# PROTOTIPE SECURITY OPERATIONS CENTER BERBASIS INTEGRASI SOFTWARE OPEN SOURCE UNTUK OPTIMASI DETEKSI DAN RESPONS ANCAMAN SIBER

**SKRIPSI**
**Diajukan untuk memenuhi sebagian persyaratan mendapatkan gelar Strata Satu Program Studi Informatika**

**DIMAS GALIH LAKSONO**
**22EO10019**

**PROGRAM STUDI INFORMATIKA**
**FAKULTAS MATEMATIKA DAN ILMU KOMPUTER**
**UNIVERSITAS NAHDLATUL ULAMA AL GHAZALI**
**CILACAP**
**2026**

# PROTOTIPE SECURITY OPERATIONS CENTER BERBASIS INTEGRASI SOFTWARE OPEN SOURCE UNTUK OPTIMASI DETEKSI DAN RESPONS ANCAMAN SIBER

**SKRIPSI**
**Diajukan untuk memenuhi sebagian persyaratan mendapatkan gelar Strata Satu Program Studi Informatika**

**DIMAS GALIH LAKSONO**
**22EO0019**

**PROGRAM STUDI INFORMATIKA**
**FAKULTAS MATEMATIKA DAN ILMU KOMPUTER**
**UNIVERSITAS NAHDLATUL ULAMA AL GHAZALI**
**CILACAP**
**2026**

## HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Dengan ini saya menyatakan bahwa penulisan skripsi dengan judul "Prototipe Security Operations Center Berbasis Integrasi Software Open Source Untuk Optimasi Deteksi Dan Respons Ancaman Siber" adalah hasil karya saya dengan arahan dari pembimbing dan belum diajukan kepada pihak manapun. Sumber informasi yang dikutip dalam skripsi ini telah dicantumkan dalam Daftar Pustaka.

Demikian pernyataan ini dibuat dengan sebenarnya. Apabila di kemudian hari terdapat ketidaksesuaian dalam pernyataan ini, maka saya bersedia menerima sanksi sesuai dengan peraturan yang berlaku.

Cilacap, Juli 2026


Dimas Galih Laksono
22EO10019

## LEMBAR PENGESAHAN

Skripsi Saudara

| | | |
|---|---|---|
| Nama | : | Dimas Galih Laksono |
| NIM | : | 22EO10019 |
| Fakultas/Prodi | : | Fakultas MIKOM /Informatika |
| Judul | : | Prototipe Security Operations Center Berbasis Integrasi Software Open Source Untuk Optimasi Deteksi Dan Respons Ancaman Siber |

Telah disidangkan oleh Dewan Penguji Fakultas Matematika dan Ilmu Komputer Universitas Nahdlatul Ulama Al Ghazali (UNUGHA) Cilacap pada hari / tanggal :

**Rabu, 01 Juli 2026**

Dan dapat diterima sebagai pemenuhan tugas akhir mahasiswa Program Strata Satu (S.1) Program Studi Informatika (S.Kom.) Fakultas Matematika dan Ilmu Komputer (FMIKOM) pada Universitas Nahdlatul Ulama Al Ghazali (UNUGHA) Cilacap.

Cilacap, 13 Juli 2026

Dewan Sidang

| Ketua | Sekretaris |
|---|---|
| **M.T Abdul Aziz Zein, M.Kom.** | **Abdul Haq, S.E., M.Cs.** |
| NIDN. 2125098601 | NIDN.0606067701 |
| Penguji 1 | Penguji 2 |
| **M.T Abdul Aziz Zein, M.Kom.** | **Verry, S.T., M.Kom.** |
| NIDN. 2125098601 | NIDN. 0628068001 |
| Pembimbing I | Pembimbing II |
| **Abdul Haq, S.E., M.Cs.** | **Sani Nurmalasari, M.Kom.** |
| NIDN. 0606067701 | NUPTK. 4341767668231113 |

Mengetahui,
Dekan Fakultas Matematika dan Ilmu Komputer

**M.T Abdul Aziz Zein, M.Kom.**
NIDN. 2125098601

## HALAMAN NOTA KONSULTAN

M.T Abdul Aziz Zein, M.Kom.

