

**ANALISIS FRAMEWORK T-POT DAN SIEM SEBAGAI SISTEM DETEKSI  
INTRUSI SERTA NOTIFIKASI *REAL-TIME* MELALUI TELEGRAM**



**MUHAMMAD KAHFI DARMAWAN**  
**NIM. 2210511007**

**PROGRAM STUDI INFORMATIKA**  
**FAKULTAS ILMU KOMPUTER**  
**UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAKARTA**  
**2026**

**ANALISIS FRAMEWORK T-POT DAN SIEM SEBAGAI SISTEM DETEKSI  
INTRUSI SERTA NOTIFIKASI *REAL-TIME* MELALUI TELEGRAM**

**MUHAMMAD KAHFI DARMAWAN**

**NIM. 2210511007**

**SKRIPSI**

**Sebagai salah satu syarat untuk memperoleh gelar Sarjana  
Komputer**

**PROGRAM STUDI INFORMATIKA**

**FAKULTAS ILMU KOMPUTER**

**UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAKARTA**

**2026**

## ABSTRAK

Meningkatnya ancaman serangan siber terhadap infrastruktur jaringan menuntut adanya sistem deteksi intrusi yang mampu merespons secara cepat dan konsisten. Penelitian ini bertujuan untuk membangun, mengimplementasikan, dan mengevaluasi sistem deteksi intrusi berbasis framework T-Pot yang terintegrasi dengan Security Information and Event Management (SIEM) menggunakan Elastic Stack, serta mekanisme notifikasi real-time melalui Telegram. Sistem yang dibangun memanfaatkan tiga komponen utama T-Pot, yaitu Cowrie sebagai SSH honeypot, Dionaea sebagai honeypot multi-protokol, dan Suricata sebagai Intrusion Detection System (IDS), yang dihubungkan dengan ElastAlert2 sebagai rule-based alerting engine. Sebagai kontribusi tambahan, dikembangkan script `malware_vt_checker.py` untuk melakukan enrichment otomatis terhadap sampel malware menggunakan VirusTotal API.

Evaluasi sistem dilakukan melalui dua tahap pengujian. Pengujian organik selama 16 hari efektif menghasilkan 6.332.283 events dari 28.224 alamat IP unik di 163 negara, termasuk pendeteksian 1.062 sampel malware dengan 198 hash unik, di mana 98,56% terklasifikasi sebagai malicious oleh VirusTotal. Pengujian terkontrol dilakukan dengan 150 iterasi yang mencakup lima skenario, yaitu brute force SSH, port scanning, DDoS/SYN flood, malware upload dengan VirusTotal, dan malware upload tanpa VirusTotal. Metrik yang diukur meliputi Mean Time to Detect (MTTD) sebagai indikator kecepatan notifikasi end-to-end dan success rate sebagai indikator konsistensi notifikasi.

Hasil pengujian menunjukkan bahwa MTTD rata-rata keseluruhan sebesar 24,902 detik dengan success rate 100% dari seluruh iterasi. Per skenario, MTTD terendah dicapai oleh skenario malware tanpa VirusTotal (15,067 detik), diikuti brute force (18,786 detik), port scanning (22,769 detik), dan DDoS (28,703 detik). Skenario malware dengan VirusTotal menghasilkan MTTD 39,185 detik akibat overhead enrichment API eksternal. Analisis bottleneck menunjukkan bahwa segmen T2→T3 (ElastAlert polling) mendominasi latency pada empat skenario pertama dengan kontribusi 92–98%, sedangkan bottleneck pada skenario malware dengan VirusTotal berada pada segmen T1→T2 (enrichment VirusTotal, rata-rata 24,185 detik). Seluruh hipotesis terpenuhi: H1 terpenuhi secara parsial (4 dari 5 skenario memenuhi target  $MTTD \leq 30$  detik), H2 terpenuhi penuh (success rate 100%), dan H3 terpenuhi melalui bukti peningkatan kualitas informasi keamanan dari event mentah menjadi alert terstruktur dengan enrichment GeoIP, klasifikasi signature, dan analisis threat intelligence.

**Kata Kunci:** *honeypot, T-Pot, SIEM, Elastic Stack, ElastAlert, intrusion detection system, MTTD, notifikasi real-time, Telegram, VirusTotal, Cowrie, Dionaea, Suricata*

## ABSTRACT

*The increasing threat of cyber attacks against network infrastructure demands an intrusion detection system capable of responding rapidly and consistently. This research aims to build, implement, and evaluate an intrusion detection system based on the T-Pot framework integrated with Security Information and Event Management (SIEM) using Elastic Stack, along with a real-time notification mechanism through Telegram. The system utilizes three core T-Pot components — Cowrie as an SSH honeypot, Dionaea as a multi-protocol honeypot, and Suricata as an Intrusion Detection System (IDS) — connected to ElastAlert2 as a rule-based alerting engine. As an additional contribution, the `malware_vt_checker.py` script was developed to perform automated enrichment of malware samples using the VirusTotal API.*

