MANAJEMEN INSIDEN RESPON SIBER MENGGUNAKAN TEKNOLOGI *NETWORK DETECTION AND RESPONSE* (NDR) *DARKTRACE*

Disusun Oleh:

N a m a : Bintang Ananda
NIM : 20523160

PROGRAM STUDI INFORMATIKA – PROGRAM SARJANA
FAKULTAS TEKNOLOGI INDUSTRI
UNIVERSITAS ISLAM INDONESIA
2024

HALAMAN PENGESAHAN DOSEN PEMBIMBING

MANAJEMEN INSIDEN RESPON SIBER MENGGUNAKAN TEKNOLOGI *NETWORK DETECTION AND RESPONSE* (NDR) *DARKTRACE*

TUGAS AKHIR JALUR MAGANG

Disusun Oleh:

N a m a : Bintang Ananda

NIM : 20523160

Yogyakarta, 09 Juli 2024

Pembimbing,

(Hari Setiaji, S.Kom., M.Eng)

HALAMAN PENGESAHAN DOSEN PENGUJI

MANAJEMEN INSIDEN RESPON SIBER MENGGUNAKAN TEKNOLOGI *NETWORK DETECTION AND RESPONSE* (NDR) *DARKTRACE*

TUGAS AKHIR JALUR MAGANG

Telah dipertahankan di depan sidang penguji sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer dari Program Studi Informatika – Program Sarjana di Fakultas Teknologi Industri Universitas Islam Indonesia

Yogyakarta, 26 Juli 2024

Tim Penguji

Hari Setiaji, S.Kom., M.Eng _____

Anggota 1

Dr. Ahmad Luthfi, S.Kom., M.Kom. _____

Anggota 2

Erika Ramadhani, S.T., M.Eng. _____

Mengetahui,

Ketua Program Studi Informatika – Program Sarjana

Fakultas Teknologi Industri

Universitas Islam Indonesia

(Dhomas Hatta Fudholi, S.T., M.Eng., Ph.D.)

HALAMAN PERNYATAAN KEASLIAN TUGAS AKHIR

Yang bertanda tangan di bawah ini:

Nama	:	Bintang Ananda
NIM	:	20523160

Tugas akhir dengan judul:

MANAJEMEN INSIDEN RESPON SIBER MENGGUNAKAN TEKNOLOGI *NETWORK DETECTION AND RESPONSE* (NDR) *DARKTRACE*

Menyatakan bahwa seluruh komponen dan isi dalam tugas akhir ini adalah hasil karya saya sendiri. Apabila di kemudian hari terbukti ada beberapa bagian dari karya ini adalah bukan hasil karya sendiri, tugas akhir yang diajukan sebagai hasil karya sendiri ini siap ditarik kembali dan siap menanggung risiko dan konsekuensi apapun.

Demikian surat pernyataan ini dibuat, semoga dapat dipergunakan sebagaimana mestinya.

Yogyakarta, 09 Juli 2024

(Bintang Ananda)

HALAMAN PERSEMBAHAN

Laporan akhir ini penulis persembahkan untuk seluruh keluarga dan teman yang selalu memberi dukungan, semangat, serta doa yang tidak terhitung jumlahnya. Persembahan juga penulis berikan kepada dosen pembimbing yang telah memberikan arahan dan masukan yang berharga. Semoga hasil karya ini dapat bermanfaat bagi banyak pihak. Terima kasih.

HALAMAN MOTO

"*The hard times that you go through, those are the times that you develop character*"

(Michelle Obama)

"Boleh jadi kamu membenci sesuatu, padahal ia amat baik bagimu, dan boleh jadi (pula) kamu menyukai sesuatu, padahal ia amat buruk bagimu. Allah mengetahui, sedang kamu tidak mengetahui."

(Q.S. Al-Baqarah ayat 216)

KATA PENGANTAR

Segala puji dan syukur penulis panjatkan kehadiran Allah SWT, yang telah melimpahkan rahmat, taufik serta hidayah-Nya sehingga penulis dapat menyelesaikan Tugas Akhir ini dengan lancar walaupun jauh dari kata sempurna. Shalawat serta salam senantiasa penulis haturkan kepada Nabi Muhammad SAW sebagai suri tauladan umat islam.

Adapun tujuan laporan ini dibuat untuk memenuhi salah satu persyaratan kelulusan jalur magang di Program Studi Informatika, Fakultas Teknologi Industri, Universitas Islam Indonesia. Tidak dapat dipungkiri dalam penyusunan Tugas Akhir ini tidak terlepas dari bantuan berbagai pihak, baik secara langsung maupun tidak. Oleh karena itu, penulis mengucapkan terima kasih kepada semua pihak yang telah membantu, diantaranya :

1. Seluruh keluarga yang selalu memberikan do'a serta dukungan selama melaksanakan kegiatan magang hingga penyelesaian pembuatan Laporan Tugas Akhir.
2. Bapak Dr. Ir. Raden Teduh Dirgahayu, S.T., M.Sc. selaku Ketua Jurusan Informatika Fakultas Teknologi Industri Universitas Islam Indonesia.
3. Bapak Dhomas Hatta Fudholi, S.T., M.Eng., Ph.D. Selaku Ketua program Studi Informatika – Program Sarjana fakultas Teknologi Industri Universitas islam Indonesia.
4. Ibu Sheila Nurul Huda, S.Kom., M.Cs., selaku dosen pembimbing akademik yang telah memberikan saran, nasehat dan bimbingan dalam kegiatan perkuliahan sehingga penulis dapat melaksanakan semua kegiatan kuliah dengan baik hingga akhir.
5. Bapak Hari Setiaji, S.Kom., M.Eng., selaku Dosen Pembimbing yang memberikan saran, nasehat, serta bimbingan mulai dari kegiatan magang hingga Pembuatan Laporan Tugas Akhir dapat Terselesaikan.
6. Bapak Luky Kurniawan selaku ketua tim Squra Lintasarta yang telah memberikan kesempatan untuk melaksanakan magang di Lintasarta.
7. Mas Mokhammad Fairizal selaku pembimbing lapangan, dan seluruh rekan kerja Squra Lintasarta yang telah memberikan kepercayaan, arahan, dan pengalaman selama magang berlangsung.
8. Teman-teman terdekat yang selalu memberikan semangat, dukungan, dan do'a.

9. Teman-teman terdekat yang selalu memberikan semangat, dukungan, dan do'a.
10. Seluruh dosen dan staff Program Studi Informatika yang memberikan ilmu pengetahuan selama perkuliahan.

Penulis menyadari bahwa laporan ini tidak luput dari kesalahan, baik dalam proses pembuatan maupun dari hasil laporan. Untuk itu, penulis menerima kritik dan saran guna menyempurnakan laporan ini. Akhir kata, penulis berharap semoga Laporan Tugas Akhir ini bermanfaat bagi penulis serta pembaca.

Yogyakarta, 09 Juli 2024

Bintang Ananda

SARI

Pada era digital yang semakin kompleks, membuat kerentanan *zero-day vulnerability* berkembang pesat. Hal ini menyebabkan perusahaan membutuhkan teknologi keamanan yang dapat melampaui metode pendeteksi berbasis tanda tangan (*Signature-Based*), yang hanya mengandalkan informasi dari jenis serangan yang pernah terjadi. Dari permasalahan tersebut, diperlukan teknologi keamanan yang menggunakan metode pendeteksian berbasis perilaku (*Behavioral-Based*) dengan memanfaatkan *Artificial Intelligence* (AI) dan *Machine Learning* (ML). Lintasarta sebagai perusahaan yang memberikan sebuah layanan (vendor) memberikan sebuah solusi dari permasalahan ini, yaitu membuat layanan *Network Detection and Response* (NDR) yang dikembangkan oleh Darktrace sebagai salah satu solusi teknologi yang mendukung metode pendeteksian ini, sehingga memungkinkan perlindungan dinamis dan efektif terhadap ancaman siber. Namun, Selama masa percobaan penggunaan NDR Darktrace di Lintasarta, terdapat permasalahan dalam penggunaannya yaitu tingginya hasil pendeteksian *False-Positive*. Hal ini membuat penulis harus merancang langkah manajemen insiden yang efektif untuk memvalidasi dan meningkatkan kemampuan deteksi dan respons dari teknologi NDR dalam mengatasi permasalahan ini. Penelitian ini bertujuan untuk membuat langkah-langkah manajemen insiden yang tepat untuk identifikasi dan respons serangan dengan efektif dan efisien beserta dengan pembuktian efisiensi langkah manajemen insiden dengan alur penggunaannya pada sebuah potensi ancaman yang terjadi di Lintasarta. Hasil penelitian ini memberikan dampak yang signifikan bagi teknologi NDR Darktrace dalam mendeteksi dan merespons berbagai macam insiden.

Kata kunci: Manajemen Insiden, *Zero-day Vulnerability*, *Behavioral Based*, *Network Detection and Response* (NDR), Darktrace.

GLOSARIUM

Akar Permasalahan	Proses investigasi untuk mencari sumber utama dari penyebab terjadinya insiden.
Analisis Log	Peninjauan dan analisis pada log aktivitas untuk memahami apa yang sedang terjadi.
Breach	Kejadian yang dimana data yang bersifat sensitif maupun system yang krusial telah diakses tanpa perizinah yang sah.
Deteksi insiden	Identifikasi bahwa sedang terjadi sebuah insiden serangan.
insiden	Peristiwa yang berpotensi untuk mengganggu operasional, keamanan, atau integritas sistem informasi pada sebuah organisasi atau perusahaan.
Threat Actor	Anggota maupun individu yang melakukan percobaan serangan pada sebuah organisasi maupun perusahaan.
Threat Hunting	Anggota yang mencari tanda-tanda potensi adanya serangan secara proaktif.
Log Aktivitas	catatan yang dibuat oleh sistem untuk mendokumentasikan semua aktivitas atau peristiwa yang terjadi dalam sistem.
Malware	jenis perangkat lunak yang dirancang untuk merusak, mengganggu, atau mendapatkan akses tidak sah ke sistem komputer.
MITRE ATT&CK	*Framework* yang dikembangkan perusahaan MITRE yang membantu dalam mengkategorikan taktik dan teknik pada serangan dari berbagai insiden.
MSSP	Sebuah perusahaan yang bertugas sebagai Penyedia Layanan Keamanan Terkelola.

DAFTAR ISI

HALAMAN JUDUL i
HALAMAN PENGESAHAN DOSEN PEMBIMBING ii
HALAMAN PENGESAHAN DOSEN PENGUJI iii
HALAMAN PERNYATAAN KEASLIAN TUGAS AKHIR iv
HALAMAN PERSEMBAHAN v
HALAMAN MOTO vi
KATA PENGANTAR vii
SARI ix
GLOSARIUM x
DAFTAR ISI xi
DAFTAR TABEL xiii
DAFTAR GAMBAR xiv
BAB 1 PENDAHULUAN 1
1.1. Latar Belakang 1
1.2. Ruang Lingkup 4
1.3. Tujuan 6
1.4. Manfaat 6
1.5. Sistematika Penulisan 6
BAB 2 LANDASAN TEORI DAN TINJAUAN PUSTAKA 8
2.1. Manajemen Insiden 8
2.2. Zero-day Vulnerability 8
2.3. Behavioural Based 9
2.4. Network Detection and Response (NDR) 9
2.5. Darktrace 10
2.6. Tinjauan Pustaka 11
BAB 3 PELAKSANAAN MAGANG 13
3.1. Manajemen Proyek 13
3.1.1. Inisialisasi Proyek 13
3.1.2. Pendefinisian Proyek 13
3.1.3. Pelaksanaan Proyek 14
3.2. Proses dan Hasil Pelaksanaan Proyek 17
3.2.1. *Detection* 17
3.2.2. *Validation* 35

3.2.3. *Containment* 39
3.2.4. *Remediation* 46
3.2.5. Hasil Percobaan Manajemen insiden 57
BAB 4 REFLEKSI PELAKSANAAN MAGANG 59
4.1. Relevansi Akademik 59
4.2. Pembelajaran Magang 61
4.2.1. Manfaat Magang 61
4.2.2. Tantangan dan Hambatan Magang 69
BAB 5 PENUTUP 72
5.1. Kesimpulan 72
5.2. Saran 72
DAFTAR PUSTAKA 74
LAMPIRAN 75

DAFTAR TABEL

Tabel 2.1 Kajian pustaka.....11
Tabel 3.1 *Syntax* validasi *Open Port*.....49
Tabel 4.1 Perbedaan Antara NTA dan NDR 62
Tabel 4.2 Perbedaan Antara IPS dan NDR.....63

DAFTAR GAMBAR

Gambar 1.1 *Gartner Peer insight* NDR 2
Gambar 1.2 Informasi Aksi Respons NDR Darktrace 3
Gambar 3.1 Metodologi Manajemen Insiden Siber 14
Gambar 3.2 Halaman Awal NDR Darktrace 16
Gambar 3.3 Tampilan Awal *Cyber AI Analyst* NDR Darktrace 19
Gambar 3.4 Tampilan MITRE ATT&CK NDR Darktrace 20
Gambar 3.5 Menu *Filters Cyber AI Analyst* NDR Darktrace 20
Gambar 3.6 Tampilan Utama *Cyber AI Analyst* NDR Darktrace 22
Gambar 3.7 Tampilan Awal *Model Breach* NDR Darktrace 23
Gambar 3.8 Menu *Model Breach* NDR Darktrace 25
Gambar 3.9 Tampilan Utama *Model Breach* NDR Darktrace 26
Gambar 3.10 Fitur Simulasi kejadi Insiden NDR Darktrace 28
Gambar 3.11 Fitur *Model Breach Event* Log NDR Darktrace 29
Gambar 3.12 Fitur *One Click Analysis* NDR Darktrace 29
Gambar 3.13 Fitur *Advance Search* NDR Darktrace 31
Gambar 3.14 Rincian Bidang Kolom *@Message Advance Search* 32
Gambar 3.15 Kustomisasi tabel *Advance Search* NDR Darktrace 34
Gambar 3.16 Menu tambahan *Advance Search* NDR Darktrace 34
Gambar 3.17 Aksi Darktrace *Respond* NDR Darktrace 40
Gambar 3.18 Konfigurasi respon otomatis NDR Darktrace 41
Gambar 3.19 Halaman utama Darktrace *Respond Action* NDR Darktrace 44
Gambar 3.20 Informasi Insiden yang ditangkap *Threat Intel* 47
Gambar 3.21 Menu ubah respons NDR Darktrace 53
Gambar 3.22 Menu mengubah *rule* NDR Darktrace 54
Gambar 3.23 Menu *Whitelist* pada NDR Darktrace 55
Gambar 3.24 Menu Pembuatan Model NDR Darktrace 56
Gambar 3.25 Grafik Mitigasi Insiden NDR Darktrace 57

BAB 1
PENDAHULUAN

1.1. Latar Belakang

Semakin majunya dunia teknologi memberikan dampak positif yang signifikan dalam dunia pekerjaan. Akan tetapi, hal tersebut juga dapat memberikan dampak negatif yang merugikan, salah satunya adalah semakin maraknya serangan siber mulai dari jenis serangan yang sudah pernah terjadi sebelumnya (*known vulberability*) sampai jenis serangan yang belum pernah terjadi sebelumnya (*unknown vulnerability*).

