JKT Jurnal Komputer Terapan
ISSN : 2443-4159 (Print) ISSN: 2460-5255 (Online)
Politeknik Caltex Riau
Empower You to Global Competition

# KECERDASAN BUATAN UNTUK SECURITY ORCHESTRATION, AUTOMATION AND RESPONSE: TINJAUAN CAKUPAN

**Venny Gustina[1*] dan Ananda[2]**
Magister Terapan Teknik Komputer (Politeknik Caltex Riau, Pekanbaru, 28265, Indonesia) [1,2]
venny22mttk@mahasiswa.pcr.ac.id [1], ananda@pcr.ac.id [2]

**Penulis Koresponden*

**ABSTRAK**

*Saat ini, banyak organisasi memiliki kemampuan pertahanan siber yang terdiri dari berbagai alat, produk, dan solusi, yang sangat menantang bagi tim Pusat Operasi Keamanan (SOC) untuk mengelola lingkungan ancaman siber yang canggih dan terus berubah. Para peneliti keamanan dan praktisi industri telah mengembangkan solusi orkestrasi, otomatisasi, dan respons keamanan (SOAR) yang akan memberdayakan tim SOC dengan menggabungkan dan mengotomatisasi berbagai tugas, proses, dan aplikasi keamanan dalam menanggapi insiden keamanan. Integrasi dan Pemanfaatan kecerdasan buatan (AI) dalam solusi SOAR menjanjikan revolusi operasi keamanan siber. Penggunaan teknologi AI/ML dalam keamanan siber dapat meningkatkan efektivitas analis SOC dalam mendeteksi, mencegah, dan merespons serangan keamanan dengan cara seperti deteksi ancaman yang lebih baik, otomatisasi tugas rutin, analisis data yang lebih cepat dan akurat, peningkatan respons terhadap serangan, dan pengurangan beban kerja. Kemampuan deteksi pada mesin SOAR mencakup deteksi HTTP IDS, Botnet, dan DDoS, dengan menggunakan model pembelajaran mesin yang dilatih pada berbagai jenis data. Mesin SOAR juga dilengkapi dengan kemampuan deteksi ancaman keamanan lainnya, seperti analisis perilaku, analisis log, analisis malware, dan analisis intelijen ancaman. Sistem SOAR yang dilengkapi dengan mesin pembelajaran berbasis jaringan saraf tiruan mampu menganalisis data secara real-time dan melakukan deteksi ancaman dengan cepat. Sehingga penggunaan teknologi AI dan analisis real-time membantu dalam mengurangi beban kerja profesional keamanan dan meningkatkan efisiensi dalam menghadapi serangan siber.*

***Kata kunci:*** *kecerdasan buatan, SOAR, honeypot, SIEM*

---

**ABSTRACT**

*Nowadays, many organizations have cyber defense capabilities consisting of various tools, products, and solutions, which is very challenging for Security Operations Center (SOC) teams to manage the sophisticated and ever-changing cyber threat environment. Security researchers and industry practitioners have developed security orchestration, automation and response (SOAR) solutions that will empower SOC teams by combining and automating various security tasks, processes and applications in response to security incidents. The integration and utilization of artificial intelligence (AI) in SOAR solutions promises to revolutionize cybersecurity operations. The use of AI/ML technologies in cybersecurity can improve the effectiveness of SOC analysts in detecting, preventing, and responding to security attacks in ways such as better threat detection, automation of routine tasks, faster and more accurate data analysis, improved response to attacks, and reduced workload. Detection capabilities on the SOAR engine include HTTP IDS, Botnet, and DDoS detection, using machine learning models trained on various types of data. The SOAR engine is also equipped with other security threat detection capabilities, such as behavioral analysis, log analysis, malware analysis, and threat intelligence analysis. SOAR systems equipped with artificial neural network-based machine learning are capable of analyzing data in real-time and performing threat detection quickly. So the use of AI technology and real-time*

*analysis helps in reducing the workload of security professionals and increasing efficiency in dealing with cyberattacks.*

***Keywords:*** *artificial intelligence, SOAR, honeypot, SIEM*

**Histori Artikel:**
Diserahkan: 26 Januari 2024 Diterima setelah Revisi: 1 Mei 2024 Diterbitkan: 14 Juni 2024

## 1. PENDAHULUAN

Dalam beberapa tahun terakhir, perpaduan antara kecerdasan buatan (AI) dan keamanan siber telah menarik perhatian yang signifikan karena meningkatnya kompleksitas dan frekuensi ancaman siber. Kecerdasan Buatan (AI) telah menjadi komponen keamanan siber yang terus berkembang. Konsep Security Orchestration, Automation and Response (SOAR) mampu merespons insiden keamanan dengan intervensi manusia yang minimal dengan mengotomatiskan proses respons. SOAR adalah kerangka kerja otomatisasi keamanan komprehensif yang menyederhanakan dan mengotomatiskan proses respons terhadap insiden keamanan, mengurangi ketergantungan pada intervensi manual, dan meningkatkan efisiensi respons insiden [2]. Upaya penelitian tentang SOAR dalam beberapa tahun terakhir telah menetapkan kemampuan kecerdasan AI yang paling penting dalam desain dan implementasi SOAR. Secara khusus, AI/ML memainkan peran unik dalam analisis keamanan siber, intelijen ancaman, dan deteksi otomatis serta proses respons insiden [5]. Salah satu bidang yang menjadi perhatian khusus adalah penerapan AI dalam sistem Security Orchestration, Automation, and Response (SOAR), yang dirancang untuk mengintegrasikan alat keamanan, mengotomatiskan respons insiden, dan mengatur operasi keamanan.

Integrasi AI dalam SOAR menjanjikan revolusi operasi keamanan dengan memungkinkan organisasi mendeteksi, merespons, dan memitigasi ancaman siber secara lebih efektif dan efisien. Dengan memanfaatkan algoritme machine learning (ML), platform SOAR yang didukung AI dapat meningkatkan deteksi ancaman, mengotomatiskan tugas yang berulang, dan memberikan kemampuan canggih kepada tim keamanan, sehingga memberdayakan pusat operasi keamanan (SOC) untuk memperkuat strategi pertahanan siber[1].

