



UNIVERSITAS PERTAHANAN RI

**IMPLEMENTASI *EXTENDED DETECTION AND RESPONSE*
PADA *SECURITY OPERATION CENTER* DAN *COMPUTER*
SECURITY INDEPENDENT RESPONSE TEAM DALAM
PENINGKATAN SISTEM KEAMANAN INFORMASI
GUNA MENINGKATKAN SISTEM
PERTAHANAN INFORMASI**

FATHAN LUQMAN 320210402006

**Skripsi yang Ditulis untuk Memenuhi Sebagian Persyaratan dalam
Mendapatkan Gelar Sarjana**

**FAKULTAS TEKNIK DAN TEKNOLOGI PERTAHANAN
PROGRAM STUDI TEKNIK ELEKTRO**

BOGOR, 2025

LEMBAR PERSETUJUAN SKRIPSI

Nama : FATHAN LUQMAN
NIM : 320210402006
Fakultas : TEKNIK DAN TEKNOLOGI PERTAHANAN
Program Studi : TEKNIK ELEKTRO
Judul Skripsi : IMPLEMENTASI *EXTENDED DETECTION AND RESPONSE* PADA *SECURITY OPERATION CENTER* DAN *COMPUTER SECURITY INDEPENDENT RESPONSE TEAM* DALAM PENINGKATAN SISTEM KEAMANAN INFORMASI GUNA MENINGKATKAN SISTEM PERTAHANAN INFORMASI

Dosen Pembimbing I



Dr. Sunarta, M.T.
Kolonel Laut (E) NRP 12898/P

Tanggal:

30 / 06 / 2025

Dosen Pembimbing II



Dr. Ir. H.A. Danang R, S.Si.,
M.Tr.Opsla., C.E.H., CSBA., IPM.,
ASEAN Eng
Kolonel Laut (E) NRP 10829/P

Tanggal : 23 Juni 2025

Mengetahui,

Kepala Program Studi
Sarjana Teknik Elektro



Dr. Sunarta, M.T.
Kolonel Laut (E) NRP 12898/P

Tanggal:

30 / 06 / 2025

Dekan
Fakultas Teknik dan Teknologi
Pertahanan Unhan RI



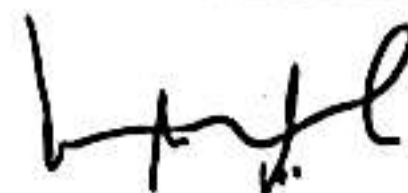
Prof. Dr. Ir. Muhamad Asvial, M.Eng.
Pembina Utama Muda IV/c

Tanggal:

30 / 06 / 2025

LEMBAR PENGESAHAN SKRIPSI

Nama : FATHAN LUQMAN
 NIM : 320210402006
 Fakultas : TEKNIK DAN TEKNOLOGI PERTAHANAN
 Program Studi : TEKNIK ELEKTRO
 Judul Skripsi : IMPLEMENTASI *EXTENDED DETECTION AND RESPONSE* PADA *SECURITY OPERATION CENTER* DAN *COMPUTER SECURITY INDEPENDENT RESPONSE TEAM* DALAM PENINGKATAN SISTEM KEAMANAN INFORMASI GUNA MENINGKATKAN SISTEM PERTAHANAN INFORMASI

No.	Nama	Tanda Tangan	Tanggal
1	Dosen Pembimbing I: Dr. Sunarta, M.T. Kolonel Laut (E) NRP.12898/P		30 - 6 / 2025
2	Dosen Pembimbing II: Dr. H.A. Danang R, S.Si., M.Tr.Opsla., C.E.H., CSBA., IPM., ASEAN Eng Kolonel Laut (E) NRP 10829/P		23 - 6 / 2025
3	Dosen Penguji I: Dr. H. Hendrana Tjahjadi S.T., M.Si.		25 - 6 / 2025
4	Dosen Penguji II: Ir. R. Apip Miptahudin, AMd., S.T., M.T., IPM., Asean Eng., ACPE.		26 - 6 / 2025
5	Dosen Penguji III: Iqbal Ahmad Dahlan S.T., M.T.		28 - 6 / 2025

PERNYATAAN ORISINALITAS

Dengan ini saya menyatakan bahwa dalam skripsi ini tidak terdapat karya atau sebagian karya yang pernah diajukan untuk memperoleh gelar sarjana pada jenjang manapun di suatu Universitas atau Perguruan Tinggi; dan sepanjang pengetahuan saya juga tidak terdapat istilah, frasa, kalimat, paragraf, subbab atau bab dari karya yang pernah ditulis atau diterbitkan; kecuali yang secara tertulis diajukan dalam naskah ini disebutkan dalam Daftar Referensi.

