IMPLEMENTING WEBSITE SECURITY INCIDENT RESPONSE ORCHESTRATION METHOD BASED ON SECURITY INFORMATION AND EVENT MANAGEMENT, SECURITY ORCHESTRATION, AUTOMATION, AND RESPONSE

I NYOMAN DARMAYOGA
Program Studi Informatika, Fakultas Sains & Teknologi
Universitas Teknologi Yogyakarta
Jl. Ringroad Utara Jombor Sleman Yogyakarta
E-mail: darmayoga1702@gmail.com

ABSTRACT

Advances in digital technology have increased the complexity of cyber threats, necessitating an integrated system for real-time incident detection, mitigation, and investigation. This research aims to develop the SYRA web application, which integrates SIEM (Wazuh), SOAR (n8n), and DFIR-IRIS using an orchestration approach to automate detection, response, notification, and investigation workflows. The research methodology includes problem identification, data collection, requirements analysis, system design, implementation, and testing and evaluation. Testing was conducted using black-box testing to verify system functionality and performance, and using three types of attacks: DDoS, SQL Injection, and XSS. The results showed that all SYRA features performed as specified, achieving a 100% attack detection rate, with average response times of approximately 4 seconds for SQL Injection and XSS attacks and 42.97 seconds for DDoS attacks. The DFIR-IRIS integration successfully provided automated incident documentation for digital forensic analysis. The SYRA system proved effective and responsive, with orchestration among components ensuring rapid, consistent detection, mitigation, and investigation, thereby enhancing the system's resilience against modern cyber threats.

Keywords: SIEM, SOAR, XSS, DDoS, SQL Injection