Signifikansi SOAR yang digerakkan oleh AI semakin ditekankan oleh temuan survei terperinci yang meninjau karya-karya yang diterbitkan di jurnal akademis, konferensi, situs web, blog, dan buku putih. Survei tersebut mengidentifikasi area utama yang perlu diselidiki oleh para peneliti keamanan untuk otomatisasi dan sistem respons keamanan yang didukung AI/ML, yang menyoroti perlunya penelitian komprehensif dalam domain ini [5].

Karena lanskap keamanan siber terus berkembang, sangat penting bagi organisasi untuk tetap menjadi yang terdepan dalam menghadapi ancaman yang muncul. Frekuensi insiden keamanan yang terjadi serta waktu yang diperlukan untuk mendeteksi, menganalisis, dan menanggapi insiden keamanan juga meningkat karena tenaga kerja dan waktu yang dibutuhkan untuk melakukan manajemen terintegrasi dan analisis solusi yang heterogen [2]. Otomatisasi keamanan dan kerangka kerja orkestrasi untuk pemantauan terus menerus dan tambalan otomatis keamanan perangkat heterogen [12]. Dengan mengadopsi teknologi SOAR yang didukung AI menghadirkan peluang menarik bagi tim keamanan untuk meningkatkan ketahanan mereka terhadap serangan siber.

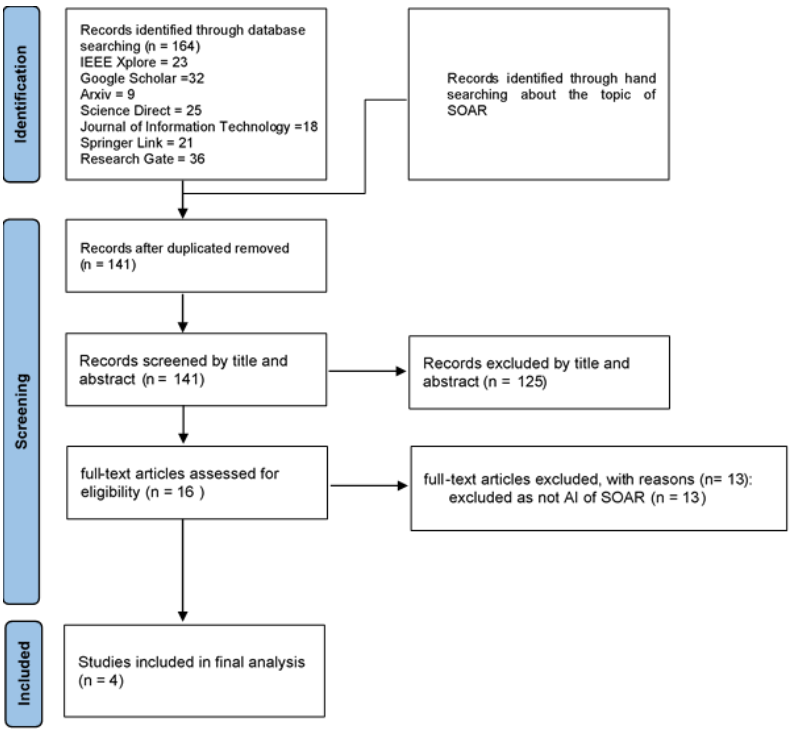
Dalam makalah ini, peneliti menyajikan tinjauan cakupan dari tujuh database (IEEE Xplore, Google Scholar, Arxiv, Science Direct, Journal of Information Technology, Springer Link, dan Research Gate) untuk meringkas literatur saat ini tentang AI dalam penelitian Orkestrasi, Otomasi, dan Respons Keamanan. Tujuan dari penelitian ini adalah untuk memberikan analisis deskriptif tentang literatur saat ini, mengidentifikasi kesenjangan penelitian, arah penelitian di

masa depan, dan dampak potensial AI pada keamanan siber yang diharapkan dapat memberikan gambaran umum tentang kecerdasan buatan dalam SOAR.

## 2. HASIL

### 2.1 Studi yang disertakan

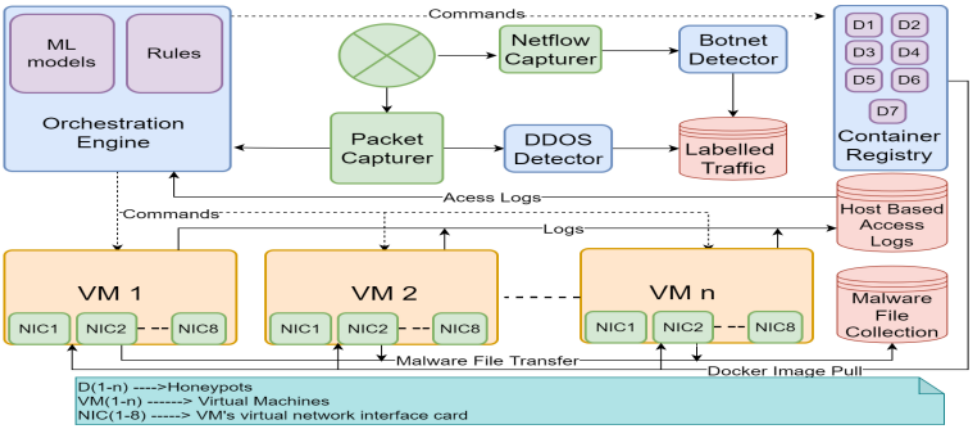
Gambar 1 menunjukkan diagram alir PRISMA dalam pemilihan makalah. Pencarian awal dari tujuh database menghasilkan 164 makalah dan peneliti mengidentifikasi melalui pencarian langsung tentang topik SOAR. Setelah mengecualikan 125 makalah dari penyaringan judul dan abstrak, peneliti mengidentifikasi 16 penelitian untuk penyaringan teks lengkap, di mana 4 penelitian diikutsertakan untuk analisis akhir [3,4,5,6].