Apabila di kemudian hari terbukti bahwa terdapat plagiat dalam skripsi ini, saya bersedia menerima sanksi sesuai dengan ketentuan peraturan/undang-undang yang berlaku.

Bogor, 30 Juni 2025



Fathan Luqman
320210402006

KATA PENGANTAR

Puji syukur penulis panjatkan ke hadirat Allah SWT, karena berkat rahmat dan karunia-Nya, penulis dapat menyelesaikan skripsi ini yang berjudul **“Implementasi *Extended Detection and Response* Pada Security Operation Center dan Cyber Security Incident Response Team Dalam Peningkatan Sistem Keamanan Informasi Guna Meningkatkan Sistem Pertahanan Informasi”** sebagai salah satu syarat untuk memperoleh gelar Sarjana di Program Studi Teknik Elektro, Universitas Pertahanan Republik Indonesia.

Skripsi ini disusun berdasarkan hasil penelitian yang dilakukan. Penelitian ini merupakan upaya untuk mengeksplorasi dan menganalisis implementasi XDR sebagai alat keamanan siber. Proses penelitian ini tidak lepas dari dukungan dan bantuan berbagai pihak, oleh karena itu, penulis ingin mengucapkan terima kasih kepada:

1. **Allah SWT** atas segala limpahan rahmat, hidayah, dan kemudahan yang diberikan selama penulis menyusun skripsi ini.
2. **Orang Tua dan Keluarga**, yang selalu memberikan dukungan moral, motivasi, materi, spiritual, serta doa yang tiada henti untuk kesuksesan penulis dalam penyusunan skripsi ini.
3. **Bapak Letnan Jenderal TNI (Purn.) Dr. Anton Nugroho, M.M.D.S, M.A.**, selaku Rektor Universitas Pertahanan Republik Indonesia.
4. **Bapak Prof. Dr. Muhamad Asvial, M.Eng.**, selaku Dekan Fakultas Teknik dan Teknologi Pertahanan (FTTP), Universitas Pertahanan Republik Indonesia.
5. **Bapak Kolonel Laut (E) Dr. Sunarta, S.T., M.T.**, selaku Kepala Program Studi Teknik Elektro Universitas Pertahanan Republik Indonesia dan Dosen pembimbing 1, yang telah memberikan arahan, bimbingan, dan dukungan selama proses perkuliahan hingga pelaksanaan penelitian ini.

6. **Bapak Kolonel Laut (E) Dr. H. A. Danang Rimbawa, S.Si., M.Tr.Opsla., C.E.H., CSBA., IPM., ASEAN Eng.** selaku Kepala Program Studi Rekayasa Pertahanan Siber Universitas Pertahanan Republik Indonesia, Dosen Pengajar dan Dosen Pembimbing 2, yang telah memberikan arahan, bimbingan, dan dukungan selama proses perkuliahan hingga pelaksanaan penelitian ini.
7. **Bapak Nugroho Wibisono, S.T., M.M., M.Kom.,** selaku pimpinan dan pembimbing pada tempat penelitian, yang telah memberikan kesempatan kepada penulis untuk menjalani penelitian di perusahaan serta senantiasa memberikan arahan dan bimbingan selama proses penelitian.
8. **Bapak Ari Nuzul Fajri, S.Kom., M.Kom.,** selaku pimpinan dan pembimbing pada tempat penelitian, yang telah memberikan kesempatan kepada penulis untuk menjalani penelitian di perusahaan serta senantiasa memberikan arahan dan bimbingan selama proses penelitian.
9. Seluruh dosen Universitas Pertahanan Republik Indonesia khususnya Program Studi Teknik Elektro yang telah memberikan bekal ilmu pengetahuan, bimbingan, didikan serta arahan yang sangat bermanfaat bagi penulis.
10. Seluruh dosen penguji yang telah memberikan bimbingan, arahan, kritik, saran, dan masukan guna menyempurnakan penelitian skripsi ini.
11. Seluruh Pimpinan, *Engineer*, dan Staf Karyawan di perusahaan tempat penelitian, yang telah berbagi ilmu, pengetahuan, dan pengalaman, serta memberikan bantuan dan dukungan selama masa penelitian.
12. Seluruh rekan-rekan kadet mahasiswa/i werving 2021 atau Cohort 2 yang terkhususnya dari Program Studi Teknik Elektro yang senantiasa menjadi lawan untuk mengasah *critical thinking* penulis dan melakukan *sharing* ilmu dan pengalaman yang berharga.

