Jurnal Review Pendidikan dan Pengajaran
http://journal.universitaspahlawan.ac.id/index.php/jrpp
Volume 7 Nomor1, 2024
P-2655-710X e-ISSN 2655-6022

Submitted : 06/01/2024
Reviewed : 09/01/2024
Accepted : 15/01/2024
Published : 21/01/2024

Gunawan Wibisono [1]
Rudy A.G. Gultom [2]
Teddy Mantoro [3]

STRATEGI PENINGKATAN KAPABILITAS SATUAN SIBER DISPAMSANAU MELALUI PEMANFAATAN ARTIFICIAL INTELLIGENCE PADA KEAMANAN SIBER BERDASARKAN NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY CYBERSECURITY FRAMEWORK VERSION 1.1

Abstrak

Perkembangan keamanan siber dan AI telah menghasilkan banyak penelitian untuk memecahkan permasalahan terkait proses identifikasi, deteksi, respon, dan pemulihan dari serangan siber. Proses tersebut sejalan dengan tugas yang diemban Satuan Siber Dinas Keamanan dan Sandi TNI AU (Satcyber Dispamsanau). Satcyber Dispamsanau merupakan salah satu Badan Pelaksana Pusat (balakpus) TNI AU yang mempunyai tugas melaksanakan kegiatan pendeteksian, identifikasi, penindakan, penanggulangan, dan pemulihan siber terhadap TNI AU IV, harus mampu menjawab tantangan dan tantangan yang ada. peluang perkembangan keamanan siber yang terus terjadi.

Kata Kunci: Keamanan Siber, Kecerdasan Buatan (AI), Satuan Siber Pengenalan Pelayanan Keamanan dan Enkripsi TNI AU (Satcyber Dispamsanau).

Abstract

The development of cybersecurity and AI has resulted in many studies to solve problems related to the process of identification, detection, response, and recovery from cyberattacks. The process is in line with the tasks carried out by the Cyber Unit of the Indonesian Air Force Security and Encryption Service (Satcyber Dispamsanau). Satcyber Dispamsanau is one of the central implementing agencies (balakpus) of the Indonesian Air Force which has the task of carrying out cyber detection, identification, enforcement, countermeasures, and recovery activities against the TNI AU IV, must be able to answer the challenges and opportunities of cyber security developments that continue to occur.

Keywords: Cybersecurity, Artificial Intelligence (AI), Cyber Unit of the Indonesian Air Force Security and Encryption Service Introduction (Satcyber Dispamsanau).

PENDAHULUAN

Istilah keamanan siber mengacu pada serangkaian teknologi, proses, dan praktik yang bertujuan untuk melindungi aset Infrastruktur Informasi Vital (IIV) organisasi yang dapat berupa jaringan, perangkat lunak, perangkat keras, ataupun sarana prasarana lain yang berkaitan dengan siber dari berbagai macam serangan yang dilakukan oleh threat actor. Perkembangan keamanan siber semakin kompleks sejalan dengan perkembangan interkoneksi perangkat, sistem, dan jaringan. Berdasarkan laporan Honeynet Project BSSN Tahun 2022, bahwa sejak Januari hingga Desember 2022 telah terjadi sebanyak 370.022.283 serangan siber dengan jumlah 1.192.315 alamat IP penyerang yang berbeda. Masifnya ancaman siber tersebut dapat terjadi sebagai salah satu akibat karena semakin banyaknya state-sponsored threat actors yang secara terus menerus meningkatkan taktik dan teknik dalam melakukan serangan siber ke target. Negara-negara tertentu yang memiliki kepentingan akan terus berupaya dalam mencapai

[1,2)]Universitas Pertahanan Republik Indonesia
[3)]Sampoerna University
email: weebegoen@gmail.com, rudygultom@idu.ac.id, teddy@ieee.org

tujuannya, salah satunya yaitu melalui cyber-espionage dengan memanfaatkan malware untuk melakukan penyerangan ke sistem milik target. Negara-negara adikuasa semakin meningkatkan eksistensi kekuatan militer yang dimilikinya, baik kekuatan militer darat, laut, dan udara, bahkan saat ini kekuatan militer di bidang siber menjadi salah satu senjata potensial yang dapat dimanfaatkan untuk meraih keunggulan dalam perang maupun persaingan global.

