Tugas Review Paper individu

Toward Intelligent Cyber Defense: A Comprehensive Study of SOAR Technologies for AI-Based DDoS Detection

Nama : Muhammad Sirojul Fuad

NIM : 1304212094

Abstrak

Jurnal Toward Intelligent Cyber Defense: A Comprehensive Study of SOAR Technologies for AI-Based DDoS Detection menyajikan tinjauan mengenai Security Orchestration, Automation, and Response (SOAR) dan peran transformatif integrasi Artificial Intelligence (AI) dan Machine Learning (ML) dalam keamanan siber modern. SOAR telah menjadi komponen vital dalam operasi keamanan siber, terutama untuk mengatasi ancaman Distributed Denial of Service (DDoS). Penelitian ini menganalisis arsitektur SOAR, komponen intinya, dan mengevaluasi platform komersial terkemuka seperti Fortinet FortiSOAR, IBM QRadar SOAR, and Palo Alto Cortex XSOAR. Jurnal ini fokus penekanannya pada bagaimana model cerdas dapat meningkatkan alur kerja SOAR, memungkinkan identifikasi ancaman yang lebih cepat dan lebih akurat melalui deteksi anomali yang cerdas dan korelasi peringatan otomatis. Namun terdapat tantangan dalam implementasi solusi SOAR berbasis AI yang meliputi pengelolaan false positives, isu kualitas dan ketidakseimbangan data dan interoperabilitas dengan alat keamanan yang ada, dan persyaratan kepatuhan peraturan. Temuan penelitian ini menyimpulkan bahwa untuk mencapai pertahanan siber yang tangguh, adaptif, dan terukur, organisasi harus mengadopsi pendekatan yang seimbang yang menggabungkan otomatisasi tingkat tinggi, dukungan keputusan berbasis AI, dan keahlian serta pengawasan manusia.

Pendahuluan dan Konteks Penelitian Jurnal

Latar Belakang Ancaman Siber

Ancaman serangan siber yang semakin meningkat, terutama serangan Distributed Denial-of-Service (DDoS), menimbulkan risiko signifikan bagi organisasi di seluruh dunia. Serangan-serangan ini berupaya membanjiri sistem dan layanan target, yang menyebabkan gangguan layanan yang parah, kerugian finansial, dan merusak reputasi organisasi maupun pihak yang terkena serangan tersebut. Konsekuensinya sangat kritis dalam sektor bernilai tinggi dan sensitif, termasuk layanan kesehatan, keuangan, dan infrastruktur kritis, di mana kegagalan sistem dapat memiliki dampak yang sangat mengganggu atau bahkan mengancam jiwa. Penyerang kini semakin sering memanfaatkan botnet, perangkat Internet of Things (IoT) yang rentan, dan strategi serangan multi-vektor untuk melancarkan serangan yang kompleks membuat mekanisme pertahanan tradisional semakin dianggap tidak memadai. Dengan demikian Security Orchestration, Automation, and Response (SOAR) muncul sebagai respon langsung terhadap otomatisasi serangan ini

Motivasi Penelitian Jurnal

Jurnal ini dimotivasi atas kebutuhan mendesak untuk mengatasi tantangan yang dihadapi Security Orchestration, Automation, and Response (SOAR) modern dalam mengelola volume peringatan dan kompleksitas ancaman yang tinggi. SOAR dipandang sebagai solusi untuk meningkatkan efisiensi operasional, merampingkan respons insiden, dan mengurangi ketergantungan pada intervensi manual dan meningkatkan konsistensi dalam operasi keamanan

Tujuan dan ruang lingkup jurnal

Tujuan utama penelitian ini adalah untuk menyajikan studi komprehensif tentang teknologi SOAR, yang meliputi pemeriksaan arsitekturnya, komponen inti, dan relevansi yang semakin besar dalam ekosistem keamanan siber dengan ruang lingkup yang mencakup analisis terhadapa platform SOAR, termasuk Fortinet FortiSOAR, IBM QRadar SOAR, and Palo Alto Cortex XSOAR, dan menganalisis bagaimanai integrasi kecerdasan buatan (XAI) memperkuat deteksi dan respon terhadap serangan DDoS. Dengan mengatasi tantangan terkait kualitas data, interoperabilitas, kepatuhan, dan risiko otomatisasi, serta perlunya pendekatan yang seimbang yang menggabungkan otomatisasi dengan keahlian manusia.