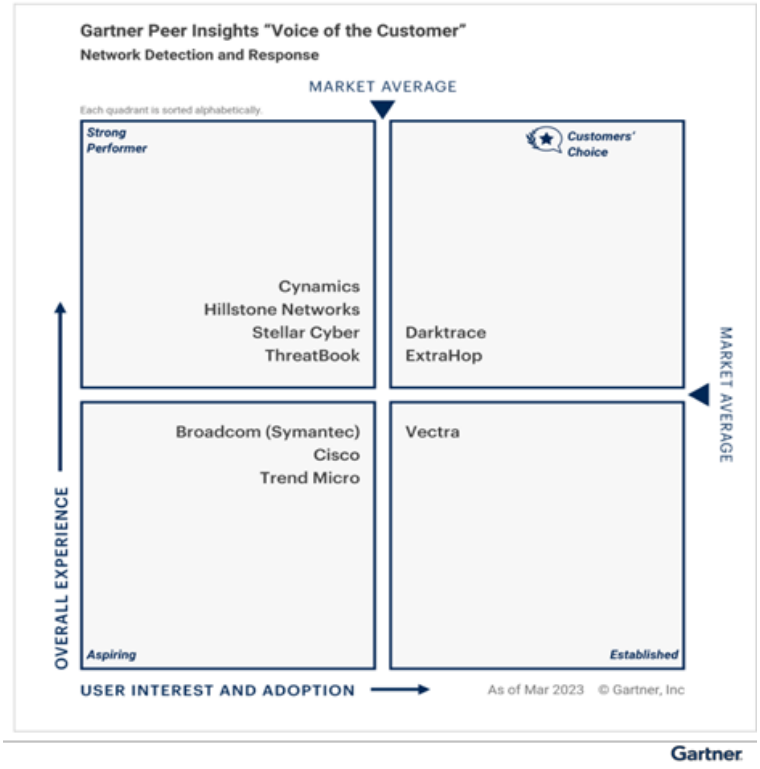
Serangan yang belum pernah terjadi biasa disebut dengan *Zero-day Attack*. *Zero-day Attack* adalah percobaan serangan dengan mengeksploitasi kerentanan yang belum pernah terjadi sebelumnya atau disebut *Zero-day Vulnerability* (Al-Rushdan et al., 2019). *Zero-day Attack* merupakan tantangan terbaru yang dialami oleh tim keamanan, hal ini dikarenakan serangan selalu terdeteksi setelah sistem disusupi, sehingga besar kemungkinan untuk menimbulkan kerugian terlebih dahulu bagi korban yang terkena serangan.

Masalah ini membuat perusahaan tidak dapat hanya mengandalkan hanya teknologi keamanan standar yang hanya dapat mendeteksi jenis serangan yang sudah diketahui (*signature-based*), seperti *Firewall, WAF, IDS/IPS, Antivirus,* dan lain sebagainya. Akan tetapi, juga memerlukan metode pendeteksian serangan yang belum diketahui. Pada permasalahan ini, teknologi siber modern saat ini sudah menggunakan *Artificial Intelligence* (AI) dan *Machine Learning* dalam melakukan pendeteksian yang disebut metode pendeteksian berbasis perilaku (*behavioural-based*).

Lintasarta sebagai sebuah perusahaan yang memberikan layanan (vendor), merancang sebuah layanan untuk mengatasi permasalahan ini. Salah satu teknologi tersebut adalah *Network Detection and Response* (NDR). NDR adalah teknologi yang dapat mendeteksi dan merespon/mitigasi ancaman secara otomatis pada tingkat jaringan (D'hoinne & Smith, 2022). NDR dikembangkan oleh berbagai macam perusahaan dengan berbagai fitur-fitur unggulan masing-masing. Lintasarta bekerja sama dengan perusahaan Darktrace dalam memberikan layanan kepada perusahaan yang membutuhkan teknologi NDR.

Darktrace sendiri adalah sebuah perusahaan keamanan yang berfokus pada keamanan siber berbasis *Artificial Intelligence* (AI) dan telah beroperasi sejak tahun 2013 (Darktrace, n.d.). Berdasarkan informasi dari *Gartner*, NDR yang dikembangkan oleh *Darktrace* menjadi

salah satu teknologi yang paling banyak digunakan oleh perusahaan di seluruh dunia karena fitur-fiturnya yang membantu dalam mendeteksi serta merespon/mitigasi serangan siber pada tingkat jaringan (Gartner, n.d.). Berikut merupakan tampilan *Gartner Peer Insight NDR* yang dapat dilihat pada gambar 1.1.



Gambar 1.1 *Gartner Peer insight* NDR

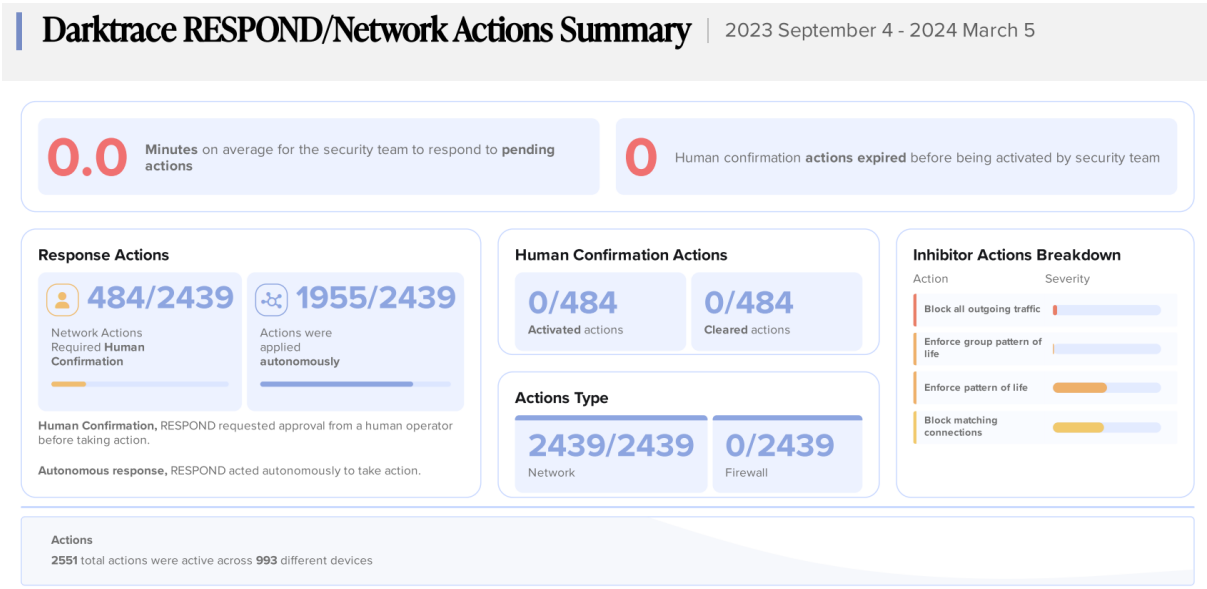
Sumber: Gartner (2023)

NDR Darktrace menggunakan *Artificial Intelligence* (AI) dan *Machine Learning* yang dikenalkan dengan sebutan *Self-Learning AI*. *Self-Learning AI* yang dikembangkan Darktrace memiliki fitur yang dapat membuat model atau aturan secara otomatis dengan mempelajari alur kerja dari Perusahaan yang dimonitoringnya sehingga dapat memberikan peringatan yang relevan dengan lingkungan perusahaan tersebut. Selain itu, NDR Darktrace dapat melakukan pencegahan atau mitigasi serangan otomatis secara *real-time* ketika mendeteksi anomali dari jaringan yang dimonitoring (Darktrace Academy, n.d.-b).

Akan tetapi, *Self-Learning AI* pada NDR Darktrace memerlukan beberapa waktu untuk mempelajari semua aset dan alur kerja pada perusahaan agar dapat bekerja secara optimal dalam mendeteksi potensi ancaman. Sehingga NDR menjadi sebuah teknologi yang tidak dapat berguna bagi perusahaan jika perusahaan tersebut baru memasang NDR ketika sedang sedang terjadi sebuah insiden pada waktu tersebut.

Selain itu, pendeteksian pada NDR dapat merupakan sebuah peringatan yang bersifat spekulatif karena lebih dominan dalam mendeteksi sebuah ancaman yang belum pernah terjadi sebelumnya. Hal ini membuat NDR berpotensi tinggi dalam memberikan sebuah peringatan palsu atau *False-Positive* yang dimana dapat mengakibatkan gangguan operasional pada perusahaan ketika hanya memanfaatkan respons serangan secara otomatis.

Permasalahan ini terjadi ketika Lintasarta menggunakan NDR Darktrace pada *environment* mereka guna untuk menguji kinerja NDR Darktrace sebelum dikomersialkan kepada calon pelanggan. Setelah beberapa bulan pengujian, tercatat bahwa aksi deteksi dan respons NDR Darktrace mencapai 2439 insiden. Dari seluruh insiden yang dimitigasi NDR Darktrace, tim SOC menyimpulkan bahwa hanya sekitar 20% insiden yang diidentifikasi sebagai sebagai serangan valid (*True-Positive*). Hal ini menjelaskan bahwa kinerja NDR Darktrace masih jauh dari sempurna jika hanya mengandalkan teknologi ini tanpa bantuan manusia dalam mengoperasikannya. Berikut merupakan informasi aksi respons dari NDR Darktrace yang dapat dilihat pada gambar 1.2.



Gambar 1.2 Informasi Aksi Respons NDR Darktrace

Walaupun tingginya hasil dari peringatan palsu (False-Negative), aksi respons serangan yang dimitigasi otomatis oleh NDR Darktrace kepada Lintasarta pada bulan-bulan awal berupa aksi respons yang tergolong tidak mengganggu kinerja karyawan Lintasarta dalam melaksanakan pekerjaannya pada perangkat mereka. Respons dominan yang dijalankan NDR Darktrace adalah respons untuk memblokir koneksi jaringan ke perangkat atau sumber tertentu

saja dan menerapkan pola perilaku dari perangkat tersebut, sehingga perangkat tersebut dapat beraktifitas berdasarkan keseharian yang dilakukannya.

Dari hal tersebut, Lintasarta menyimpulkan bahwa pembuatan langkah manajemen insiden belum menjadi prioritas dalam kasus NDR Darktrace karena banyaknya dokumen atau file yang perlu dikerjakan terlebih dahulu agar NDR Darktrace dapat dikomersialkan kepada calon pelanggan. Sampai terdapat suatu masalah krusial yang dimana terjadi pendeteksian palsu pada perangkat salah satu atasan Lintasarta.

Permasalahan terjadi ketika NDR Darktrace melakukan respons serangan secara otomatis yang membuat perangkat tersebut tidak dapat melakukan koneksi internet. Respons serangan yang dilakukan yaitu Memblokir seluruh lalu lintas jaringan yang keluar dari perangkat, sehingga perangkat tidak dapat mengakses maupun informasi apapun serta mengirimkan pesan melalui jaringan.

Hal ini terjadi ketika di luar jam kerja, sehingga pembatalan aksi respons serangan yang dilakukan NDR Darktrace tidak dilakukan dengan cepat dan membuat kerugian serta kemarahan dari atasan perusahaan. Sehingga, langkah manajemen insiden langsung dijadikan prioritas untuk dikerjakan agar insiden yang serupa tidak terjadi lagi kedepannya bagi perusahaan maupun calon pelanggan yang akan berlangganan NDR.

Manajemen insiden Siber biasanya akan dilakukan oleh tim internal maupun tim keamanan dari eksternal pada kasus yang memilih MNDR (perusahaan yang memberikan kepercayaan kepada tim Lintasarta untuk mengoperasikan NDR di perusahaan mereka) atau bisa disebut *Manage Security Service Provider* (MSSP) agar NDR Darktrace dapat bekerja secara optimal dalam memberikan hasil pendeteksian yang valid (*True-Positive*). Untuk menerapkan dan menjalankan proses ini, terdapat poin-poin yang perlu didokumentasikan pada insiden yang terdeteksi dan tim keamanan perlu memahami fitur-fitur yang disediakan NDR Darktrace agar dapat melakukan deteksi, investigasi, respons, dan konfigurasi pada poin-poin NDR Darktrace agar teknologi dapat bekerja secara optimal.

1.2. Ruang Lingkup

Pelaksanaan magang sebagai *Cyber Security* di bagian divisi pengembangan produk (*Product Development*) PT. Aplikanusa Lintasarta berlangsung selama enam bulan dan dimulai dari bulan september 2023 sampai bulan maret 2024. Proses magang dilaksanakan dengan dua metode, yaitu tiga hari melakukan *Work From Office* (WFO) dan dua hari melakukan *Work From Home* (WFH) untuk setiap pekannya.

Product development memiliki tugas untuk pada perencanaan strategis, pemasaran, dan pengelolaan siklus hidup produk dari konsep hingga akhir. Mereka harus memiliki pemahaman pada pengembangan pasar saat ini dan pengembangan strategi pemasaran untuk memastikan produk dapat mencapai keberhasilan di pasar dengan memahami kebutuhan pelanggan, merencanakan posisi produk, dan memastikan koordinasi yang baik dengan tim penjualan dan pemasaran. Selama pelaksanaan magang, penulis aktif berkontribusi dalam pengembangan lima proyek, yakni *Threat Intel*, *Network Detection and response*, *Vulnerable Category*, dan *Digital Forensic*.

Pada teknologi *Threat Intel* dilakukan sebagai bagian dari tahap pelatihan penulis untuk memahami pekerjaan yang akan dilakukan pada proyek selanjutnya. Tahap yang diikuti oleh penulis dalam proyek ini dimulai dari tahap desain utama, yang meliputi pembuatan *whitebook* tentang *work instruction* pengoperasian teknologi *Threat Intel*. Selanjutnya, penulis diminta untuk menyusun presentasi *PowerPoint* terkait *service catalog* untuk dapat dipresentasikan kepada tim *sales*. Terakhir, penulis melakukan validasi hasil dari teknologi *Threat Intel* untuk menghindari terjadinya hasil *False-Positive*.

Teknologi *Network Detection and response* merupakan pekerjaan utama yang diberikan kepada penulis selama melaksanakan kegiatan magang. Tahap yang diikuti penulis dalam proyek ini adalah mencari informasi seperti fundamental dari NDR, kelebihan dan kekurangan NDR dari berbagai *competitor*, mencari *In-Scope* dan *Out-Of-Scope*, dan hal lain yang berkaitan untuk dimasukkan kedalam *whitebook* NDR. Selanjutnya penulis diminta untuk membuat *PowerPoint* terkait *service catalog* untuk dapat dipresentasikan kepada tim *sales* dan template proposal NDR yang akan digunakan *pre-sales* untuk kebutuhan pengadaan barang. Terakhir. Pemgang ikut dalam membuat alur manajemen insiden siber pada teknologi NDR agar teknologi dapat berjalan dengan optimal.

Vulnerable Category merupakan tugas untuk membantu rekan kerja dalam melakukan analisa untuk melakukan *manual penetration testing*. Tahap yang diikuti penulis dalam proyek ini adalah ikut membantu dalam mencari informasi lengkap dari suatu jenis serangan seperti mencari *payload*, *tools*, POC, dan bukti dari serangan tersebut. Pada tugas ini terdapat lebih dari 100 jenis serangan yang dikelompokkan berdasarkan device, tujuan, dan metode serangannya. *Tools* yang digunakan pada pekerjaan ini adalah Burp Suite, Metasploit, beberapa *tools* yang ada di kali linux, dan mencoba di web yang menjadi target secara langsung.

Teknologi *Digital Forensic* merupakan tugas yang bertujuan membantu rekan kerja dalam pekerjaannya. Tahap yang diikuti penulis pada proyek ini adalah dengan membuat *work instruction* tentang teknologi untuk melakukan manajemen pada alat *Digital Forensic* yang bernama *Asgard Management Center*. Selain itu, penulis juga diminta untuk membuat untuk menyusun presentasi *PowerPoint* terkait *service catalog* untuk dapat dipresentasikan kepada tim *sales*.

1.3. Tujuan

Tujuan dibuatnya laporan tugas akhir ini adalah untuk membuat dan merangkai langkah-langkah manajemen insiden yang bisa diterapkan pada NDR Darktrace beserta dibuktikan efektivitas penggunaannya dalam sebuah kasus nyata terkait potensi insiden yang dideteksi NDR Darktrace. Hal ini dilakukan agar NDR Darktrace bisa mendeteksi dan merespons semua insiden yang dideteksi dengan langkah-langkah pencegahan yang tepat secara otomatis maupun manual pada kasus tertentu agar bisa melindungi lingkungan perusahaan dengan lebih efektif dan efisien.

1.4. Manfaat

Dari proses Implementasi ini terdapat beberapa manfaat yang diperoleh, yaitu:

a. Pengetahuan yang lebih mendalam tentang manajemen insiden siber terutama pada teknologi keamanan yang menggunakan pendeteksian berbasis perilaku.
b. Hasil dari pengimplementasian ini diharapkan dapat membantu perusahaan dalam meningkatkan keamanan, melakukan deteksi dan respon serangan secara cepat dan mengoptimalkan kinerja teknologi keamanan.

