OpenIOC, plain text, CSV, MISP XML or JSON output to integrate with other systems (network IDS, host IDS, custom tools
- **import**: bulk-import, batch-import, free-text import, import from OpenIOC, GFI sandbox, ThreatConnect CSV or MISP format.
- Flexible **free text import** tool to ease the integration of unstructured reports into MISP.
- A gentle system to **collaborate** on events and attributes allowing MISP users to propose changes or updates to attributes/indicators.
- **data-sharing**: automatically exchange and synchronization with other parties and trust-groups using MISP.
- **feed import**: flexible tool to import and integrate MISP feed and any threatintel or OSINT feed from third parties. Many default feeds are included in standard MISP installation.
- **delegating of sharing**: allows a simple pseudo-anonymous mechanism to delegate publication of event/indicators to another organization.
- Flexible **API** to integrate MISP with your own solutions. MISP is bundled with PyMISP which is a flexible Python Library to fetch, add or update events attributes, handle malware samples or search for attributes.
- **adjustable taxonomy** to classify and tag events following your own classification schemes or existing taxonomies. The taxonomy can be local to your MISP but also shareable among MISP instances. MISP comes with a default set of well-known taxonomies and classification schemes to support standard classification as used by ENISA, Europol, DHS, CSIRTs or many other organizations.
- **intelligence vocabularies** called MISP galaxy and bundled with existing threat actors, malware, RAT, ransomware or MITRE ATT&CK which can be easily linked with events in MISP.
- **expansion modules in Python** to expand MISP with your own services or activate already available misp-modules.
- **sighting support** to get observations from organizations concerning shared indicators and attributes. Sighting can be contributed via MISP user-interface, API as MISP document or STIX sighting documents. Starting with MISP 2.4.66, Sighting has been extended to support false-negative sighting or expiration sighting.
- **STIX support**: export data in the STIX format (XML and JSON) including export/import in STIX 2.0 format.

- **integrated encryption and signing of the notifications** via PGP and/or S/MIME depending of the user preferences.
- **Real-time publish-subscribe channel** within MISP to automatically get all changes (e.g. new events, indicators, sightings or tagging) in ZMQ (e.g. misp-dashboard) or Kafka.

3.6 Your college network information

IT infrastructure of VIT has been widely spread across connecting 56 buildings with very high-speed robust network backbone. Our Computer network is built on CISCO switching platform with backbone running on 10Gig at present. 12000+ IP enabled devices are connected to this fast network. Understanding the demands of faculty and students to use digital media for their research, teaching & learning process, 10Gbps of internet bandwidth is made available through three major Internet service providers.

Table 1: VIT-Internet Service Providers

S.No	Service Provider	Bandwidth
1	JIO	6 GBPS
2	AIRTEL	6 GBPS
3	BSNL	1 GBPS

Over 2548 WIFI access points are positioned across the campus to facilitate internet access to our students, faculty and guests while they are in the campus. Seamless internet access given to students through Hotspots and well planned WIFI network at Hostel rooms.

Number of students: Number of Computers available to students for academic purposes	**33322 : 8293**

VIT has invested heavily in building up the energy efficient SmartRow Data Centre in 1000 Sq.Ft. area. The features include 10 Smart Row Racks, 3 Libert CRV In-Row Cooling Solution, 90KVA Modular UPS with batteries, Fire Alarm Systems, Biometric Access Control Systems, CCTV and Remote Monitoring & Management Software. VIT maximizes the use of efficient energy solutions at the Data Center while minimizing the impact on the environment. The comprehensive infrastructure includes 68 physical servers with 366TB of storage for Private Cloud with 220+ Virtual Machines and 500 Virtual Desktop Infrastructure (VDI) implemented for the students to work with engineering software anytime anywhere from any device. Our campus IT facility secured by implementing the best of the security solution from Palo Alto, McAfee, CISCO AMP and

K7 which includes Next Generation firewall, Application firewall, Email Security, Advance Malware Protection, Endpoint Threat Protection, OpenDNS etc.