Hal tersebut dibuktikan dengan peristiwa perang antara Russia dan Ukraina yang saat ini masih berlangsung. Sebelum terjadinya perang secara fisik, sejak tahun 2014 perang siber antar kedua negara telah terjadi. Kedua negara tersebut memanfaatkan teknologi siber untuk saling melakukan penyerangan terhadap IIV, organisasi pemerintah, maupun individu. Melalui perang tersebut, maka membuktikan bahwa pemanfaatan siber dalam operasi militer merupakan salah satu komponen penting untuk mendukung kesuksesan dalam mencapai keunggulan militer. Sejalan dengan Dez dan Guyonneau (2019), bahwa peperangan digital merupakan perang jangka panjang dengan tujuan untuk melemahkan musuh di dunia maya untuk mendapatkan keuntungan di bidang militer, ekonomi, politik, dan kemasyarakatan. Tren perang pun telah bergeser dengan mengoptimalkan pemanfaatan Ilmu Pengetahuan dan Teknologi (IPTEK) sehingga perang konvensional antar negara hampir tidak lagi ditemukan, namun perang yang lebih dominan adalah perang siber atau cyber warfare (Kurniawan et al., 2023).

Persaingan antar negara dalam pemanfaatan siber untuk penguatan sistem pertahanan (defensive objective) maupun pembuatan cyber weapon (offensive objective) semakin meningkat. Terlebih lagi saat ini muncul teknologi baru yang disebut dengan Artificial Intelligence (AI). AI menjadi teknologi yang mampu memberikan analisis dan solusi untuk melindungi organisasi dari serangan siber dan mencegah terjadinya permasalahan yang lebih kompleks dengan cara menganalisis jutaan anomali siber secara efektif. Karena alasan tersebut, maka AI semakin banyak diintegrasikan ke dalam struktur keamanan siber dan digunakan dalam berbagai persoalan untuk mengotomatisasi pekerjaan atau mendukung tugas dari tim keamanan (Kaur, Gabrijelčič and Klobučar, 2023).

Berkembangnya keamanan siber dan AI telah menghasilkan banyak penelitian untuk memecahkan permasalahan terkait proses identifikasi, deteksi, respons, dan pemulihan dari serangan siber. Proses tersebut sejalan dengan tugas yang dilakukan oleh Satuan Siber Dinas Pengamanan dan Persandian TNI Angkatan Udara (Satsiber Dispamsanau). Satsiber Dispamsanau merupakan salah satu badan pelaksana pusat (balakpus) TNI AU yang memiliki tugas untuk melaksanakan kegiatan deteksi, identifikasi, penindakan, penanggulangan, dan pemulihan siber terhadap IIV TNI AU, harus mampu menjawab tantangan dan peluang dari perkembangan keamanan siber yang terus terjadi. Dihadapkan dengan adanya teknologi AI, maka Satsiber Dispamsanau perlu melakukan pengembangan dan peningkatan kemampuan serta kapabilitas sibernya. Perlu adanya strategi khusus agar Satsiber Dispamsanau mampu mengoptimalkan kemampuan dan kapabilitas tersebut.

Salah satu strategi yang dapat diterapkan yaitu dengan pemanfaatan AI pada program keamanan siber dengan mengacu pada National Institute of Standards and Technology (NIST) Cybersecurity Frameworks Version 1.1. Framework tersebut berisi panduan, praktik, dan pedoman untuk membantu organisasi dalam mengembangkan, mengimplementasikan, dan meningkatkan program keamanan siber pada suatu organisasi. Dengan menerapkan framework ini dalam pemanfaatan AI pada Satsiber Dispamsanau, maka diharapkan terwujud suatu strategi untuk meningkatkan kapabilitas dan kemampuan yang dimiliki. Berdasarkan uraian tersebut, maka pertanyaan penelitian ini yaitu "Bagaimana strategi pemanfaatan AI pada Satsiber Dispamsanau berdasarkan NIST Cybersecurity Framework Version 1.1?"