1.5. Sistematika Penulisan

Sistematika penulisan disusun untuk memberikan gambaran umum terhadap keseluruhan isi laporan. Laporan tugas akhir ini terdiri dari lima bab dengan susunan sistematika penulisan sebagai berikut :

a. BAB 1 PENDAHULUAN

   Bab ini membahas mengenai latar belakang, ruang lingkup magang, tujuan, manfaat, dan sistematika penulisan.

b. BAB 2 LANDASAN TEORI DAN TINJAUAN PUSTAKA

Bab ini membahas teori-teori yang memiliki keterikatan dengan topik laporan sebagai landasan teori dalam penyusunan laporan dan juga berisi penelitian/pekerjaan apa saja yang sudah dilakukan dari berbagai referensi makalah yang relevan dengan topik laporan.

c. BAB 3 PELAKSANAAN MAGANG

Bab ini berisikan tahapan dalam pelaksanaan magang, manajemen proyek yang dikerjakan dan bukti dari hasil terkait proyek yang dikerjakan.

d. BAB 4 REFLEKSI PELAKSANAAN MAGANG

Bab ini menguraikan hasil refleksi yang penulis dapat selama pelaksanaan magang di PT. Aplikanusa Lintasarta dari sisi teknis maupun non-teknis.

e. BAB 5 KESIMPULAN DAN SARAN

Bab ini berisikan kesimpulan dalam pengerjaan proyek dan saran dari penulis selama proses kegiatan magang.

BAB 2
LANDASAN TEORI DAN TINJAUAN PUSTAKA

2.1. Manajemen Insiden

Manajemen Insiden merupakan sebuah proses yang digunakan untuk menerima dan menerjemahkan sebuah permasalahan atau insiden, lalu mendapatkan dan mengumpulkan informasi yang diperlukan agar bisa segera diselesaikan sampai kasus permasalahan dapat ditutup. Manajemen Insiden dapat membantu organisasi dalam menangani berbagai macam kasus TI yang sudah dilaporkan agar bisa segera ditanggulangi segala penyebab permasalahannya (Vira et al., 2022).

Dalam konteks keamanan siber, Manajemen Insiden terbagi menjadi beberapa tahapan, yaitu *Detection*, *Validation*, *Containment*, dan *Recovery*. Dalam pelaksanaannya, Manajemen Insiden mengandalkan *tools* dan fitur-fitur yang dirancang khusus dalam suatu teknologi untuk membantu organisasi menangani insiden keamanan dengan lebih efektif dan efisien. Dengan menggunakan tahapan ini, organisasi dapat meningkatkan respons terhadap ancaman, mengurangi dampak insiden, dan memulihkan sistem keamanan mereka dengan lebih cepat dan tepat.

2.2. Zero-day Vulnerability

Zero-day Vulnerabilty adalah kerentanan pada perangkat lunak maupun perangkat keras yang sebelumnya tidak diketahui dan dapat di eksploitasi oleh *Threat Actor* sebelum tim keamanan memiliki kesempatan untuk mengeluarkan perbaikan. Dengan demikian, *Zero-day Vulnerability* menjadi sebuah ancaman serangan yang dimana tim keamanan memiliki waktu nol hari untuk merespons dan menerapkan perbaikan setelah pemberitahuan adanya indikasi serangan (Prakash, 2023).

Serangan ini menjadi tantangan terberat yang dialami oleh tim keamanan karena teknologi keamanan tradisional tidak mampu mendeteksi serangan yang belum pernah terdaftar dalam sistem mereka. Oleh karena itu, diperlukan teknologi yang mampu mendeteksi serangan *zero-day vulnerability* agar bisnis dapat bertahan pada era digital saat ini.

2.3. Behavioural Based

Behavioral based atau yang biasa dibilang pendeteksian berbasis perilaku merupakan sebuah metode *Dynamic Analysis* yang bertujuan untuk mempelajari dan memahami perilaku sebuah *malware*. Pendekatan *Behavioral based* tidak bergantung pada pola atau tanda-tanda yang telah diketahui sebelumnya, melainkan secara langsung menganalisis log aktivitas dan mengidentifikasi perilaku yang mencurigakan atau tidak biasa secara *real-time* (Muhtadi et al., 2019).

2.4. Network Detection and Response (NDR)

Network Detection and Response (NDR) adalah sebuah teknologi yang dapat mendeteksi perilaku tidak normal dengan menggunakan deteksi berbasis perilaku pada lalu lintas jaringan yang di monitor (D'hoinne & Smith, 2022). NDR memiliki peran serupa dengan *Intrusion Prevention System* (IPS) yang melakukan analisis pesan atau log dari data mentah antara jaringan internal dan jaringan publik (Denny S et al., 2017).

Perbedaan utama antara NDR dan IPS adalah metode deteksinya. NDR menggunakan metode deteksi berbasis perilaku, sementara IPS menggunakan metode deteksi berbasis informasi sebelumnya. Oleh karena itu, walaupun NDR dan IPS memiliki tugas pendeteksian dalam ranah yang sama, mereka memiliki tujuan dan langkah pencegahan yang berbeda. Untuk mengikuti perkembangan saat ini, ada beberapa kemampuan inti yang dapat dilakukan oleh NDR, yaitu:

a. NDR memiliki kemampuan untuk mengumpulkan aktivitas dari data mentah pada lalu lintas jaringan secara cermat dan terperinci. NDR dapat melakukan pemantauan secara *real-time* berdasarkan sumber dari internal maupun eksternal. Fungsi dari melakukan analisis data mentah adalah agar NDR dapat mengidentifikasi pola-pola perilaku yang mencurigakan atau tidak biasa yang mungkin tidak dapat dideteksi oleh teknologi lainnya.
b. NDR dapat melakukan pengayaan metadata menggunakan informasi dari pengguna, *IP Address*, jenis protokol, dan lainnya pada saat melakukan transaksi atau interaksi dalam jaringan. Dengan adanya pengayaan metadata, NDR dapat menggali informasi tambahan yang relevan dari data mentah pada lalu lintas jaringan.
c. NDR memiliki kemampuan untuk melakukan monitoring jaringan, baik perusahaan yang menggunakan jaringan lokal maupun perusahaan yang menggunakan infrastruktur berbasis *cloud*.

d. NDR memanfaatkan *Artificial Intelligence* (AI) dan *Machine Learning* untuk membantunya dalam melakukan analisis dan pemahaman pola-pola kompleks dalam lalu lintas jaringan yang sering kali sulit dideteksi oleh manusia. Dengan memanfaatkan teknologi ini, NDR dapat terus belajar untuk mengidentifikasi perilaku abnormal dan secara proaktif menghasilkan peringatan atau tindakan respons yang sesuai terhadap ancaman keamanan yang sedang berkembang.
e. NDR dapat melakukan *enrichment* pada peringatan insiden dengan menggabungkan informasi tambahan dari berbagai sumber. *Enrichment* pada teknologi NDR menggunakan data historis dan tren keamanan pada rentang waktu tertentu, sehingga dapat membantu tim analis dalam mempelajari pola-pola ancaman yang muncul dari waktu ke waktu.
f. NDR memiliki kemampuan untuk melakukan respon serangan secara otomatis berdasarkan hasil pembelajaran teknologi tersebut. Dengan adanya fitur ini, NDR dapat melakukan tindakan pencegahan utama pada potensi ancaman sehingga dapat meminimalkan kerusakan yang ditimbulkan oleh serangan dan mengurangi beban kerja bagi tim keamanan dalam menangani insiden keamanan.

2.5. Darktrace

Darktrace adalah perusahaan keamanan siber yang menyediakan solusi komprehensif untuk melindungi aset penting perusahaan dengan memanfaatkan teknologi *Artificial Intelligence (AI)* dan *Machine Learning*. Darktrace sudah berdiri sejak tahun 2013 oleh sekelompok pakar matematika dan pertahanan siber. Darktrace memiliki tujuan untuk membebaskan seluruh dunia dari berbagai jenis serangan siber (Darktrace, n.d.).

Darktrace tidak hanya menyediakan perlindungan yang kuat terhadap berbagai serangan siber, tetapi juga menawarkan solusi yang dapat menangani berbagai aspek keamanan dalam lingkungan perusahaan. produk keamanan siber yang ditawarkan oleh Darktrace dibagi menjadi beberapa bagian berdasarkan fungsinya, yaitu Darktrace *PREVENT*, *DETECT*, *RESPOND*, dan *HEAL*. Setiap produk tersebut dirancang untuk melindungi beberapa area cakupan, seperti *Cloud*, *Apps*, *Email*, *Endpoint*, *Network*, dan *Operational Technology* (OT) (Darktrace, n.d.).

2.6. Tinjauan Pustaka

Kajian terhadap beberapa pustaka yang disajikan pada Tabel 2.1 berisi tentang uraian singkat mengenai masalah yang ada pada beberapa penelitian dan juga hasil atau solusi yang didapatkan. Adanya kajian Pustaka ini bertujuan untuk mencari keterkaitan dan referensi terkait proyek yang dikerjakan.

Tabel 2.1 Kajian pustaka

No	Nama Penulis	Judul	Uraian Singkat	Hasil
1	Ahmad, A., Desouka, K., Manynard, S., Naseer, H. & Baskerville, R. (2019)	*How integration of cyber security management and incident response enables organizational learning*	Penelitian ini membahas tentang melakukan integrasi manajemen keamanan siber dan respons insiden untuk meningkatkan pembelajaran organisasi.	Hasil menunjukkan bahwa integrasi ini meningkatkan efektivitas dan efisiensi dalam manajemen insiden siber.
2	Patterson, C., Nurse, J. & Fransqueira, V.	*Learning from cyber security incidents: A systematic review and future research agenda*	Penelitian ini mengkaji tentang *framework* NIST 800-61 untuk evaluasi respons insiden siber di sebuah organisasi. Kerangka ini digunakan berguna untuk meningkatkan fungsi kriteria respons insiden keamanan.	Hasil dari penelitian ini adalah pembuktian bahwa penerapan *framework* yang dikembangkan tersebut dapat meningkatkan efektivitas manajemen insiden siber dan penulis menyarankan untuk diterapkan secara luas dalam industri.
3	Cao C, & Zhan, Z,	*Incident management process for the cloud computing environments*	Penelitian ini membahas tentang pentingnya proses manajemen insiden yang efektif dalam lingkungan cloud computing. Penelitian ini merangkai sebuah *framework* manajemen insiden yang disesuaikan dengan tantangan dan karakteristik unik dari lingkungan cloud itu sendiri.	penulis menghasilkan sebuah framework manajemen insiden yang sesuai pada lingkungan cloud. Framework yang dikembangkan berisi panduan tentang bagaimana mengatasi masalah tentang ketergantungan pada penyedia cloud dalam mengelola insiden siber.

Berdasarkan Tabel 2.1 dapat disimpulkan bahwa semua penelitian tersebut tidak bisa langsung dibilang memiliki keterkaitan dengan proyek pada Tugas Akhir ini, Akan tetapi penelitian tersebut dapat menjadi referensi penting dalam pembuatan Tugas Akhir ini. Salah satu alasannya yaitu, pada penelitian satu membuat pemahaman bahwa teknologi keamanan itu tidak bisa berdiri sendiri, Hal ini didasarkan dengan dikarenakan setiap teknologi memiliki batasan dalam melakukan deteksi, sehingga ada kemungkinan terjadinya sebuah insiden tanpa terdeteksi oleh alat keamanan tersebut. Oleh karena itu, diperlukannya kinerja dari teknologi keamanan lain untuk menutup batasan tersebut dalam mendeteksi dan merespon insiden.

Selain itu, pada penelitian dua dan tiga dapat dilihat bahwa memiliki metodologi yang berbeda. Akan tetapi, kedua penelitian tersebut memiliki keterkaitan dengan Tugas Akhir yang dibuat, yaitu membuat alur atau langkah dalam yang bertujuan untuk meningkatkan fungsi dari respons berbagai macam insiden dari suatu teknologi menggunakan suatu kerangka kerja.

BAB 3
PELAKSANAAN MAGANG

3.1. Manajemen Proyek

Tahapan manajemen proyek yang dilakukan dalam pelaksanaan untuk operasi dan pembuatan alur manajemen insiden siber pada teknologi NDR Darktrace adalah sebagai berikut:

3.1.1. Inisialisasi Proyek

Sebelum melangkah lebih jauh dalam proses terkait NDR Darktrace, penting untuk memahami fundamental dari NDR terlebih dahulu. Fundamental dari NDR yang perlu dipahami adalah pemahaman lebih tentang apa itu NDR, perbedaan NDR dengan teknologi keamanan lainnya, dan fitur-fitur yang dimiliki NDR dalam melakukan tugasnya dalam melakukan monitoring. Dengan memahami secara komprehensif terkait fungsi dan peran NDR dalam mengamankan aset perusahaan, maka dapat ditentukan apa kemungkinan permasalahan yang dapat terjadi dan gambaran cara penyelesaian masalah tersebut.

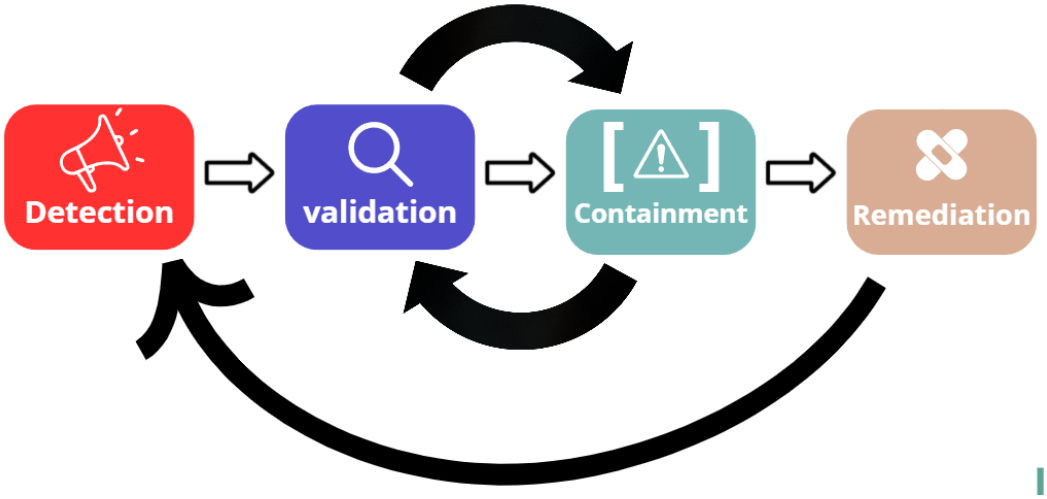
3.1.2. Pendefinisian Proyek

Setelah tahap inisialisasi proyek, langkah selanjutnya adalah pendefinisian proyek manajemen insiden siber pada teknologi NDR Darktrace. NDR Darktrace merupakan sebuah teknologi yang bertugas untuk mengamankan serangan siber pada lalu lintas jaringan dengan memanfaatkan *Artificial Intelligence* (AI) dan *Machine Learning* yang dikembangkan oleh perusahaan Darktrace. Dengan teknologi ini, perusahaan dapat mengamankan berbagai potensi ancaman normal maupun yang bersifat abnormal.

Akan tetapi, penggunaan pendeteksian yang mengandalkan *Artificial Intelligence* (AI) dan *Machine Learning* memberikan peringatan yang bersifat prediktif, membuat teknologi ini memiliki kemungkinan untuk memberikan hasil *False-Positive* yang dapat merugikan kegiatan operasional perusahaan. Dari permasalahan tersebut, maka diperlukan manajemen insiden siber yang efektif untuk menghindari hal tersebut.

3.1.3. Pelaksanaan Proyek

Proses manajemen insiden siber akan diterapkan secara berulang ketika teknologi NDR Darktrace mendeteksi sebuah potensi ancaman. Ketika suatu ancaman terdeteksi, maka tim keamanan akan melakukan Manajemen Insiden untuk memvalidasi serangan dan mengambil langkah untuk memitigasi serangan yang paling tepat. Metodologi yang digunakan pada manajemen insiden ini adalah metodologi yang dikembangkan Lintasarta dengan referensi dari metodologi NIST800-61 (Cichonski et al., 2012). Berikut merupakan gambar metodologi manajemen insiden siber yang dapat dilihat pada gambar 3.1.