*System evaluation was conducted in two phases. Organic testing over 16 effective days captured 6,332,283 events from 28,224 unique IP addresses across 163 countries, including the detection of 1,062 malware samples with 198 unique hashes, of which 98.56% were classified as malicious by VirusTotal. Controlled testing was performed with 150 iterations across five scenarios: SSH brute force, port scanning, DDoS/SYN flood, malware upload with VirusTotal, and malware upload without VirusTotal. Metrics measured include Mean Time to Detect (MTTD) as an indicator of end-to-end notification speed and success rate as an indicator of notification consistency.*

*Results show an overall average MTTD of 24.902 seconds with a 100% success rate across all iterations. Per scenario, the lowest MTTD was achieved by malware without VirusTotal (15.067 seconds), followed by brute force (18.786 seconds), port scanning (22.769 seconds), and DDoS (28.703 seconds). The malware scenario with VirusTotal yielded an MTTD of 39.185 seconds due to external API enrichment overhead. Bottleneck analysis revealed that the  $T2 \rightarrow T3$  segment (ElastAlert polling) dominates latency in four of five scenarios, contributing 92–98% of total MTTD, while the bottleneck in the malware with VirusTotal scenario shifts to the  $T1 \rightarrow T2$  segment (VirusTotal enrichment, averaging 24.185 seconds). All hypotheses were confirmed: H1 was partially fulfilled (4 of 5 scenarios met the  $MTTD \leq 30$  second target), H2 was fully fulfilled (100% success rate), and H3 was confirmed through evidence of improved security information quality — transforming raw events into structured alerts enriched with GeoIP context, signature classification, and threat intelligence analysis.*

**Keywords:** *honeypot, T-Pot, SIEM, Elastic Stack, ElastAlert, intrusion detection system, MTTD, real-time notification, Telegram, VirusTotal, Cowrie, Dionaea, Suricata*

# LEMBAR PERSETUJUAN SKRIPSI

## LEMBAR PERSETUJUAN

Yang bertanda tangan di bawah ini:

Nama : Muhammad Kahfi Darmawan

NIM : 2210511007

Program Studi : Informatika Program Sarjana/~~Sistem Informasi Program Sarjana/Sains Data~~  
~~Program Sarjana/Sistem Informasi Program Diploma~~ (\*Coret yang tidak perlu)

Jenis Tugas Akhir : Skripsi / ~~Proyek / Artikel Publikasi~~ (\*Coret yang tidak perlu)

Judul Proposal Tugas Akhir : ANALISIS FRAMEWORK T-POT DAN SIEM SEBAGAI  
SISTEM DETEKSI INTRUSI SERTA NOTIFIKASI REAL-TIME MELALUI TELEGRAM

Dinyatakan telah memenuhi syarat dan menyetujui untuk mengikuti ujian sidang Tugas Akhir.

Jakarta, 27 April 2026

Menyetujui,

Dosen Pembimbing 1,



Ditandatangani secara digital oleh  
Henki Bayu Seta

Verifikasi di [design.upnvj.ac.id](https://design.upnvj.ac.id)

Henki Bayu Seta, S.Kom., M.TI

NIDN. 0309118104

Dosen Pembimbing 2,



Ditandatangani secara digital oleh  
Hamonangan Kinantan Prabu

Verifikasi di [design.upnvj.ac.id](https://design.upnvj.ac.id)

Hamonangan Kinantan P., S.T, MT

NIDN. 0002088502

Mengetahui,

Koordinator Program Studi,



Ditandatangani secara digital oleh  
Ridwan Raafi'udin

Verifikasi di [design.upnvj.ac.id](https://design.upnvj.ac.id)

Dr. Ridwan Raafi'udin, S.Kom., M.Kom

NIDN. 002058804

## LEMBAR PENGESAHAN SKRIPSI

### LEMBAR PENGESAHAN

Judul : Analisis Framework T-Pot dan SIEM sebagai Sistem Deteksi Intrusi  
serta Notifikasi *Real-Time* melalui Telegram  
Nama : Muhammad Kahfi Darmawan  
NIM : 2210511007  
Program Studi : S1 Informatika

Disetujui oleh :

Penguji 1:

Dr. Widya Cholil, M.I.T

Penguji 2:

Anis Fitri Nur Masruriyah, S.Kom., M.Kom.

Pembimbing 1:

Henki Bayu Seta, S.Kom, MTI.

Pembimbing 2:

Hamonangan Kinantan Prabu, M.T.

Diketahui oleh:

Koordinator Program Studi:

Dr. Ridwan Raafi'udin, S.Kom., M.Kom.