**Gambar 1 Diagram alir PRISMA untuk pemilihan paper**

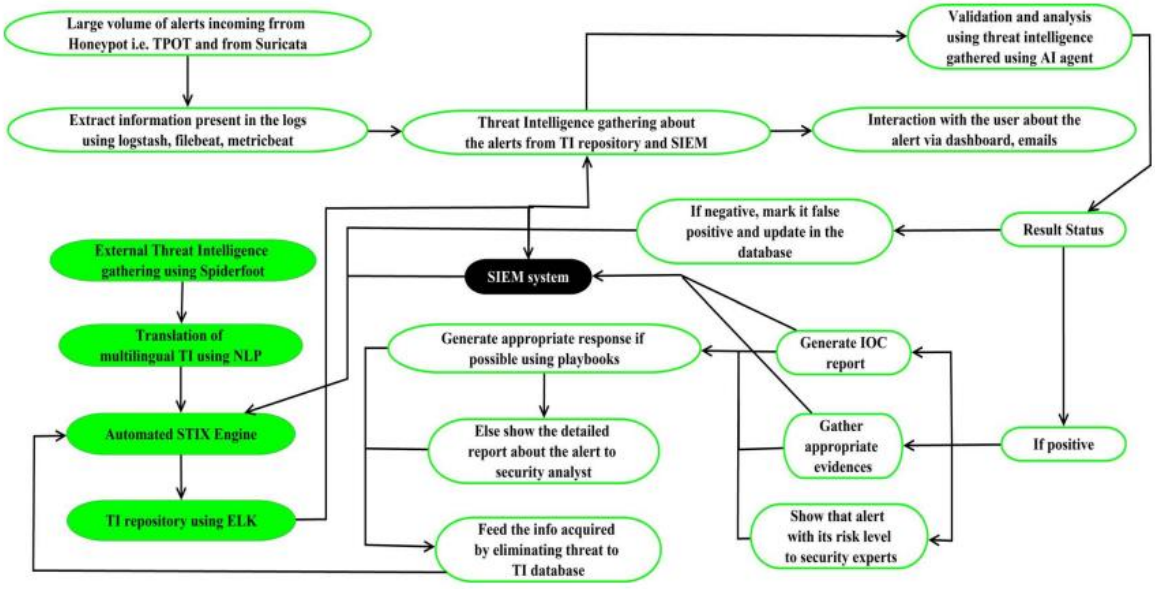
### 2.2 Karakteristik dan metodologi studi

Teknologi penipuan dan honeypot, yang dapat memberikan rasa kerentanan palsu kepada penyerang dan mengumpulkan informasi intelijen tentang metode ancaman, diperkenalkan oleh padapenelitian [3] berdasarkan arsitektur mesin SOAR yang ditunjukkan pada gambar 2. Arsitektur ini merekomendasikan Security Orchestration, Automation, and Response (SOAR) Engine yang secara dinamis menerapkan honeypot khusus yang disesuaikan dengan perilaku penyerang untuk meningkatkan keamanan organisasi Jaringan IT/OT. Model arsitektur hirarkis yang terdiri dari alat keamanan, integrasi, pemrosesan data, semantik, orkestrasi, dan lapisan antarmuka pengguna dalam mendesain platform SOAR [11]. Mesin SOAR dirancang untuk meningkatkan keterlibatan penyerang di honeypot, menghemat sumber daya, dan mengingatkan tim keamanan organisasi untuk mengambil tindakan lebih awal. Untuk orkestrasi, arsitektur ini mendukung berbagai VLAN. Mesin ini akan mengidentifikasi botnet, serangan DDoS, dan pengumpulan malware di honeypot jaringan. Kemudian menunjukkan hasil eksperimen di mana honeypot diatur secara dinamis oleh SOAR Engine, mendeteksi serangan, dan melibatkan penyerang untuk waktu yang lebih lama daripada honeypot statis [3].