Gambar 3.1 Metodologi Manajemen Insiden Siber

Implementasi pada proses manajemen insiden dilakukan melalui beberapa tahap yang terstruktur ketika NDR Darktrace mendeteksi adanya sebuah anomali pada jaringan yang masuk ke alat NDR. Berikut adalah langkah-langkah implementasi manajemen insiden yang dijalankan:

a. *Detection*

Fase pertama adalah fase yang dimana teknologi NDR Darktrace mengidentifikasi adanya indikasi atau bukti terjadinya serangan atau insiden keamanan di dalam lingkungan jaringan atau sistem perusahaan. Pada fase ini, tim keamanan akan langsung mulai menganalisis apa yang sedang terjadi pada sistem perusahaan agar bisa dilakukannya mitigasi sebelum mengalami kerugian lebih jauh.

Alat keamanan saat ini umumnya memberikan peringatan dan memberitahu apa yang terjadi berdasarkan anomali untuk mendeteksi serangan abnormal serta temuan dari pola-pola serangan yang sudah pernah terjadi di sebelumnya. Dengan memanfaatkan fitur ini, maka dapat membantu tim keamanan dalam mendeteksi dan mengetahui ancaman yang terjadi dengan cepat dan tepat.

b. *Validation*

Validation adalah fase dimana tim keamanan akan melakukan identifikasi terhadap suatu insiden yang muncul berdasarkan informasi yang ditemukan pada fase *Detection*. Tujuan dari fase ini adalah untuk memastikan bahwa peringatan yang diterima pada fase sebelumnya adalah valid *(True-Positive*). Pada tahap ini, tim keamanan dapat menentukan apakah suatu ancaman perlu ditindak lanjuti atau perlu untuk memperbaiki metode deteksi pada teknologi keamanan.

c. Containment

Containment adalah fase untuk melakukan mitigasi atau respons terhadap suatu serangan yang sudah divalidasi pada fase sebelumnya. Tujuan dari fase ini adalah untuk mencegah penyebaran lebih lanjut dari suatu insiden, membatasi kerusakan yang mungkin terjadi, serta memastikan bahwa langkah pencegahan yang diterapkan sudah dapat melindungi aset perusahaan dari percobaan serangan tersebut.

d. Remediation

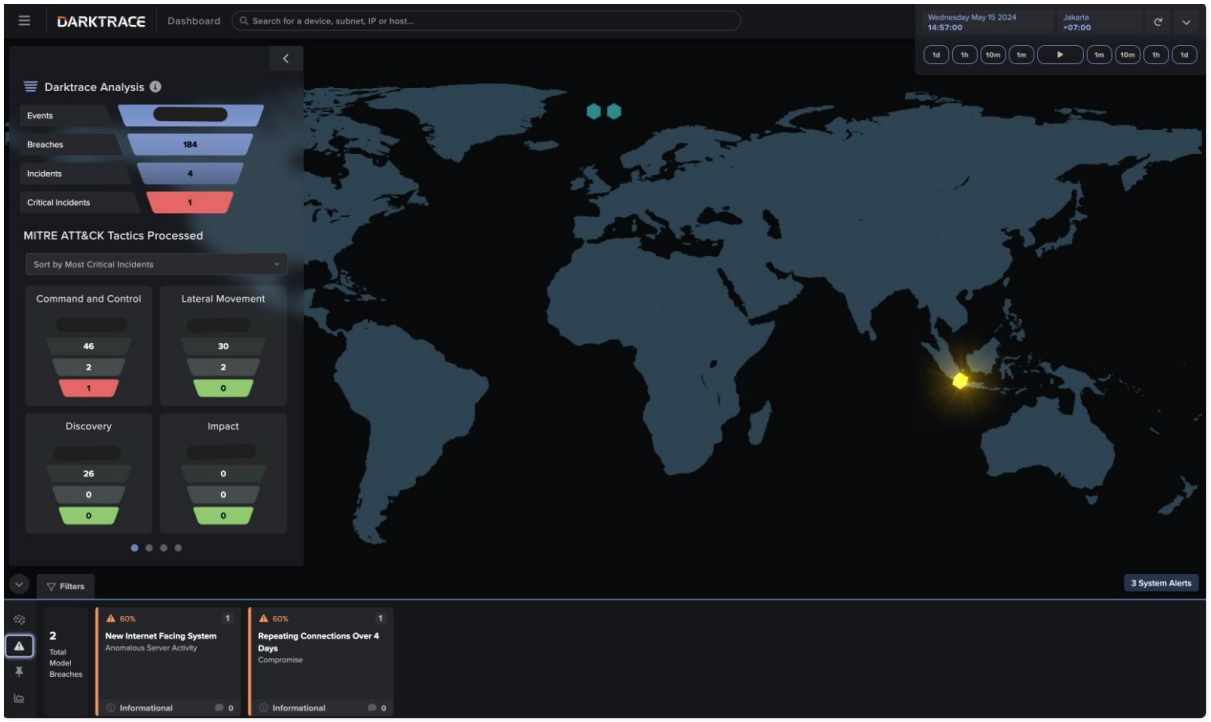
Remediation adalah fase yang diambil setelah serangan keamanan atau insiden keamanan telah ditangani dengan baik. Tujuan dari tahap ini adalah untuk memperbaiki celah kerentanan pada aset TI perusahaan serta meningkatkan metode pendeteksian dari teknologi keamanan yang digunakan perusahaan agar memberikan informasi yang lebih akurat pada serangan yang serupa di masa depan.

Dalam mendukung dan membuktikan efektivitas dari penerapan manajemen insiden yang dibuat, Laporan dari setiap proses akan dibuktikan dengan sebuah penjelasan dari sebuah kasus nyata dari perusahaan Lintasarta. Insiden yang diambil adalah salah satu insiden yang dideteksi pada NDR Darktrace pada saat penulis sudah selesai membuat alur manajemen insiden yang diharapkan dapat membantu tim keamanan Lintasarta untuk mengoperasikan NDR Darktrace dengan baik.

Pada proses penentuan langkah manajemen insiden siber pada teknologi NDR Darktrace, terdapat beberapa *tools* pendukung yang membantu proses pengerjaan dapat berhasil dengan yang diinginkan. Berikut merupakan *tools* yang digunakan dalam pembuatan manajemen insiden siber:

a. NDR Darktrace

NDR Darktrace memiliki berbagai fitur yang membantu tim keamanan dalam mengkonfigurasi dan mengelola hasil pendeteksian ancaman siber secara efektif. Fitur-fitur konfigurasi yang disediakan oleh Darktrace bersifat fleksibel, yang dimana memungkinkan tim keamanan untuk memperbaiki beberapa *rules* maupun model yang dibuat oleh NDR secara manual. Selain itu, tim keamanan dapat menyesuaikan konfigurasi *Artificial Intelligence* (AI) dan *Machine Learning* sesuai dengan keinginan perusahaan. Berikut merupakan Tampilan awal NDR Darktrace yang dapat dilihat pada gambar 3.2.



Gambar 3.2 Halaman Awal NDR Darktrace

b. Microsoft Word

Microsoft Word digunakan sebagai media dokumentasi untuk membuat *work instruction* dalam pembuatan alur manajemen insiden siber pada teknologi NDR Darktrace. *Work instruction* merupakan laporan yang berisi tentang panduan cara melakukan suatu hal agar dapat selesai sesuai dengan yang diharapkan. Pada work instruction ini diharapkan tim keamanan yang mengoperasikan NDR Darktrace dapat memahami apa yang perlu mereka lakukan ketika terjadi suatu insiden pada perusahaan.

c. Microsoft Teams

Microsoft Teams digunakan sebagai media komunikasi secara daring untuk membahas terkait progres hasil kerja setiap individu. Selain itu, Microsoft Teams membantu dalam konsultasi daring terkait alur pekerjaan membingungkan dan perlu diperbaiki agar alur pekerjaan seusai yang diinginkan perusahaan.

3.2. Proses dan Hasil Pelaksanaan Proyek

Pembuatan langkah-langkah alur manajemen insiden siber menggunakan teknologi NDR Darktrace beserta penjelasan dari setiap hasil pada saat melakukan uji coba manajemen insiden yang penulis kerjakan akan dibagi dalam beberapa tahapan. Berikut merupakan penjelasan lengkap yang berkaitan dengan tahapan-tahapannya:

3.2.1. *Detection*

Pada fase pertama, NDR Darktrace akan memberikan sebuah peringatan tentang adanya anomali dari log jaringan yang sedang dimonitor. NDR Darktrace dilengkapi dengan beberapa fitur pendukung untuk melihat dan memahami apa yang terjadi secara lebih mendalam. Setiap metode deteksi memiliki keunggulan dan dapat saling membantu dalam memahami situasi serangan yang sedang terjadi.

Pada kasus nyata yang terjadi di Lintasarta, NDR Darktrace mendeteksinya adanya potensi serangan pada tanggal 27 November 2023. NDR Darktrace membuat title serangan *Device / Attack and Recon Tools*. Berdasarkan title dari serangan tersebut, dapat disimpulkan bahwa adanya sebuah aktivitas yang mencurigakan. Aktivitas ini merupakan aktivitas yang dimana penyerang berusaha untuk mengumpulkan informasi tentang target sebelum mereka melancarkan serangan yang lebih berbahaya berdasarkan celah yang dia dapat dari perusahaan tersebut.

Hal ini didetesi NDR Darktrace karena server CRM Lintasarta yang tidak pernah melakukan koneksi mencurigakan tiba-tiba melakukan *HTTP Request* ke server CSWS yang mengandung user agent NMAP di dalam *syntaxnya*. Dari informasi dasar ini, tim keamanan sudah dapat memahami apa yang sedang terjadi dan potensialnya serangan jika insiden ini bersifat valid.

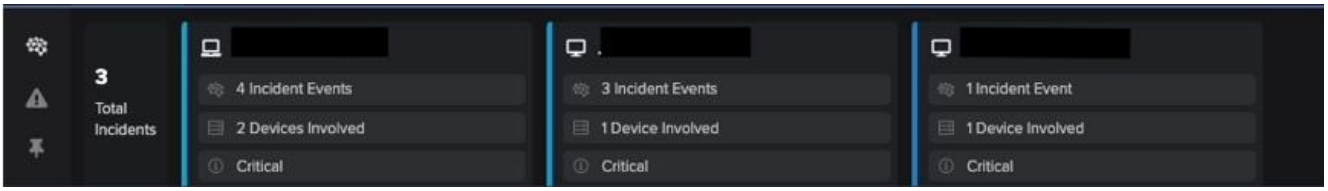
Jika insiden ini emang dilakukan oleh penyerang, maka Lintasarta akan mendapatkan kerugian yang lebih jauh lagi. Hal ini terjadi karena *reconnaissance* merupakan sebuah langkah awal dimana penyerang berusaha mencari celah / kerentanan dari perusahaan agar mereka dapat melakukan akses tidak sah, pencurian data perusahaan, bahkan sampai membuat kerusakan pada sistem perusahaan.

Serta hal ini juga dapat berdampak buruk bagi kepercayaan dan kepuasan pelanggan dikarenakan Lintasarta sendiri adalah sebuah perusahaan yang memberikan layanan kepada perusahaan lain (vendor). Yang dimana hal ini dapat membuat ragu bagi pelanggan yang berlangganan maupun akan berlangganan kepada Lintasarta karena perlu dipertanyakan terkait integritas dan keandalan perusahaan dalam melaksanakan tugasnya.

Untuk dapat melakukan validasi dari ancaman yang dideteksi, tim keamanan harus mencari dan mengumpulkan informasi sebanyak mungkin yang berkaitan dengan insiden ini. NDR Darktrace memiliki fitur yang lengkap dalam mengatasi permasalahan ini, dari sini penulis sudah membuat alur dari setiap fitur yang harus dilihat dan dipahami oleh tim keamanan agar dapat memberikan konteks pemahaman yang lebih dan pengumpulan informasi secara mendetail untuk keperluan pada fase *validation*. Berikut merupakan alur metode pendeteksian yang perlu dilakukan tim keamanan pada teknologi NDR Darktrace:

a. *General Incidents*

NDR Darktrace dapat mendeteksi sebuah insiden berdasarkan anomali secara *real-time*. Ketika tim keamanan mendapatkan peringatan tentang adanya serangan, disarankan untuk mengakses *Cyber AI Analyst* pada halaman utama NDR Darktrace. *Cyber AI Analyst* merupakan langkah utama yang perlu dilihat karena fitur ini dapat menampilkan semua insiden yang dideteksi oleh NDR Darktrace, sehingga tim keamanan bisa segera melakukan analisis dan penyelidikan tentang apa yang sedang terjadi. Berikut merupakan tampilan awal *Cyber AI Analyst* NDR Darktrace yang dapat dilihat pada gambar 3.3.

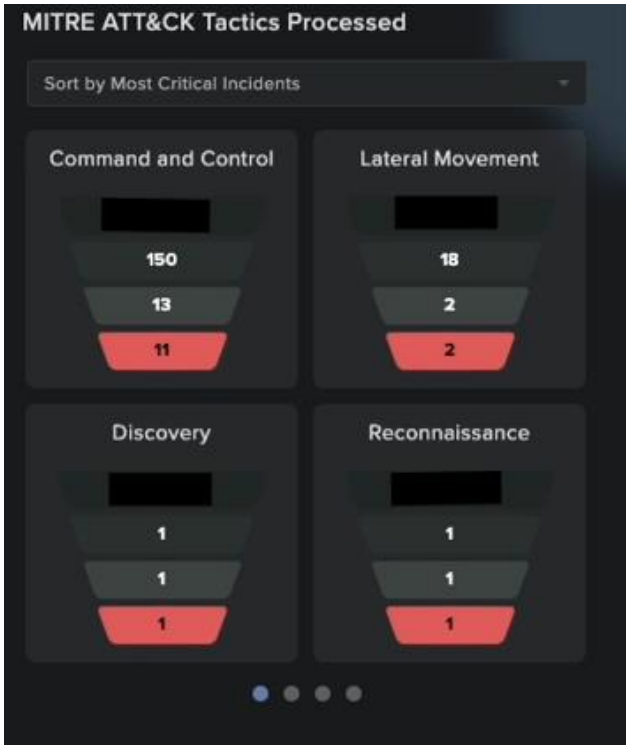


Gambar 3.3 Tampilan Awal *Cyber AI Analyst* NDR Darktrace

Tampilan *Cyber AI Analyst* pada halaman awal NDR Darktrace memberikan empat informasi terkait insiden apa yang terjadi. Informasi dapat berupa sebagai berikut:

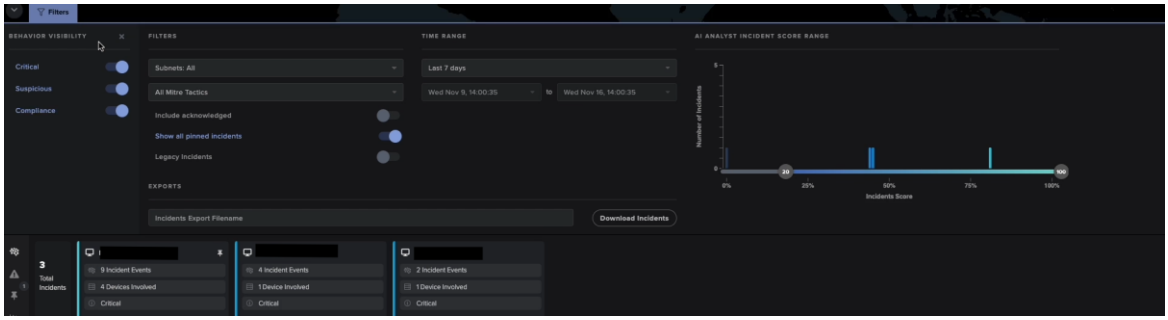
i. Informasi pada baris pertama adalah jenis perangkat yang diserang. Selain jenis perangkat, pada baris pertama juga menampilkan nama dari perangkat tersebut beserta persentase potensi bahayanya dari serangan tersebut.
ii. *Incident Events* menampilkan jumlah insiden yang terjadi pada device tersebut dalam rentang waktu yang sudah ditentukan.
iii. *Device Involved* memberitahukan informasi terkait jumlah perangkat yang terlibat pada insiden.
iv. Pada baris terakhir adalah informasi tentang kategori dari serangan tersebut. Pada kategori serangan, terdapat tiga kemungkinan hasil yaitu *Critical*, *Suspicious*, dan *Compliance*.

