BAB 2
TINJAUAN PUSTAKA

2.1 Landasan Teori

Beberapa teori dasar yang mendukung penelitian ini meliputi konsep-konsep utama yang digunakan untuk membangun sistem.

2.1.1 Malware Information Sharing Platform

Malware Information Sharing Platform (MISP) platform *Open Source* yang memungkinkan organisasi untuk berbagi informasi seperti intelijen ancaman, indikator, informasi pelaku ancaman, atau segala jenis ancaman yang terstruktur dalam MISP. Pengguna MISP mendapatkan manfaat dari pengetahuan kolaboratif tentang malware atau ancaman yang ada. Tujuan dari Platform ini adalah untuk membantu meningkatkan langkah-langkah penanggulangan terhadap serangan target dan menyiapkan tindakan pencegahan serta deteksi. MISP merupakan platform terbuka untuk berbagai informasi yang mendukung kolaborasi antar pengguna dari berbagai komunitas dalam pertukaran indikator ancaman dan data terkait lainnya (Alsehri, 2021).

Gambar 2. 1 Tampilan Dashboard MISP
Sumber : https://www.misp-project.org/

MISP bekerja sebagai sebuah ekosistem intelijen ancaman yang terstruktur, memulai operasinya dengan pengumpulan informasi dari berbagai sumber. Data dapat dimasukkan secara manual oleh analis setelah identifikasi *Indikator Kompromi* (IoC) baru dari investigasi internal atau laporan eksternal. Selain itu,

MISP dapat dikonfigurasi untuk secara otomatis mengimpor feed intelijen ancaman dari berbagai sumber, baik dari komunitas keamanan maupun penyedia komersial. Integrasi melalui API juga memungkinkan sistem keamanan lain seperti SIEM atau platform insiden untuk secara otomatis mengirimkan data IoC yang terdeteksi.

Fungsi dan Fitur MISP

1. Pengelolaan IoC

   MISP memungkinkan pengguna untuk menyimpan dan mengelola berbagai jenis IoC seperti alamat IP, domain, URL, file hash, serta artefak lainnya dalam bentuk event dan attribute yang terstruktur.
2. Klasifikasi dan metadata

   Setiap data yang dimasukkan dapat dilengkapi dengan metadata seperti tingkat ancaman (*threat level*), tingkat kepercayaan (*confidence*), serta *tagging* untuk memudahkan proses klasifikasi dan pencarian.
3. Korelasi Data Otomatis

   MISP mampu melakukan korelasi antar indikator secara otomatis untuk menemukan keterkaitan antar data, sehingga membantu analis dalam mengidentifikasi pola serangan.
4. Standarisasi Pertukaran Data

   MISP mendukung standar pertukaran intelijen ancaman seperti STIX (Structured Threat Information Expression) dan TAXII (Trusted Automated Exchange of Indicator Information), sehingga memudahkan interoperabilitas antar sistem
5. Integrasi dengan sistem keamanan lain

   MISP dapat diintegrasikan dengan berbagai sistem kamanan seperti SIEM, IDS/IPS, dan platform monitoring lainnya untuk meningkatkan kemampuan deteksi dan respon insiden.

Dalam penelitian ini, MISP berfungsi sebagai pusat pengelolaan *Threat Intelligence* yang digunakan untuk mengumpulkan, mengelola, menyimpan, dan mendistribusikan *Indicator of Compromise* (IoC). Informasi ancaman dikelola dalam bentuk *event* sebagai wadah informasi ancaman dan *Attribute* representasi IoC, seperti Domain, URL, Ip address, ataupaun Hash file. *Event* yang

dipublikasikan kemudian diteruskan ke *TheHive* melalui integrasi API untuk proses analisis lebih lanjut menggunakan Cortex.