Dosen Fakultas Matematika dan Ilmu Komputer
Universitas Nahdlatul Ulama Al Ghazali Cilacap

**NOTA KONSULTAN**

Hal : Skripsi Saudara Dimas Galih Laksono
Lampiran : -

Kepada
Yth. Dekan Fakultas Matematika dan Ilmu Komputer
Universitas Nahdlatul Ulama Al Ghazali Cilacap
di Cilacap

*Assalamu'alaikum Wr. Wb.*
Setelah membaca, memeriksa dan melakukan perbaikan seperlunya maka skripsi saudara:

Nama : Dimas Galih Laksono
NIM : 22EO10019
Prodi : Informatika
Judul : Prototipe Security Operations Center Berbasis Integrasi Software Open Source Untuk Optimasi Deteksi Dan Respons Ancaman Siber

Dapat diajukan ke Fakultas Matematika dan Ilmu Komputer, Universitas Nahdlatul Ulama Al Ghazali Cilacap untuk memenuhi syarat memperoleh gelar Strata Satu (S1).
*Wassalamu'alaikum Wr. Wb.*

Cilacap, 13 Juli 2026

M.T Abdul Aziz Zein, M.Kom.
NIDN. 2125098601

**NOTA PEMBIMBING**

Cilacap, 23 juni 2026

Kepada Yth :
Fakultas Matematika dan Komputer (FMIKOM)
UNUGHA Cilacap
di Cilacap

*Assalamu'alaikum Wr. Wb.*
Setelah melakukan bimbingan, telaah, arahan dan koreksi tahap penulisan skripsi saudari:

| | |
|---|---|
| Nama | : Dimas Galih Laksono |
| NIM | : 22EO10019 |
| Fakultas | : Matematika dan Ilmu Komputer |
| Prodi | : Informatika |
| Judul | : Prototipe Security Operations Center Berbasis Integrasi Software Open Source Untuk Optimasi Deteksi Dan Respons Ancaman Siber |

Kami berpendapat bahwa skripsi tersebut sudah dapat diajukan ke sidang skripsi. Bersamaan ini kami kirimkan skripsi tersebut, semoga dapat segera disidangkan.

Atas perhatiannya kami ucapkan terima kasih.
*Wassalamu'alaikum Wr. Wb.*

Mengetahui,

| Pembimbing I | Pembimbing II |
|---|---|
| Abdul Haq, S.E., M.Cs | Sani Nurmalasari, M.Kom |
| NIDN.0606067701 | NUPTK.4341767668231113 |

## HALAMAN MOTO

"Dan jika kamu membalas, maka balaslah dengan (balasan) yang sama dengan siksaan yang ditimpakan kepadamu. Tetapi jika kamu bersabar, sesungguhnya itulah yang lebih baik bagi orang yang sabar"

(QS. An-Nahl : 126)

"Jangan takut untuk melangkah lambat, takutlah jika kamu hanya berdiri diam tanpa pernah bergerak sama sekali"

(Confucius)

"Jika kamu merasa duniamu kejam dan sulit, jangan menyerah. Teruslah berjuang, karena kamu tidak akan pernah tahu hasil akhir dari sebuah perjuangan sebelum kamu benar-benar menyelesaikannya"

(Eren Yeager)

# KATA PENGANTAR

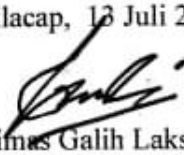
Puji syukur kepada Allah SWT atas segala limpahan nikmat dan karuniaNya, sehingga penulis dapat menyelesaikan penulisan skripsi. Sholawat dan salam senantiasa penulis haturkan kepada Nabi Muhammad SAW sebagai pembimbing seluruh umat manusia.

Skripsi ini tidak akan selesai tanpa adanya bantuan dari banyak pihak, karena itu penulis menyampaikan terima kasih kepada :

1. Bapak M.T Abdul Aziz Zein, M.Kom, Dekan FMIKOM UNUGHA
2. Bapak Abdul Haq, S.E., M.Cs, pembimbing I yang telah dengan sabar memberikan bimbingan dan petunjuk dalam menyelesaikan skripsi ini.
3. Ibu Sani Nurmalasari, M.Kom, pembimbing II yang telah dengan sabar memberikan bimbingan dan petunjuk dalam menyelesaikan skripsi ini.
4. Ibu Riski Aspriyani, M.Pd, sebagai Pembimbing Akademis
5. Bapak-Ibu dosen Program Studi Informatika FMIKOM UNUGHA
6. Semua pihak yang tidak dapat kami sebutkan satu persatu

Semoga Allah SWT membalas jerih payah dan pengorbanan yang telah diberikan dengan balasan yang lebih baik. Amiin. Penulis berharap semoga karya kecil ini bermanfaat bagi pembaca.

Cilacap, 13 Juli 2026



Dimas Galih Laksono

# ABSTRAK

DIMAS GALIH LAKSONO. Prototipe Security Operations Center Berbasis Integrasi Software Open Source Untuk Optimasi Deteksi Dan Respons Ancaman Siber. Dibimbing oleh Abdul Haq, S.E., M.Cs. dan Sani Nurmalasari, M.Kom.