Cyber AI Analyst sudah terintegrasi dengan MITRE ATT&CK *framework*. MITRE ATT&CK adalah sebuah *framework* yang mengkategorikan berbagai taktik dan teknik serangan siber berdasarkan pengamatan serangan di dunia nyata (MITRE, n.d.). Pada saat ini MITRE ATT&CK sudah mengkategorikan 14 taktik dan 350 jenis serangan siber di seluruh dunia. Dengan MITRE ATT&CK, tim keamanan akan lebih mudah dalam memahami bagaimana penyerang bekerja, mengidentifikasi celah keamanan, serta mengembangkan strategi pertahanan yang lebih efektif. Berikut merupakan tampilan MITRE ATT&CK NDR Darktrace yang dapat dilihat pada gambar 3.4.



Gambar 3.4 Tampilan MITRE ATT&CK NDR Darktrace

Walaupun *Cyber AI Analyst* sudah menampilkan serangan yang relevan, tim keamanan dapat memperkecil maupun memperbesar list anomali serangan yang dideteksi oleh NDR Darktrace menggunakan fitur *filters*. Pada fitur *filters*, dapat membantu dalam mengkategorikan dan mencari serangan yang paling krusial bagi perusahaan agar bisa di mitigasi secepat mungkin sebelum menyebabkan kerugian yang lebih jauh. Berikut merupakan tampilan filters Cyber AI Analyst NDR Darktrace yang dapat dilihat pada gambar 3.5.



Gambar 3.5 Menu *Filters Cyber AI Analyst* NDR Darktrace

Pada menu filter, terdapat beberapa opsi pilihan yang berguna untuk membantu tim keamanan dalam mencari jenis serangan yang diinginkan. Berikut merupakan jenis *filters* yang dapat diterapkan pada *Cyber AI Analyst*:

i. *Subnet* dapat berguna untuk memperkecil maupun memperluas lokasi perusahaan yang akan diperlihatkan pada *Cyber AI Analyst*. Untuk mempermudah dalam melihat lokasi subnet yang ada indikasi serangan, lihat pada bangunan kubus pada halaman awal NDR Darktrace. NDR Darktrace membagi warna kubus subnet menjadi tiga kategori, untuk warna biru atau ungu mengindikasikan bahwa subnet tersebut tidak ada anomali, warna kuning atau oranye atau merah mengindikasikan ada anomali, dan warna hijau mengindikasikan bahwa subnet tersebut sudah dilakukan tindakan respons serangan.

ii. Mitre *Tactics* berfungsi untuk menampilkan jenis serangan berdasarkan taktik serangan dari insiden yang ditemukan NDR Darktrace. Taktik yang disediakan sudah terintegrasi dengan MITRE ATT&CK yang berjumlah 14 taktik.

iii. *Time Range* berfungsi untuk menampilkan serangan pada rentang waktu yang ditentukan. Untuk informasi penentuan rentang waktu yang tepat, pada perusahaan dalam skala besar, disarankan untuk memilih rentang waktu tiga hari atau dibawahnya untuk mempermudah dalam membaca dan memahami serangan apa yang terjadi. Sedangkan pada perusahaan skala kecil, disarankan untuk memilih rentang waktu tujuh hari agar lebih mudah memahami apa yang sedang terjadi secara lebih mendalam.

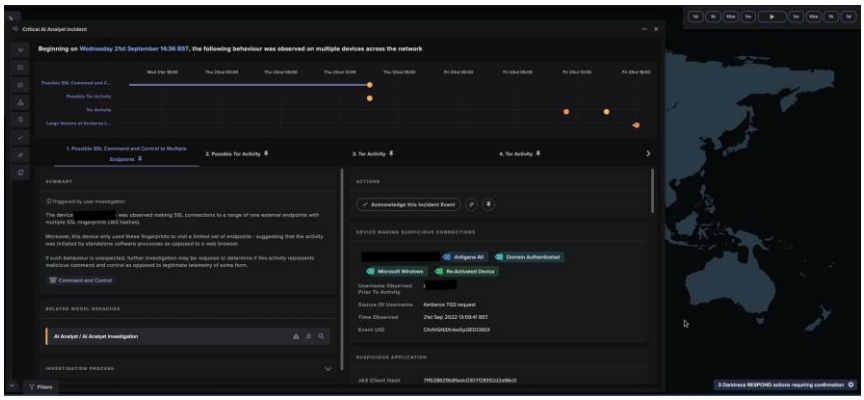
iv. *Score Range* berfungsi untuk menampilkan rentang skor serangan pada suatu insiden. NDR Darktrace dapat secara otomatis menentukan skor sebuah serangan itu berpotensi atau tidak menggunakan *enrichment* data yang ditawarkan dalam bentuk persentase. Pada tabel *Score Range*, adanya indikasi serangan dapat dilihat pada garis yang vertikal untuk memudah dalam mengetahui adanya serangan dan persentase serangan dengan lebih cepat pada rentang waktu tersebut.

v. *Include acknowledged* berfungsi untuk melihat jenis serangan yang sudah dilakukan respond dan mitigasi oleh tim keamanan.

vi. *Show all Pinned incident* berfungsi untuk melihat semua jenis serangan yang sudah disimpan oleh tim keamanan sebelumnya. Dengan ini, tim keamanan tetap dapat melihat jenis serangan *acknowledged* tanpa terpengaruh oleh rentang waktu yang telah ditentukan sebelumnya.

vii. *Legacy Incidents* akan menampilkan semua insiden bahkan insiden yang sudah lama dalam rentang waktu tiga bulan sehingga time range pada fitur sebelumnya tidak berfungsi.

Setelah menentukan sebuah insiden yang perlu untuk perlu untuk diinvestigasi, tim keamanan akan diarahkan ke menu utama dari *Cyber AI Analyst*. Pada fitur ini, terdapat beberapa informasi penting terkait peristiwa insiden yang dipilih. Dengan informasi yang diberikan, tim keamanan mendapatkan gambaran apa yang sedang terjadi dan perangkat yang berkaitan dengan serangan tersebut. Berikut merupakan tampilan utama *Cyber AI Analyst* NDR Darktrace yang dapat dilihat pada gambar 3.6.



Gambar 3.6 Tampilan Utama *Cyber AI Analyst* NDR Darktrace

Pada menu halaman utama, terdapat informasi lengkap terkait insiden yang terjadi pada device tersebut dalam rentang waktu tertentu. Berikut merupakan penjelasan tentang tentang informasi yang diberikan pada halaman utama *Cyber AI Analyst* NDR Darktrace:

i. *Range Time* menampilkan insiden-insiden yang terjadi pada perangkat. Setiap insiden waktu tertentu akan ditampilkan dengan bulatan berwarna kuning. Semakin berwarna merah bulatan mengindikasikan bahwa serangan tersebut lebih berpotensi bahaya.

ii. Setelah itu terdapat menu yang menampilkan kategori insiden apa yang terjadi pada perangkat. Setiap kategori yang dipilih, maka pada menu dibawahnya akan menampilkan hasil yang sesuai dengan kategori tersebut.

iii. Pada menu *summary* akan menampilkan secara singkat tentang insiden yang dipilih pada kategori insiden. Selain itu, pada menu *summary* juga menampilkan taktik dari MITTRE ATT&Ck yang sesuai dari serangan tersebut.

iv. Menu *Related Model breaches* menampilkan informasi terkait model insiden apa yang terjadi sehingga anomali tersebut bisa dikategorikan sebagai insiden. Model

insiden adalah *rules* yang mengkategorikan bahwa suatu log bisa memberikan peringatan insiden. Model insiden dapat dibuat secara otomatis oleh NDR Darktrace itu sendiri maupun secara manual.

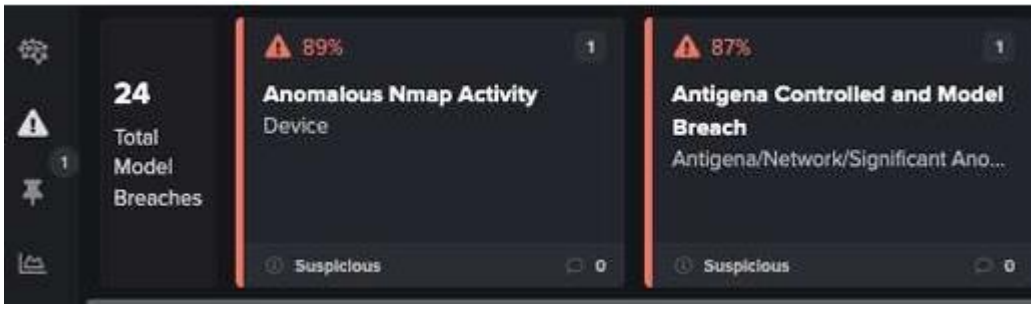
v. Menu action adalah beberapa aksi yang bisa kita lakukan pada informasi yang diberikan *Cyber AI Analyst*. Aksi yang dapat dilakukan adalah membuat serangan tersebut menjadi *acknowledge* sehingga tidak memberikan peringatan, membuat semua serangan yang serupa seperti kategori serangan tersebut menjadi *acknowledge*, dan menyimpan serangan tersebut agar bisa dianalisis dan diinvestigasi kapanpun tanpa perlu peduli rentang waktu kapan pun.

vi. Menu *Device Making Suspicious Connection* menampilkan informasi detail terkait perangkat yang melanggar model insiden.

vii. Menu *Suspicious Application* memberikan informasi terkait aplikasi yang membuat perangkat melanggar model insiden dan menu *Suspicious Endpoints Contacted by Applications* memberikan informasi tentang perangkat yang berhubungan dengan perangkat korban, sehingga menghasilkan peringatan insiden.

b. *Deep Understanding of incident*

Setelah memahami tentang apa yang terjadi dari *Cyber AI Analyst*, tim keamanan dapat mencari akar dari permasalahan menggunakan fitur dari NDR Darktrace yang bernama *Model Breach*. *Model Breach* adalah fitur lanjutan dari *Cyber AI Analyst* yang dimana memberikan semua rincian informasi terkait adanya suatu potensi serangan. Dengan *Model Breach*, tim keamanan bisa mencari bukti apakah anomali tersebut merupakan sebuah insiden atau tidak (*False-Positive*). Berikut merupakan tampilan awal dari Model breach yang dapat dilihat pada gambar 3.7.

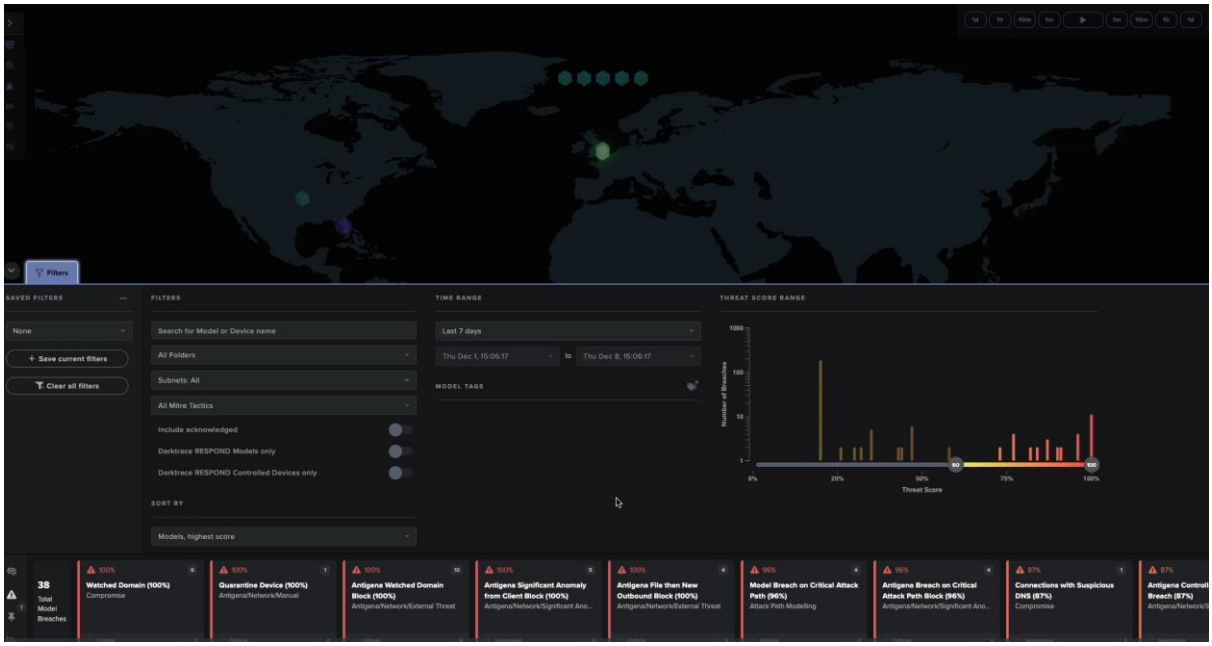


Gambar 3.7 Tampilan Awal *Model Breach* NDR Darktrace

Pada Tampilan *model breach* pada menu utama NDR Darktrace, terdapat empat informasi utama yang membantu dalam jenis serangan apa yang terjadi. Berikut penjelasan dari informasi dari *Model Breach*:

i. Persentase menunjukkan seberapa berpotensialnya suatu serangan pada perusahaan. NDR Darktrace mengkategorikan sebuah jenis serangan dari kiri kekanan berdasarkan persentase dan seberapa baru serangan tersebut terjadi.
ii. Pada pojok kanan atas, angka tersebut menjelaskan jumlah serangan yang serupa pada kategori serangan tersebut. Dengan bantuan ini, tim keamanan akan terbantu dalam mengatasi serangan yang serupa dalam satu waktu.
iii. *Anomalous Nmap Activity* pada contoh kalimat diatas mempresentasikan title dari serangan yang terjadi. Title tersebut bersifat fleksibel, sehingga walaupun NDR Darktrace membuat title suatu serangan secara otomatis, tim keamanan tetap dapat menggantinya sesuai dengan keutuhan pada menu *Model Editor*.
iv. *Device* pada contoh kalimat diatas adalah lokasi pengkategorian dan rule dari suatu serangan pada menu *Model Editor*. *Model Editor* adalah pusat informasi yang rule dari berbagai jenis serangan yang dapat dideteksi NDR Darktrace.
v. Suspicious pada contoh diatas adalah kategori berbahayanya suatu serangan yang ditentukan secara otomatis oleh NDR Darktrace. Terdapat tiga jenis pengkategorian pada serangan di Model Breach, yaitu *Critical*, *Compliance*, dan *Informational*.
vi. Pada angka pojok bawah kanan menjelaskan komentar oleh tim keamanan lainnya dalam mengatasi insiden tersebut. NDR Darktrace menyediakan fitur komentar ini dapat digunakan tim keamanan untuk membantu dalam berkomunikasi tentang progres mitigasi dari insiden tersebut.

Sama seperti *Cyber AI Analyst*, *Model Breach* juga memiliki menu *filters* yang membantu tim keamanan dalam menemukan jenis serangan yang harus segera dimitigasi. Menu *filters* pada *model Breach* memiliki menu pilihan yang lebih rinci dari menu *filters* yang ada pada *Cyber AI Analyst*. Berikut merupakan tampilan menu filters Model Breach pada NDR Darktrace yang dapat dilihat pada gambar 3.8.