2.1.2 Cyber Threat Intelligence

Threat Intelligence adalah proses pengumpulan, analisis dan interpretasi data atau informasi yang berkaitan dengan ancaman keamanan siber. Informasi yang dikumpulkan berupa data, pola serangan, taktik, teknik dan prosedur yang digunakan oleh penyerang, serta sumber daya yang terlibat dalam aktivitas jahat.

Gambar 2. 2 Alur Threat Intelligence
Sumber: https://www.balbix.com/insights/cyber-threat-intelligence-guide/

Cyber Threat Intelligence (CTI) proses pengambilan berbagai informasi tentang serangan siber dan memahami bagaimana serangan itu terjadi. Hal ini dapat membantu memprediksi dan mencegah serangan siber. Dapat disebut juga Intelijen ancaman, yaitu sebuah metode untuk memperingatkan sebuah organisasi berdasarkan data yang diperoleh dari berbagai sumber yang telah dianalisis. Sumber ancaman pelanggaran data berupa malware, ancaman orang dalam, rekayasa sosial (Hidayat et al, 2025).

2.1.3 Security Operation Center (SOC)

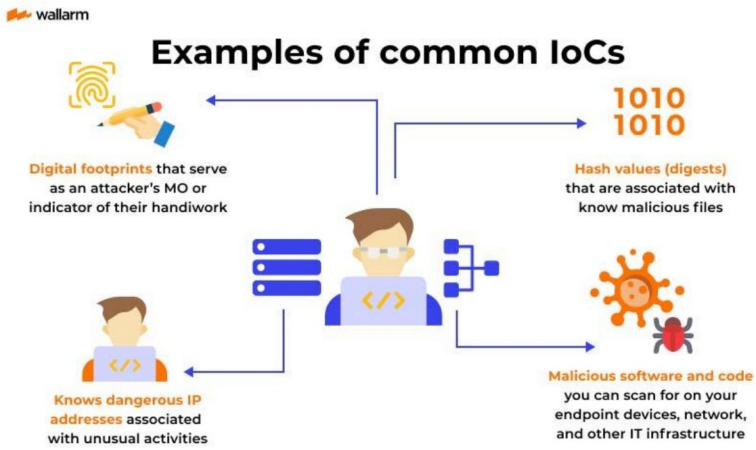
Security Operation Center adalah pusat keamanan yang bertanggung jawab untuk mendeteksi dan merespons insiden keamanan secara real-time melalui monitoring, analisis dan koordinasi tindakan keamanan. Penilitian menunjukan bahwa implementasi SOC membutuhkan strategi yang matang serta sumber daya dan teknologi yang tepat untuk mendukup operasi keamanan secara efektif.

Gambar 2. 3 Fungsi SOC
Sumber: https://goipgroup.com/security-operations-center-soc-roles-and-responsibilities/

Security Operations Center (SOC) merupakan pusat operasional tempat tim keamanan menjalankan berbagai fungsi perlindungan aset perusahaan. Aktivitas yang dilakukan mencakup pencegahan serangan, pemantauan keamanan, penanganan insiden, serta pengumpulan dan analisis data keamanan. Melalui proses deteksi ancaman dan analisis perilaku, SOC berperan penting dalam menjaga keamanan jaringan dan sistem serta mencegah terjadinya serangan siber (Nayyul, 2024).

2.1.4 Indicators Of Compromise (IoC)

Indicators of Compromise adalah artefak digital yang menunjukkan aktivitas berbahaya seperti malware atau intrusi. IOC didefinisikan sebagai artefak forensik atau bukti digital yang ditemukan pada jaringan atau sistem operasi yang menunjukkan adanya intrusi atau pelanggaran keamanan.



Gambar 2. 4 Contoh IoC
Sumber: https://www.balbix.com/insights/cyber-threat-intelligence-guide/

IoC berfungsi seperti "rekam jejak" atau sidik jari digital yang ditinggal oleh penyerang, yang memungkinkan tim keamanan untuk mengidentifikasi aktivitas berbahaya yang mungkin telah melewati pertahanan. IoC merupakan sekumpulan informasi atau artefak forensik yang digunakan untuk mengidentifikasi sistem atau komputer yang telah terinfeksi oleh malware. Identifikasi IoC yang akurat memungkinkan tim respons insiden untuk memahami karakteristik serangan dan menentukan cakupan kerusakan yang terjadi pada infrastruktur organisasi (Rahayu & Trianto, 2021).