Artificial Intelligence pada Keamanan Siber

Keamanan siber (cybersecurity) merupakan serangkaian kebijakan, prosedur, dan mekanisme teknis yang bertujuan untuk melindungi, mendeteksi, memperbaiki, dan mempertahankan suatu sistem dari kerusakan, penggunaan atau modifikasi tanpa izin, maupun eksploitasi sistem informasi dan komunikasi secara tidak sah (Kaur, Gabrijelčič, dan Klobučar, 2023). Sedangkan menurut NIST Cybersecurity Framework, keamanan siber merupakan suatu proses untuk melindungi informasi dengan cara mencegah, mendeteksi, dan merespon serangan siber. Berdasarkan dua definisi tersebut, dapat diperoleh pokok pengertian terkait keamanan siber yaitu serangkaian proses baik teknis maupun manajerial yang bertujuan untuk melindungi suatu sistem terhadap ancaman dan serangan siber. Sedangkan definisi dari artifical intelligence

menurut Horvitz (2022) yaitu salah satu bidang ilmu komputer dengan memanfaatkan algoritma komputer untuk pengembangan prinsip dan mekanisme tertentu guna menyelesaikan tugas-tugas yang umumnya dilakukan dengan pemahaman manusia, seperti persepsi, penalaran, bahasa, dan pembelajaran. Yamin et al. (2021) menyatakan bahwa integrasi antara keamanan siber dan artificial intelligence dapat dilakukan untuk menciptakan teknologi baru dalam domain siber.

Semakin meluasnya perkembangan teknologi keamanan siber, saat ini pengembangan teknologi artificial intelligence juga mengalami peningkatan secara signifikan. Pemanfaatan artificial intelligence diterapkan dalam semua tahap keamanan termasuk pada tahap pencegahan, deteksi, investigasi, remediasi, penemuan dan pengklasifikasian ancaman, threat intelligence, dan pelatihan maupun simulasi keamanan siber (Horvitz, 2022). Menurut Mallick (2018), bahwa artificial intelligence memiliki peran yang sangat penting terhadap keamanan siber yang dimanfaatkan untuk defensive maupun offensive objective. Artificial intelligence mampu melakukan analisis prediktif untuk mengantisipasi serangan siber dengan menghasilkan model ancaman secara dinamis dari berbagai sumber data yang tersedia dalam jumlah yang besar.

NIST Cybersecurity Framework

NIST Cybersecurity Framework merupakan kerangka kerja keamanan siber yang bertujuan untuk memberikan panduan dalam mengidentifikasi, merancang, mengimplementasikan, mengelola, dan meningkatkan program keamanan siber pada suatu organisasi. Kerangka kerja ini terdiri dari dari empat komponen inti yaitu fungsi, kategori, subkategori, dan referensi informatif. Fungsi merupakan komponen dari NIST Cybersecurity Framework yang terdiri dari 5 fungsi utama dalam keamanan siber yaitu identifikasi, proteksi, deteksi, respons, dan pemulihan. Pada setiap fungsi tersebut terdiri dari beberapa kategori yang menjadi fokus dalam pengelolaan keamanan siber. Fungsi-fungsi tersebut memberikan gambaran secara komprehensif tentang pengelolaan keamanan siber pada organisasi. Berikut merupakan kategori pada masing-masing fungsi tersebut.

Gambar 1. Lima fungsi pada NIST Cybersecurity Framework (Sumber: NIST)

1. Identifikasi – Asset management, business environment, governance, risk assessment, dan risk management strategy.
2. Proteksi – Identity management and access control, awareness and training, data security, information protection processes and procedures, maintenance, dan protective technology.
3. Deteksi – Anomalies and events, security continuous monitoring, dan detection processes.
4. Respons – Response planning, communication, analysis, mitigation, dan improvements.
5. Pemulihan – Recovery planning, improvements, dan communications.