Gambar 3.8 Menu *Model Breach* NDR Darktrace

Berikut merupakan penjelasan menu-menu pilihan yang dapat dilipih pada menu *filters Model Breach* yang tidak tersedia pada menu *filters Cyber AI Analyst*:

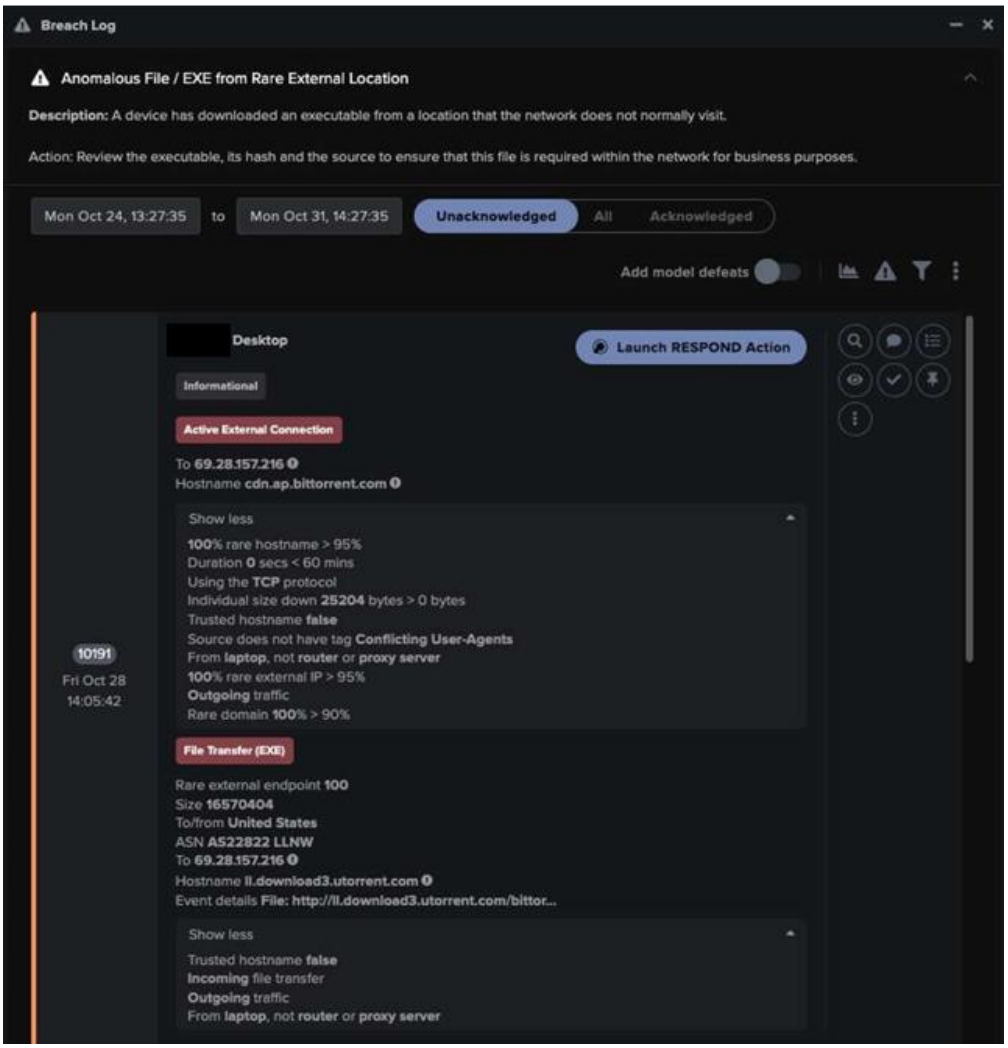
i. Darktrace *Respond Model* only pada menu *filters* membuat *Model Breach* hanya menampilkan sebuah insiden yang dimana perangkat tersebut dapat melakukan Darktrace *Respond* secara otomatis maupun manual. Darktrace *Respond* adalah sebuah teknologi dari Darktrace yang membantu NDR Darktrace dalam memitigasi dan merespons secara langsung sebuah insiden secara langsung di NDR Darktrace. Pada dasarnya, Darktrace *Respond* akan berjalan pada suatu perangkat jika perangkat tersebut sudah dimasukkan *tag* Darktrace *Respond* sebelumnya.

ii. Darktrace *Respond Controlled Devices* Only berfungsi untuk menampilkan jenis serangan yang dimana Darktrace *respond* sudah berjalan pada perangkat tersebut. Dengan kata lain, menu ini membantu dalam melihat jenis insiden yang sudah dilakukan pencegahan serangan lebih lanjut dengan bantuan dari Darktrace *Respond*.

iii. *Sort By* berfungsi untuk mengurutkan sebuah insiden yang akan ditampilkan pada menu awal *Model Breach* NDR Darktrace. Pada menu ini, pengurutan dapat diurut berdasarkan tiga bagian utama, yaitu *Devices* (Perangkat), *Models*, dan *User*.

iv. *Model Tags* berfungsi untuk menampilkan sebuah insiden berdasarkan tag atau ketentuan yang diinginkan oleh tim keamanan. Pada umumnya, tag dapat berupa *user*, *device*, dan jenis insiden.

Setelah menentukan informasi insiden yang akan dilakukan investigasi pada menu utama NDR Darktrace, aplikasi akan mengarahkan ke menu utama *Model breach*. Pada menu utama, terdapat informasi yang relevan tentang insiden yang telah dipilih. Pada menu utama, tim keamanan dapat melihat beberapa informasi penting yang berkaitan dengan insiden, informasi penting tersebut berupa perangkat yang terserang, faktor eksternal yang membuat perangkat tersebut terdeteksi melakukan sesuatu yang mencurigakan, dan penjelasan terkait *rules* yang telah dilanggar perangkat tersebut sehingga bisa terdeteksi sebagai ancaman. Berikut merupakan tampilan utama Model Breach NDR Darktrace yang dapat dilihat pada gambar 3.9.



Gambar 3.9 Tampilan Utama *Model Breach* NDR Darktrace

Selain dapat melihat informasi tentang perangkat dikategorikan sebagai insiden, *Model Breach* juga memiliki tombol-tombol aksi yang membantu tim keamanan dalam menginvestigasi lebih jauh tentang insiden tersebut. Setiap aksi tersebut, memiliki peran penting bagi tim keamanan dalam menentukan apakah sebuah insiden itu berpotensi merugikan atau tidak.

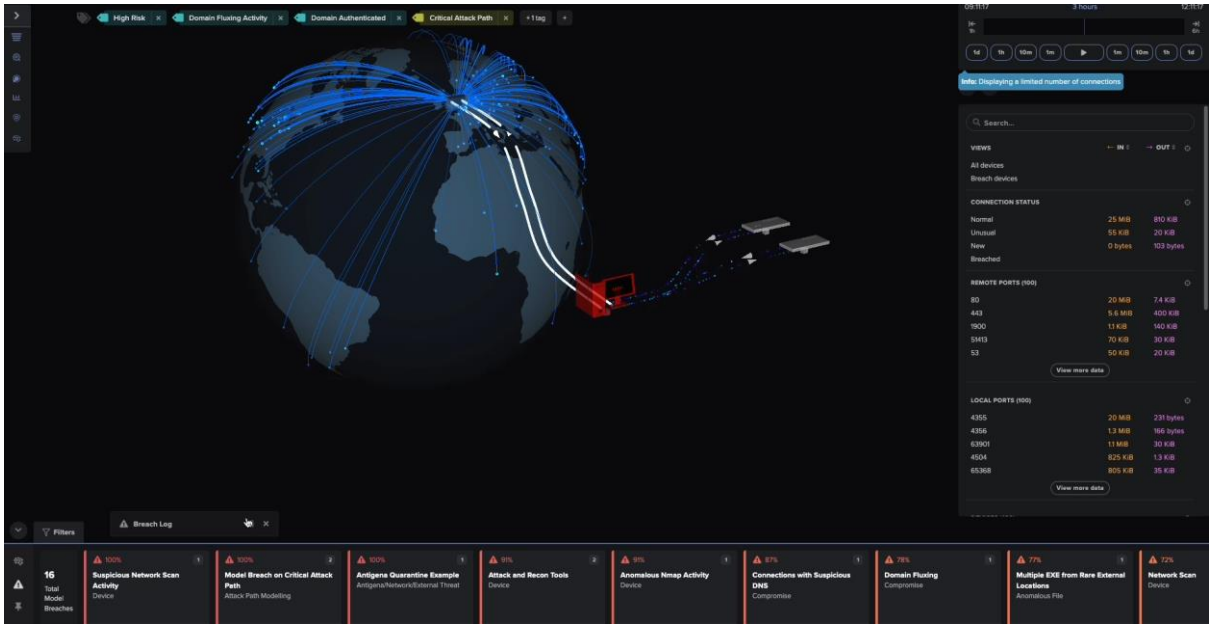
Untuk mempermudah dalam memahami setiap aksi yang dapat dilakukan pada menu *Model breach*. Berikut merupakan penjelasan dari semua aksi pada *Model Breach* NDR Darktrace:

i. *Launch Respond Action*

Fitur ini berfungsi untuk melakukan tindakan mitigasi pada insiden yang dipilih. Untuk tindakan pencegahan serangan lebih lanjut, NDR Darktrace menyediakan beberapa opsi pilihan respons yang dapat membantu tim keamanan dalam mengambil keputusan yang paling tepat. Untuk penjelasan fitur yang dapat dilakukan Darktrace *Respond* akan dijelaskan pada pembahasan berikutnya.

ii. *Magnify Glass Icon*

NDR Darktrace memiliki keunggulan yang dimana dia bisa melakukan simulasi alur kegiatan pada perangkat dengan visual yang mudah dilihat dan dipahami secara *real-time*. Dengan menekan fitur ini, simulasi alur jaringan akan langsung terfokus pada waktu terjadinya kejadian pada insiden yang dipilih. Selain itu, pada menu simulasi juga dapat melakukan membalikkan maupun memajukan waktu kejadian sehingga tim keamanan bisa lebih mudah memahami kejadian dari suatu insiden. Berikut merupakan tampilan simulasi kejadian suatu insiden pada NDR Darktrace yang dapat dilihat pada gambar 3.10.



Gambar 3.10 Fitur Simulasi kejadi Insiden NDR Darktrace

Pada bagian kanan dari gambar menjelaskan jumlah data yang digunakan perangkat dalam melakukan komunikasi. NDR Darktrace dapat mengetahui jenis setiap port yang digunakan perangkat dalam berkomunikasi dan akan mencatat data yang masuk maupun keluar. NDR Darktrace akan mulai mencatat jumlah penggunaan data yang masuk maupun keluar ketika NDR Darktrace mencurigai adanya tindakan serangan atau anomali.

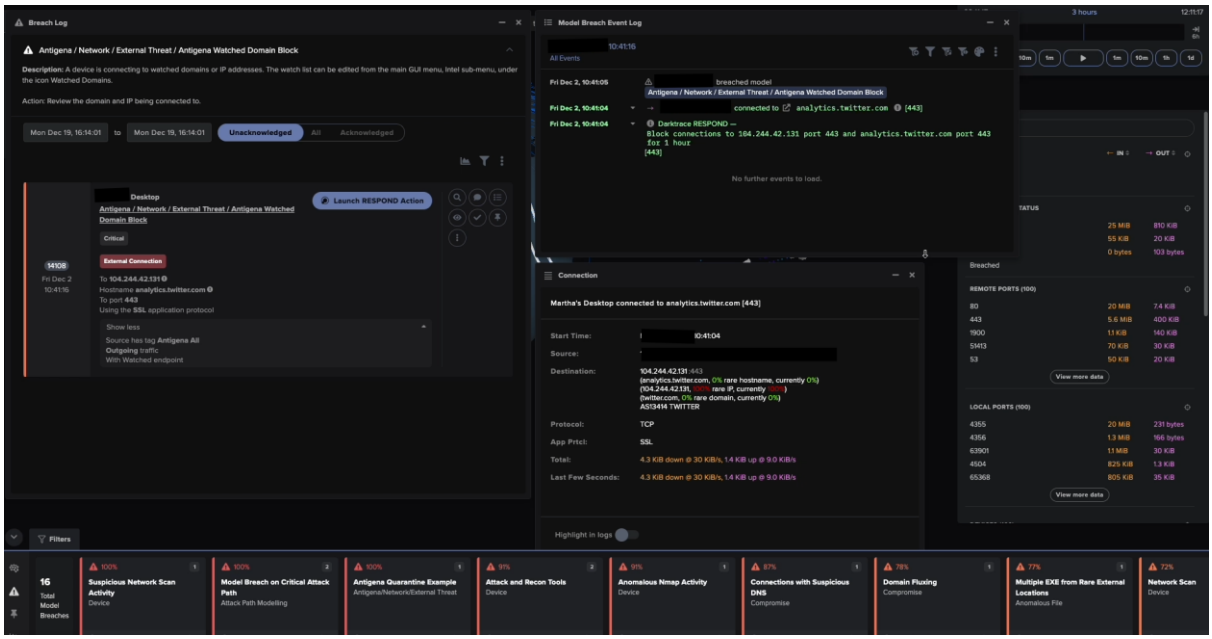
iii. *Bubble Chat Icon*

Fitur ini berfungsi sama seperti *chat icon* yang sudah dijelaskan sebelumnya. Ikon *chat* akan terpisah hanya untuk jenis insiden yang dipilih, sehingga mempermudah tim keamanan dalam mengetahui terkait progres dari insiden tersebut. Ketika fitur *chat* ini digunakan, maka jumlah chat Model Breach pada menu utama akan bertambah, sehingga mempermudah dalam tim keamanan mengetahui jika sudah ada lanjutan progres pada insiden tersebut.

iv. *Log Icon*

Log Icon akan menampilkan halaman *Model Event Breach log* ini, memiliki fitur yang berfungsi untuk melihat log peristiwa yang relevan dengan insiden yang dipilih. Dengan fitur ini, tim keamanan bisa melihat alur kejadian terpusat pada kejadian dengan lebih cepat. Pada log *Icon* juga memperlihatkan aksi yang dikirim user maupun ditangkap pada perangkat dengan arah dan warna pada tanda panah di tengah antara tanggal kejadian dan informasi kejadian.

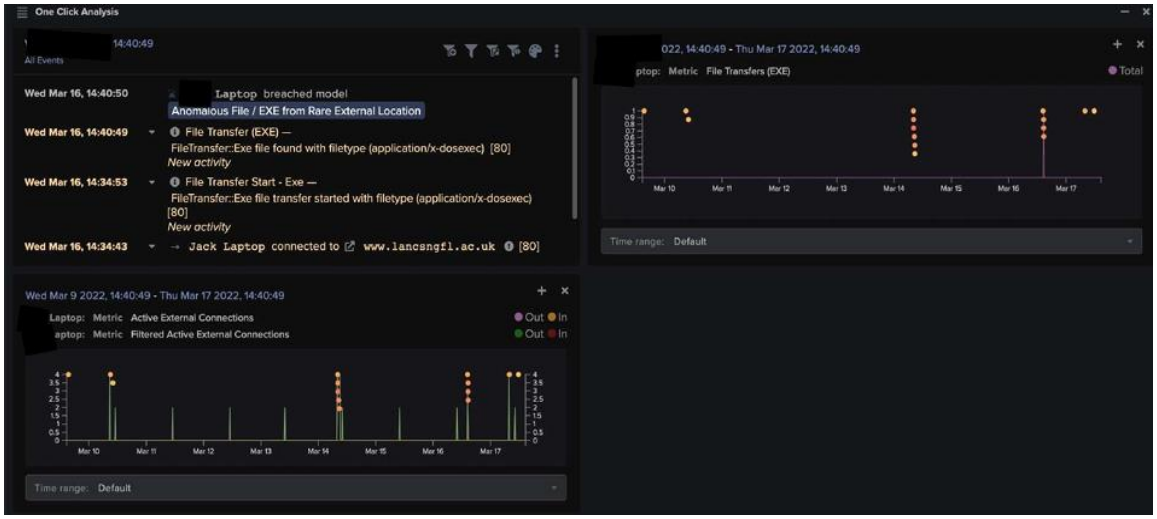
Berikut merupakan tampilan *model Breach Event Log* pada NDR Darktrace yang dapat dilihat pada gambar 3.11.



Gambar 3.11 Fitur *Model Breach Event* Log NDR Darktrace

v. *Eye Icon*

Eye Icon ini akan menampilkan halaman *One Click Analysis*, yang dimana fitur ini memiliki isi yang kurang lebih sama dengan *Model Event Breach log*, Fitur ini dapat menampilkan data log peristiwa sekaligus dengan grafik data yang berkaitan dengan insiden yang dipilih. Fitur ini dinamakan NDR Darktrace dengan sebutan *One Click Analysis*. Berikut merupakan tampilan log data dan grafik data insiden pada NDR Darktrace yang dapat dilihat pada gambar 3.12.