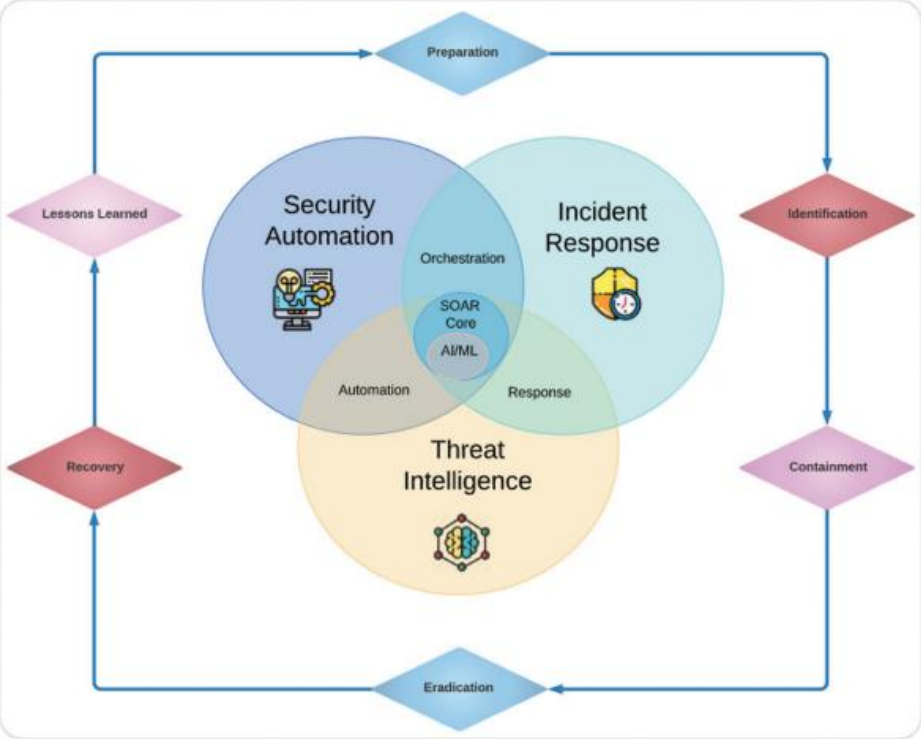

**Gambar 2 Arsitektur Mesin SOAR**

Selain pada penelitian [3], penelitian [4] juga membahas tentang Security Orchestration, Automation, and Response (SOAR) berbasis AI yang mengintegrasikan intelijen ancaman, penjagaan privasi, dan kemampuan Security Information and Event Management (SIEM). Dengan menggunakan TPOT multi honeypot berbasis open source dan pertahanan garis depan seperti firewall dan Intrusion Detection System untuk menganalisis pola serangan dan memberikan masukan ke sistem AI. Sistem yang diusulkan meliputi Automated Standardisation and Privacy Preservation Engine dan Suricata Network Threat Detection Engine. Automated Standardisation and Privacy Preservation Engine, bertanggung jawab untuk mengubah data intelijen ancaman ke dalam format yang terstandardisasi dan menjaga privasi sebelum data tersebut diberikan ke SIEM. Mesin ini lebih berfokus pada pemrosesan dan pengorganisasian data intelijen ancaman. Spiderfoot berperan dalam mengumpulkan data intelijen ancaman yang diperlukan untuk analisis serangan. Jika ancaman baru tidak tersedia di repositori, data ini akan dikumpulkan dari intelijen ancaman opensource menggunakan Spiderfoot. Sementara itu, Suricata Network Threat Detection Engine adalah sistem yang digunakan untuk mendeteksi ancaman jaringan seperti serangan dan aktivitas yang mencurigakan. Mesin ini berfokus pada analisis log dan muatan yang digunakan oleh penyerang. Gambar 3 adalah Alur Kerja Sistem Keamanan, Orkestrasi, Otomasi, dan Respon berbasis AI yang diusulkan.




**Gambar 3 Alur Kerja Sistem Keamanan, Orkestrasi, Otomasi, dan Respons berbasis AI**

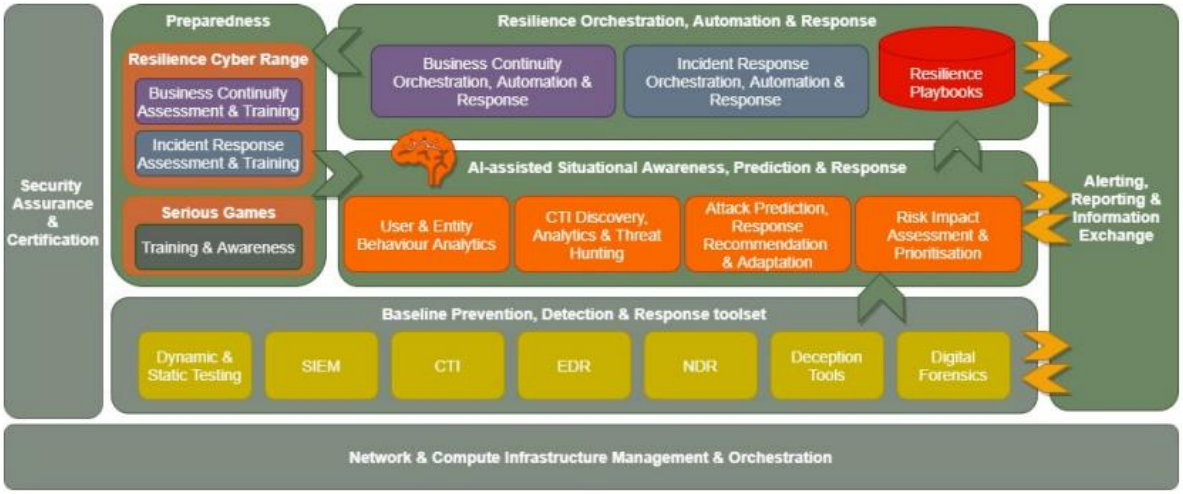
Program keamanan proaktif membutuhkan intelijen ancaman yang berkorelasi dengan baik untuk menemukan pola serangan, potensi kerentanan, dan risiko yang sedang berlangsung pada organisasi. Umumnya, korelasi ini harus diotomatisasi dan dapat memberikan informasi apakah insiden yang sedang berlangsung memiliki faktor yang sama dengan insiden sebelumnya. Memanfaatkan AI/ML dalam orkestrasi, otomatisasi, respons insiden, dan kemampuan intelijen ancaman, seperti yang digambarkan pada gambar 4, merupakan komponen penting lainnya dari solusi SOAR kontemporer dan masa depan [5]. Ada dua kerangka kerja respons insiden yang terutama digunakan di industri, kerangka kerja NIST [14] dan kerangka kerja SANS [7]. Pada gambar tersebut, sistem SOAR menggunakan kerangka kerja SANS dalam proses respons insiden. Fase-fase kerangka kerja SANS PICERL terdiri dari Perencanaan, Identifikasi, Penahanan, Pemberantasan, Pemulihan, dan Pelajaran yang Dipetik. Namun, kerangka kerja SANS PICERL dalam penelitian ini berfokus pada Fase Identifikasi, Penahanan, Pemberantasan, dan Pemulihan (ICER). Hal ini dilakukan karena sumber daya yang tersedia tidak membahas bagaimana platform tersebut mendukung fase perencanaan dan pembelajaran.




**Gambar 4 Sistem SOAR dengan kerangka kerja respons insiden SANS PICERL**

Dalam konteks keamanan, PHOENI2X Cyber Resilience Framework (CRF) dirancang untuk menyediakan kemampuan orkestrasi, otomatisasi, dan respons yang didukung oleh kecerdasan buatan (AI). Pusat keamanan PHOENI2X (Pusat Ketahanan Siber) akan berfungsi sebagai pusat operasi keamanan yang mengintegrasikan kecerdasan buatan untuk meningkatkan pemahaman situasional, prediksi, pencegahan, deteksi, dan respons terhadap ancaman keamanan. Dengan menggunakan teknologi kecerdasan buatan seperti User and Entity Behaviour Analytics (UEBA), PHOENI2X menstandarisasi perilaku pengguna dan entitas serta mengidentifikasi perubahan yang mencurigakan sebagai peringatan dini. Selain itu, dengan menggunakan teknologi grafik pengetahuan, PHOENI2X memungkinkan analisis dan penelusuran ancaman, menghubungkan dan mengkorelasikan data yang heterogen, dan menggunakan pemikiran untuk menemukan informasi baru secara real-time. PHOENI2X juga menggabungkan mekanisme otomatisasi dan orkestrasi yang dikenal sebagai Resilience Playbooks (RP). Organisasi dapat menggunakan RP untuk mengotomatiskan pelaksanaan tindakan, melacak kemajuan, dan mengevaluasi efektivitas RP. RP mencakup proses pemulihan, respons insiden, dan kelangsungan bisnis Dalam kerangka kerja Kerangka Kerja Ketahanan Siber (CRF), PHOENI2X menggabungkan kecerdasan buatan,

orkestrasi keamanan, otomatisasi, dan respons (SOAR) untuk meningkatkan pemahaman situasional, prediksi, pencegahan, deteksi, dan respons terhadap ancaman keamanan seperti yang ditunjukkan pada gambar 5 [6].