Table 2: Network Security Devices deployed in VIT.

Description	Model	Nos.
Palo Alto Networks Enterprise Firewall	PaloAlto	2
Checkpoint Internal Firewall	Checkpoint	2
Proxy Server	CISCO WSA	1
APPWALL 200 MBPS Web Application Firewall	Radware	1
F Secure Messaging Security Gateway	F-Secure	1
Vulnerablity Scanner	Nessus	1
Open DNS	CISCO	1
Advance Endpoint Protection	CISCO	1
Anti Virus	K7 Computing	1

3.7 How you think you deploy soc in your college

The most important factor for any institution is the need to be ready to face increasingly complicated and more debilitating threats. A SOC can provide the central expertise and coordination functions not typically available in higher ed. Properly implemented, a SOC meets

the institution's security needs to address, recognize, and prevent cybersecurity threats in a cost-effective and efficient matter. Today we have more resources available for colleges and universities and other institutions who manage their own SOC or who have outsourced functions for a SOC, some of which describe how a SOC can be implemented and function. The SOC will require well-established incident response procedures to succeed in its mission to identify, detect, and stop malicious activities on the campus network. Part of the incident response procedure is identifying what classifies as an incident or an event. This is also important for identifying metrics used to report and learn about the types and frequency of attacks affecting the network in order to invest in technology and establish processes to address the most severe and critical attacks

Some common university computer security incidents include:

- Automated notifications sent to POCs for systems under their care.
- E-mails sent tricking a user into opening a virus-infected file that results in a malware package executing.
- Phishing or spear-phishing e-mails sent with the intent of tricking a user into giving their credentials by clicking on a masked link to a website that looks similar to a university login page in order to harvest their credentials.
- Use of botnets to perform DDoS attacks against web or other electronic resources.
- Compromised account credentials used to send spam using university resources.
- E-mails sent with masked links exploiting vulnerabilities in a web browser or web browser plugin to infect a system and communicate with external hosts.
- A virus executed via trickery through e-mail or carefully placed removable media, which results in an attacker obtaining or encrypting data and holding the data ransom (*ransomware*).
- Data leaking through legitimate software used in an illegitimate manner due to vulnerabilities, exploits, or misconfigurations.

The SOC team should maintain updated incident response procedures on the chosen documentation website for the various types of incidents that affect the campus. These procedures should include the processes, people, and tools needed for identifying individuals involved with adverse events or incidents, the tools used to investigate incidents, and the processes required to obtain, maintain, and create an effective incident response procedure.

3.8 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

Many forms of cyber attacks are common today, including zero-day exploits, malware, phishing, man-in-the-middle attacks, and denial of service attacks. Different ways of attacking computer systems and networks constantly evolve as cybercriminals find new vulnerabilities to exploit. Cyber Threat Intelligence (CTI) helps organizations stay informed about new threats so that they can protect themselves. Cyber security experts organize, analyze, and refine the information they gather about attacks to learn from and use it to protect businesses better. Threat intelligence (or security intelligence) also helps stop or mitigate an attack that is in progress. The more an IT team understands about an attack, the better they will be able to make an informed decision about how to combat it. Threat intelligence and cyber threat tools help organizations understand the risks of different types of attacks, and how best to defend against them. Cyber threat intelligence also helps mitigate attacks that are already happening. An organization's IT department may gather its own threat intelligence, or they may rely on a threat intelligence service to gather information and advise on best security practices. Organizations that employ software defined networking (SDN) can use threat intelligence to quickly reconfigure their network to defend against specific types of cyber attacks.

3.9 Incident response

Incident response (IR) refers to an organization's processes and systems for discovering and responding to cybersecurity threats and breaches. The goal of IR is the detection, investigation, and containment of attacks in an organization. Lessons learned from IR activities also inform downstream prevention and mitigation strategies to enhance an organization's overall security posture.