NIP. 198805022021211001

Dekan Fakultas Ilmu Komputer:

Prof. Dr. Ir. Supriyanto, S.T., M.Sc., IPM

NIP. 197605082003121002

Tanggal Ujian Tugas Akhir :

22 Mei 2026



## PERNYATAAN ORISINALITAS

### PERNYATAAN ORISINALITAS

Tugas akhir ini adalah hasil karya saya sendiri dan semua sumber yang dikutip maupun yang dirujuk telah saya nyatakan benar

Nama : Muhamamad Kahfi Darmawan  
NIM : 2210511007  
Tanggal : 24 Juli 2026  
Judul Skripsi : **ANALISIS FRAMEWORK T-POT DAN SIEM SEBAGAI  
SISTEM DETEKSI INTRUSI SERTA NOTIFIKASI  
REAL-TIME MELALUI TELEGRAM**

Bilamana pada kemudian hari ditemukan ketidaksesuaian dengan pernyataan saya ini, maka saya bersedia dituntut dan diproses sesuai dengan ketentuan yang berlaku.

Jakarta, 24 Juli 2026

Yang menyatakan.



Muhammad Kahfi Darmawan

# **PERNYATAAN PERSETUJUAN PUBLIKASI KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIS**

## **PERNYATAAN PERSETUJUAN PUBLIKASI KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIS**

Sebagai civitas akademik Universitas Pembangunan Nasional "Veteran" Jakarta, saya yang bertanda tangan di bawah ini,

Nama : Muhammad Kahfi Darmawan  
NIM : 2210511007  
Fakultas : Ilmu Komputer  
Program Studi : S-1 Informatika

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan karya ilmiah saya kepada Universitas Pembangunan Nasional "Veteran" Jakarta Hak Bebas Non-Eksklusif (*Non-Exclusive Royalty Free Right*) untuk publikasi dengan judul:

### **ANALISIS FRAMEWORK T-POT DAN SIEM SEBAGAI SISTEM DETEKSI INTRUSI SERTA NOTIFIKASI REAL-TIME MELALUI TELEGRAM**

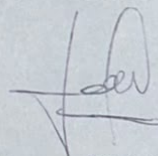
Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti ini Universitas Pembangunan Nasional "Veteran" Jakarta berhak menyimpan, mengalih media atau memformatkan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempublikasi artikel ilmiah selama tetap mencantumkan nama saya sebagai penulis atau pencipta dan sebagai pemilik Hak Cipta.

Dengan pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Jakarta

Pada tanggal : 24 Juli 2026

Yang menyatakan,



Muhammad Kahfi Darmawan

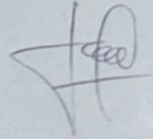
**PERNYATAAN MENGENAI SKRIPSI DAN SUMBER INFORMASI SERTA  
PELIMPAHAN HAK CIPTA**

**PERNYATAAN MENGENAI SKRIPSI DAN SUMBER INFORMASI SERTA  
PELIMPAHAN HAK CIPTA**

Dengan ini saya menyatakan bahwa skripsi dengan judul "ANALISIS FRAMEWORK T-POT DAN SIEM SEBAGAI SISTEM DETEKSI INTRUSI SERTA NOTIFIKASI REAL-TIME MELALUI TELEGRAM" adalah karya saya dengan arahan dari dosen pembimbing dan belum diajukan dalam bentuk apapun kepada perguruan tinggi mana pun. Sumber informasi yang berasal atau dikutip dari saya yang diterbitkan maupun tidak diterbitkan dari penulis lain telah disebutkan dalam teks dan dicantumkan dalam Daftar Pustaka di bagian akhir skripsi ini

Dengan ini saya melimpahkan hak cipta dari karya tulis saya kepada Universitas Pembangunan Nasional "Veteran" Jakarta.

Jakarta, 24 Juli 2026



Muhammad Kahfi Darmawan

NIM. 2210511007

## KATA PENGANTAR

Puji dan syukur penulis panjatkan ke hadirat Allah SWT atas segala rahmat, karunia, serta kesempatan yang diberikan, sehingga penulis dapat menyelesaikan Tugas Akhir yang berjudul “Analisis Framework T-Pot dan SIEM sebagai Sistem Deteksi Intrusi serta Notifikasi Real-Time melalui Telegram” dengan baik.

Penyusunan Tugas Akhir ini dilakukan sebagai salah satu syarat untuk menyelesaikan pendidikan pada Program Studi Informatika, Fakultas Ilmu Komputer, Universitas Pembangunan Nasional Veteran Jakarta. Dalam proses penyusunannya, penulis menyadari bahwa banyak pihak yang turut berperan, baik melalui bimbingan, dukungan, maupun bantuan secara langsung maupun tidak langsung.