Arsitektur SOAR dan Perbandingan dengan SIEM

Definisi SOAR

SOAR adalah singkatan dari Security Orchestration, Automation, and Response, sebuah istilah yang diciptakan oleh Gartner pada tahun 2015. Teknologi ini menggabungkan kemampuan manajemen intelijen ancaman, respons insiden, orkestrasi, dan otomatisasi. Solusi SOAR dirancang untuk mengelola alur kerja, menyimpan data insiden, memanfaatkan intelijen dengan lebih baik.

Definisi SIEM

Security Information and Event Management (SIEM) adalah solusi keamanan yangmembantu organisasi mendeteksi ancaman, mengotomatisasi tanggapan insiden, dan memastikan kepatuhan dengan mengumpulkan dan menganalisis data keamanan secara real-time. Awalnya, SIEM hanya menggabungkan Security Information Management (SIM) dan Security Event Management (SEM) tanpa campur tangan kecerdasan buatan (AI). Seiring waktu, SIEM telah berkembang untuk mengintegrasikan AI, machine learning, dan User and Entity Behavior Analytics (UEBA) untuk deteksi ancaman yang lebih canggih. Fungsi utama SIEM meliputi manajemen log, korelasi peristiwa, pemantauan insiden, dan pelaporan kepatuhan. Hal ini terjadi setelah SIEM mengumpulkan data dari berbagai infrastruktur. Akhirnya, SIEM membantu mematuhi standar seperti PCI-DSS dan GDPR melalui pelaporan otomatis.

Perbedaan Fungsionalitas SOAR dan SIEM

Solusi SOAR berfokus pada otomatisasi dan penyederhanaan operasi keamanan. SOAR mengurangi beban kerja manual melalui otomatisasi. Fungsi ini membuat SOAR menjadi alat untuk meningkatkan efisiensi operasional dan mempercepat manajemen insiden keamanan, daripada berfokus utama pada deteksi dan kepatuhan. Sistem SIEM berfokus pada pengumpulan data komprehensif, analisis, dan pembangkitan peringatan (mengumpulkan dan mengkorelasikan log dari berbagai sumber, pemantauan real-time, dan pembangkitan peringatan berdasarkan aturan dan templat yang telah ditentukan sebelumnya), deteksi ancaman, dan pelaporan kepatuhan. Hal ini memerlukan intervensi manual yang lebih besar untuk penyelidikan dan tanggapan

Table perbandingan SOAR dan SIEM:

Fitur	SOAR	SIEM
Tujuan	Mengotomasi tugas keamanan	Mengumpulkan dan menganalisis event keamanan
Otomatisasi	Tingkat otomasi tinggi menggunakan playbooks	Otomasi terbatas memerlukan analisis manual
Integrasi	Berintegrasi dengan berbagai alat keamanan	Memusatkan data log dari berbagai sumber
Intelejen	AI dan ML untuk respon cerdas	Analisis dan pelaporan dasar

Playbooks

SOAR playbook adalah kumpulan alat dan proses yang terorganisir untuk merespon insiden keamanan. dengan mengoordinasikan alat keamanan, playbook ini mengintegrasikan orkestrasi, otomatisasi, dan respon. Playbook menggunakan kondisi untuk memicu aktivitas seperti menjalankan skrip, menambahkan tugas, memperbarui data, atau memulai tindakan eksternal.

Menggunakan desainer playbook, alur kerja dapat dibuat melalui antarmuka visual, sementara aturan dan alur kerja memberikan fleksibilitas untuk menangani skenario kompleks.