Tujuan dan penggunaan Indicator of Compromise (IoC) antara lain :

1) Mendeteksi Ancaman secara dini
   IoC Membantu mengidentifikasi aktivitas berbahaya sebelum berkembang menjadi serangan yang lebih besar.
2) Mendukung Proses Investigasi Insiden
   IoC memberikan informasi penting yang membantu tim keamanan dalam menelusuri sumber dan metode serangan.
3) Menentukan cakupan dampak serangan
   Dengan menganalisis IoC, organisasi atau team dapat mengetahui sejauh mana sistem yang terdampak
4) Meningkatkan respon dan mitigasi

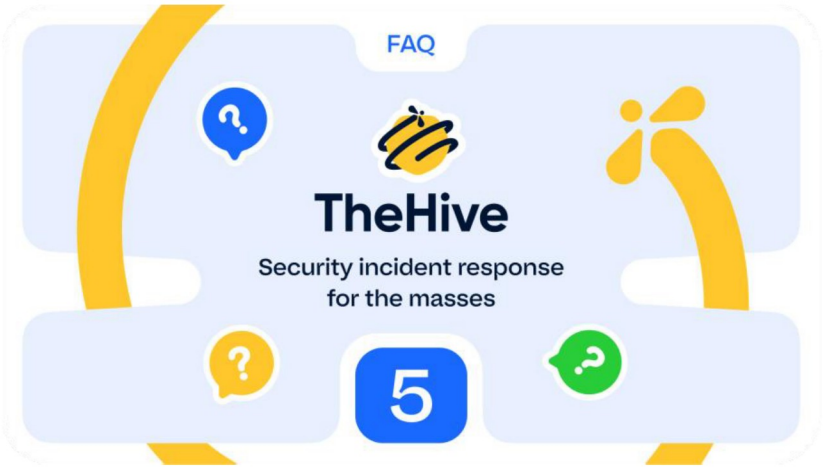
IoC memungkinkan tim keamanan untuk mengambil tindakan cepat seperti pemblokiran IP, domain, atau file berbahaya.

5) Mendukung integrasi dengan sistem keamanan

IoC dapat diintegrasikan dengan berbagai sistem seperti SIEM, IDS/IPS, maupun MISP untuk mengintegrasikan efektivitas deteksi dan respon terhadap ancaman.

2.1.5 The Hive

TheHive merupakan sebuah platform open-source yang dikembangkan untuk mendukung pengelolaan respons insiden keamanan siber secara terorganisir dan efektif. Platform ini menyediakan berbagai fitur, antara lain integrasi dengan alat analisis dan otomatisasi respons seperti Cortex, kemampuan pencatatan serta pengelolaan kasus keamanan, dan mekanisme kolaborasi yang mendukung kerja tim keamanan. Dengan adanya fleksibilitas dalam pengaturan workflow dan aturan operasional, TheHive memungkinkan proses investigasi dilakukan secara sistematis dan efisien (Nayyul, 2024).