13. Seluruh keluarga Tong Basodara, Warcomhed, dan Warci yang telah memberikan dukungan dalam bentuk apapun.
14. Seluruh pihak yang terlibat yang penulis tidak dapat sebutkan satu per satu, penulis ucapkan terima kasih yang sebesar-besarnya.

Penulis berharap hasil penelitian ini dapat memberikan kontribusi yang bermanfaat bagi perkembangan ilmu pengetahuan, khususnya dalam bidang keamanan siber dan jaringan komputer, serta dapat menjadi referensi bagi penelitian selanjutnya.

Akhir kata, penulis menyadari bahwa skripsi ini masih jauh dari sempurna. Oleh karena itu, saran dan kritik yang konstruktif sangat penulis harapkan untuk perbaikan di masa yang akan datang. Semoga skripsi ini dapat memberikan manfaat bagi semua pihak.

Bogor, Juni 2025

Fathan Luqman
320210402006

ABSTRAK

IMPLEMENTASI EXTENDED *DETECTION* AND RESPONSE PADA SECURITY OPERATION CENTER DAN COMPUTER SECURITY INDEPENDENT RESPONSE TEAM DALAM PENINGKATAN SISTEM KEAMANAN INFORMASI GUNA MENINGKATKAN SISTEM PERTAHANAN INFORMASI

Perkembangan teknologi digital yang pesat meningkatkan kompleksitas ancaman siber, yang kini semakin canggih dan terorganisir, menargetkan individu, perusahaan, dan infrastruktur kritis. Oleh karena itu, sistem keamanan informasi yang mampu mendeteksi dan merespons ancaman secara otomatis menjadi kebutuhan mendesak. Penelitian ini bertujuan mengkaji implementasi *Extended Detection and Response* (XDR) dalam *Security Operation Center* (SOC) dan *Computer Security Incident Response Team* (CSIRT) guna meningkatkan efektivitas sistem keamanan informasi. Metode yang digunakan adalah eksperimen dengan pengujian dalam lingkungan yang dikontrol menggunakan Wazuh sebagai platform XDR. Studi ini menganalisis bagaimana XDR mengumpulkan, menganalisis, dan merespons data log secara *real-time* untuk mendeteksi ancaman dengan lebih akurat. Hasil penelitian menunjukkan bahwa XDR mampu meningkatkan deteksi ancaman dengan mengintegrasikan log dari berbagai sumber, termasuk *endpoint*, jaringan, dan layanan *cloud*, serta mengotomatiskan mitigasi insiden untuk respons yang lebih cepat. Integrasi *Machine Learning* dalam XDR juga terbukti meningkatkan akurasi deteksi serangan, mengurangi *false positives*, dan mempercepat analisis insiden. Kesimpulannya, XDR menjadi solusi komprehensif bagi sistem keamanan informasi modern, terutama dalam konteks SOC dan CSIRT, dengan kemampuannya dalam analitik berbasis deteksi, korelasi data multi-sumber, dan respons otomatis terhadap ancaman. Berdasarkan pengujian ini juga dihasilkan bahwa efisiensi XDR dalam melakukan pendeteksian dan mitigasi serangan malware adalah sebesar 98,3% dengan menggunakan hingga 60 *malware* dan waktu respon kurang dari 10 detik. Oleh karena itu, implementasi XDR direkomendasikan bagi organisasi yang ingin meningkatkan sistem keamanan mereka secara lebih adaptif dan proaktif dalam menghadapi ancaman siber yang terus berkembang.