METODE

Dalam penelitian ini, metodologi yang digunakan yaitu literature review. Metodologi penelitian literature review merupakan pendekatan yang digunakan untuk mengumpulkan, mengevaluasi, dan menyintesis literatur yang relevan dengan topik penelitian. Penelitian dengan topik pemanfaatan artificial intelligence pada keamanan siber, maka peneliti melakukan pencarian secara sistematis yang berelasi dengan topik tersebut ke berbagai sumber akademik dapat meliputi jurnal ataupun buku untuk mengidentifikasi penelitian-penelitian yang telah dilakukan sebelumnya. Setelah literatur yang relevan diperoleh, maka selanjutnya dilakukan analisis dan sintesis pokok-pokok yang berelasi dengan penelitian untuk membangun pemahaman yang mendalam terhadap topik tersebut.

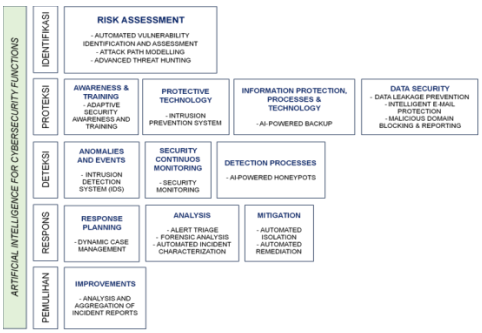
HASIL DAN PEMBAHASAN

Dalam era digital yang semakin maju sejalan dengan dengan meningkatnya tren ancaman dan serangan siber, pemanfaatan artifical intelligence dalam keamanan siber dapat menjadi komponen penting untuk mendukung terwujudnya ketahanan siber suatu organisasi atau negara. Satsiber Dispamsanau sebagai bagian organisasi dari TNI Angkatan Udara, memiliki tanggung jawab dan tantangan yang besar terhadap keamanan siber pada postur pertahanan negara. Pertahanan suatu negara tidak hanya terbatas pada pertahanan secara fisik untuk mencapai kedaulatan nasional, namun pertahanan negara telah memasuki era baru yaitu pertahanan siber yang harus mampu mengatasi segala jenis kemungkinan terjadinya serangan dan ancaman siber terhadap IIV TNI AU. Untuk mampu menjawab tantangan tersebut, Satsiber Dispamsanau memiliki tugas dan fungsi meliputi:

1. Melaksanakan kegiatan, operasi pencegahan dan penangkalan dalam rangka mendeteksi, mencegah, dan melindungi IIV TNI AU yang meliputi pusat data (data center), perangkat keras (hardware), dan piranti lunak (software) sistem informasi, jaringan komunikasi data, data-data digital, serta media sosial yang berdampak pada pelaksanaan tugas TNI AU dari berbagai macam dimensi ancaman ataupun serangan siber.
2. Melaksanakan kegiatan dan operasi penanggulangan dari berbagai bentuk serangan siber pasca insiden dengan melaksanakan mitigation plan dan forensic dalam rangka penyiapan sistem pertahanan siber yang handal.
3. Melaksanakan kegiatan dan operasi pemulihan dampak dari berbagai bentuk serangan siber, seperti penyelamatan data yang disimpan dalam perangkat atau sistem, serta perbaikan hardware dan pemulihan software terdampak.
4. Melaksanakan kegiatan, operasi penindakan untuk mampu melumphkan atau menghancurkan potensi ancaman siber.

Pemetaan Pemanfaatan Artificial Intelligence Berdasarkan NIST Cybersecurity Framework

Sejalan dengan hal tersebut, berdasarkan NIST Cybersecurity Framework, terdapat lima fungsi dalam keamanan siber, meliputi identifikasi, proteksi, deteksi, respons, dan pemulihan. Kelima fungsi keamanan siber tersebut mencakup penggunaan artificial intelligence mulai dari pencegahan serangan hingga proses yang lebih kompleks dan secara aktif dalam mencari ancaman baru dan serangan balik terhadap lawan atau bakal lawan. Penerapan artificial intelligence dalam keamanan siber dapat dilakukan dengan melakukan pemetaan terhadap teknologi artificial intelligence ke tiap fungsi keamanan siber, sehingga penerapan artificial intelligence tidak hanya terbatas pada salah satu fungsi keamanan siber, namun dapat menjangkau seluruh fungsi secara komprehensif. Berikut Gambar 2 merupakan rekomendasi model penerapan artificial intelligence pada tiap fungsi keamanan siber yang dapat menjadi strategi untuk diadopsi oleh Satsiber Dispamsanau guna melaksanakan tugas dan fungsinya secara optimal.