Gambar 3.12 Fitur *One Click Analysis* NDR Darktrace

Pada grafik yang diberikan, NDR Darktrace menawarkan fitur untuk dapat menyesuaikan grafik sesuai dengan kebutuhan dalam melakukan investigasi insiden. Hal yang dapat diubah pada grafik ialah tim keamanan dapat menambah informasi di dalam grafik untuk mencari relasi serangan insiden yang dideteksi NDR Darktrace dan membuat grafik secara terpisah sebanyak yang diperlukan.

vi. *Tick Icon*

Fitur ini berfungsi untuk mengubah status sebuah insiden menjadi *Acknowledge* atau bukan ancaman. Dengan adanya fitur ini, insiden yang sebelumnya masuk ke dalam daftar berbahaya akan langsung disembunyikan dari menu utama. Hal ini memungkinkan tim keamanan untuk lebih fokus pada insiden-insiden yang benar-benar memerlukan perhatian, mengurangi kebingungan dan memastikan bahwa sumber daya dialokasikan secara efisien untuk menangani ancaman yang paling signifikan. Selain itu, fitur ini membantu dalam memelihara kebersihan data dan memastikan bahwa hanya insiden yang relevan dan belum ditangani yang tetap terlihat, meningkatkan produktivitas dan efektivitas tim keamanan.

vii. *Pin Icon*

Fitur ini berguna untuk menyematkan sebuah insiden agar tetap dapat ditampilkan pada list insiden walaupun insiden tersebut sudah dilakukan mitigasi. Dengan adanya fitur ini, tim keamanan dapat terus memantau insiden yang telah diatasi untuk keperluan dokumentasi serta melakukan analisis lebih lanjut. Selain itu, fitur ini juga berguna untuk memberikan referensi bagi tim keamanan dalam menangani insiden serupa di masa mendatang, sehingga meningkatkan kesiapan dan respons terhadap ancaman siber yang mungkin terjadi.

viii. *Three Dots Icon*

Fitur ini menyediakan menu-menu tindakan tambahan dalam mengatasi insiden yang sudah dipilih sebelumnya. Menu yang disediakan pada ikon ini berfokus dalam memberi tahu informasi tekait kategori dari serangan tersebut. Jenis informasi yang disediakan adalah melihat *Model* serangan yang langsung mengarahkan ke *Model Editor*, fungsi tombol ini adalah untuk melihat *rules* deteksi dari serangan tersebut, dan juga tim keamanan dapat mengganti atau memperbaiki *rules* tersebut jika ada kejanggalan. Selain itu, terdapat menu yang menjelaskan MITRE ATT&CK dari insiden tersebut.

c. *Manual Detection*

NDR Darktrace memiliki fitur untuk menampilkan data jaringan dalam bentuk log aktivitas, log aktifitas ini dapat memperlihatkan semua alur kegiatan yang sedang berjalan pada jaringan yang sedang dimonitor. Fitur ini dinamakan oleh Darktrace sebagai *Advanced Search*. Dengan fitur *Advanced Search*, tim keamanan dapat melakukan penelusuran mendalam terhadap aktivitas jaringan, mengidentifikasi pola-pola mencurigakan, dan melakukan analisis forensik. Berikut merupakan tampilan Advance Search pada NDR Darktrace yang dapat dilihat pada gambar 3.13.

Gambar 3.13 Fitur *Advance Search* NDR Darktrace

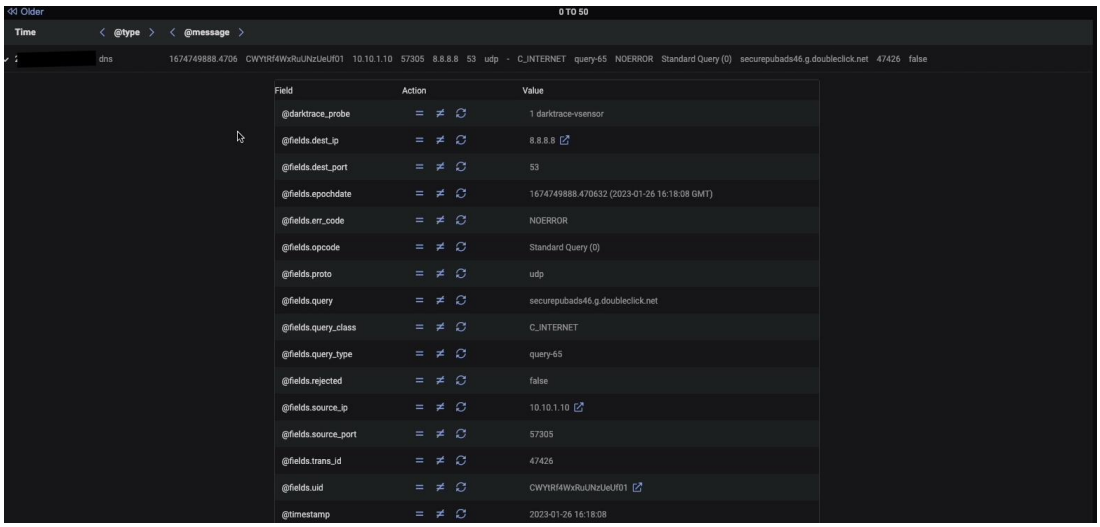
Advance Search biasanya akan digunakan oleh tim *Threat hunting* dalam mendeteksi potensi ancaman. *Threat Hunting* adalah tim keamanan ahli yang dapat melakukan pendeteksian secara proaktif dalam mendeteksi dan respon sebuah insiden sebelum insiden tersebut dapat menyebabkan kerusakan dan kerugian bagi perusahaan [10]. *Dengan Advanced Search*, Threat hunting dapat terbantu dalam menganalisis potensi ancaman secara manual melalui analisis data jaringan dalam bentuk log aktivitas.

Advance Search dapat menyimpan log sampai kurang lebih tiga bulan, akan tetapi tidak disarankan untuk melakukan analisis log menggunakan *Advance Search* dalam waktu selama itu. Hal ini terjadi karena cukup beratnya informasi yang harus dikeluarkan dan dapat membuat *Advance Search* tidak berjalan dengan yang seharusnya. NDR Darktrace sendiri menyarankan

untuk menerapkan analisis log dalam waktu tujuh hari pada perusahaan kecil dan menengah serta tiga hari untuk perusahaan besar.

Pada grafik yang ditampilkan pada *Advance Search*, diperlihatkan jumlah peristiwa yang terjadi pada periode waktu tertentu. Grafik yang disediakan bersifat fleksibel, yang dimana tim keamanan dapat menyeret grafik pada jangka waktu tertentu dan grafik akan mengecil menyesuaikan dengan rentang waktu yang ditentukan. Dengan fitur ini, dapat membantu tim keamanan dalam mengidentifikasi log jaringan yang perlu dilakukan analisis. Hal ini dikarenakan tingginya penggunaan jaringan dapat menandakan kemungkinan terjadi anomali atau potensi serangan pada periode waktu tersebut.

Tabel yang ditampilkan berisi informasi tentang semua alur penggunaan jaringan pada perangkat yang terdaftar dengan NDR Darktrace. Umumnya memberikan tiga informasi, yaitu *Time*, *@Type*, dan *@Message*. *Time* mempresentasikan waktu aktivitas perangkat dalam berkomunikasi dengan jaringan yang terdeteksi oleh NDR Darktrace. Pada @Type menjelaskan jenis lalu lintas atau aktivitas yang terjadi, umumnya *@Type* memiliki empat jenis, yaitu conn, http, ssl, dan dns. Dan pada kolom *@Message* memiliki isi tentang semua informasi penting dari log yang digabungkan agar lebih mudah dalam mencari informasi. Pada kolom *@Messege* juga dapat merincikan setiap bidang dari semua informasi yang ditangkap NDR Darktrace. Berikut merupakan rincian setiap bidang pada kolom *@Message Advance Search* NDR Darktrace yang dapat dilihat pada gambar 3.14.



Gambar 3.14 Rincian Bidang Kolom *@Message Advance Search*

NDR Darktrace juga memberikan tiga aksi untuk setiap rincian dari informasi. Aksi ini berfungsi untuk mencari log jaringan sesuai dengan *Field* dan *Value* yang dipilih. Aksi tersebut akan langsung otomatis mengisi *query* pada menu *search* sehingga mempermudah dalam menambahkan informasi yang ingin dicari. Berikut merupakan penjelasan dari setiap aksi yang bisa dilakukan:

i. Simbol ”sama dengan” berguna untuk menambahkan *query* dengan dengan *Field* dan *Value* sesuai dengan yang dipilih. Simbol ini berfungsi untuk menampilkan informasi yang sesuai dengan *Field* dan *Value* yang dipilih. Jika sudah ada *query* pada menu *search*, maka akan otomatis menambahkan operator ”*AND*” dan menambahkan query dengan *Field* dan *Value* yang dipilih.

ii. Simbol ”tidak sama dengan” berguna untuk menetapkan *boolean* ”*NOT*” pada query dengan *Field* dan *Value* yang dipilih. Simbol ini berfungsi untuk menampilkan informasi yang mengecualikan dengan *Field* dan *Value* yang dipilih. Jika sudah ada query pada menu *search*, maka akan otomatis menambahkan operator ”*AND NOT*” dan menambahkan query dengan Field dan Value yang dipilih.

iii. Simbol ”panah berputar” berguna untuk memasukkan *querry ip source* dan *ip address* dari *Field* dan *Value* yang dipilih. Jika sudah ada *querry* pada menu *search*, maka *querry* tersebut akan terhapus dan menambahkan *querry ip source* dan *ip address* dari *Field* dan *Value* yang dipilih

Selain itu, tabel yang disediakan NDR Darktrace juga dapat disesuaikan dengan informasi yang dibutuhkan. Informasi yang dapat dipilih dapat ditemukan pada bagian *Columns* dalam menu *Advance Search*. Dengan memilih salah satu yang ada pada menu *Columns*, maka tabel yang pada Advance Search akan secara otomatis berubah dengan menu yang telah dipilih. Berikut merupakan tampilan kustomisasi tabel pada menu *Advance Search* NDR Darktrace yang dapat dilihat pada gambar 3.15.

Gambar 3.15 Kustomisasi tabel *Advance Search* NDR Darktrace

Advance Search pada NDR Darktrace juga memiliki fitur yang membantu dalam mencari hasil yang diinginkan dengan cepat. Nilai yang ditampilkan akan menyesuaikan dengan *Columns* yang dipilih sehingga memberikan hasil yang relevan dengan yang dicari. Pada menu ini terdapat tiga informasi yang ditampilkan, yaitu persentase dari hasil pada halaman tabel tersebut, nama dari *Value* itu sendiri, dan aksi yang membantu dalam menyaring hasil berdasarkan bidang tersebut. Berikut merupakan menu tambahan *advance Search* NDR Darktrace yang dapat dilihat pada gambar 3.16.

Gambar 3.16 Menu tambahan *Advance Search* NDR Darktrace

3.2.2. *Validation*

Pada fase ini, tim keamanan akan melakukan analisis pada hasil informasi terkait insiden yang ditemukan pada fase *Detection*. Fase ini adalah fase yang dimana tim keamanan akan menentukan apakah insiden tersebut sebuah ancaman atau kesalahan pendeteksian / ancaman palus dari teknologi NDR Darktrace. Pada fase ini, ada beberapa hal yang perlu dilakukan oleh tim keamanan dalam melakukan validasi insiden, yaitu:

a. Pengumpulan Bukti

Tim keamanan perlu untuk mengumpulkan berbagai macam bukti yang relevan untuk mendukung kebenaran dari hasil pendeteksian NDR Darktrace. Bukti yang diberikan dapat berupa log sistem, file yang dicurigai, dan data lainnya yang menunjukkan aktivitas mencurigakan atau berbahaya. Selain itu juga, tim keamanan juga bisa mencari referensi lainnya menggunakan teknologi keamanan yang tersedia dari perusahaan, untuk memperkuat bukti kebenaran dari insiden. Berikut merupakan pengumpulan dan pengelompokkan bukti dari serangan sebelumnya:

i. Detail Insiden

- Detail Insiden : Senin, 27 November 2023, 18:10:52
- *Victim Hostname* : csws.lintasarta.net
- *Attacker Hostname* : crm.Lintasarta.net

ii. Rincian teknis Insiden

- Target memanfaatkan protokol HTTP dengan mengirimkan *request 'OPTION*' agar dapat mengetahui fitur apa saja yang didukung oleh server atau sumber daya tertentu di server, seperti metode *request* yang diperbolehkan dalam domain atau kebijakan CORS.
- Kebijakan CORS membantu penyerang dalam mencari tahu domain mana saja yang diperbolehkan untuk berinteraksi dengan server.
- *'OPTION*' dapat kemungkinan dimanfaatkan penyerang untuk mengeksplorasi kelemahan dalam konfigurasi server yang dapat dimanfaatkan lebih lanjut.
- Menggunakan *User Agent* "Mozilla/5.0". *User Agent* yang digunakan kompatibel dengan aksi *NMAP Scripting Engine* yang dimana ini adalah salah satu kemampuan NMAP dalam melakukan *Automation Scanning*

beserta beberapa *syntax* yang berhubungan pencarian celah dari informasi domain dalam konteks jaringan.

- IP dari si penyerang dapat diasumsikan adalah ip ” 180.248.32.42”.
- Hal ini dibuktikan dengan informasi berupa ’*X-Forwarded-For*’ dengan ip ”180.248.32.42”. pada kasus biasanya, informasi ini membuktikan adanya pemanfaatan proxy yang diterukan ke ip ”180.248.32.42”. Dengan bantuan proxy, penyerang dapat menyembunyikan identitasnya beserta mengakses informasi penting yang sebelumnya tidak dapat diakses tanpa perlunya vpn dari Lintasarta.

iii. Analisis dan Keterangan Tambahan

- Ketika *Attacker Hostname* melakukan melakukan *request*, terdapat balasan ”*HTTP Response Code*: 0”. Hal ini mengidentifikasikan bahwa *Victim Hostname* tidak dapat merespon request dari *Attacker Hostname*.
- Ada beberapa kemungkinan kenapa ini bisa terjadi, yaitu aksi request diblokir secara otomatis oleh sistem keamanan yang digunakan perusahaan, terjadinya kegagalan jaringan pada saat melakukan request, dan adanya kesalahan konfigurasi yang dilakukan oleh tim teknisi.
- Aksi request dari *Attacker Hostname* belum pernah tercatat pada log aktivitas dari NDR Darktrace maupun alat keamanan lainnya, sehingga aktivitas dapat dianggap sebuah anomali yang perlu ditindaklanjuti.

b. Konfirmasi dari Sumber Eksternal

Walaupun hasil dari pendeteksian NDR Darktrace adalah pendeteksian berbasis perilaku yang dimana teknologi ini dapat mendeteksi serangan yang belum pernah terjadi sebelumnya atau *zero-day*. Akan tetapi ada kemungkinan besar bahwa insiden tersebut menggunakan taktik dan teknik yang kurang lebih sama dengan serangan yang sudah pernah terjadi sebelumnya. Dengan memanfaatkan informasi yang ada di sumber eksternal, maka tim keamanan dapat terbantu dalam memastikan bahwa ancaman tersebut adalah *True-Positive* dan bukan *False-Positive*.