Cybersecurity incidents are inevitable. Having a robust incident response program can be the difference between sinking and swimming. The frequency, sophistication, and severity of attack methods continue to increase, and it's crucial for a security operations center (SOC) to have documented and tested responses prepared for the threats they will face. The IR process helps answer crucial questions about an attack, such as how an attacker got in, what actions they took, and if sensitive information was compromised. Confidently answering these questions will not only improve an organization's security posture but also help with assessing potential legal or regulatory liabilities. Additionally, an effective IR strategy can reduce the economic impacts often associated with cybersecurity incidents or breaches.

Attack methods like malware outbreaks (including ransomware and spyware), DDoS, and credential theft can be costly and disruptive if an organization is not adequately prepared to respond.

3.10 Qradar & Understanding about tool

QRadar SIEM as shown in figure 4 monitors and correlates threat intel, network, and user behavior anomalies to prioritize high-fidelity alerts. Easy-to-use dashboards provide details to investigate and remediate threats in near real time.

Figure 4: Snapshot of Qradar Dashboard

Conclusion:-

- **Stage 1: - what do you understand from Web application testing ?**

Web application testing is very important to check for bugs or vulnerabilities on the website. There are multiple steps in web application testing.

Web testing is designed to check all aspects of the web application's functionality, including looking for bugs with usability, compatibility, security, and general performance.

- **Stage 2: - what you understand from the Nessus report.**

Nessus report gives the user a clear pictorial representation of the vulnerabilities if any in the website. In the demo, I have taken a vulnerable website namely demo.testfire.net and listed the vulnerabilities. There were 4 medium and 5 low vulnerabilities. We can generate the report in HTML or CSV format.