Gambar 2. Penerapan Artificial Intelligence pada fungsi Keamanan Siber

Fungsi Identifikasi

Penilaian risiko adalah proses mengidentifikasi, memperkirakan, dan memberikan prioritas pada risiko keamanan siber yang terkait dengan pelaksanaan tugas kegiatan dan operasi siber, aset operasional, maupun individu yang mengawaki tugas keamanan siber. Proses penilaian risiko melibatkan analisis terhadap informasi ancaman, kerentanan, dan serangan untuk menentukan sejauh mana berdampak pada organisasi dan seberapa besar kemungkinan

persitiwa tersebut akan terjadi. Penilaian risiko secara manual memerlukan waktu yang cukup lama, kompleks, dan membutuhkan ketelitian yang tinggi untuk meminimalisir kesalahan dalam perhitungan. Pemanfaatan artificial intelligence dapat mengatasi permasalahan tersebut karena dengan teknologi yang terotomatisasi, maka penilian dapat lebih efektif dan efisien. Beberapa teknologi yang dapat diterapkan terkait penilian risiko keamanan siber yaitu automated vulnerability identification and assessment, automated threat hunting, dan attack path modelling. Berikut adalah deskripsi dari teknologi tersebut:

1. **Automated Vulnerability Identification and Assessment**

Teknologi ini melakukan penilian terhadap kelemahan atau kerentanan suatu sistem secara otomatis dengan cara mengidentifikasi, mengklasifikasikan, dan mengeksplorasi celah keamanan suatu sistem dengan cara memanfaatkan repositori celah keamanan, common vulnerabilities and exposure databases (CVE), dan vendor vulnerability release untuk mengidentifikasi celah yang mungkin ada serta membuat rekomendasi keamanan untuk sistem. Artificial Intelligence ini memiliki kemampuan untuk melakukan pengecekan terhadap keamanan source code dengan deep learning dan dan transfer learning.

2. **Automated Threat Hunting**

Teknologi artificial intelligence ini merupakan teknologi untuk melakukan pencarian ancaman secara otomatis di seluruh jaringan pada sistem dan endpoint untuk mendeteksi kemungkinan terjadinya malicious atau suspicious yang berisiko terhadap keamanan suatu sistem. Teknologi ini mengidentifikasi dan mengkategorisasikan potensi ancaman dengan menggunakan data threat intelligence yang telah dikumpulkan. Metode yang digunakan yaitu dilakukan baik menggunakan anomaly-based ataupun dengan open-source cyber threat intelligence (OSCTI).

3. **Attack Path Modelling**

Teknologi ini memanfaatkan pemetaan terhadap kerentanan keamanan pada jaringan untuk menilai risiko, mengidentifikasi kerentanan, dan mengambil keputusan terhadap potensi terjadinya serangan siber. Artificial intelligence diimplementasikan dengan teknik pemodelan menggunakan intrusion alerts ataupun vulnerability description. Sistem tersebut menggunakan analisis alerts, log, dan network traffic untuk mensimulasikan serangan dalam mengambil tindakan pencegahan secara real-time.

Fungsi Proteksi

Fungsi proteksi menjamin perlindungan dalam merencanakan dan menerapkan kontrol/pengendalian yang tepat untuk membatasi atau mencegah meluasnya dampak dari potensi ancaman dan serangan siber yang terjadi. Hal ini dapat mencakup kontrol teknis dan prosedural untuk melindungi secara proaktif terhadap ancaman secara internal dan eksternal. Artificial intelligence dapat meningkatkan ketahanan sistem dengan cara meningkatkan security awareness pengguna dengan menerapkan adaptive cybersecurity training, pemanfaatan data leakage prevention and integrity monitoring, automated information protection maupun security protection mechanisms.