Oleh karena itu, penulis ingin menyampaikan rasa terima kasih yang sebesar-besarnya kepada:

1. Allah SWT, atas segala nikmat, kesehatan, serta kemudahan yang diberikan sehingga penulis dapat menyelesaikan Tugas Akhir ini hingga akhir.
2. Prof. Dr. Ir. Supriyanto, ST., M.Sc., IPM, selaku Dekan Fakultas Ilmu Komputer UPN Veteran Jakarta yang telah menyediakan lingkungan akademik yang mendukung proses pembelajaran dan pengembangan diri mahasiswa.
3. Dr. Ridwan Raafi'udin, S.Kom., M.Kom., selaku Ketua Program Studi S1 Informatika yang telah memberikan arahan serta kebijakan yang membantu kelancaran proses studi penulis.
4. Bapak Henki Bayu Seta, S.Kom., M.TI., selaku Dosen Pembimbing I yang telah memberikan banyak masukan, arahan, serta wawasan dalam proses penyusunan penelitian ini.
5. Bapak Hamonangan Kinantan Prabu, S.T., M.T., selaku Dosen Pembimbing II yang dengan penuh kesabaran membimbing serta membantu penulis dalam menyempurnakan penelitian ini.
6. Bapak Muhammad Panji Muslim, S.Pd., M.Kom., selaku Dosen Pembimbing Akademik yang senantiasa memberikan dukungan dan arahan selama masa perkuliahan.
7. Seluruh dosen dan staf Fakultas Ilmu Komputer yang telah memberikan ilmu, pengalaman, serta bantuan selama penulis menempuh pendidikan.

8. Kedua orang tua tercinta, Bapak Fachri Darmawan dan Ibu Evi Nurhayati, yang selalu memberikan doa, dukungan, serta motivasi tanpa henti sehingga penulis dapat menyelesaikan studi ini.
9. Elsyia Putri Ramadhani, yang selalu hadir memberikan semangat, dukungan, serta menjadi tempat berbagi cerita dalam setiap proses yang dilalui penulis selama penyusunan Tugas Akhir ini.
10. Diri penulis sendiri yang telah berusaha bertahan, belajar, dan terus melangkah hingga mampu menyelesaikan tahap ini.

Penulis menyadari bahwa Tugas Akhir ini masih memiliki banyak kekurangan, baik dari segi isi maupun penyajian. Oleh karena itu, penulis sangat terbuka terhadap kritik dan saran yang membangun demi perbaikan di masa mendatang. Semoga penelitian ini dapat memberikan manfaat dan kontribusi, khususnya dalam bidang keamanan siber.

Akhir kata, penulis mengucapkan terima kasih kepada semua pihak yang telah membantu, dan semoga segala kebaikan yang diberikan mendapatkan balasan yang setimpal dari Allah SWT.

Jakarta, 29 April 2026

Muhammad Kahfi Darmawan

## DAFTAR ISI

|                                                              |          |
|--------------------------------------------------------------|----------|
| <b>BAB I.....</b>                                            | <b>1</b> |
| <b>PENDAHULUAN.....</b>                                      | <b>1</b> |
| 1.1. Latar Belakang.....                                     | 1        |
| 1.2. Rumusan Masalah.....                                    | 3        |
| 1.3. Batasan Masalah.....                                    | 3        |
| 1.4. Tujuan dan Manfaat Penelitian.....                      | 4        |
| 1.5. Sistematika Penelitian.....                             | 6        |
| <b>BAB II.....</b>                                           | <b>8</b> |
| <b>TINJAUAN PUSTAKA.....</b>                                 | <b>8</b> |
| 2.1. Konsep Keamanan Jaringan.....                           | 8        |
| 2.2. Serangan terhadap Jaringan.....                         | 9        |
| 2.2.1. Passive Attack.....                                   | 9        |
| 2.2.2. Active Attack.....                                    | 9        |
| 2.3. Klasifikasi Serangan Jaringan pada Aspek CIA Triad..... | 11       |
| 2.3.1. Confidentiality.....                                  | 11       |
| 2.3.2. Integrity.....                                        | 14       |
| 2.3.3. Availability.....                                     | 16       |
| 2.4. Intrusion Detection System (IDS).....                   | 17       |
| 2.4.1. Jenis-jenis IDS.....                                  | 18       |
| 2.4.2. Metode Deteksi pada IDS.....                          | 19       |
| 2.4.3. Platform IDS.....                                     | 20       |
| 2.5. Honeypot.....                                           | 21       |
| 2.5.1. Cara Kerja Honeypot.....                              | 22       |
| 2.5.2. Klasifikasi Honeypot.....                             | 23       |
| 2.5.3. Honeypot Cowrie.....                                  | 25       |
| 2.5.4. Honeypot Dionaea.....                                 | 26       |
| 2.6. Framework T-Pot.....                                    | 27       |
| 2.6.1. Arsitektur T-Pot.....                                 | 27       |
| 2.6.2. Komponen T-Pot.....                                   | 29       |
| 2.6.3. Monitoring & Logging di T-Pot.....                    | 30       |
| 2.7. Security Information and Event Management (SIEM).....   | 32       |
| 2.7.1. Arsitektur SIEM.....                                  | 32       |
| 2.7.2. Platform SIEM.....                                    | 33       |
| 2.8. Metrik Security Operations Center (SOC).....            | 35       |
| 2.8.1. Mean Time to Detect (MTTD).....                       | 36       |
| 2.8.2. Mean Time to Respond (MTTR).....                      | 37       |
| 2.9. Mekanisme Notifikasi Real-Time.....                     | 38       |
| 2.9.1. ElastAlert.....                                       | 39       |
| 2.9.2. Telegram sebagai Delivery Channel.....                | 40       |
| 2.10. Literature Review.....                                 | 40       |