Sebuah vignette dalam platform SOAR adalah skenario singkat yang menggambarkan jenis insiden keamanan tertentu. Playbook adalah alur kerja otomatis untuk merespons insiden-insiden tersebut. Pemetaan antara keduanya memastikan bahwa ketika sebuah vignette terdeteksi, playbook yang sesuai dipicu, mengotomatisasi tugas seperti penyaringan peringatan, pengendalian, dan pemulihan, mengurangi upaya manual dan waktu respons.

Respon Social Engineering dalam SOAR

Social Engineering adalah teknik manipulasi yang memanfaatkan kesalahan manusia, berfokus pada cara orang berpikir dan bertindak. Teknik ini dimanfaatkan untuk memperoleh informasi pribadi atau berharga, serta memanfaatkan ketidaktahuan pengguna. Dalam

kejahatan siber, pengguna yang tidak waspada dibujuk untuk mengungkapkan data sensitif, menginstal malware, atau memberikan akses ke sistem yang tidak dimaksudkan untuk diakses. Serangan dapat terjadi secara online, secara langsung, atau melalui interaksi lain.

Tabel teknik Social Engineering:

Teknik	Desktipsi	Kerentanan yang dimanfaatkan
Phishing	Mengirim email palsu	Kepercayaan pada komunikasi email kurangnya kewaspadaan terhadap tanda-tanda penipuan
Pretexting	Membuat skenario palsu untuk mendapatkan akses atau informasi	Kepatuhan terhadap otoritas, rasa urgensi, dan kepercayaan pada cerita yang meyakinkan
Baiting	Menawarkan imbalan atau hadiah untuk memancing korban mengklik link atau memasang malware	Rasa ingin tahu, keinginan mendapat imbalan

Tiga Pilar Fungsional SOAR

1. **Security Orchestration**

   Proses integrasi berbagai alat keamanan yang berbeda seperti firewalls, antivirus, dan platform intelijen ancaman untuk menciptakan layanan keamanan yang terpadu. Tujuan utama orkestrasi adalah memungkinkan operasi keamanan berlangsung tanpa perlu berpindah antar alat yang berbeda

2. **Security Automation**

   Eksekusi tugas-tugas terkait pencapaian keamanan yang terjadi secara otomatis. Tugas-tugas ini mencakup pembuatan tiket insiden, analisis peringatan memperkaya data ancaman, dan analisis log. Otomatisasi ini berfungsi untuk mengurangi upaya manusia dan mempercepat waktu respons

3. **Incident Response**

Berfungsi sebagai unit pusat yang mengumpulkan event dan peringatan dari berbagai sumber masukan. Setelah pengumpulan, insiden diselidiki dan dianalisis untuk menghasilkan respons yang optimal

Platform SOAR Komersial

Fortinet FortiSOAR

FortiSOAR adalah platform SOAR yang digunakan bersama SIEM, UEBA, atau EDR yang membantu tim SOC mencegah serangan dengan mengintegrasikan manajemen insiden dan mengotomatisasi analisis yang mengarah pada penyelidikan dan tanggapan yang efektif. FortiSOAR adalah platform SOAR terkemuka yang digunakan bersama SIEM, UEBA, EDR, atau platform deteksi ancaman lainnya. FortiSOAR membantu tim keamanan IT/OT mencegah serangan dengan mengonsolidasikan manajemen insiden dan mengotomatisasi berbagai aktivitas analis yang diperlukan untuk penyelidikan dan respons ancaman yang efektif.