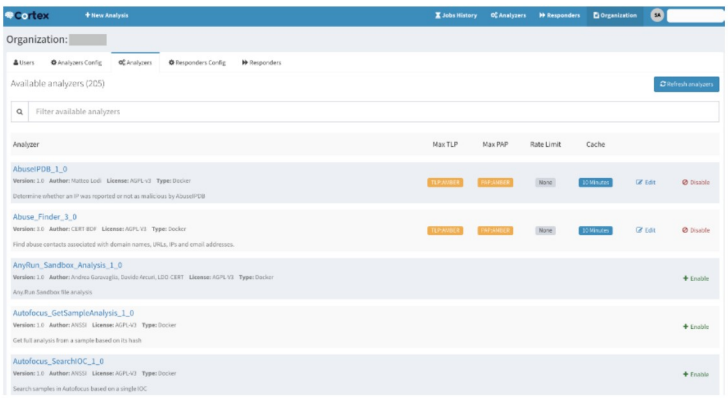


Gambar 2. 5 TheHive Platform Incident

Selain itu, platform ini mendukung visulisasi dan alaisis data yang komprehensif serta dirancang untuk menangani data dalam jumlah besar dan kompleks. Fitur multi-tenancy yang dimiliki TheHive juga memungkinkan pengelolaan beberapa organisasi atau unit kerja dalam satu sistem, sehingga menjadikannya solusi yang skalabel dan adaptif terhadap kebutuhan manajemen respons insiden.

2.1.6 Cortex

Cortex adalah mesin automated analysis yang digunakan untuk memproses IoC secara otomatis dari platform CTI seperti MISP, mempercepat konteks analisis data ancaman. Cortex umumnya dipakai dalam workflow SOC untuk enrichment data dan otomatisasi.

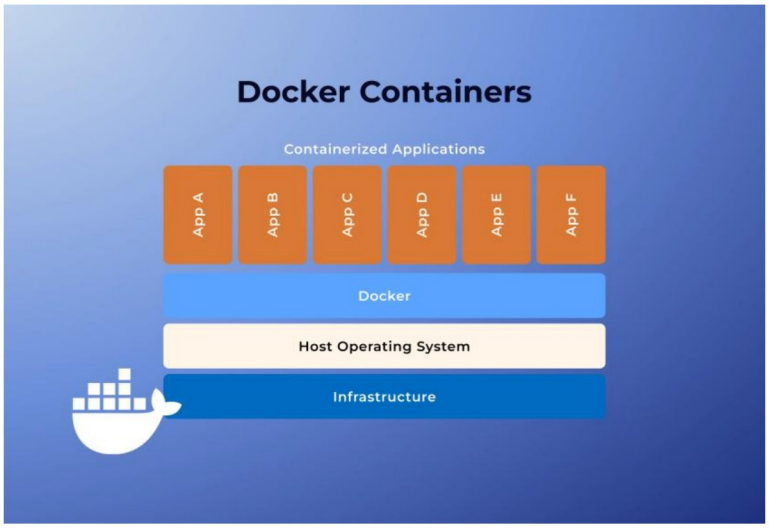


Gambar 2. 6 *Dashboard Cortex*

Cortex merupakan platform open source yang berfungsi sebagai mesin analisis otomatis (*automated analysis engine*) dalam ekosistem *Security Operations Center* (SOC). Cortex dirancang untuk melakukan proses enrichment dan analisis terhadap berbagai observable atau data ancaman seperti alamat Ip, domain, URL, hash file, dan artefak digitlan lainnya secara otomatis. Cortex merupakan platform analisis keamanan yang fleksibel dan mendukung lebih dari 100 jenis analisator untuk memproses berbagai artefak dan indikator kompromi (Nayyul, 2024).

2.1.7 Docker

Docker adalah platform *containerization* yang memungkinkan aplikasi dan dependensinya dijalankan secara terisolasi dalam lingkungan kontainer yang ringan dan portabel. Dalam konteks threat monitoring dan intelligence SOC, Docker sering digunakan untuk *deploy* layanan seperti SIEM, ELK Stack, dan platform intelijen ancaman karena kemampuannya menyediakan isolasi, portabilitas, dan konsistensi konfigurasi aplikasi di berbagai environment.