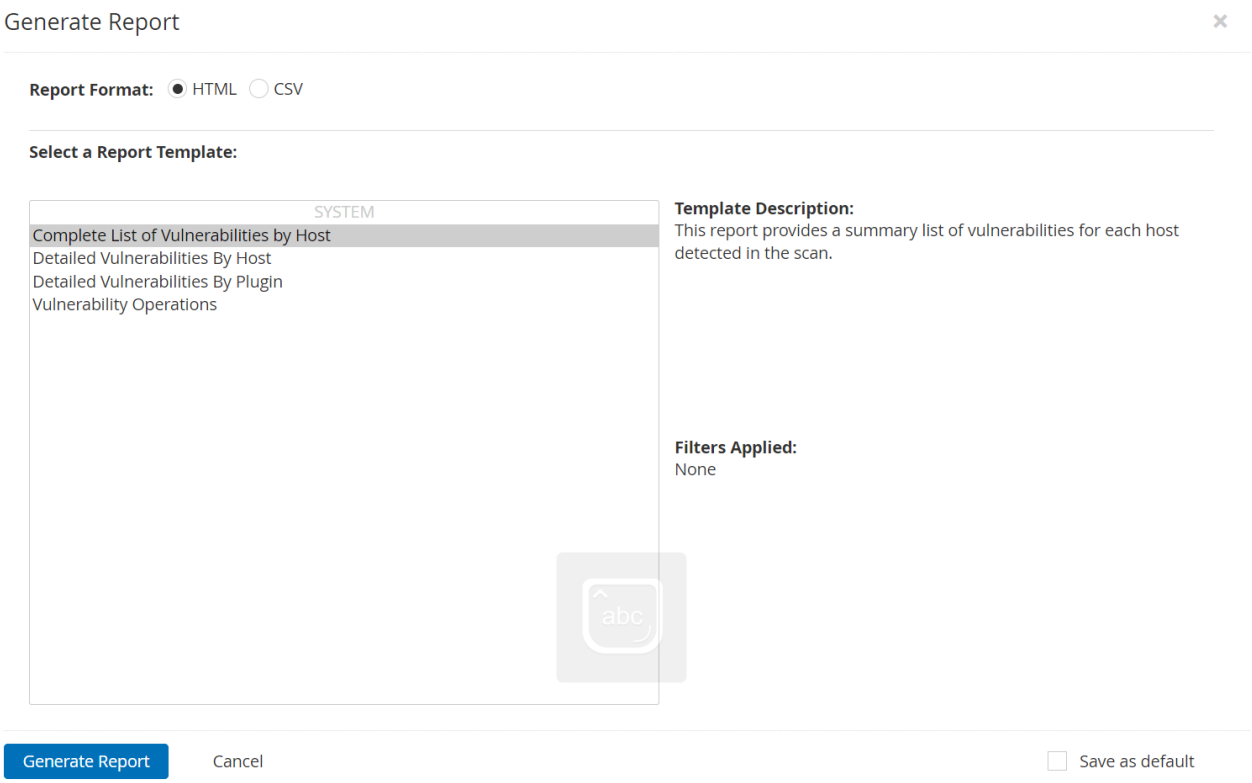

Figure 5: Snapshot of Report Generation in Nessus

The various templates which we can use are shown in figure 5. This tool is very useful for SOC analyst to identify and mitigate the vulnerabilities. Every vulnerability description and solution is provided by the tool. The risk information and severity is also mentioned.

- **Stage 3 :- what you understand from Qradar Dashboard.**

The Qradar dashboard provides views of network security, activity or data that is collected. The content that is displayed on the Dashboard tab is user specific. Changes that are made within a session affect only your system. For example, you can make these customizations:

- Add and remove dashboard items from your dashboards.
- Move and position items to meet your requirements.

- When you position items, each item is automatically resized in proportion to the dashboard.
- Add custom dashboard items that are based on any data.

  For example, you can add a dashboard item that provides a time series graph or a bar chart that represents top 10 network activity.

  To create custom items, you can create saved searches on the **Log Activity** tab and choose how you want the results that are represented in your dashboard. Each dashboard chart displays real-time up-to-the-minute data. Time series graphs on the dashboard refresh every 5 minutes.

Future Scope :-

- **Stage 1: - future scope of web application testing**

  Future software testing will need to address data privacy, data masking, and synthetic test data generation. Non-functional Testing: Beyond functional testing, there will be a focus on non-functional testing aspects like usability, accessibility, and compliance with industry regulations.

- **Stage 2 :- future scope of testing process you understood .**

  In trying to comprehend the future scope of Software Testing, it is important to understand that future of Software Testing will inevitably be conditioned by the upcoming technologies and the needs of the time. There is no denying the fact that there will be greater emphasis on quality through quality assurance, in order to ensure a delightful brand experience. Organizations shall strive to achieve the dual combination of delivering the best value at best quality. Additionally, the future of Testing in Software is expected to be dominated by Test Automation using Artificial Intelligence and Machine Learning.

- **Stage 3 :- future scope of SIEM**

  The future of SIEM lies in predictive analytics and machine learning, which can help organizations prevent attacks before they occur. Predictive analytics is linked with big data and data science. Nowadays, organizations have a large amount of data in different repositories, and data scientists extract insights using deep learning and machine learning algorithms. Techniques such as logistic and linear regression models, neural networks and decision trees are used to make predictions. These modeling techniques use initial predictive learnings to make additional predictive insights.

Topics explored :-

Web Application Testing, SOC and SIEM

Tools explored :-

Kali Linux and Metasploitable VM, Nessus, IBM Qradar

References:

[1]https://er.educause.edu/articles/2017/1/create-a-security-operations-center-on-your-campus
[2] https://www.paloaltonetworks.com/cyberpedia/what-is-incident-response
[3]https://mediacenter.ibm.com/media/IBM+Security+QRadar+SIEM+Overview/1_onai4u1f#:~:text=Details,com%2Fproducts%2Fqradar%2Dsiem
[4] https://www.ibm.com/products/qradar-siem
[5]https://www.ibm.com/docs/en/qradar-on-cloud?topic=siem-dashboard-management
[6] Di Lucca, Giuseppe A., and Anna Rita Fasolino. "Testing Web-based applications: The state of the art and future trends." *Information and Software Technology* 48.12 (2006): 1172-1186.
[7] https://securityintelligence.com/posts/the-future-of-siem-embracing-predictive-analytics/

—---------THE END —----------