Date	10 March 2025
Team ID	PNT2025TMID04146
Project Name	Advanced Techniques in Rule Creation for Threat Detection
Maximum Marks	8 Marks

List of teammates–

S.no	name	collage	contact
1	Arjun Dhumal	St.vincent Palloti	8329073510
2	Manasvi Bansod	St.vincent Palloti	8530941510

Abstract:

The objective of this project is to explore advanced techniques in rule creation for threat detection in the domain of cybersecurity analytics. By utilizing dynamic, machine learning-based, and context-aware rules, this project aims to enhance detection capabilities in Security Information and Event Management (SIEM) systems and automate threat response in real-time. The project also integrates vulnerability scanning using Nessus, along with SOC and SIEM tools, to improve detection accuracy and minimize false positives.

Scope of the Project :

The project aims to improve threat detection methodologies by:
- Integrating machine learning and behavior-based rule creation techniques into SIEM systems.
- Implementing real-time dynamic rule adaptation to the network environment.
- Conducting vulnerability assessments using tools like Nessus to fine-tune detection rules.
- Evaluating the effectiveness of these techniques through practical testing and SOC analysis.

Objectives of the Project :

1. To explore and evaluate advanced rule creation techniques for enhancing threat detection.
2. To assess the effectiveness of Nessus vulnerability scanning in identifying security gaps and customizing detection rules.
3. To implement and test dynamic rule adaptation based on the network's current state.
4. To understand the role of SOC and SIEM tools in real-time cybersecurity monitoring and incident response.
5. To provide a comprehensive solution for improving cybersecurity defense systems.

The Thought Behind the Project:

Step 1: Various Ideas

The team discussed various ideas on improving threat detection methods. Initially, we focused on traditional signature-based detection, but later pivoted towards more adaptive and machine learning-driven techniques. We explored integrating anomaly detection and context-aware rules that could adapt to the ever-evolving threat landscape.

Step 2: Selecting some features and grouping them :

We grouped features based on their ability to enhance detection capabilities, reduce false positives, and adapt to changes:

- Anomaly Detection: Identifying abnormal patterns in network behavior.
- Context-Aware Rules: Customizing rules based on real-time conditions (e.g., network topology, user behavior).
- Machine Learning Models: Enabling systems to learn from previous attacks and adapt.

Step 3: Priority Chart

We prioritized the features based on their impact:

1. Machine Learning Integration
2. Dynamic Rule Adaptation
3. Context-Aware Detection
4. Anomaly Detection

Step 4: Empathy Map :

- User Pain Points: Security analysts often face information overload, inaccurate alerts, and high false positive rates.
- Needs: A smarter, more efficient threat detection system that adapts to new threats and reduces manual intervention.
- Goals: Increase detection accuracy and response speed.
- Tasks: Implement rules that are flexible, real-time, and adaptable to changing environments.

Project Planning:

The project was planned with several phases:
- Phase 1: Research and tool exploration.
- Phase 2: Implementation of rule creation techniques and integration with Nessus.
- Phase 3: Testing and fine-tuning the detection rules.
- Phase 4: Evaluation using SOC and SIEM tools.

Cybersecurity Template.docx

> Stage – 1:

List of Vulnerability Table —

S.no	Vulnerability Name	CWE - No
1	SQL Injection	CWE-89
2	Cross-Site Scripting	CWE-79
3	Buffer Overflow	CWE-119

REPORT:-

Vulnerability Name:- SQL Injection

CWE : - CWE-89

Description: SQL Injection occurs when an attacker is able to manipulate SQL queries through unsanitized input fields.

Business Impact: It can lead to unauthorized access to sensitive data, database compromise, or denial of service.

Stage – 2

Overview Nessus is a powerful vulnerability scanner that helps in identifying potential weaknesses in networks and applications. It provides a comprehensive assessment, detecting issues like missing patches, misconfigurations, and known vulnerabilities in the system.

Nexus as a Centralized Threat Intelligence Platform:

In some cybersecurity contexts, **Nexus** can refer to a platform or hub where threat intelligence data from various sources is aggregated, correlated, and analyzed. This kind of "Nexus" acts as a centralized point of connection for threat data, helping organizations to detect, understand, and respond to threats more efficiently. These platforms often integrate information about attack patterns, indicators of compromise (IOCs), vulnerabilities, and threat actor tactics, techniques, and procedures (TTPs).

Features of a Nexus in Cybersecurity Intelligence:

- **Centralized Threat Data**: Aggregates threat data from different sources like SIEM systems, threat feeds, internal data, and more.
- **Correlation and Analysis**: Helps to connect the dots between different threat signals and incidents across an organization's IT infrastructure.
- **Collaboration Hub**: Facilitates sharing threat intelligence between security teams, organizations, and industry groups.
- **Incident Response and Automation**: Helps automate threat detection, response, and remediation by integrating with other security tools like firewalls, endpoint detection, and SIEM platform.

Target website —

Target ip address:- sql injection

List of vulnerability —

s.no	Vulnerability name	Severity	plugins
1	SQL Injection	High	12345
2	XSS	Medium	67890

REPORT:-

Vulnerability Name : SQL Injection

severity : - high

Plugin: 12345
Port :- 80

Description: Allows attackers to run arbitrary SQL queries, possibly gaining control over the database.

Solution: Allows attackers to run arbitrary SQL queries, possibly gaining control over the database.

Business impact: Data theft, loss of integrity, and potential system compromise.

Report

Title: Understanding the Ability of SOC / SIEM in Real-Time Threat Detection

- **SOC (Security Operations Center):** A SOC is a dedicated team that monitors and defends an organization's IT infrastructure. It uses various tools like SIEM for threat detection, analysis, and response.
- **SOC Cycle**: The SOC cycle involves continuous monitoring, alerting, triaging, incident response, and recovery.
- **SIEM** (Security Information and Event Management): SIEM tools aggregate logs and data from various sources to identify potential security incidents.
- **SIEM Cycle:** It involves data collection, correlation, analysis, alerting, and response.
- **MISP** (Malware Information Sharing Platform): MISP is used for sharing threat intelligence and helps in creating accurate threat detection rules.
- Deploying SOC in Your College: Implementing a small-scale SOC using open-source tools like Suricata for intrusion detection and SIEM for log aggregation.

Conclusion

- **Stage 1 :**
- Web Application Testing – Understanding of how vulnerabilities like SQL Injection and XSS can be exploited in a web app.
-
- **Stage 2 :**
- Nessus Report – The importance of vulnerability scanning and how Nessus helps to identify critical issues
- **Stage 3 :**
- SOC / SIEM – Understanding the role of SOC and SIEM in effective cybersecurity defense.

Future Scope :-

- **Stage 1 :- future scope of web application testing**
- Future scope in web application testing could include more advanced techniques like dynamic analysis and fuzz testing.
- **Stage 2 :- future scope of testing process you understood**
- Testing processes could evolve with automation and continuous integration, making testing faster and more efficient.
- **Stage 3 :- future scope of SOC / SEIM**
- The future of SOC/SEIM will likely include greater integration with machine learning to predict and respond to threats faster.

Topics explored :-

- Advanced Rule Creation

-Vulnerability Scanning with Nessus

- SOC & SIEM Integration

- Machine Learning in Cybersecurity

Tools explorer

-Nessus

-Splunk

-IBM QRadar

--MISP

—-----THE END —----------