|                                                             |           |
|-------------------------------------------------------------|-----------|
| <b>BAB III.....</b>                                         | <b>47</b> |
| <b>METODE PENELITIAN.....</b>                               | <b>47</b> |
| 3.1. Jenis dan Pendekatan Penelitian.....                   | 47        |
| 3.2. Tahapan Penelitian.....                                | 48        |
| 3.2.1. Identifikasi Masalah.....                            | 48        |
| 3.2.2. Studi Literatur.....                                 | 48        |
| 3.2.3. Perancangan Sistem.....                              | 49        |
| 3.2.4. Pengujian Serangan Organik.....                      | 55        |
| 3.2.5. Pengujian Serangan Terkontrol.....                   | 56        |
| 3.2.6. Pengumpulan Data.....                                | 62        |
| 3.2.7. Analisis Data.....                                   | 64        |
| 3.2.8. Kesimpulan.....                                      | 66        |
| 3.3. Variabel Penelitian.....                               | 66        |
| 3.3.1. Kecepatan Notifikasi.....                            | 66        |
| 3.3.2. Konsistensi Notifikasi.....                          | 67        |
| 3.4. Hipotesis Penelitian.....                              | 68        |
| 3.4.1. Hipotesis Kecepatan Deteksi (MTTD).....              | 68        |
| 3.4.2. Hipotesis Konsistensi Notifikasi.....                | 69        |
| 3.4.3. Hipotesis Efektivitas Korelasi Event.....            | 70        |
| 3.5. Analisis Kebutuhan.....                                | 70        |
| 3.5.1. Kebutuhan Perangkat Keras.....                       | 70        |
| 3.5.2. Kebutuhan Perangkat Lunak.....                       | 70        |
| 3.5.3. Kebutuhan Jaringan.....                              | 72        |
| 3.5.4. Kebutuhan Virtual Machine (VM).....                  | 73        |
| 3.6. Waktu dan Tempat.....                                  | 73        |
| 3.7. Jadwal Kegiatan.....                                   | 73        |
| <b>BAB IV.....</b>                                          | <b>75</b> |
| <b>HASIL DAN PEMBAHASAN.....</b>                            | <b>75</b> |
| 4.1. Implementasi Sistem.....                               | 75        |
| 4.1.1. Modifikasi Framework T-Pot.....                      | 75        |
| 4.1.2. Konfigurasi SIEM Pipeline.....                       | 79        |
| 4.1.3. Implementasi Custom Script VirusTotal API.....       | 82        |
| 4.1.4. Konfigurasi Engine Deteksi dan Notifikasi.....       | 89        |
| 4.2. Hasil Pengujian Serangan Organik.....                  | 98        |
| 4.2.1. Gambaran Umum Data Serangan Organik.....             | 98        |
| 4.2.2. Hasil Deteksi Cowrie (SSH Honeypot).....             | 100       |
| 4.2.3. Hasil Deteksi Suricata (IDS).....                    | 112       |
| 4.2.4. Hasil Deteksi Dionaea (Multi-protocol Honeypot)..... | 117       |
| 4.2.5. Analisis Tren Temporal Serangan.....                 | 124       |
| 4.2.6. Notifikasi ElastAlert pada Pengujian Organik.....    | 129       |
| 4.3. Hasil Pengujian Serangan Terkontrol.....               | 130       |