Kata kunci: *Extended Detection and Response* (XDR), *Security Operation Center* (SOC), *Computer Security Incident Response Team* (CSIRT), Keamanan Siber, Deteksi Ancaman, Wazuh

ABSTRACT

IMPLEMENTATION OF EXTENDED *DETECTION* AND RESPONSE IN THE SECURITY OPERATION CENTRE AND COMPUTER SECURITY INDEPENDENT RESPONSE TEAM IN IMPROVING INFORMATION SECURITY SYSTEMS TO IMPROVE INFORMATION DEFENCE SYSTEMS

The rapid development of digital technology increases the complexity of cyber threats, which are now increasingly sophisticated and organised, targeting individuals, enterprises and critical infrastructure. Therefore, an information security system capable of automatically detecting and responding to threats is an urgent need. This research aims to examine the implementation of Extended Detection and Response (XDR) in the Security Operation Centre (SOC) and Computer Security Incident Response Team (CSIRT) to improve the effectiveness of information security systems. The method used is experimental with testing in a controlled environment using Wazuh as the XDR platform. This study analyses how XDR collects, analyses and responds to log data in real-time to detect threats more accurately. The results show that XDR is able to improve threat detection by integrating logs from multiple sources, including endpoints, networks, and cloud services, and automating incident mitigation for faster response. The integration of Machine Learning in XDR is also proven to improve attack detection accuracy, reduce false positives, and speed up incident analysis. In conclusion, XDR is a comprehensive solution for modern information security systems, especially in the context of SOC and CSIRT, with its capabilities in detection-based analytics, multi-source data correlation, and automated response to threats. Based on this test, the efficiency of XDR in detecting and mitigating malware attacks is 98.3% using up to 60 malware and responds time under 10 second. Therefore, the implementation of XDR is recommended for organisations looking to enhance their security systems in a more adaptive and proactive manner in the face of evolving cyber threats.

Keywords: Extended *Detection* and Response (XDR), Security Operation Center (SOC), Computer Security Incident Response Team (CSIRT), Cybersecurity, Threat *Detection*, Wazuh

DAFTAR ISI

LEMBAR PERSETUJUAN SKRIPSI.....	ii
LEMBAR PENGESAHAN SKRIPSI	iii
PERNYATAAN ORISINALITAS	iv
KATA PENGANTAR	v
ABSTRAK	viii
ABSTRACT	ix
DAFTAR ISI	x
DAFTAR GAMBAR	xiii
DAFTAR TABEL	xv
DARTAR SINGKATAN	xvi
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	3
1.3 Batasan Masalah	3
1.4 Tujuan	4
1.5 Manfaat	5
1.5.1 Manfaat Teoritis	5
1.5.2 Manfaat Praktis	6
BAB II TINJAUAN PUSTAKA.....	7
2.1 <i>Grand Theory</i>	7
2.1.1 Keamanan Siber (<i>Cyber Security</i>).....	7
2.1.2 <i>Information Technology Service Management (ITSM)</i>	10
2.1.3 <i>Security Operation Center (SOC)</i>	11
2.1.4 <i>Computer Security Incident Response Team (CSIRT)</i>	13
2.1.5 <i>Network Operation Center (NOC)</i>	15
2.2 <i>Middle Theory</i>	17
2.2.1 <i>Malicious Software (Malware)</i>	17

