UNIVERSITAS BUDI LUHUR
Kampus Pusat : Jl. Raya Ciledug - Petukangan Utara - Jakarta Selatan 12260
Telp : 021-5853753 (hunting), Fax : 021-5853489, http://www.budiluhur.ac.id
FAKULTAS TEKNOLOGI INFORMASI
FAKULTAS EKONOMI DAN BISNIS
FAKULTAS ILMU SOSIAL DAN STUDI GLOBAL
FAKULTAS TEKNIK
FAKULTAS KOMUNIKASI DAN DESAIN KREATIF

BERITA ACARA SIDANG PENDADARAN TUGAS AKHIR

S/UBL/FTI/1000/VII/26

Pada hari ini, Kamis 16 Juli 2026 telah dilaksanakan Ujian Sidang Pendadaran Tugas Akhir sebagai berikut:

Judul: PROTOTIPE SISTEM DETEKSI DAN RESPON KEAMANAN JARINGAN BERBASIS MACHINE LEARNING MENGGUNAKAN METADATA ZEEK, INTEGRASI SIEM DAN NOTIFIKASI TELEGRAM BOT

Nama : Septian Tri Mahendra
NIM : 2211501453
Dosen Pembimbing : Joko Christian Chandra, S.Kom., M.Kom.

Berdasarkan penilaian pada Presentasi + Demo, Penulisan, Penguasaan Materi, Penguasaan Program maka Mahasiswa tersebut di atas dinyatakan:

LULUS

dengan nilai angka : **87** huruf : **A**

Mahasiswa tersebut di atas wajib menyerahkan hasil perbaikan tulisan Tugas Akhir dalam bentuk terjilid sesuai dengan Panduan Perbaikan Tugas Akhir, selambat-lambatnya Kamis 30 Juli 2026.

Panitia Penguji:

1 Ketua Sri Mulyati, S.Kom., M.Kom.
2 Anggota Painem, S.Kom., M.Kom.
3 Moderator Joko Christian Chandra, S.Kom., M.Kom.

Keterangan:
Nilai Huruf: A:85-100 A-:80-84,99 B+:75-79,99 B:70-74,99 B-:65-69,99 C:60-64,99 D:40-59,99 E-:0-39,99

UNIVERSITAS BUDI LUHUR
FAKULTAS TEKNOLOGI INFORMASI

Kartu Bimbingan Tugas Akhir

NIM: 2211501453
Nama: Septian Tri Mahendra
Pembimbing: Joko Christian Chandra, S.Kom., M.Kom.

No.	Tanggal	Materi
1	16-04-2026	bimbingan tema dan konsep riset
2	04-05-2026	draft bab 1, perbaikan terkait rumusan masalah
3	19-05-2026	draft bab 2 dan metodologi
4	27-05-2026	perbaikan bab 1-2 dan draft bab 3
5	09-06-2026	Perbaikan bab 3 dan gambar
6	17-06-2026	Draft bab 4 dan demo
7	29-06-2026	demo aplikasi perbaikan
8	02-07-2026	perbaikan bab 4, diskusi bab 5

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS BUDI LUHUR

LEMBAR PENGESAHAN

Nama	: Septian Tri Mahendra
Nomor Induk Mahasiswa	: 2211501453
Program Studi	: Teknik Informatika
Bidang Peminatan	: Cyber Security
Jenjang Studi	: Strata 1
Judul	: PROTOTIPE SISTEM DETEKSI DAN RESPON KEAMANAN JARINGAN BERBASIS MACHINE LEARNING MENGGUNAKAN METADATA ZEEK, INTEGRASI SIEM DAN NOTIFIKASI TELEGRAM BOT

Laporan Tugas Akhir ini telah disetujui, disahkan dan direkam secara elektronik sehingga tidak memerlukan tanda tangan tim penguji.

Jakarta, Kamis 16 Juli 2026

Tim Penguji:

Ketua	: Sri Mulyati, S.Kom., M.Kom.
Anggota	: Painem, S.Kom., M.Kom.
Pembimbing	: Joko Christian Chandra, S.Kom., M.Kom.
Ketua Program Studi	: Dr. Indra, S.Kom., M.T.I.