**Gambar 5 Arsitektur Konseptual PHOENI2X**

## 2.3 Kemampuan deteksi

Deteksi HTTP IDS, Botnet, dan DDoS sebagai bagian dari Mesin SOAR. Berikut kemampuan deteksi pada mesin SOAR [3], yaitu:

1. HTTP IDS (Sistem Deteksi Intrusi)

   Mengklasifikasikan tiga jenis serangan HTTP, yaitu XSS (Cross-Site Scripting), SQLi (SQL Injection), dan OSC (Operating System Command Injection). Menggunakan model pembelajaran mesin yang dilatih pada Set Data ECML/PKDD 2007 dan Set Data HTTP CSIC Torpeda 2012. Sehingga memberikan deteksi akurat atas permintaan serangan dan permintaan tidak berbahaya. Mencapai akurasi, presisi, recall, dan F-score yang tinggi.

2. Deteksi Botnet

   Mengklasifikasikan lalu lintas jaringan sebagai botnet atau lalu lintas biasa. Menggunakan model pembelajaran mesin yang dilatih pada kumpulan data CTU-13, yang menangkap lalu lintas botnet yang dicampur dengan lalu lintas reguler. Sehingga memberikan akurasi, presisi, recall, dan F-score yang tinggi serta mampu mengungguli metode deteksi botnet yang ada dalam hal akurasi.

3. Deteksi DDoS

   Mengklasifikasikan setiap paket sebagai paket DDoS atau paket biasa dengan mengekstrak fitur seperti protokol yang digunakan, port sumber, port tujuan, dan panjang paket. Kemudian mendeteksi paket DDoS berdasarkan keberadaan protokol serangan tertentu dan port yang ditargetkan. Selanjutnya memberikan deteksi serangan DDoS yang akurat. Secara keseluruhan, modul deteksi di SOAR Engine menunjukkan akurasi dan efektivitas tinggi dalam mengidentifikasi dan mengklasifikasikan berbagai jenis serangan, termasuk serangan HTTP, lalu lintas botnet, dan serangan DDoS.

Selain dari tiga deteksi yang disebutkan sebelumnya, terdapat beberapa kemampuan deteksi lainnya yang digunakan untuk mendeteksi ancaman keamanan termasuk analisis perilaku, analisis log, analisis malware, dan analisis intelijen ancaman. Pembelajaran mesin dapat dilibatkan untuk mengidentifikasi pola dan perilaku yang mencurigakan. Selain itu, teknik pembelajaran

mendalam (deep learning) dapat digunakan untuk deteksi intrusi. Dalam hal ini, jaringan saraf mendalam digunakan untuk mengklasifikasikan data dan mengidentifikasi ancaman keamanan. Menggabungkan antara teknik deteksi ancaman dengan teknik pengolahan bahasa alami (natural language processing) untuk mengekstraksi informasi ancaman dari sumber-sumber tak terstruktur [5].

Pada penelitian [4], sistem SOAR tersebut dilengkapi dengan mesin pembelajaran berbasis jaringan saraf tiruan (neural networks) yang dilatih menggunakan data insiden yang disimpan dalam big data. Sistem ini mampu menganalisis data secara real-time dan melakukan deteksi ancaman dengan cepat. Sistem ini terdiri dari tiga fase utama, antara lain: Pra-pemrosesan Data, Mesin Pembelajaran Berbasis Jaringan Saraf Tiruan, dan Mesin Deteksi Real-Time. Pada fase pertama, data mentah disiapkan untuk dimasukkan ke dalam tiga model pembelajaran mendalam (deep learning). Hal ini dilakukan melalui agregasi data, dekomposisi, normalisasi Term Frequency-Inverse Document Frequency (TF-IDF), dan pembuatan profil acara dari vektor acara. Selanjutnya, sistem menggunakan SIEM (Security Information and Event Management) untuk mengumpulkan semua Informasi Ancaman yang diperoleh tentang peringatan (alert). SIEM akan menggabungkan semua informasi ini dan menganalisisnya untuk mencari pola tersembunyi. Jika aktivitas mencurigakan terdeteksi, SIEM akan menghasilkan peringatan kepada agen AI. Ketika serangan terjadi, SIEM akan mencari informasi terkait dalam repositori untuk mendapatkan informasi rinci yang diperlukan. Hal ini membantu AI dalam mengatasi serangan dengan lebih efisien. Informasi yang terkumpul tentang peringatan akan digunakan oleh AI untuk membuat keputusan apakah peringatan tersebut benar positif atau salah positif. Jika peringatan salah positif, informasi terkait akan disimpan dalam Repositori Intelijen Ancaman untuk tujuan masa depan. Namun, jika peringatan benar positif, laporan Indikator Kompromi, bukti tentang serangan, tingkat serangan, dan informasi lainnya tentang serangan akan ditampilkan kepada analis keamanan. Selain itu, panduan tindakan (playbooks, runbooks, dll) yang ada untuk ancaman tersebut juga akan digunakan untuk mempercepat proses respons. Kemampuan deteksi dalam penelitian ini didukung oleh penggunaan teknologi AI, mesin pembelajaran berbasis jaringan saraf tiruan, dan analisis real-time. Sistem ini mampu mengumpulkan dan menganalisis data ancaman secara otomatis, mengidentifikasi pola tersembunyi, dan menghasilkan peringatan kepada agen AI. Hal ini membantu dalam mengurangi beban kerja profesional keamanan dan meningkatkan efisiensi dalam menghadapi serangan siber.