|                                                                            |            |
|----------------------------------------------------------------------------|------------|
| 4.3.1. Lingkungan dan Prosedur Pengujian.....                              | 131        |
| 4.3.2. Skenario 1 – SSH Brute Force (Cowrie).....                          | 132        |
| 4.3.3. Skenario 2 – Port Scanning (Suricata).....                          | 136        |
| 4.3.4. Skenario 3 – DDoS / SYN Flood (Suricata).....                       | 141        |
| 4.3.5. Skenario 4 – Malware Upload via SMB (Dionaea + VirusTotal).....     | 146        |
| 4.3.6. Skenario 5: Malware Upload tanpa VirusTotal.....                    | 151        |
| 4.3.7. Perbandingan MTDD Antar Skenario.....                               | 157        |
| 4.4. Analisis Kinerja Metrik SOC.....                                      | 159        |
| 4.4.1. Analisis Mean Time to Detect (MTDD).....                            | 159        |
| 4.4.2. Analisis Breakdown Latency per Segmen Pipeline.....                 | 161        |
| 4.4.3. Analisis Konsistensi Notifikasi (Success Rate).....                 | 163        |
| 4.4.4. Identifikasi Bottleneck Pipeline.....                               | 165        |
| 4.4.5. Perbandingan Kinerja Antar Skenario.....                            | 166        |
| 4.4.6. Diskusi Hasil Analisis.....                                         | 168        |
| 4.5. Evaluasi Hipotesis Penelitian.....                                    | 169        |
| 4.5.1. Evaluasi Rumusan Masalah 1: Pembangunan Sistem Deteksi Intrusi..... | 169        |
| 4.5.2. Evaluasi Rumusan Masalah 2: Kecepatan Notifikasi (H1).....          | 170        |
| 4.5.3. Evaluasi Rumusan Masalah 3: Konsistensi Notifikasi (H2).....        | 172        |
| 4.5.4. Evaluasi Hipotesis H3: Efektivitas Korelasi Event.....              | 173        |
| 4.5.5. Ringkasan Evaluasi Hipotesis.....                                   | 175        |
| <b>BAB V.....</b>                                                          | <b>177</b> |
| <b>KESIMPULAN DAN SARAN.....</b>                                           | <b>177</b> |
| 5.1. Kesimpulan.....                                                       | 177        |
| 5.2. Saran.....                                                            | 178        |
| <b>DAFTAR PUSTAKA.....</b>                                                 | <b>180</b> |

## DAFTAR GAMBAR

|                                                                                             |     |
|---------------------------------------------------------------------------------------------|-----|
| Gambar 2.1 CIA Triad.....                                                                   | 8   |
| Gambar 2.2 Mekanisme Operasional Honeypot Modern dengan Integrasi Logging dan Analitik..... | 23  |
| Gambar 2.3 Arsitektur T-Pot.....                                                            | 28  |
| Gambar 2.4 Workflow Monitoring dan Logging T-Pot.....                                       | 31  |
| Gambar 2.5 Arsitektur SIEM.....                                                             | 33  |
| Gambar 3.1 Flowchart Tahapan Penelitian.....                                                | 48  |
| Gambar 3.2 Arsitektur Sistem Deteksi Intrusi Berbasis T-Pot.....                            | 49  |
| Gambar 3.3 Topologi Pengujian Terkontrol.....                                               | 51  |
| Gambar 3.4 Topologi Serangan Organik.....                                                   | 52  |
| Gambar 3.5 Alur Kerja Script Enrichment Malware.....                                        | 55  |
| Gambar 3.6 Alur Pencatatan Waktu.....                                                       | 57  |
| Gambar 3.7 Skenario Brute Force.....                                                        | 58  |
| Gambar 3.8 Skenario Port Scanning.....                                                      | 59  |
| Gambar 3.9 Skenario DDoS.....                                                               | 60  |
| Gambar 3.10 Skenario Malware menggunakan VT Enrichment.....                                 | 61  |
| Gambar 3.11 Skenario Malware tanpa VT Enrichment.....                                       | 62  |
| Gambar 4.1 Tampilan log Cowrie di Kibana.....                                               | 80  |
| Gambar 4.2 Tampilan log Dionaea di Kibana.....                                              | 80  |
| Gambar 4.3 Tampilan log Suricata di Kibana.....                                             | 81  |
| Gambar 4.4 Tampilan field GeoIP hasil di Kibana.....                                        | 81  |
| Gambar 4.5 Tampilan field malware enrichment.....                                           | 86  |
| Gambar 4.6 Output Terminal Script Malware Enrichment.....                                   | 86  |
| Gambar 4.7 Service malware-checker.service Dalam Kondisi Aktif.....                         | 88  |
| Gambar 4.8 Testing Notifikasi Telegram.....                                                 | 95  |
| Gambar 4.9 Verifikasi Rule ElastAlert ke Telegram.....                                      | 97  |
| Gambar 4.10 Pie Chart Komponen T-Pot berdasarkan Total Events.....                          | 99  |
| Gambar 4.11 Distribusi Geografis Attack.....                                                | 100 |
| Gambar 4.12 Distribusi Percobaan Login Berhasil dan Gagal pada Cowrie.....                  | 102 |
| Gambar 4.13 Top 5 IP Berdasarkan Jumlah Login yang Berhasil.....                            | 103 |
| Gambar 4.14 Distribusi Geografis Aktivitas Brute Force.....                                 | 111 |
| Gambar 4.15 Distribusi Kategori Alert Suricata.....                                         | 113 |
| Gambar 4.16 Top 5 Port yang Paling Sering Dipindai.....                                     | 116 |
| Gambar 4.17 Distribusi Geografis Aktivitas Scanning.....                                    | 117 |
| Gambar 4.18 Pie Chart Distribusi Koneksi Dionaea per Protokol.....                          | 118 |
| Gambar 4.19 Status Malware yang Terdeteksi.....                                             | 120 |
| Gambar 4.20 Tipe Malware yang Terdeteksi.....                                               | 121 |
| Gambar 4.21 Distribusi Tag Exploit Berdasarkan VirusTotal.....                              | 122 |
| Gambar 4.22 Tren Jumlah Events per Hari pada Fase 1.....                                    | 125 |
| Gambar 4.23 Tren Jumlah Events per Hari pada Fase 2.....                                    | 125 |