1. Adaptive Security Awareness and Training

Teknologi ini memberikan solusi dalam peningkatan security awareness dan training dari personel yang mengawaki tugas dan bertanggung jawab dalam keamanan siber. Artificial intelligence dapat digunakan dalam proses pemberian materi dan training dengan cara penyediaan teknologi yang adaptif dengan memanfaatkan natural language processing algorithm ataupun dengan memanfaatkan machine learning yang dapat berfungsi sebagai intelligent trainer untuk memberikan pelatihan secara interaktif dan efektif.

2. Protective Technology

Teknologi ini menjamin keamanan dan ketahanan sistem dan IIV yang dimiliki. Teknologi ini menggunakan fitur khusus yang dapat mencegah kerusakan ataupun dampak buruk dari adanya ancaman dan serangan siber dengan cara mengidentifikasi dan mencegah upaya infeksi, penetrasi, atapun ekstraksi informasi dari sistem. Artificial intelligence dapat digunakan dalam bentuk intrusion prevention system (IPS) dengan cara menganalisis log dan sekaligus melakukan tindakan sesuai dengan tipe dan jenis ancaman untuk mencegah terjadinya upaya serangan siber.

3. Information Protection, Processes, and Procedures

Teknologi ini menjamin keamanan informasi melalui pemanfaatan artificial intelligence powered backup untuk melakukan back-up data dan penyimpanan secara aman. Metode yang digunakan yaitu melalui dynamic back-up scheduling dan optimized backup scheduling. Metode tersebut memanfaatkan intelligent scheduling algorithm untuk meningkatkan efisiensi dan stabilisasi proses backup dan penyimpanan.

4. Data Security

Data security berfokus pada keamanan data sesuai dengan kondisi informasi baik dalam proses data at rest dan data in transit, serta siklus dalam pengelolaan data. Pemanfaatan artificial intelligence digunakan dengan teknologi data leakage prevention, intelligent e-mail protection, dan malicious domain blocking and reporting. Data leakage prevention merupakan teknologi yang bertujuan untuk mendeteksi kemungkinan adanya data breaches secara otomatis dengan cara mengumpulkan informasi secara komprehensif ke berbagai sumber data. Teknologi ini dapat memantau aktivitas pengguna secara real-time, mengidentifikasi perilaku yang mencurigakan, dan memberikan peringatan atau tindakan pencegahan saat aktivitas yang mencurigakan terdeteksi. Selain itu, tekonologi ini dapat melakukan klasifikasi data secara otomatis berdasarkan tingkat sensitivitasnya sehingga dengan metode machine learning, teknologi ini dapat mengenali data sensitif dan memberikan perlindungan tambahan ke data tersebut.

Selain data leakage prevention, teknologi lain yang mendukung data security yaitu intelligence e-mail protection. Teknologi ini bertujuan untuk mencegah serangan siber yang berfokus pada target email. Teknologi artificial intelligence dapat menganalisis email sehingga dapat mengklasifikasikan kategori email yang bersifat suspicious yang berisi spam atau link phising. Teknologi yang mirip dengan email protection yaitu malicious domain blocking and reporting. Teknologi ini bertujuan untuk mecegah pengguna untuk mengakses malicious domain/website. Sistem bekerja dengan menganalisis dan identifikasi user behavior saat mengakses domain/website tertentu dengan memanfaatkan machine learning algorithm. Sistem akan memberikan peringatan dan pencegahan saat user mengakses ke suspected malicious domain yang dapat berisi ransomware/malware, botnet, ataupun web phising.

Fungsi Deteksi

Fungsi deteksi bertujuan untuk menjamin keamanan dengan cara melakukan upaya preventif untuk mencegah timbulnya dampak terhadap potensi ancaman dan serangan siber. Deteksi memanfaatkan artificial intelligence untuk mempercepat kemampuan deteksi dan dapat melakukannya dengan tepat sesuai dengan jenis dan tipe serangan dari analisis log yang masuk ke sistem. Berikut adalah beberapa teknologi yang digunakan untuk dapat menjamin keamanan melalui fungsi deteksi.