2.2.2	<i>Zero day exploit</i>	21
2.2.3	<i>Domain Name Server Spoofing (DNS Spoofing)</i>	23
2.2.4	<i>Distributed Denial of Service (Ddos)</i>	26
2.2.5	<i>Phising</i>	27
2.2.6	<i>Wazuh</i>	29
2.3	<i>Applied Theory</i>	31
2.3.1	Konsep <i>Extended Detection and Response (XDR)</i>	31
2.3.2	Pembeda Antara SIEM, XDR dan SOAR	34
2.4	Hasil Penelitian Terdahulu	38
2.5	Kerangka Berpikir.....	41
BAB III METODOLOGI PENELITIAN.....		45
3.1	Metode dan Desain Penelitian.....	45
3.2	Tempat dan Waktu Penelitian	46
3.3	Alat.....	47
3.4	Prosedur Penelitian.....	47
3.4.1	Analisis kebutuhan	48
3.4.2	Desain	48
3.4.3	Perencanaan Sistem.....	50
3.4.4	Implementasi	50
3.4.5	Pengujian	51
3.4.6	Evaluasi	51
3.5	Metode Analisis.....	51
BAB IV HASIL DAN PEMBAHASAN.....		52
4.1	Hasil.....	52
4.1.1	<i>Detection and Deleting Malware</i>	52
4.1.2	Deteksi Serangan Domain Server	54
4.1.2.1	<i>Brute force</i>	55
4.1.2.2	<i>Network Intrusion Detection System</i>	56
4.1.2.3	<i>Denial of Service Attack</i>	58
4.2	Pembahasan.....	60
4.2.1	Analisis Kebutuhan	60
4.2.2	Perancangan Desain	61
4.2.3	Implementasi	61

4.2.3.1 Integrasi Wazuh dengan VirusTotal	62
4.2.3.2 Integrasi Wazuh dengan Suricata	62
4.2.3.3 Penambahan <i>Rule</i>	64
4.2.4 Pengujian	65
4.2.4.1 Pengujian <i>Detecting and Deleting Malware</i>	66
4.2.4.2 Pengujian <i>Brute Force</i>	67
4.2.4.3 Pengujian <i>Intrusion Detecting System (IDS)</i>	68
4.2.4.4 Pengujian <i>DoS Attack</i>	73
BAB V KESIMPULAN DAN SARAN.....	77
5.1 Kesimpulan	77
5.1.1 Analisis dan Evaluasi Kinerja XDR dalam Deteksi <i>Malware</i> dan Respon terhadap Ancaman	77
5.1.2 Identifikasi Jenis Serangan Utama pada Domain Server dan Faktor Penyebabnya.....	78
5.1.3 Strategi Peningkatan Optimalisasi Tim SOC dan CSIRT melalui Implementasi XDR.....	78
5.2 Saran	79
DAFTAR PUSTAKA.....	81
LAMPIRAN.....	84
LAMPIRAN 1 Lembar Sertifikat Magang dan Penelitian	84
LAMPIRAN 2 Kegiatan Set Up dan Mounting Server	84
LAMPIRAN 3 Lembar Perizinan Penelitian ke 1	85
LAMPIRAN 4 Lembar Perizinan Penelitian ke 2	86
LAMPIRAN 5 Lembar Nota Dinas Telkomsat ke 1	87
LAMPIRAN 6 Lembar Nota Dinas Telkomsat ke 2	88
LAMPIRAN 7 Uji Plagiarisme.....	89

DAFTAR GAMBAR

Gambar 1.1 Data Statistik Serangan Siber di Indonesia	2
Gambar 2.1 Cyber Security Framework	7
Gambar 2.2 CIA Triad Diagram	8
Gambar 2.3 Diagram ITSM	10
Gambar 2.4 Arsitektur SOC	11
Gambar 2.5 Diagram CSF CSIRT	13
Gambar 2.6 Siklus Penanganan Insiden	14
Gambar 2.7 Diagram NOC Service	15
Gambar 2.8 Jenis Malware	18
Gambar 2.9 Diagram Alur Malware	22
Gambar 2.10 Cara Kerja DNS Spoofing	24
Gambar 2.11 Diagram Ddos	26
Gambar 2.12 Cara Mitigasi Phising	28
Gambar 2.13 GUI Wazuh	29
Gambar 2.14 Diagram XDR	31
Gambar 2.15 GUI XDR Wazuh	32
Gambar 2.16 Perbedaan XDR dengan SIEM	34
Gambar 2.17 Kerangka Berpikir	43
Gambar 3.1 Diagram Alir Penelitian	45
Gambar 3.2 Diagram Alir Prosedur Penelitian	48
Gambar 3.3 Cara Kerja XDR	49
Gambar 3.4 Arsitektur jaringan	50
Gambar 4.1 Diagram Hasil Pengujian	52
Gambar 4.2 Log Malware Detection	53
Gambar 4.3 Log File Integrity Monitoring	54
Gambar 4.4 konfigurasi Script Hydra	55
Gambar 4.5 Log Activity	55
Gambar 4.6 Daftar Pengujian NIDS	56