|                                                                                       |     |
|---------------------------------------------------------------------------------------|-----|
| Gambar 4.24 Timeline Aktivitas Serangan per Jam Fase 1 (8-13 Maret 2026).....         | 127 |
| Gambar 4.25 Timeline Aktivitas Serangan per Jam Fase 2 (27 Maret - 5 April 2026)..... | 127 |
| Gambar 4.26 Heatmap Aktivitas Serangan Fase 1 (UTC+0).....                            | 129 |
| Gambar 4.27 Heatmap Aktivitas Serangan Fase 2 (UTC+0).....                            | 129 |
| Gambar 4.28 MTTD per Iterasi Skenario Brute Force.....                                | 135 |
| Gambar 4.29 Box plot MTTD 30 iterasi Brute Force.....                                 | 136 |
| Gambar 4.30 MTTD per Iterasi Skenario Port Scanning.....                              | 140 |
| Gambar 4.31 Box plot MTTD 30 iterasi Port Scanning.....                               | 141 |
| Gambar 4.32 MTTD per Iterasi Skenario DDoS / SYN Flood.....                           | 145 |
| Gambar 4.33 Box plot MTTD 30 iterasi DDoS / SYN Flood.....                            | 146 |
| Gambar 4.34 MTTD per Iterasi Skenario Malware Upload (Dionaea + VirusTotal).....      | 150 |
| Gambar 4.35 Box plot MTTD 30 iterasi Malware Upload.....                              | 151 |
| Gambar 4.36 MTTD per Iterasi Skenario Malware Upload Tanpa VirusTotal.....            | 155 |
| Gambar 4.37 Box plot MTTD 30 iterasi Malware Upload tanpa VirusTotal.....             | 156 |
| Gambar 4.38 Perbandingan MTTD Mean Kelima Skenario.....                               | 159 |
| Gambar 4.39 Distribusi MTTD Tiap Skenario.....                                        | 161 |
| Gambar 4.40 Grafik Success Rate Notifikasi per Skenario.....                          | 165 |