1. Anomalies and Events

Teknologi ini disebut dengan Intrusion Detection System (IDS) yang merupakan perangkat dan teknik untuk memantau lalu lintas sistem dan jaringan yang masuk ke sistem melalui dengan cara menganalisis aktivitas anomali dan suspicious. IDS dapat tediri dari anomaly-based maupun signature-based. Artificial intelligence melalui machine learning akan melakukan pengklasifikasian anomali dari log yang masuk ke sistem dengan cara mencocokannya ke malicious anomaly database ataupun dengan mempelajari behaviour dari threat actor.

2. Security Continuous Monitoring

Teknologi ini menjamin monitoring terhadap keamanan jaringan dan sistem dengan real-time dan berkelanjutan. Monitoring dapat dilakukan secara otomatis dan dapat mengklasifikasikan anomaly sesuai dengan severity dan prioritas alert yang menjadi potensi ancaman. Pemanfaatan artificial intelligence tersebut dapat mengatasi permasalahan keterbatasan personel dalam melakukan monitoring dan analisis secara terus-menerus dan real-time.

3. Detection Processes

Artificial intelligence dapat digunakan untuk membangun suatu AI-powered honeypot. Teknologi ini bertujuan untuk mempelajari teknik dan perilaku serangan siber untuk meningkatkan keamanan sistem dan dapat menjadi database serangan siber. Honeypot yang didukung dengan artificial intelligence menggunakan algoritma machine learning untuk memprediksi serangan dari data honeypot yang telah diperoleh.

Fungsi Respons

Fungsi renspons bertujuan untuk merencanakan dan mengembangkan proses yang efektif dalam mengatasi masalah, menganalisis insiden sehingga mempermudah dalam menentukan penyebab, ruang lingkup, dan damapknya, melakukan pengendalian insiden. Dengan memanfaatkan artificial intelligence, insiden dapat diatasi dengan waktu yang cepat sehingga dapat membantu analis untuk mengambil tindakan yang tepat. Beberapa penerapan artificial intelligence dalam fungsi ini yaitu meliputi:

1. Response Planning

Melalui teknologi ini, dilakukan perencanaan terhadap prosedur respons mengenai tindakan yang tepat selama dan setelah insiden siber terjadi. Artificial intelligence melalui Dynamic case management dapat diterapkan dengan melakukan analisis dari learning from evidence untuk selalu memperbarui tindakan dan respons yang tepat untuk ke depannya. Melalui analisis tersebut maka sistem akan berjalan secara otomatis untuk memberikan rekomendasi respons terhadap insiden siber.

2. Analysis

Analisis merupakan inti dari penentuan, investigasi, dan peninjauan insiden, ancaman, dan serangan siber serta bagaimana menentukan pengklasifikasian serangan dan respons yang tepat. Beberapa teknologi artificial intelligence yang dapat diterapkan berkaitan dengan proses analisis tersebut yaitu alert triage, forensic analysis, dan automatic incident characterization. Alert triage merupakan pemrosesan alert dan triase nya dengan cara menyelidiki tiap alert yang terdeteksi di sistem dengan cara efisien dan akurat untuk memprioritaskan dan menganalisis korelasi antar alert untuk menentukan apakah alert tersebut akan dieksalasi menjadi respons insiden atau hanya bersifat false-positive. Teknologi yang dapat mendukung lainnya yaitu forensic analysis. Teknologi ini bertujuan untuk menganalisis timeline dari serangan atau ancaman yang potensial ke sistem termasuk atribusi dari serangan dan bukti dari tiap evidence serangan/ancaman siber. Pemanfaatan artificial intelligence lainnya yaitu incident characterization, teknologi ini bertujuan untuk mengidentifikasi kategori insiden sesuai dengan rencana respons yang ditetapkan. Hal ini mengidentifikasi kekritisan insiden dan hubungannya dengan insiden lain untuk selanjutnya secara otomatis akan memprioritaskan insiden yang tepat untuk dilanjutkan proses investigasi.