IBM Security QRadar SOAR

IBM Security QRadar SOAR menawarkan layanan yang dirancang untuk mempercepat proses respons melalui penggunaan playbooks dinamis dan dukungan rekomendasi respons berbasis AI. latform ini juga fokus pada penyederhanaan operasional, termasuk penandaan waktu pada tindakan kritis dan integrasi intelijen ancaman real-time

Palo Alto Networks Cortex XSOAR

Cortex XSOAR dari Palo Alto Networks menawarkan otomatisasi terpadu, manajemen kasus, kolaborasi real-time, dan manajemen intelijen ancaman dalam satu platform Tunggal. Platform ini bertujuan untuk menyederhanakan operasi keamanan, yang secara langsung mempercepat waktu respons, mengurangi beban pada analis, dan meminimalkan tugas manual. Bukti kuantitatif dari keberhasilan implementasi Cortex XSOAR disajikan melalui studi kasus NDIT di North Dakota, yang menggunakan platform tersebut untuk mengotomatisasi proses dan berhasil menghemat kebutuhan sekitar 8-10 analis tambahan. Data ini memberikan argumen yang kuat mengenai nilai SOAR yang diukur dalam optimalisasi modal manusia selain mitigasi risiko

Microsoft Sentinel

Microsoft menggambarkan Microsoft Sentinel sebagai pembaruan untuk Security Operations Centers (SOC) yang mendeteksi dan merespons ancaman paling kompleks, serta menyediakan solusi manajemen informasi dan peristiwa keamanan yang tangguh, semuanya secara proaktif sambil mengurangi biaya hingga 48% dibandingkan dengan solusi SIEM saat ini.

Vectra AI

Integrasi Vectra dan Splunk memudahkan penemuan, penyaringan, penyelidikan, dan tanggapan terhadap insiden keamanan dari dasbor pusat berdasarkan kecerdasan buatan. Integrasi ini diimplementasikan langsung dari Splunkbase.

Peran platform ini ditekankan dalam menghilangkan ambiguitas yang dibuat oleh penyerang akibat banyaknya peringatan yang mereka kirimkan, yang menyembunyikan bahaya sebenarnya di baliknya. Security Operations Centers (SOC) dapat mendeteksi ancaman tersembunyi, menganalisis data secara efektif, dan mengantisipasi serangan penyerang, yang meningkatkan kemampuan mereka untuk bertahan dan mengendalikan.

Cortex XSOAR membantu menyederhanakan operasi keamanan dengan mengintegrasikan otomatisasi, manajemen kasus, kolaborasi real-time, dan manajemen intelijen ancaman.

Splunk

Splunk adalah platform Security Information and Event Management (SIEM) yang populer. Platform ini mengumpulkan log keamanan dari berbagai sumber, mendeteksi anomali, dan memberikan peringatan.

Splunk didasarkan pada filosofi penggunaan AI yang bertanggung jawab, sambil tetap melibatkan partisipasi manusia dalam proses penyelesaian. AI dirancang untuk melengkapi, bukan menggantikan manusia. Splunk menawarkan kepada pelanggan dan mitra kemampuan untuk memperluas model Splunk atau menerapkan model mereka sendiri ke data di seluruh Splunk.

Otomatisasi Respons Email Phishing Menggunakan Splunk SOAR

Skenario ini dipilih karena merupakan skenario umum di mana otomatisasi mengurangi waktu respons. proses ini diasumsikan akan diproses oleh Splunk SOAR. Sebuah laporan

sampai ke Security Operations Centers (SOC), misalnya dari seorang karyawan, tentang email yang mencurigakan. Kini giliran SOC untuk mengotomatiskan investigasi dan respons cepat.

Tahapan – tahapannya:

1. Trigger and Ingestion
   Splunk SOAR menerima laporan email mencurigakan dari sistem email (misalnya Gmail) atau peringatan dari SIEM. Sistem kemudian mengekstrak elemen penting seperti alamat pengirim, subjek, isi pesan, serta lampiran atau tautan yang ada.
2. Automated Analysis
   Email dianalisis menggunakan Natural Language Processing (NLP) dan sumber intelijen ancaman (seperti VirusTotal dan URLhaus) untuk mendeteksi indikasi phishing. Sistem juga memeriksa keaslian domain pengirim dan riwayat interaksinya dengan organisasi
3. Decision and Response
   Berdasarkan hasil analisis, sistem mengklasifikasikan pesan sebagai berbahaya, mencurigakan, atau aman.
   - Jika berbahaya, sistem memblokir domain, menghapus pesan dari semua kotak masuk, dan menonaktifkan tautan
   - Jika mencurigakan, email diisolasi dan diteruskan ke analis manusia
   - Jika aman, tidak ada tindakan lanjut
4. Post-Incident Actions
   Hasil investigasi dimasukkan ke model pembelajaran mesin untuk meningkatkan kemampuan deteksi phishing di masa depan. Proses ini melibatkan supervised learning dan pembaruan playbook otomatis
5. Feedback and Continuous Improvement
   Semua langkah dan hasil dievaluasi untuk menemukan kelemahan, memperbarui model AI, serta membagikan pembelajaran kepada tim intelijen ancaman guna meningkatkan respons di masa mendatang