## DAFTAR TABEL

|                                                                                          |     |
|------------------------------------------------------------------------------------------|-----|
| Tabel 2.1 Layanan dan Port yang Didukung Dionaea.....                                    | 26  |
| Tabel 2.2 Penelitian Terdahulu.....                                                      | 41  |
| Tabel 3.1 Komponen Perangkat Keras.....                                                  | 70  |
| Tabel 3.2 Komponen Perangkat Lunak.....                                                  | 71  |
| Tabel 3.3 Komponen Jaringan.....                                                         | 72  |
| Tabel 3.4 Spesifikasi VM Penelitian.....                                                 | 73  |
| Tabel 3.5 Jadwal Kegiatan.....                                                           | 74  |
| Tabel 4.1 Status Container T-Pot Setelah Modifikasi.....                                 | 77  |
| Tabel 4.2 Distribusi Events Serangan per Komponen.....                                   | 98  |
| Tabel 4.3 Statistik Events pada Cowrie.....                                              | 101 |
| Tabel 4.4 Top 5 Username yang Digunakan Attacker.....                                    | 104 |
| Tabel 4.5 Top 5 Password yang Digunakan Attacker.....                                    | 105 |
| Tabel 4.6 Top 10 Command yang Sering Digunakan.....                                      | 106 |
| Tabel 4.7 Daftar File yang Diupload oleh Attacker.....                                   | 108 |
| Tabel 4.8 Top 5 Alamat IP Penyerang.....                                                 | 111 |
| Tabel 4.9 Top 5 Distribusi Alert Suricata berdasarkan Kategori.....                      | 112 |
| Tabel 4.10 Statistik Koneksi Dionaea per Protokol.....                                   | 117 |
| Tabel 4.11 Rekapitulasi Hasil Analisis VirusTotal.....                                   | 121 |
| Tabel 4.12 Perbandingan Volume Events Fase 1 dan Fase 2.....                             | 125 |
| Tabel 4.13 Distribusi Notifikasi ElastAlert per Rule.....                                | 130 |
| Tabel 4.14 Spesifikasi Lingkungan Pengujian Terkontrol.....                              | 131 |
| Tabel 4.15 Parameter Serangan Brute Force.....                                           | 132 |
| Tabel 4.16 Data Skenario Brute Force (08 April 2026).....                                | 133 |
| Tabel 4.17 Statistik Deskriptif MTTD Skenario Brute Force.....                           | 134 |
| Tabel 4.18 Parameter Serangan Port Scanning.....                                         | 136 |
| Tabel 4.19 Data 30 Iterasi Skenario Port Scanning (10 April 2026).....                   | 137 |
| Tabel 4.20 Statistik Deskriptif MTTD Skenario Port Scanning.....                         | 138 |
| Tabel 4.21 Parameter Serangan DDoS (SYN Flood).....                                      | 141 |
| Tabel 4.22 Data 30 Iterasi Skenario DDoS / SYN Flood (12 April 2026).....                | 142 |
| Tabel 4.23 Statistik Deskriptif MTTD Skenario DDoS.....                                  | 143 |
| Tabel 4.24 Parameter Skenario Malware Upload.....                                        | 146 |
| Tabel 4.25 Data 30 Iterasi Skenario Malware Upload (12 April 2026).....                  | 147 |
| Tabel 4.26 Statistik Deskriptif MTTD Skenario Malware Upload.....                        | 148 |
| Tabel 4.27 Parameter Skenario Malware Upload tanpa VirusTotal.....                       | 152 |
| Tabel 4.28 Data 30 Iterasi Skenario Malware Upload tanpa VirusTotal (16 April 2026)..... | 153 |
| Tabel 4.29 Statistik Deskriptif MTTD Skenario Malware Upload tanpa VirusTotal.....       | 154 |
| Tabel 4.30 Perbandingan Statistik MTTD Kelima Skenario.....                              | 157 |
| Tabel 4.31 Rekapitulasi MTTD per Skenario.....                                           | 159 |
| Tabel 4.32 Mean Latency per Segmen Pipeline (satuan: detik).....                         | 162 |
| Tabel 4.33 Rekapitulasi Success Rate per Skenario.....                                   | 163 |

|                                                                               |     |
|-------------------------------------------------------------------------------|-----|
| Tabel 4.34 Identifikasi Bottleneck per Skenario.....                          | 165 |
| Tabel 4.35 Matriks Perbandingan Kinerja Antar Skenario.....                   | 167 |
| Tabel 4.36 Evaluasi Komparatif: Skenario 4 vs Skenario 5.....                 | 171 |
| Tabel 4.37 Evaluasi H1 per Skenario.....                                      | 172 |
| Tabel 4.38 Evaluasi H2 per Skenario.....                                      | 172 |
| Tabel 4.39 Perbandingan Informasi Event Mentah vs Setelah Integrasi SIEM..... | 174 |
| Tabel 4.40 Ringkasan Evaluasi Hipotesis Penelitian.....                       | 175 |

## DAFTAR LAMPIRAN

|                                                                           |     |
|---------------------------------------------------------------------------|-----|
| Lampiran A.1 Konfigurasi Netplan Mode Pengujian Terkontrol.....           | 186 |
| Lampiran A.2 Konfigurasi Netplan Mode Serangan Organik.....               | 186 |
| Lampiran B Tampilan T-Pot Dashboard di Kibana.....                        | 187 |
| Lampiran C.1 Rule ElastAlert untuk Deteksi Brute Force di SSH Cowrie..... | 187 |
| Lampiran C.2 Rule ElastAlert untuk Deteksi Port Scan di Suricata.....     | 188 |
| Lampiran C.3 Rule ElastAlert untuk Deteksi DDoS di Suricata.....          | 189 |
| Lampiran C.4 Rule ElastAlert untuk Deteksi Malware di Dionaea.....        | 190 |
| Lampiran D Contoh Notifikasi Telegram.....                                | 192 |
| Lampiran E Script Custom Enrichment VirusTotal.....                       | 192 |
| Lampiran F Script Bash Serangan Brute Force.....                          | 196 |
| Lampiran G Script Bash Serangan Port Scan.....                            | 198 |
| Lampiran H Script Bash Serangan DDoS.....                                 | 200 |
| Lampiran I Script Bash Malware.....                                       | 201 |
| Lampiran J Cek Plagiasi melalui Turnitin.....                             | 204 |

## DAFTAR RUMUS

|                             |    |
|-----------------------------|----|
| Rumus 3.1 Success Rate..... | 67 |
|-----------------------------|----|