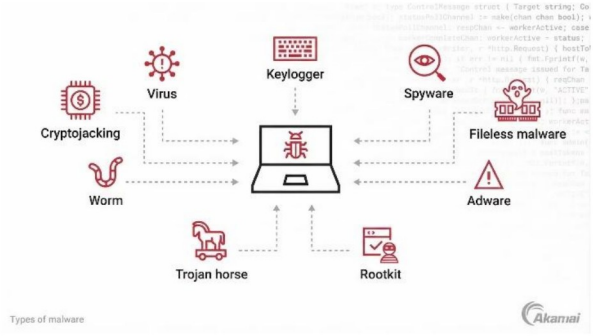


Gambar 2. 7 Docker Containers

Penelitian oleh (Alam et al., 2024) menggambarkan penggunaan Docker dalam konteks sistem monitoring, di mana Docker Container digunakan untuk menjalankan komponen perangkat lunak pemantauan dan kontrol. Meski fokus penelitian bukan keamanan kontainer, penggunaan Docker terbukti dapat menyederhanakan pengelolaan komponen monitoring secara efisien melalui isolasi layanan dan kemudahan deployment di lingkungan laboratorium cerdas.

2.1.8 Malware

Malware (malicious software) merupakan perangkat lunak berbahaya yan dirancang untuk merusak, menggangu, atau mendapatkan akses tidak sah ke sistem komputer. Malware memanfaatkan kelemahan sistem dan beroperasi tanpa diketahui oleh pengguna. Malware mencakup beberapa jenis seperti virus, worm, troja, spyware dan ransomware yang memiliki tujuan utama untuk mengeksploitasi sistem atau mencuri informasi pengguna. Penyebab malware dapat dilakukan dari berbagai media contohnya seperti email, unduhan aplikasi, ataupun eksploitasi kerentanan sistem (Ultvi et al., 2026).



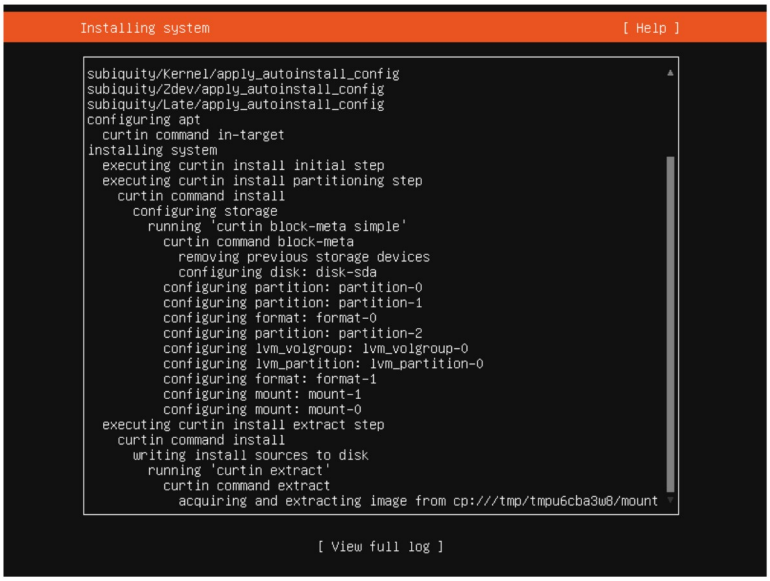
Gambar 2. 8 Jenis Malware

Malware merupakan ancaman utama dalam keamanan siber yang memerlukan metode deteksi khusus seperti analisis statis dan dinamis untuk memahami karakteristik dan perilakunya (Khalda et al., 2025). Analisis statis dilakukan tanpa menjalankan program sedangan analisis dinamis dilakukan dengan mengamati perilaku malware saat dieksekusi dalam lingkungan terkendali.