Keterbatasan Teknologi SOAR-AI yang Ada

Meskipun platform SOAR yang terintegrasi dengan kecerdasan buatan merupakan inovasi yang penting, efektif, dan tak tergantikan bagi organisasi, teknologi ini tetap menghadapi sejumlah tantangan, antara lain:

False Positives

Hasil analisis AI terkadang bisa keliru, dan karena platform SOAR terintegrasi langsung dengan model AI tersebut, aktivitas yang sebenarnya tidak berbahaya dapat diklasifikasikan sebagai ancaman yang harus dihentikan. Hal ini tentu menambah beban kerja bagi para analis keamanan

Data Quality and Bias Issues

Tantangan ini berkaitan dengan data yang digunakan untuk melatih model AI. Data tersebut mungkin sudah usang, tidak lengkap, atau bahkan bias, sehingga menghasilkan keputusan atau deteksi yang juga bias dan tidak akurat

Limited Contextual Awareness

Keputusan berbasis konteks masih menjadi tantangan besar bagi AI dalam sistem SOAR. Kurangnya pemahaman mendalam terhadap proses, pola serangan, atau faktor kontekstual lainnya dapat menyebabkan respons yang tidak efektif, bahkan berpotensi merugikan Over-reliance on Automation

Ketergantungan penuh pada otomatisasi dapat berbahaya dan menimbulkan konsekuensi serius, seperti memblokir lalu lintas yang sah atau meningkatkan insiden yang sebenarnya tidak kritis. Karena itu, meskipun otomatisasi memiliki kekuatan dan efisiensi tinggi, peran manusia tetap penting dan tidak boleh diabaikan dalam proses operasi keamanan Compliance and Legal Challenges Kepatuhan terhadap berbagai undang-undang privasi dan regulasi keamanan yang berlaku bagi sistem respons insiden berbasis AI merupakan tantangan besar dalam menjaga keamanan dan keandalan sistem

Kesimpulan

Penelitian ini berhasil menyajikan studi komprehensif yang mengukuhkan posisi SOAR sebagai keharusan strategis dalam pertahanan siber. OAR menyediakan kerangka kerja arsitektur yang diperlukan (Orchestration, Automation, Respone) untuk menangani ancaman modern seperti DDoS dengan kecepatan dan konsistensi yang mustahil dicapai melalui

intervensi manual, hal ini menunjukkan bahwa kekuatan SOAR terletak pada kemampuannya untuk beradaptasi, didorong oleh integrasi AI/ML, yang memfasilitasi deteksi anomali yang lebih cerdas dan korelasi peringatan yang otomatis. Pemanfaatan Explainable AI (XAI) selanjutnya memperkuat sistem dengan memastikan transparansi dan menjaga kepercayaan analis, yang sangat penting untuk mencapai operasi keamanan yang resilient dan scalable. Meskipun integrasi antara SOAR dan AI ini menunjukkan kekuatan yang luar biasa dalam dunia keamanan siber, seperti halnya setiap pendekatan ilmiah lainnya, kombinasi keduanya tetap menghadapi berbagai tantangan yang diharapkan dapat terus diatasi seiring dengan evolusi pertahanan di masa mendatang

Link video : https://youtu.be/eo4sRocaySo