PERANCANGAN SECURITY ORCHESTRATION, AUTOMATION, AND RESPONSE UNTUK RESPONS INSIDEN SEMI-OTOMATIS (STUDI KASUS: UPA TIK UPN VETERAN JAKARTA)

Bayu Erik Wibisono

ABSTRAK

Kompleksitas serangan siber yang semakin meningkat menuntut sistem deteksi dan respons cepat yang terintegrasi. Penelitian ini merancang sistem Security Orchestration, Automation, and Response (SOAR) melalui pendekatan semi-otomatis dengan memanfaatkan Wazuh sebagai Security Information and Event Management (SIEM), MISP sebagai Threat Intelligence, IRIS untuk manajemen insiden, serta Shuffle sebagai SOAR. Sistem juga dilengkapi notifikasi Google Chat untuk peringatan dini serta kontrol atas sistem. Pengujian dilakukan terhadap serangan aplikasi web seperti SQL Injection, File Inclusion, serta deteksi *malware*. Hasilnya, Wazuh berhasil mendeteksi serangan yang diujikan. Nilai kinerja menunjukkan waktu Mean Time to Detect (MTTD) sebesar 6.66 detik, Mean Time to Acknowledge (MTTA) sebesar 18 detik, dan Mean Time to Respond (MTTR) sebesar 10 detik, serta setiap *workflow* dapat dijalankan dalam waktu kurang dari 35 detik menandakan proses deteksi dan respons berjalan cepat. Secara keseluruhan, sistem SOAR yang dibangun meningkatkan visibilitas keamanan, otomatisasi respons, serta efektivitas penanganan insiden.

Kata Kunci: SOAR, SIEM, CTI, Manajemen Kasus, Semi-Otomatisasi

DESIGN OF SECURITY ORCHESTRATION, AUTOMATION, AND RESPONSE FOR SEMI-AUTOMATED INCIDENT RESPONSE (CASE STUDY: UPA TIK UPN VETERAN JAKARTA)

Bayu Erik Wibisono

ABSTRACT

The increasing complexity of cyberattacks demands an integrated system capable of rapid detection and response. This study designs a semi-automated Security Orchestration, Automation, and Response (SOAR) system by utilizing Wazuh as Security Information and Event Management (SIEM), MISP as Threat Intelligence platform, IRIS for incident management, and Shuffle as SOAR. The system is also equipped with Google Chat notifications for early warnings and system control. Testing was conducted against web application attacks such as SQL Injection, File Inclusion, and malware detection. The results show that Wazuh successfully detected the tested attacks. The performance metrics show a Mean Time to Detect (MTTD) of 6.66 seconds, a Mean Time to Acknowledge (MTTA) of 18 seconds, and a Mean Time to Respond (MTTR) of 10 seconds, with each workflow executed in under 35 seconds, demonstrating a fast detection and response process. Overall, the implemented SOAR system enhances security visibility, response automation, and the effectiveness of incident handling.

Keywords: SOAR, SIEM, CTI, Case Management, Semi-Automation