PROTOTIPE SISTEM DETEKSI DAN RESPON KEAMANAN JARINGAN BERBASIS *MACHINE LEARNING* MENGGUNAKAN METADATA ZEEK, INTERGRASI SIEM DAN NOTIFIKASI TELEGRAM BOT

TUGAS AKHIR

Oleh:

Septian Tri Mahendra

2211501453

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS BUDI LUHUR

JAKARTA
2026

ABSTRAK

PROTOTIPE SISTEM DETEKSI DAN RESPON KEAMANAN JARINGAN BERBASIS *MACHINE LEARNING* MENGGUNAKAN METADATA ZEEK, INTEGRASI SIEM DAN NOTIFIKASI TELEGRAM BOT

Oleh: Septian Tri Mahendra (2211501453)

Ancaman keamanan jaringan komputer terus berkembang seiring meningkatnya kompleksitas dan frekuensi serangan siber, sehingga pendekatan deteksi berbasis *signature* konvensional memiliki keterbatasan dalam mengenali serangan baru (*zero-day*). Penelitian ini bertujuan merancang dan membangun prototipe Sistem Deteksi dan Respons Keamanan Jaringan menggunakan pendekatan deteksi hibrida yang mengintegrasikan Suricata, Zeek, algoritma Isolation Forest, ELK Stack, dan Telegram Bot. Metode yang digunakan adalah *Prototype* meliputi analisis kebutuhan, perancangan, implementasi, serta pengujian. Sistem diimplementasikan pada empat *virtual machine* menggunakan VirtualBox. Lapisan deteksi memanfaatkan Suricata dengan *ruleset Emerging Threats Open* dan *custom rule*, serta Isolation Forest berbasis metadata Zeek. Hasil deteksi disimpan di Elasticsearch, divisualisasikan melalui Kibana, dan dikirimkan melalui Telegram Bot. Pengujian terhadap enam skenario serangan menunjukkan *detection rate* 100%, menghasilkan 738 alert Suricata dan 388 anomali. Rata-rata latensi notifikasi sebesar 31,2 detik, sedangkan mekanisme anti-spam menurunkan volume notifikasi hingga 98,3%. Integrasi *signature*, *machine learning*, SIEM, dan notifikasi *real-time* menghasilkan sistem keamanan jaringan yang efektif, komprehensif, dan hemat biaya.

Kata Kunci: Network Intrusion Detection System, *Hybrid Detection*, Suricata, Zeek, *Isolation Forest*, ELK Stack, SIEM, Telegram Bot, *Machine Learning*, Keamanan Jaringan.

DAFTAR ISI

DAFTAR PUSTAKA

Ahmad, Z., Khan, A. S., Shiang, C. W., Abdullah, J., & Ahmad, F. (2021). Network intrusion detection system: A systematic study of machine learning and deep learning approaches. Transactions on Emerging Telecommunications Technologies, 32(1), e4150.

Akbari, I., Tahoun, M., & Khoukhi, L. (2022). Machine learning for network intrusion detection: A survey. IEEE Access, 10, 45230–45258.

Bertoli, G. C., Pereira Júnior, L. A., Saotome, O., dos Santos, A. L., Verri, F. A. N., Marcondes, C. A. C., Barbieri, S., Rodrigues, M. S., & Parente de Oliveira, J. M. (2021). An End-to-End Framework for Machine Learning-Based Network Intrusion Detection System. IEEE Access, 9, 106790–106805.

Buczak, A. L., & Guven, E. (2021). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials.

Elastic. (2025). Elastic machine learning documentation.

Elastic. (2025). Elastic Security documentation.

Kumar, S., Gupta, S., & Arora, S. (2021). Research Trends in Network-Based Intrusion Detection Systems: A Review. IEEE Access, 9, 157761–157779.

Le Jeune, L., Goedemé, T., & Mentens, N. (2021). Machine Learning for Misuse-Based Network Intrusion Detection: Overview, Unified Evaluation and Feature Choice Comparison Framework. IEEE Access, 9, 63995–64015.

Open Information Security Foundation. (2025). Suricata User Guide (Version 7.x).

Pacheco, J., Benitez, V., Felix-Herran, L. C., & Satam, P. (2023). Toward a Reliable Evaluation of Machine Learning Schemes for Network-Based Intrusion Detection. IEEE Transactions on Network and Service Management.

Sarhan, M., Layeghy, S., & Portmann, M. (2021). Towards a Standard Feature Set for Network Intrusion Detection System Datasets. IEEE Access.

Sarhan, M., Layeghy, S., Moustafa, N., & Portmann, M. (2022). NetFlow Datasets for Machine Learning-Based Network Intrusion Detection Systems. Data, 7(7).

Scarfone, K., & Mell, P. (2021). Guide to Intrusion Detection and Prevention Systems (IDPS). National Institute of Standards and Technology (NIST).

Stallings, W. (2022). Network Security Essentials: Applications and Standards (7th ed.). Pearson.

Telegram. (2025). Telegram Bot API.

The Zeek Project. (2025). Zeek Documentation (Book of Zeek).