IMPLEMENTASI OSSIM DAN SPLUNK UNTUK MONITORING DAN ANALISA SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)
EMITA ARIANI, Ir. Alif Subardono, S.T., M.Eng.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

INTISARI

IMPLEMENTASI OSSIM DAN SPLUNK UNTUK MONITORING DAN ANALISA *SECURITY INFORMATION AND EVENT MANAGEMENT* (*SIEM*)

Emita Ariani
20/457210/SV/17657

Seiring dengan perkembangan teknologi yang sangat pesat, ancaman terhadap keamanan aplikasi web juga mengalami peningkatan. Oleh karena itu, diperlukan suatu sistem keamanan yang mampu memantau, menganalisis, dan mendeteksi ancaman terhadap setiap aktivitas yang terjadi pada lalu lintas jaringan atau aplikasi web secara *real-time*. *Security Information and Event Management (SIEM)* merupakan solusi yang tepat untuk hal ini karena SIEM mampu mengelola, mengorelasi, menganalisis, dan mendeteksi ancaman keamanan secara *real-time*. Penelitian ini bertujuan untuk membandingkan dua *tool* SIEM, yaitu OSSIM dan Splunk dalam memonitoring dan mendeteksi berbagai jenis serangan keamanan. Pengujian serangan dalam penelitian ini terdiri dari beberapa skenario, yaitu skenario pengujian serangan tunggal, skenario pengujian kombinasi dua serangan, skenario pengujian kombinasi tiga serangan, skenario pengujian kombinasi empat serangan, dan skenario pengujian kombinasi lima serangan. Hasil penelitian ini menunjukkan bahwa OSSIM lebih efektif dalam mengidentifikasi serangan karena dapat mengklasifikasikan jenis serangan yang terdeteksi sehingga memudahkan proses identifikasi dan analisis. Sedangkan Splunk menampilkan hasil berupa *log* mentah sehingga Splunk memiliki keunggulan dalam transparansi data visibilitas yang lebih komprehensif, sehingga mendukung proses analisis yang lebih mendalam.

Kata kunci: OSSIM, Splunk, *Security Information and Event Management (SIEM)*, deteksi serangan

IMPLEMENTASI OSSIM DAN SPLUNK UNTUK MONITORING DAN ANALISA SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)
EMITA ARIANI, Ir. Alif Subardono, S.T., M.Eng.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

ABSTRACT

IMPLEMENTATION OF OSSIM AND SPLUNK FOR MONITORING AND ANALYSIS OF SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

Emita Ariani
20/457210/SV/17657

The rapid advancement of technology has been accompanied by a significant increase number of threats to web application security. Consequently, organizations require a security solution capable of monitoring network traffic and web application activities while detecting potential threats in real-time. Security Information and Event Management (SIEM) provides these capabilities by collecting, correlating, analyzing, and detecting security events from multiple data sources. This study aims to compare the performance of two SIEM tools, OSSIM and Splunk, in monitoring and detecting various types of cyber-attacks. This study employed several attack testing scenarios, including single attacks and combinations of two, three, four, and five attacks. The results of this study indicate that OSSIM is more effective in identifying attack events because it can classify the types of detected attacks, thereby facilitating the identification and analysis process. In contrast, Splunk presents the results as raw logs, providing greater data transparency and more comprehensive visibility, thereby facilitating more in-depth attack analysis.

Keywords: *OSSIM, Splunk, Security Information and Event Management (SIEM), attack detection*