

**Penerapan *Security Information And Event Management (SIEM)***

**Pada Dinas Komunikasi Dan Informatika Kota Salatiga**



**Program Studi Teknik Informatika**

**Fakultas Teknologi Informasi**

**Universitas Kristen Satya Wacana**

**Salatiga**

**2023**

**Perancangan Dan Implementasi *Security Information and Event Management* (SIEM) pada Layanan Virtual Server**

**Artikel Ilmiah**

**Diajukan Kepada**

**Fakultas Teknologi Informasi**

**Untuk Memperoleh Gelar Sarjana Komputer**



**Program Studi Teknik Informatika**

**Fakultas Teknologi Informasi**

**Universitas Kristen Satya Wacana**

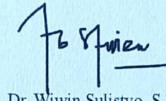
**Salatiga**

**2023**

**Lembar Pengesahan**

Judul Artikel : Perancangan Dan Implementasi Security Information and Event management (SIEM) pada Layanan Virtual Server  
Nama Mahasiswa : HUELILIK DYAN HELUKA  
NIM : 672018215  
Program Studi : Teknik Informatika  
Fakultas : Teknologi Informasi

Menyetujui,

  
Dr. Wiwin Sulistyowati, S.T., M.Kom.  
Pembimbing 1



Dinyatakan Lulus Proses Review Tanggal : 10 Juli 2023

*Reviewer :*

- Dian W. Chandra, S.Kom., M.Cs.



**Penerapan Security Information And Event Management (SIEM) Pada Dinas  
Komunikasi Dan Informatika Kota Salatiga**

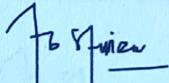
Oleh,

**HUELILIK DYAN HELUKA**  
**672018215**

**LAPORAN PENELITIAN**

Diajukan Kepada Program Studi Teknik Informatika guna memenuhi sebagian dari persyaratan  
untuk mencapai gelar Sarjana Komputer

Disetujui oleh,

  
Dr. Wiwin Sulistyo, S.T., M.Kom.  
Pembimbing 1

Diketahui oleh,

   
Prof. Jr. Daniel H. F. Manongga, M.Sc., Ph.D. Budhi Kristianto, S.Kom., M.Sc., Ph.D.  
Dekan Ketua Program Studi

**FAKULTAS TEKNOLOGI INFORMASI  
UNIVERSITAS KRISTEN SATYA WACANA  
SALATIGA  
2023**

## **Pernyataan**

Yang bertandatangan di bawah ini,

Nama Mahasiswa	:	Huelilik Dyan Heluka
NIM	:	672018170
Program Studi	:	Teknik Informatika
Fakultas	:	Teknologi Informasi

Menyatakan dengan sesungguhnya bahwa tugas akhir dengan judul :

### **Penerapan Security Information And Event Management (SIEM) Pada Dinas Komunikasi Dan Informatika Kota Salatiga**

Yang dibimbing oleh :

Dr. Wiwin Sulistyo, S.T., M.Kom

Adalah benar-benar hasil karya saya.

Di dalam tugas akhir ini tidak terdapat keseluruhan atau sebagian tulisan atau gagasan orang lain yang saya ambil dengan cara menyalin atau meniru dalam bentuk rangkaian kalimat atau gambar serta symbol yang saya klaim seolah-olah sebagai karya saya tanpa memberikan pengakuan pada penulis atau sumber aslinya.

Salatiga, Februari 2023

Yang memberi pernyataan

Huelilik Dyan Heluka

# **Penerapan Security Information And Event Management (SIEM)**

## **Pada Dinas Komunikasi Dan Informatika Kota Salatiga**

**Huelilik Dyan Heluka 1) , Wiwin Sulisty 2)**

Program Studi Teknik Informatika

Fakultas Teknologi Infromasi

Universitas Kristen Satya Wacana

Jl. O. Notohamidjojo, Salatiga 50711, Indonesia

Email : [672018170@student.uksw.edu](mailto:672018170@student.uksw.edu) , [wiwinsulistyo@uksw.edu](mailto:wiwinsulistyo@uksw.edu)

### **Abstrak**

Perangkat yang dapat diakses melalui jaringan internet telah memberikan kenyamanan dan koneksi yang luar biasa dalam kehidupan sehari-hari. Namun, kenyataannya adalah bahwa perangkat tersebut juga menjadi sasaran menarik bagi para aktor jahat. Ancaman keamanan seperti serangan malware, serangan virus komputer, dan serangan Siber lainnya dapat dengan mudah menyerang perangkat yang terhubung ke internet. Untuk mengatasi tantangan ini, diperlukan solusi yang efektif dan canggih. SIEM merupakan platform keamanan yang menggabungkan teknologi security information management (SIM) and security event management (SEM). SIEM Bekerja dengan cara mengumpulkan log dari berbagai sumber kemudian menormalisasi dan mengagregasi data peristiwa log yang kemudian diproses menggunakan parameter kontekstual yang terdapat di dalam SIEM, yang dikumpulkan dari berbagai sumber internal dan eksternal perangkat Endpoint seperti Sistem Operasi, kontainer, dan perangkat jaringan. Penelitian ini bertujuan untuk mengimplementasikan SIEM Wazuh dengan tujuan utama yaitu melakukan sentralisasi log untuk mendeteksi dengan cepat serangan pada VPS, terutama pada serangan aplikasi web dan serangan pada protokol SSH. Dengan hasil akhir implementasi SIEM, data log dari setiap aplikasi dapat disentralisasi dan divisualisasikan dalam sebuah dashboard, serta SIEM mampu mendeteksi serangan pada aplikasi web dan protokol SSH yang sebelumnya tidak terdeteksi.

**Kata kunci:** Security Operation Center; SIEM; Open Source; Wazuh;

### **Abstract**

Devices accessible through the Internet have provided incredible convenience and connectivity in everyday life. However, the reality is that the device is also an attractive target for bad actors. Security threats such as malware attacks, computer virus attacks, and other cyberattacks can easily attack devices connected to the Internet. To overcome these challenges, effective and sophisticated solutions are needed. SIEM is a security platform that combines security information management (SIM) and security event management technology. (SEM). SIEM Works by collecting logs from various sources and then normalizing and aggregating log event data that is then processed using contextual parameters contained in SIEM collected from various internal and external endpoint devices such as Operating systems and network devices. The research is aimed at implementing the Wazuh SIEM with the primary objective of centralizing logs to quickly detect attacks on VPS, especially web application attacks and SSH protocol attacks. With the final results of SIEM implementation, log data from each application can be decentralized and visualized in a dashboard, and SIEM is able to detect attacks on previously undetected web applications and SSH protocols.

**Keyword:** Security Operation Center; SIEM; Open Source; Wazuh;