(Ultvi et al., 2026) Menjelasakan bahwa Berdasarkan karakteristik, malware terdiri dari beberapa jenis, yaitu Virus, worm, trojan, spyware, adware, ransomware dan backdoor. Virus bekerja dengan menginfeksi file atau program lain dan aktif ketika file tersebut dijalankan. Worm dapat menyebar secara otomatis melalui jaringan tanpa memerlukan media perantara. Trojan dirancang menyerupai aplikasi sah sehingga dapat mengelabui pengguna untuk menjalankannya. Spyware berfungsi memantau aktivitas pengguna serta mengumpulkan informasi sensitif tanpa sepengetahuan pengguna. Adware merupakan malware yang menampilkan iklan secara berlebihan sehingga dapat mengganggu kinerja sistem. Sementara itu ransomware mengenkripsi data korban dan meminta tebusan sebagai syarat untuk memulihkan akses terhadap data. Backdoor merupakan jenis malware yang memungkinkan pihak tidak berwenang memperoleh akses tersembunyi ke dalam sistem tanpa melalui mekanisme autentikasi semestinya.

2.1.9 Linux Ubuntu

Linux Ubuntu adalah distribusi *open-source* berbasis Linux yang populer digunakan sebagai sistem operasi server dan *platform* pengujian dalam penelitian keamanan siber. Ubuntu menyediakan lingkungan stabil dan aman untuk menjalankan berbagai layanan terkait *threat intelligence*, termasuk SIEM, ELK Stack, dan agent monitoring seperti Wazuh karena keandalan, dukungan komunitas, serta fleksibilitasnya untuk konfigurasi keamanan.



Gambar 2. 9 Instalasi Ubuntu

Linux ubuntu suatu sistem distribusi debian yang bersifat open source dan sering digunakan sebagai keperluan server karena memiliki keamanan dan kestabilan yang baik (Rahmadani et al., 2025). Penelitian lain juga menekankan peran Ubuntu sebagai basis *Operating System* untuk sistem monitoring jaringan yang mengumpulkan dan menganalisis *log* keamanan perangkat dan jaringan, memfasilitasi proses pemantauan dan deteksi ancaman secara real-time menggunakan perangkat lunak seperti SIEM atau middleware pemantauan.

2.2 Penelitian Terdahulu

Penelitian Pertama "*Implementasi Security Information And Event Management* (SIEM) Menggunakan Wazuh Pada Politeknik Caltex Riau" oleh (Zahira, 2023) yaitu menerapkan sistem pendeteksi serangan dan menghasilkan sebuah log menggunakan Wazuh pada Politeknik Caltex Riau. Skenario pengujian yang dilakukan mulai dari instalasi Wazuh Server (SIEM), Wazuh Agent (website), lalu Wazuh Dashboard untuk pemantauan, lalu menambahkan dua server PCR sebagai agen Wazuh untuk dipantau. Serangan yang dilakukan yaitu DoS Attack, BruteForce, dan SQL Injection yang di simulasikan di wazuh agent. Hasil dari penelitian ini adalah wazuh berhasil mendeteksi serangan keamanan yang dilakukan pada Politeknik Caltex Riau.

Penelitian Kedua "*Implementasi Security Orchestration and Response* (SOAR) Sistem Menggunakan Shuffle Di Politeknik Caltex Riau" oleh (Nayyul, 2024) bertujuan untuk meningkatkan respons dan mitigasi terhadap serangan siber. Shuffle sebagai platform SOAR yang bertanggung jawab atas orkestrasi dan otomatisasi alur kerja keamanan. Projek ini mengintegrasikan berbagai tools keamanan seperti Wazuh, TheHive, Cortex yang nantinya akan saling terhubung dan mendapat respons yang terkoordinasi dan efektif. Serangan yang dilakukan pada penelitian ini yaitu SQL Injection, SSH Brute Force, DDOS.

Penelitian Ketiga "Implementasi IDS/IPS Menggunakan OPNsense dan Event Log Management Menggunakan ELK" oleh (Sidi, 2024) bertujuan untuk mengimplementasikan sistem keamanan yang kuat yang mampu mendeteksi dan mencegah intrusi jaringan, sekaligus menyediakan visualisasi log serangan yang efektif. Alat utama yang digunakan yaitu OPNsense untuk fungsi *Intrusion Detection System/ Intrusion Prevention System* (IDS/IPS) dan *Elasticsearch, logstash, Kibana* (ELK) untuk manajemen log peristiwa, OPNsense sebuah Firewall yang digunakan untuk mendeteksi dan mencegah berbagai serangan seperti Port Scanning, DDOS, dan SSH BruteForce.