Prediksi serangan yang dibantu AI menggunakan pendekatan berbasis pembelajaran mendalam, seperti Generative Adversarial Networks (GANs) dan teknik Transfer Learning, digunakan untuk memprediksi dan mendeteksi perubahan dinamis dalam ancaman. Model bahasa terlatih digunakan untuk memprediksi eksploitasi kerentanan sistem. AI dan teknik penambangan data juga digunakan untuk memprediksi insiden keamanan siber dan menghasilkan tindakan pemeliharaan sistem untuk mencegah serangan. Analisis perilaku pengguna dan entitas dapat digunakan untuk mendeteksi serangan jaringan secara real-time. Ini berfokus pada analisis pola perilaku pengguna dan mengidentifikasi anomali yang mungkin mengindikasikan serangan orang dalam atau aktivitas jahat lainnya. Selanjutnya deteksi serangan rekayasa sosial bisa digunakan untuk meningkatkan kesadaran dan melatih analis keamanan untuk mengidentifikasi dan mempertahankan diri dari serangan rekayasa sosial. Program-program ini mensimulasikan skenario dunia nyata dan memberikan pelatihan langsung untuk meningkatkan kesiapsiagaan [6].

### 2.4 Performa model AI

Performa model AI di SOAR Engine dengan model-model yang diimplementasikan menunjukkan akurasi yang lebih baik dalam beberapa kasus. Dalam kasus deteksi HTTP IDS dengan fitur XSS, model Decision Tree di SOAR Engine mencapai akurasi 98,81%, sedangkan makalah referensi memiliki akurasi sebesar 99,27%. Pada model SVM di SOAR Engine untuk fitur SQLi mencapai akurasi 98,12%, sedangkan makalah referensi memiliki akurasi sebesar 95,57%. Demikian pula, model LR di SOAR Engine untuk fitur OSCi mencapai akurasi 98,44%, sedangkan makalah

referensi memiliki akurasi sebesar 97,85%. Dalam kasus deteksi Botnet memberikan nilai akurasi sebesar 99,95% daripada metode yang sudah ada [8] sebesar 99,89%. Selanjutnya dalam kasus deteksi DDoS memberikan nilai akurasi sebesar 99,94% daripada metode yang sudah ada [10] sebesar 97,86%. Hasil ini menunjukkan bahwa model AI yang diimplementasikan di SOAR Engine berkinerja kompetitif dan dalam beberapa kasus bahkan mengungguli tolok ukur yang disebutkan dalam makalah tersebut [3].

Pada penelitian [4], performa model AI tidak secara spesifik dibahas dalam konteks yang diberikan. Namun, penelitian ini mengusulkan penggunaan teknologi AI untuk mengurangi beban pekerjaan profesional keamanan, seperti menganalisis jutaan log dengan cepat, menjalankan prosedur yang diperlukan, dan menargetkan area di mana intervensi manusia diperlukan. Selain itu, penelitian ini juga bertujuan untuk mengotomatisasi pengumpulan Threat Intelligence dan menerjemahkan Threat Intelligence dalam berbagai bahasa. Threat Intelligence digunakan untuk mengumpulkan informasi tentang ancaman yang telah terjadi sebelumnya dan digunakan untuk mengidentifikasi dan mencegah serangan yang serupa di masa depan. Repository Threat Intelligence menyimpan informasi tentang ancaman yang diketahui, dan jika ancaman baru terdeteksi, data tersebut akan dikumpulkan dari sumber ancaman terbuka menggunakan alat open source bernama Spiderfoot. Selain itu, ada juga penggunaan Threat Intelligence multibahasa yang diterjemahkan menggunakan teknologi NLP berbasis terjemahan. Informasi tentang ancaman yang ditemukan akan digunakan untuk membuat laporan Indicators of Compromise, bukti tentang serangan, tingkat serangan, dan informasi lainnya yang akan ditunjukkan kepada analis keamanan. Data terkait ancaman ini juga akan dimasukkan ke dalam repository Threat Intelligence untuk digunakan di masa depan.

Sama hal nya dengan penelitian [4], performa model AI tidak secara spesifik dibahas pada penelitian [5]. Namun, penelitian ini menjelaskan bagaimana AI/ML dapat berperan sebagai pengganda daya yang memberdayakan analis SOC (Security Operations Centre) dengan lebih lanjut. Dengan menggunakan AI/ML, analis SOC dapat meningkatkan efektivitas mereka dalam mendeteksi, mencegah, dan merespons serangan keamanan. AI/ML dapat membantu mengatasi kompleksitas dan volume data yang tinggi dalam lingkungan keamanan yang terus berkembang, sehingga memungkinkan analis untuk bekerja dengan lebih efisien dan efektif. Ada beberapa cara AI/ML dapat meningkatkan efektivitas analis SO, yaitu:

1. Deteksi ancaman yang lebih baik

   AI/ML dapat digunakan untuk menganalisis data keamanan secara real-time dan mengidentifikasi pola dan perilaku yang mencurigakan. Dengan menggunakan algoritma pembelajaran mesin, AI dapat mempelajari pola serangan yang kompleks dan mendeteksi ancaman yang sebelumnya tidak terdeteksi. Hal ini memungkinkan analis SOC untuk merespons lebih cepat terhadap ancaman yang muncul.

2. Automasi tugas rutin

   Dengan menggunakan AI/ML, tugas-tugas rutin dalam operasi keamanan dapat diotomatisasi. Misalnya, AI dapat mengotomatisasi analisis log, pemantauan jaringan, dan pemulihan sistem setelah serangan. Hal ini memungkinkan analis SOC untuk fokus pada tugas-tugas yang lebih kompleks dan membutuhkan pemikiran manusia.

3. Analisis data yang lebih cepat dan akurat

   AI/ML dapat membantu analis SOC dalam menganalisis dan menginterpretasikan data keamanan dengan lebih cepat dan akurat. Algoritma pembelajaran mesin dapat mengidentifikasi pola dan tren yang tidak terlihat oleh manusia, sehingga memungkinkan analis untuk mengambil keputusan yang lebih baik dan lebih cepat.

4. Peningkatan respons terhadap serangan

   Dengan menggunakan AI/ML, analis SOC dapat merespons serangan dengan lebih efektif. AI dapat memberikan rekomendasi tindakan yang tepat berdasarkan analisis data dan pengetahuan yang telah dipelajari sebelumnya. Hal ini memungkinkan analis untuk mengambil tindakan yang lebih cepat dan lebih efektif dalam menangani serangan.