Serangan siber tidak lagi menjadi ancaman yang bersifat potensial, melainkan telah menjadi realitas yang dihadapi hampir setiap institusi. Ancaman siber tidak hanya berpotensi menyebabkan gangguan operasional dan kerusakan sistem, tetapi juga dapat mengakibatkan kebocoran data serta kerugian *finansial*. *Security Operations Center* merupakan salah satu solusi yang dapat digunakan untuk melakukan pemantauan, deteksi, analisis, dan respons terhadap ancaman siber secara terpusat. Namun, implementasi SOC konvensional umumnya membutuhkan biaya investasi yang tinggi sehingga sulit diterapkan oleh organisasi dengan keterbatasan sumber daya.

Dalam penelitian ini dilakukan beberapa tahapan, yaitu studi literatur, perancangan arsitektur dan alur kerja SOC, implementasi sistem, pengujian, analisis hasil pengujian, serta penarikan kesimpulan. Prototipe SOC dibangun dengan mengintegrasikan berbagai *software open source*, yaitu Wazuh sebagai *Intrusion Detection System (IDS), Endpoint Detection and Response (EDR)* dan *Intrusion Prevention System (IPS)*, Graylog sebagai sistem manajemen *log (centralized log management),* MISP sebagai platform *threat intelligence*, serta VirusTotal sebagai *Extended Detection and Response (XDR)* untuk mendukung analisis dan korelasi ancaman keamanan. Selain itu, Telegram Bot dan *Email Notification* digunakan sebagai media notifikasi keamanan secara *real-time*. Pengujian sistem dilakukan terhadap berbagai mekanisme keamanan, meliputi *File Integrity Monitoring (FIM),* Docker *Monitoring*, *Active Response*, Anti *Malware*, *Threat Intelligence*, serta simulasi serangan yang mengacu pada OWASP Top 10 dan MITRE ATT&CK guna mengevaluasi kemampuan deteksi dan respons terhadap ancaman siber.

Hasil penelitian menunjukkan bahwa prototipe *Security Operations Center* berbasis integrasi *software open source* berhasil diimplementasikan dan seluruh komponen dapat terintegrasi dengan baik. Sistem mampu melakukan *monitoring log* secara terpusat, mendeteksi berbagai aktivitas dan ancaman keamanan, memanfaatkan *threat intelligence*, serta menjalankan respons otomatis terhadap insiden keamanan. Berdasarkan hasil pengujian yang dilakukan, sistem menunjukkan tingkat akurasi deteksi yang tinggi dan mampu menghasilkan *alert* serta notifikasi keamanan secara *near real-time*. Dengan demikian, prototipe SOC yang dibangun dapat menjadi alternatif solusi yang efektif, terintegrasi, dan lebih terjangkau dalam mendukung proses deteksi dan respons ancaman siber.

Kata kunci : *Cyber Security, Cyber Defense, Security Operations Center, Blue Team.*

*ABSTRACT*

DIMAS GALIH LAKSONO. *Prototype of a Security Operations Center Based on Integrated Open-Source Software for Optimizing Cyber Threat Detection and Response*. *Supervised by 1st* Abdul Haq, S.E., M.Cs. and *2nd* Sani Nurmalasari, M.Kom.

*Cyberattacks are no longer merely potential threats but have become a reality faced by nearly every institution. Cyber threats not only have the potential to cause operational disruptions and system damage, but can also lead to data breaches and financial losses. A Security Operations Center (SOC) is one of the solutions that can be used to centrally monitor, detect, analyze, and respond to cyber threats. However, conventional SOC implementations generally require high investment costs, making them difficult to adopt for organizations with limited resources.*

*This study was conducted through several stages, namely literature review, SOC architecture and workflow design, system implementation, testing, analysis of test results, and conclusion drawing. The SOC prototype was developed by integrating various open-source software tools, namely Wazuh as an Intrusion Detection System (IDS), Endpoint Detection and Response (EDR) and Intrusion Prevention System (IPS), Graylog as a centralized log management system, MISP as a threat intelligence platform, and VirusTotal as an Extended Detection and Response (XDR) component to support threat analysis and correlation. In addition, Telegram Bot and Email Notification were used as real-time security alerting mechanisms. System testing was carried out across various security mechanisms, including File Integrity Monitoring (FIM), Docker Monitoring, Active Response, Anti-Malware, and Threat Intelligence, as well as attack simulations based on the OWASP Top 10 and MITRE ATT&CK frameworks to evaluate detection and response capabilities against cyber threats.*

*The results of the study indicate that the prototype of the Security Operations Center based on integrated open-source software was successfully implemented and all components were effectively integrated. The system is capable of centralized log monitoring, detecting various security activities and threats, utilizing threat intelligence, and executing automated responses to security incidents. Based on the testing results, the system demonstrated a high level of detection accuracy and was able to generate alerts and security notifications in near real-time. Therefore, the developed SOC prototype can serve as an effective, integrated, and more affordable alternative solution to support cyber threat detection and response processes.*

Keywords*: Cybersecurity, Cyber Defense, Security Operations Center, Blue Team.*

## DAFTAR ISI

## DAFTAR GAMBAR

## DAFTAR TABEL