3. Mitigation

Pemanfaatan artificial intelligence dalam mitigation dapat mencakup automated isolation dan automated remediation. Automated isolation merupakan teknologi berbasis AI yang dapat melakukan isolasi terhadap perangkat secara otomatis sebagai tindak lanjut dari terdeteksinya Indicator of Compromise (IoC). Hal ini dapat memutuskan konektivitas dari suatu perangkat dengan sistem sehingga perangkat yang terinfeksi tidak menyebarkannya ke perangkat yang lain dalam jaringan pada suatu sistem. Automated remediation memiliki fungsi dalam melakukan resolusi dan perbaikan secara otomatis terhadap sistem yang terinfeksi IoC. Teknik AI digunakan untuk memilih tindakan perbaikan yang tepat untuk menghilangkan acaman.

Fungsi Pemulihan

Tujuan utama dari fungsi pemulihan adalah untuk menjaga ketahanan dan kemampuan dalam melakukan pemulihan terhadap IIV yang terdampak serangan siber. AI akan memproses dengan cepat dan efektif sehingga sistem dapat berjalan dengan normal dengan keamanan yang terjamin. AI dapat diterapkan dalam analysis and aggregation of incident reports, yaitu bahwa teknik AI dapat digunakan untuk pengumpulan data, agregasi, ekstraksi informasi, visualisasi, dan prediksi data insiden secara efisien.

SIMPULAN

Berdasarkan analisis yang telah dilakukan, telah dilakukan pemetaan terhadap pemanfaatan artificial intelligence dalam keamanan siber berdasarkan NIST Cybersecurity Frameworks Version 1.1. Melalui pemetaan yang dilakukan pada tiap fungsinya, Satsiber Dispamsanau dapat menerapkan pemanfaatan AI tersebut sehingga dapat mendukung tugas dan tanggung jawab Satsiber Dispamsanau dalam memberikan jaminan keamanan terhadap IIV TNI AU. Secara umum artificial intelligence dapat menjadi teknologi pendukung dalam pelaksanaan kegiatan dan operasi siber yang dilakukan karena artificial intelligence dapat mempercepat dan secara efektif mampu mengatasi keterbatasan kemampuan yang dimiliki oleh personel. Namun

demikian, bahwa pemanfaatan artificial intelligence harus disesuaikan dengan kondisi dan interoperabilitas dari sistem yang dimiliki oleh Satsiber Dispamsanau.

Penelitian selanjutnya dapat dilakukan analisis kelebihan, kelemahan, tantangan, dan peluang pemanfaatan artificial intelligence oleh Satsiber Dispamsanau sehingga pemanfaatannya dapat menghasilkan strategi yang optimal dan tepat sasaran.

DAFTAR PUSTAKA

Badan Siber dan Sandi Negara (2022) Laporan Tahunan 2022 Honeynet Project Bssn - IHP. Available at: https://cloud.bssn.go.id/s/qSJenLAmr2ooF2Q.

Dez, A. Le and Guyonneau, R. (2019) 'Artificial Intelligence in Digital Warfare: Introducing the Concept of the Cyberteammate', Jstor, 4(2), pp. 103–116.

Horvitz, E. (2022) Artifical Intelligence and Cybersecurity : Rising Challenges and Promising Directions.

Kaur, R., Gabrijelčič, D. and Klobučar, T. (2023) 'Artificial intelligence for cybersecurity: Literature review and future research directions', Information Fusion, 97(January). doi: 10.1016/j.inffus.2023.101804.

Kurniawan, T. et al. (2023) Perang Rusia-Ukraina dalam Perspektif Siber.

Mallick, P. K. (2018) 'Artificial Intelligence in the Armed Forces: An Analysis', CLAWS Journal, pp. 63–79.

NIST (2018) 'Framework for Improving Critical Infrastructure Cybersecurity Version 1.1', National Institute of Standards and Technology. doi: 10.1109/isit.2003.1228152.

Yamin, M. M. et al. (2021) 'Weaponized AI for cyber attacks', Journal of Information Security and Applications, 57, pp. 1–35. doi: 10.1016/j.jisa.2020.102722.