5. Pengurangan beban kerja

   Dengan otomatisasi tugas-tugas rutin dan analisis data yang lebih cepat, AI/ML dapat mengurangi beban kerja analis SOC. Hal ini memungkinkan mereka untuk fokus pada tugas-tugas yang membutuhkan pemikiran kritis dan pemecahan masalah yang kompleks.

Sebuah studi mengungkapkan bahwa organisasi meningkatkan laju adopsi AI/ML dalam keamanan siber dan secara keseluruhan, hampir tiga perempat perusahaan (73%) yang disurvei mengatakan mereka sedang menguji kasus penggunaan AI/ ML untuk keamanan siber. Survei tersebut juga mengungkapkan bahwa 28% menggunakan produk keamanan yang tertanam AI/ML, dan 30% menggunakan algoritme AI/ML yang dipatenkan. Sisanya, 42%, saat ini menggunakan (atau berencana menggunakannya pada tahun depan) baik solusi eksklusif maupun produk tertanam [9].

Peran model AI dalam Kerangka Ketahanan Siber PHOENI2X adalah untuk menyediakan kemampuan orkestrasi, otomatisasi, dan respons yang dibantu AI. Model AI digunakan untuk meningkatkan kesadaran situasional dengan memprediksi, mencegah, mendeteksi, dan merespons serangan dunia maya. Ini juga digunakan untuk prediksi serangan, kategorisasi, dan respons. Model AI dilatih menggunakan teknik pembelajaran mesin, seperti pembelajaran mendalam dan pembelajaran transfer, untuk menganalisis beragam sumber data, termasuk teks forum peretas, scraping web permukaan atau web gelap, serangan peristiwa dunia maya, dan saluran media sosial. Ini digunakan untuk analisis sentimen, kontekstualisasi data yang diekstraksi, dan identifikasi potensi upaya persuasi dalam serangan rekayasa sosial. Model AI juga digunakan untuk klasifikasi, regresi, dan pemodelan statistik dalam kasus penggunaan Analisis Perilaku Pengguna dan Entitas (UEBA), yang memungkinkan deteksi aktivitas anomali dan ancaman orang dalam. Secara keseluruhan, model AI memainkan peran penting dalam mengotomatisasi dan mengoptimalkan proses ketahanan siber, meningkatkan waktu respons, dan meminimalkan dampak serangan siber.

## 3. KESIMPULAN

Integrasi kecerdasan buatan (AI) dalam Security Orchestration, Automation, and Response (SOAR) menjanjikan revolusi dalam operasi keamanan dengan meningkatkan deteksi ancaman, mengotomatiskan tugas yang berulang, dan memberdayakan tim keamanan. Adopsi teknologi SOAR yang didukung AI dapat membantu organisasi meningkatkan ketahanan mereka terhadap serangan siber. Keamanan jaringan IT/OT organisasi dapat ditingkatkan dengan teknologi penipuan dan honeypot dengan memberi penyerang perasaan kerentanan palsu dan mengumpulkan informasi intelijen tentang metode ancaman.

Kemampuan deteksi pada mesin SOAR mencakup deteksi serangan HTTP IDS, deteksi botnet, dan deteksi DDoS dengan menggunakan model pembelajaran mesin yang dilatih pada berbagai jenis data. Selain itu, terdapat juga kemampuan deteksi lainnya seperti analisis perilaku, analisis log, analisis malware, dan analisis intelijen ancaman. Sistem SOAR dilengkapi dengan mesin pembelajaran berbasis jaringan saraf tiruan yang mampu menganalisis data secara real-time dan melakukan deteksi ancaman dengan cepat. Penggunaan teknologi AI dan analisis real-time membantu dalam mengurangi beban kerja profesional keamanan dan meningkatkan efisiensi dalam menghadapi serangan siber.

Model AI yang diimplementasikan di SOAR Engine memiliki performa yang kompetitif dan bahkan mengungguli tolak ukur yang disebutkan dalam makalah referensi. Selain itu, penggunaan teknologi AI/ML dalam keamanan siber dapat meningkatkan efektivitas analis SOC dalam mendeteksi, mencegah, dan merespons serangan keamanan, serta mengurangi beban kerja mereka.

## 4. KETERBATASAN PENELITIAN DAN PEKERJAAN MASA DEPAN

### 4.1 Keterbatasan Penelitian

Mengatasi tantangan keamanan siber, termasuk deteksi penyerang di dalam jaringan internal, diperlukan orkestrasi dinamis dan teknologi penipuan yang spesifik bagi organisasi. Orkestrasi dinamis dalam mengatur honeypot secara dinamis untuk memastikan deteksi yang tertunda dan mengotomatiskan penyebaran sesuai dengan kepentingan penyerang. Teknologi Penipuan yang spesifik bagi organisasi diperlukan, karena umpan intelijen ancaman sumber terbuka tidak cukup untuk menyediakan intelijen ancaman spesifik organisasi. Mendeteksi penyerang di dalam jaringan internal organisasi merupakan hal yang menantang, terutama karena adanya penyerang orang dalam yang terlatih dan dapat membedakan honeypot dari sistem yang sebenarnya. Keterbatasan ini menunjukkan perlunya teknologi penipuan yang lebih canggih dan disesuaikan untuk mengatasi tantangan yang terus berkembang dalam keamanan siber serta keterbatasan dalam cakupan literatur dan dukungan bahasa pada sistem terjemahan ancaman multibahasa.
Keterbatasan lainnya menunjukkan kurangnya perbandingan langsung antara berbagai model pembelajaran mesin yang dibangun untuk SOAR, serta kurangnya eksperimen empiris untuk mendukung efektivitas dan efisiensi model-model ini dalam lingkungan keamanan yang berbeda. Sehingga memerlukan jumlah data yang besar terkait insiden yang sama, yang dapat mempengaruhi kinerja model pada data baru. Sebagian besar data yang dikumpulkan juga cenderung serupa satu sama lain, yang dapat mengurangi kinerja model pada data baru dan terdapat keterbatasan dalam mencegah serangan zero-day exploit, drive-by attacks, dan eavesdropping attacks.