Gambar 4.7 Log Activity IDS	57
Gambar 4.8 SYN Flood DoS Attack Command Script	58
Gambar 4.9 ICMP Flood DoS Attack Command Script.....	58
Gambar 4.10 UDP Flood DoS Attack Command Script	58
Gambar 4.11 Log Event SYN Flood	59
Gambar 4.12 Log Event ICMP Flood.....	59
Gambar 4.13 Script Integrasi VirtusTotal	62
Gambar 4.14 Command Script Install Suricata.....	63
Gambar 4.15 Inform Routing Suricata to Network.....	63
Gambar 4.16 Configuration Packet.....	63
Gambar 4.17 Config Rule Suricata	64
Gambar 4.18 Config Rule VirusTotal	64

DAFTAR TABEL

Tabel 2.1 Perbedaan Antara XDR dengan SIEM	35
Tabel 2.2 Hasil Penelitian Terdahulu	38
Tabel 3.1 Jadwal Penelitian.....	46
Tabel 4.1 Kebutuhan dalam implementasi XDR	60
Tabel 4.2 Rule Level	67
Tabel 4.3 Penjelasan Script Tools Hydra	68
Tabel 4.4 Penjelasan Script SYN Flood	74
Tabel 4.5 Penjelasan Script ICMP Flood	74
Tabel 4.6 Penjelasan Script UDP Flood.....	75

DARTAR SINGKATAN

APT	: <i>Advanced Persistent Threats</i>
CIA	: <i>Confidentiality, Integrity, and Availability</i>
CERT	: <i>Computer Emergency Response Team</i>
CSIRT	: <i>Computer Security Incident Response Team</i>
CVE	: <i>Common Vulnerability and Exposure</i>
DDOS	: <i>Distributed Denial of Service</i>
DNS	: <i>Domain Name Server</i>
DOS	: <i>Denial of Service</i>
EDR	: <i>Endpoint Detection and Response</i>
FIM	: <i>File Integrity Monitoring</i>
HTTP	: <i>HyperText Transfer Protocol</i>
ICMP	: <i>Internet Control Message Protocol</i>
IDS	: <i>Intrusion Detection Systems</i>
IEC	: <i>International Electrotechnical Commission</i>
IOT	: <i>Internet of Things</i>
IP	: <i>Internet Protocol</i>
IPS	: <i>Intrusion Protection System</i>
ISO	: <i>International Organization for Standardization</i>
ITSM	: <i>Information Technology Service Management</i>
KEMHAN	: <i>Kementerian Pertahanan Republik Indonesia</i>
MALWARE	: <i>Malicious Software</i>
MFA	: <i>Multi Factor Authentication</i>
MDR	: <i>Managed Detection and Response</i>
ML	: <i>Machine Learning</i>
MXDR	: <i>Managed Extended Detection and Response</i>
NDR	: <i>Network Detection and Response</i>
NIC	: <i>Network Interface Card</i>
NIDS	: <i>Network Intrusion Detection System</i>
NOC	: <i>Network Operation Center</i>
PDF	: <i>Portable Document Format</i>

PENTEST	: <i>Penetration Test</i>
POLRI	: Kepolisian Republik Indonesia
PUP	: <i>Potentially Unwanted Program</i>
SIEM	: <i>Security Information and Event Management</i>
SOC	: <i>Security Operation Center</i>
SOAR	: <i>Security Orchestration, Automation, and Response</i>
SSH	: <i>Secure Shell</i>
SYN	: <i>Synchronize</i>
TCP	: <i>Transmission Control Protocol</i>
TI	: Teknologi Informasi
TNI	: Tentara Nasional Indonesia
UDP	: <i>User Datagram Protocol</i>
UID	: <i>User Identifier</i>
UNHAN	: Universitas Pertahanan Republik Indonesia
VA	: <i>Vulnerability Assessment</i>
VIT	: <i>Vision Transformer</i>
VM	: <i>Virtual Machine</i>
WIFI	: <i>Wireless Fidelity</i>
XDR	: <i>Extended Detection and Response</i>