Penelitian Keempat "Integrasi Wazuh dan Suricata dengan Notifikasi Telegram" oleh (Shidiqi, 2024) untuk memperkuat keamanan jaringan dengan mengintegrasikan Wazuh sebagai sistem manajemen log dan suricata sebagai sistem deteksi intrusi. Integrasi ini bertujuan untuk membangun sistem notifikasi serangan yang responsif dan efisien melalui Telegram, memastikan administrator jaringan menerima peringatan secara tepat waktu. Jenis serangan yang dilakukan yaitu Port Scanning, *Distributed Denial Of Service* (DDOS), SSH Brute Force.

Penelitian Kelima "Monitoring Keamanan Jaringan Menggunakan Suricata Melalui Telegram" oleh (Fikri, 2024) membangun sistem keamanan jaringan yang efektif untuk mendeteksi dan mencegah serangan siber. Proyek ini mencakup implementasi *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS) menggunakan suricata. Untuk mendukung monitoring dan analisis, proyek ini mengintegrasikan Suricata dengan *Elasticsearch, Logstash, Kibana* (ELK). ELK berperan mengumpulkan, memproses, menganalisis dan memvisualisasikan log suricata secara efektif. Pengiriman log ke ELK Stack dilakukan melalui Filebeat.

Serangan yang disimulasikan yaitu DoS Syn Flood, SSH Login Attempt, dan MySQL Prompt Login Attempt.

Table 2. 1 Penelitian Terdahulu

Judul Penelitian	Tujuan	Tools
Implementasi Security Information And Event Management (SIEM) Menggunakan Wazuh Pada Politeknik Caltex Riau (Zahira, 2023)	Memantau log yang didapat dari Wazuh dan menganalisis apakah terdapat sebuah ancaman yang terjadi pada sistem.	Wazuh
Implementasi Security Orchestration, Automation And Response (SOAR) Sistem Menggunakan Shuffle Di Politeknik Caltex Riau (Nayyul, 2024)	Meningkatkan respons dan mitigasi terhadap serangan siber menggunakan sistem keamanan SIEM dan SOAR dalam mendeteksi insiden keamanan.	Wazuh, Cortex, TheHive
Implementasi IDS/IPS Menggunakan OPNsense dan Event Log Management Menggunakan ELK (Sidi, 2024)	Proyek ini bertujuan untuk mendeteksi dan mencegah intrusi menggunakan OPNsense, dan juga menggunakan pemantauan dan analisis log menggunakan tools ELK	Elasticsearch Logstash Kibana, OPNsense
Integrasi Wazuh Dan Suricata Dengan Notifikasi Telegram (Shidiqi, 2024)	Proyek ini bertujuan untuk mengoptimalkan waktu respons notifikasi telegram dan menerima alert secara tepat waktu	Wazuh Suricata
Monitoring Keamanan Jaringan Menggunakan Suricata Melalui Telegram (Fikri, 2024)	Tujuan proyek ini yaitu mendeteksi dan mencegah serangan. Dengan menerapkan IDS dan IPS menggunakan suricata serta mengirim notifikasi jika adanya serangan melalui telegram.	Suricata ELK

Judul Penelitian	Tujuan	Tools
Implementasi Dan Integrasi Malware Information Sharing Platform Sebagai Sistem Threat Intelligence Pada Security Operation Center (Ardani, 2026)	Proyek ini bertujuan mengimplementasikan dan mengintegrasikan MISP sebagai Threat Intelligence untuk mendukung pengelolaan dan informasi ancaman	Misp Thehive Cortex