### 4.2 Pekerjaan Masa Depan

Beberapa pekerjaan masa depan dari kecerdasan buatan untuk security orchestration, automation and response, yaitu:

1. Eksplorasi lebih lanjut tentang kinerja model AI dalam konteks spesifik SOAR, untuk memahami bagaimana AI dapat secara efektif mengurangi beban kerja profesional keamanan dan mengotomatiskan tugas-tugas seperti menganalisis log dalam jumlah besar, menjalankan prosedur yang diperlukan, dan menunjukkan area yang membutuhkan intervensi manusia.
2. Investigasi terhadap otomatisasi pengumpulan dan penerjemahan Intelijen Ancaman, memanfaatkan AI untuk mengumpulkan informasi tentang ancaman yang diketahui, serta menerjemahkan Intelijen Ancaman ke dalam berbagai bahasa. Penelitian ini dapat berfokus pada peningkatan efisiensi dan akurasi pengumpulan dan penerjemahan Intelijen Ancaman, yang sangat penting untuk mengidentifikasi dan mencegah serangan siber serupa di masa depan.
3. Eksplorasi integrasi teknik AI dan Machine Learning (ML) untuk mendeteksi ancaman siber tertentu, seperti serangan botnet dan serangan Distributed Denial of Service (DDoS). Hal ini dapat melibatkan pengembangan dan penyempurnaan algoritme berbasis AI untuk mendeteksi secara tepat waktu dan akurat ancaman siber yang terus berkembang.
4. Penelitian tentang pengembangan sistem berbasis AI untuk menghasilkan laporan komprehensif tentang Indikator Kompromi (IoC), bukti serangan, dan tingkat keparahan. Hal ini dapat melibatkan penggunaan AI untuk mengumpulkan dan menyajikan informasi terkait ancaman yang relevan kepada analis keamanan, sehingga meningkatkan proses pengambilan keputusan dalam menanggapi insiden.

## 5. DAFTAR PUSTAKA

[1] J. Johnson, C. B. Jones, A. Chavez, and S. Hossain-McKenzie, "SOAR4DER: Security Orchestration, Automation, and Response for Distributed Energy Resources." Power Systems Cybersecurity, pp. 387-411, Feb. 2023, doi: 10.1007/978-3-031-20360-2_16.

[2] M. Lee, J. Jang-Jaccard, and J. Kwak, "Novel Architecture of Security Orchestration, Automation and Response in 營 nternet of Blended Environment." Computers, Materials & Continua, vol. 73, no. 1, pp. 199-223, Mar. 2022, doi: 10.32604/cmc.2022.028495.

[3] U. Bartwal, S. Mukhopadhyay, R. Negi, and S. Shukla, "Security Orchestration, Automation, and Response Engine for Deployment of Behavioural Honeypots." 2022 IEEE Conference on Dependable and Secure Computing (DSC), Sep. 2022, doi: 10.1109/dsc54232.2022.9888808.

[4] R. Vast, S. Sawant, A. Thorbole, and V. Badgujar, "Artificial Intelligence based Security Orchestration, Automation and Response System." 2021 6th International Conference for Convergence in Technology (I2CT), May 2021, doi: 10.1109/i2ct51068.2021.9418109.

[5] J. Kinyua and L. Awuah, "AI/ML in Security Orchestration, Automation and Response: Future Research Directions." Intelligent Automation & Soft Computing, vol. 28, no. 2, pp. 527-545, Apr. 2021, doi: 10.32604/iasc.2021.016240.

[6] K. Fysarakis, "PHOENI2X – A European Cyber Resilience Framework With Artificial-Intelligence-Assisted Orchestration, Automation & Response Capabilities for Business Continuity and Recovery, Incident Response, and Information Exchange." 2023 IEEE International Conference on Cyber Security and Resilience (CSR), Aug. 2023, doi: 10.1109/csr57506.2023.10224995.

[7] SANS. "Incident Response Steps and Frameworks for SANS and NIST." 2020. https://cybersecurity.att.com/blogs/security-essentials/incident-response-steps-comparison-guide (accessed: Dec. 31, 2023).

[8] M. Alshamkhany, W. Alshamkhany, M. Mansour, M. Khan, S. Dhou, and F. Aloul, "Botnet Attack Detection using Machine Learning." 2020 14th International Conference on Innovations in Information Technology (IIT), pp. 203-208, Dec. 2020, doi: 10.1109/iit50501.2020.9299061.

[9] Capgemini Research Institute. "Reinventing cybersecurity with artificial intelligence, the new frontier in digital security." 2019. https://www.capgemini.com/wp-content/uploads/2019/07/AI-in-Cybersecurity_Report_20190711_V06.pdf (accessed: Jan. 18, 2024).

[10] S. Sambangi and L. Gondi, "A machine learning approach for ddos (distributed denial of service) attack detection using multiple linear regression", Proceedings, vol. 63, no. 1, Dec. 2020, doi: 10.3390/proceedings2020063051.

[11] C. Islam, M. A. Babar, and S. Nepal, "A Multi-Vocal Review of Security Orchestration." ACM Computing Surveys, vol. 52, no. 2, pp. 1-45, Apr. 2019, doi: 10.1145/3305268.

[12] Y. Zheng, A. Pal, S. Abuadbba, S. R. Pokhrel, S. Nepal, and H. Janicke, "Towards IoT Security Automation and Orchestration." 2020 Second IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA), Oct. 2020, doi: 10.1109/tps-isa50397.2020.00018.

[13] M. Hafiz, and B. Soewito, "Information Security Systems Design Using SIEM, SOAR and Honeypot." Jurnal Pendidikan Tambusai, vol. 6, no. 2, pp. 15527-15541, Aug. 2022, doi: 10.31004/jptam.v6i2.4850.

[14] P. Cichonski, T. Millar, T. Grance, and K. Scarfone, "Computer Security Incident Handling Guide : Recommendations of the National Institute of Standards and Technology." Aug. 2012, doi: 10.6028/nist.sp.800-61r2.

[15] K. K. Watson. "Orchestration of Information Technology (IT) Automation Frameworks." Apr.2021.https://www.cisa.gov/sites/default/files/publications/Orchestration%2520of%25

20Information%2520Technology%2520Automation%2520Frameworks_508c.pdf (accessed: Dec. 31, 2023).

[16] I. P. E. D. Nugraha, "A Review on the Role of Modern SOC in Cybersecurity Operations." International Journal of Current Science Research and Review, vol. 4, no. 5, May 2021, doi: 10.47191/ijcsrr/v4-i5-13.