Pada konteks serangan, tim keamanan melakukan pencarian informasi dari jenis serangan yang sesuai dari insiden yang sedang dianalisis. Berkat bantuan dari integrasi MITRE ATT&CK pada NDR Darktrace, tim keamanan lebih mudah dalam mencari referensi dari serangan yang sedang terjadi. Setelah beberapa waktu dekat mencari informasi, tim keamanan dapat mencari relasi yang sesuai terkait TTP (*Tactics, Technique, and Procedure*), yaitu:

i. *Reconnaissence*

Insiden masuk kepada suatu percobaan pencarian informasi dengan kode teknik ”T1595” yang masuk kedalam kategori ”*Active Scanning*”. Serta untuk sub-teknik yang dilakukan oleh penyerang ada dua hal yaitu:

- ”T1595.001” yang menjelaskan penggunaan NMAP untuk melakukan *Scanning IP* dengan tujuan mencari informasi tentang *host*, *open port*, dan *service* yang sedang berjalan.
- ”T1595.002” yang menjelaskan Penggunaan Nmap untuk melakukan *vulnerability scanning* guna menentukan kelemahan potensial dalam keamanan.

ii. *Command and Control*

Insiden masuk kedalam kategori komando dan kendali dengan kode teknik ”T1071” yang masuk kedalam kategori ” *Application Layer Protocol*”. Serta untuk sub-teknik yang dilakukan ada satu poin yaitu:

- ”T1071.001” yang dibuktikan dengan *HTTP Method* sebagai ’*OPTIONS*’ sehingga teridentifikasi sebagai upaya pengujian konfigurasi keamanan web server perusahaan.

iii. *Devense Evasion*

Insiden dapat masuk ke dalam penyembunyian identitas dengan kode teknik ”T1564” yang masuk kedalam kategori ” *Hide Artifacts*”. Serta untuk sub-teknik dari serangan masuk ke poin:

- ” T1564.002” yang dibuktikan dengan Penggunaan ”*X-Forwarded-For*” untuk kemungkinan menyembunyikan asal usul sebenarnya dari permintaan, sehingga mempersulit pelacakan. Walaupun cukup besar kemungkinan untuk keperluan hal yang lebih ekstrim.

c. Evaluasi Konteks

Ketika sedang melakukan validasi insiden, perlu untuk mencari informasi dari tim internal perusahaan terkait penggunaan teknologi yang dimonitoring NDR Darktrace. Tujuan dilakukakannya evaluasi konteks adalah untuk memastikan apakah ada alasan yang valid bagi aktivitas yang dideteksi. Hal ini diperlukan karena perusahaan akan terus beroperasi secara berubah-ubah dalam setiap waktunya, sehingga terkadang teknologi keamanan akan mengkategorikan perubahan tersebut sebagai anomali dan membuat sebuah peringatan adanya insiden. Oleh karena itu, penting bagi tim keamanan dalam melakukan validasi kepada anggota internal perusahaan terlebih dahulu untuk memastikan kebenaran dari insiden tersebut.

Pada insiden yang terjadi, tim keamanan langsung melakukan verifikasi kepada beberapa departemen tim keamanan yang ada di lintasarta, yaitu SQURA tempat penulis bekerja dalam mengembangkan produk keamanan siber, CISO sebagai departemen yang berfokus dalam mengamankan semua aset penting perusahaan internal, dan SOC sebagai departemen yang melakukan monitoring semua alat keamanan yang digunakan oleh klien (eksternal) Lintasarta sekaligus bekerja sama dengan tim CISO untuk monitoring aset perusahaan internal untuk beberapa alat keamanan.

Setelah melakukan komunikasi dengan ketiga tim departemen keamanan siber yang ada di Lintasarta, dapat disimpulkan bahwa tidak ada satupun orang dari mereka yang sengaja melakukan hal tersebut. Selain itu, untuk memperkuat bukti dari insiden, tim keamanan mencoba melakukan komunikasi kepada beberapa orang yang bertugas atau dapat melakukan akses ke server yang diserang namun hasilnya adalah tidak ada yang melakukan.

Setelah melakukan semua hal-hal yang telah disebutkan, tim keamanan dapat menyimpulkan bahwa insiden yang sedang terjadi masuk kedalam kategori insiden yang valid (*True-Positive*). Oleh karena itu, maka langkah selanjutnya perlu dilakukan secepat mungkin agar insiden ini tidak sampai tahap yang dimana dapat merugikan Lintasarta lebih jauh jika dibiarkan.

Sebelumnya perlu dijelaskan bahwa *validation* insiden pada NDR Darktrace dapat dikategorikan menjadi tiga kategori kemungkinan. Tiga hasil ini dapat membantu tim keamanan untuk memastikan bahwa teknologi NDR Darktrace digunakan dengan efektif hanya pada insiden valid yang memerlukan tindakan lebih lanjut. Berikut merupakan hasil pada fase *validation* teknologi NDR Darktrace:

a. Hasil *True-Positive*

Hasil *True-Positive* adalah kondisi dimana NDR Darktrace mengidentifikasi adanya serangan yang valid atau memberikan dampak negatif bagi perusahaan. Pada hasil ini, tim keamanan harus hendak melakukan segala persiapan dan melakukan konsultasi kepada atasan untuk menentukan langkah tindakan mitigasi insiden agar dapat melindungi infrastruktur perusahaan dari kerugian yang lebih besar akibat serangan siber.

b. Hasil False-Negative

Hasil *False-Positive* adalah kondisi yang dimana bahwasannya sistem mengidentifikasi sebuah sebuah ancaman peringatan palsu yang tidak perlu dilakukan mitigasi ancaman. Kesalahan ini dapat mengakibatkan berbagai masalah bagi tim keamanan dan organisasi secara keseluruhan. Jika pada hasil ini terjadi, tim keamanan harus menentukan langkah yang harus diambil agar NDR Darktrace dapat meningkatkan efisiensi tim keamanan, mengurangi gangguan yang tidak perlu, dan tidak memberikan peringatan ancaman yang serupa di masa mendatang.

c. Hasil False-Positive

Hasil *False-Negative* adalah kondisi yang dimana sistem NDR Darktrace tidak mendeteksi potensi ancaman apapun, Sedangkan teknologi lain yang serupa seperti IPS dan *Firewall* mendeteksi adanya ancaman pada perusahaan. Jika hasil ini terjadi, maka tim keamanan harus menentukan langkah apa yang perlu dilakukan agar NDR Darktrace dapat mendeteksi ancaman yang serupa di masa depan.

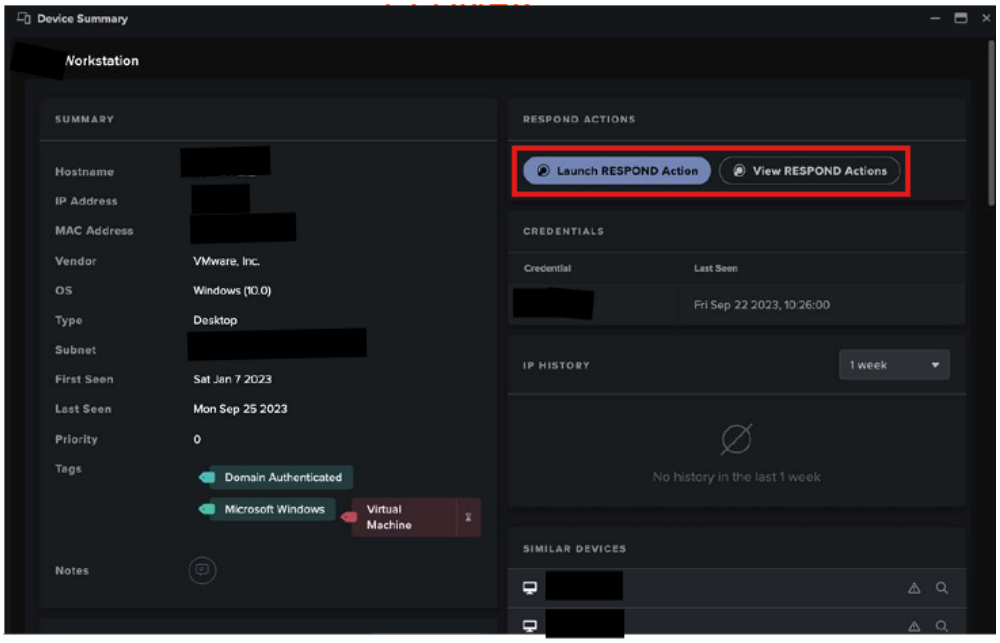
3.2.3. *Containment*

Fase *Containment* merupakan sebuah fase tindakan yang dimana tim keamanan mulai melakukan pencegahan untuk mengendalikan dan membatasi penyebaran serangan atau insiden keamanan yang terjadi di dalam jaringan atau sistem. Pada fase *Containment*, terdapat tugas-tugas yang harus dilakukan oleh tim keamanan dalam mengendalikan penyebaran, yaitu:

a. Respons Insiden

Respon insiden pada dasarnya diutamakan pada insiden yang valid atau *True-Positive*. NDR Darktrace memiliki fitur yang bernama Darktrace *Respond*. Dengan Darktrace Respond, tim keamanan dapat melakukan aksi pencegahan utama dari insiden dengan rentang waktu yang telah ditentukan. Untuk mempermudah tim keamanan dalam menerapkan respon pada

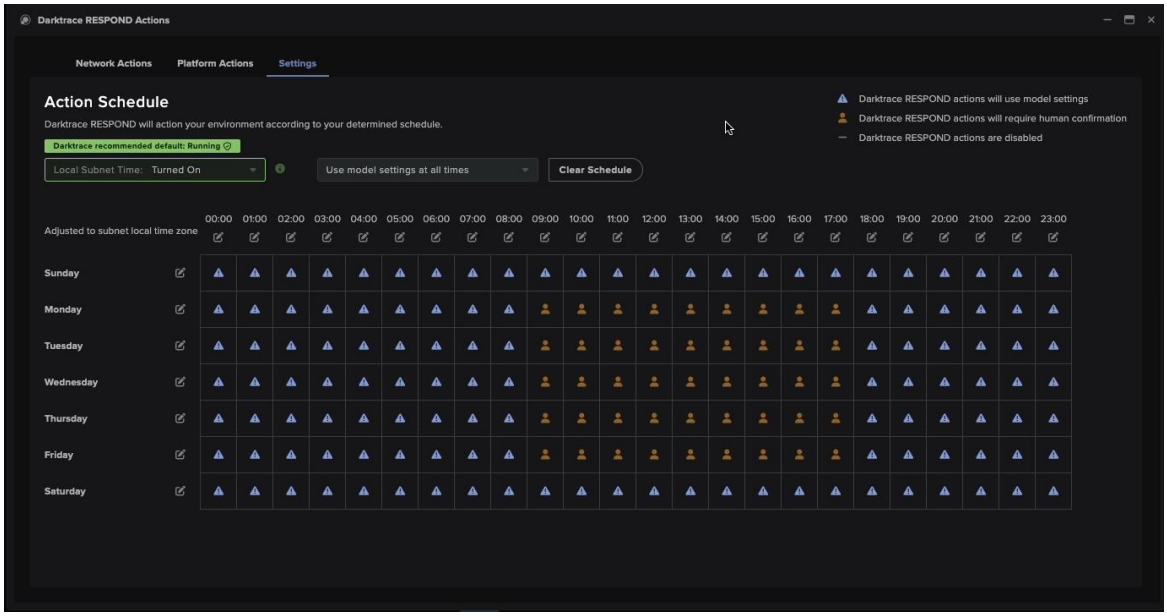
insiden, NDR Darktrace meletakkan aksi Darktrace *Respond* pada setiap jenis insiden yang ada pada *Cyber AI Analyst*, *Model Breach*, Maupun *Advance Search*. Berikut merupakan aksi Darktrace *Respond* NDR Darktrace yang dapat dilihat pada gambar 3.17.



Gambar 3.17 Aksi Darktrace *Respond* NDR Darktrace

Walaupun tim keamanan dapat melakukan respons insiden manual, pada dasarnya NDR Darktrace memiliki kemampuan untuk merespons serangan secara otomatis. NDR Darktrace dapat menentukan langkah respons tersebut berdasarkan dari hasil pembelajaran teknologi itu sendiri dari informasi perusahaan dengan memanfaatkan *Self-Learning AI*.

Dikarena respons insiden secara otomatis pada waktu kerja dapat menyebabkan kerugian pada perusahaan, NDR Darktrace membagi respon otomatis menjadi dua macam yaitu *Human Confirmation Mode* dan *Model Settings Mode*. *Human Confirmation Mode* adalah salah satu jenis response insiden otomatis yang dimana respons insiden akan berjalan ketika tim keamanan sudah memvalidasi kebenaran dari insiden tersebut, sedangkan *Model Settings Mode* adalah jenis respon insiden otomatis yang dimana NDR Darktrace akan langsung melakukan aksi respons ketika NDR Darktrace mendeteksi adanya insiden. Respons otomatis ini dapat dikonfigurasi oleh tim keamanan untuk menentukan kapan waktu menggunakan jenis respon insiden tersebut. Berikut merupakan gambara konfigurasi respon otomatis pada NDR Darktrace yang dapat dilihat pada gambar 3.18.



Gambar 3.18 Konfigurasi respon otomatis NDR Darktrace

Pada kasus insiden insiden sebelumnya, NDR Darktrace sudah melakukan respons insiden secara otomatis. Hal ini terjadi karena insiden sudah terjadi pada jam luar kerja Lintasarta, sehingga NDR Darktrace akan melakukan respons insiden secara otomatis ketika terjadi anomali. Hal ini dapat dilihat pada gambar 3.18 yang mana respons insiden yang perlu dilakukan konfirmasi manusia adalah pada waktu jam kerja, yaitu senin-jumat pada pukul 09.00 – 17.00. Oleh sebab itu, NDR Darktrace akan melakukan respons insiden secara otomatis diluar jam yang telah ditentukan.

Respons insiden yang diambil pada kasus ini oleh NDR Darktrace adalah "*Quarantine Device*". Dengan bantuan respons ini, perangkat server cswc.Lintasarta.net tidak akan dapat melakukan koneksi internet kemanapun karena koneksi masuk (*inbound*) maupun keluar (*outbound*) telah diblokir dengan bantuan NDR Darktrace.

Selain itu, tim keamanan tetap mencari informasi dari ip "180.248.32.42" dengan bantuan *advance search* maupun alat keamanan lainnya untuk mencari informasi serta mencari lebih jauh tentang apa yang sudah dilakukan oleh ip tersebut pada aset-aset yang ada Lintasarta. Serta tim keamanan memberlakukan blokir koneksi dari ip ini melalui firewall agar ip tersebut dapat dihentikan gerak-geriknya secara keseluruhan (Jika tidak menggunakan *proxy*).

Perlu diketahui bahwa respons yang digunakan NDR Darktrace menggunakan metode respons yang bernama TCP *Reset*. TCP *Reset* merupakan mekanisme yang digunakan untuk memutus koneksi TCP yang berpotensi berbahaya dalam jaringan (Darktrace Academy, n.d.-a). Dengan metode respons ini, NDR Darktrace dapat memberikan banyak opsi respons

insiden, sehingga tim keamanan dapat memiliki banyak opsi dalam melakukan mitigasi serangan. Darktrace *Respond* menawarkan berbagai macam jenis respons insiden yang dapat diterapkan pada perangkat yang terindikasi mengalami insiden. Berikut merupakan penjelasan dari setiap jenis respons yang dapat dilakukan pada NDR Darktrace:

i. *Enforce Group Pattern of Life*

Respons ini bertujuan untuk menerapkan pola kehidupan pada kelompok. Dengan menggunakan menu respons ini, maka perangkat tersebut hanya dapat mengirimkan data atau informasi dalam jumlah besar kepada perangkat yang dianggap normal oleh NDR Darktrace. Hal yang dianggap normal oleh NDR Darktrace adalah sumber informasi yang biasa diakses oleh perangkat tersebut dalam mengerjakan tugasnya sehari-hari. Jika perangkat tersebut mengirimkan data atau informasi dalam jumlah besar kepada perangkat eksternal selain yang terdaftar, maka NDR Darktrace akan langsung memutuskan koneksi jaringan dari perangkat tersebut.

ii. *Block All Outgoing Traffic*

Repons ini bertujuan untuk memblokir seluruh lalu lintas jaringan yang keluar dari perangkat. Dengan menerapkan respons ini, maka perangkat yang terlibat tidak akan bisa mengakses informasi apapun atau mengirimkan pesan melalui jaringan. Hal ini dilakukan untuk memastikan bahwa perangkat yang telah dikompromikan tidak dapat berkomunikasi dengan server penyerang atau menyebarkan malware ke perangkat lain dalam jaringan.

iii. *Block All Incoming Traffic*

Respons ini bertujuan untuk memblokir seluruh lalu lintas jaringan yang masuk ke perangkat. Dengan menerapkan respons ini, maka perangkat yang terlibat tidak akan bisa menerima informasi apapun atau pesan melalui jaringan. Hal ini dilakukan untuk memastikan bahwa perangkat yang telah dikompromikan tidak dapat menerima instruksi dari penyerang atau mengunduh tambahan malware.

iv. *Block Matching Connection*

Respons ini bertujuan untuk memblokir lalu lintas jaringan pada perangkat kepada sumber informasi yang terdeteksi berbahaya. Dengan menerapkan respons ini, maka perangkat yang terlibat tidak akan bisa mengakses informasi dari sumber informasi yang dianggap berbahaya, namun perangkat tetap dapat mengakses maupun mengunduh informasi dari sumber yang lain.

v. *Quarantine Device*

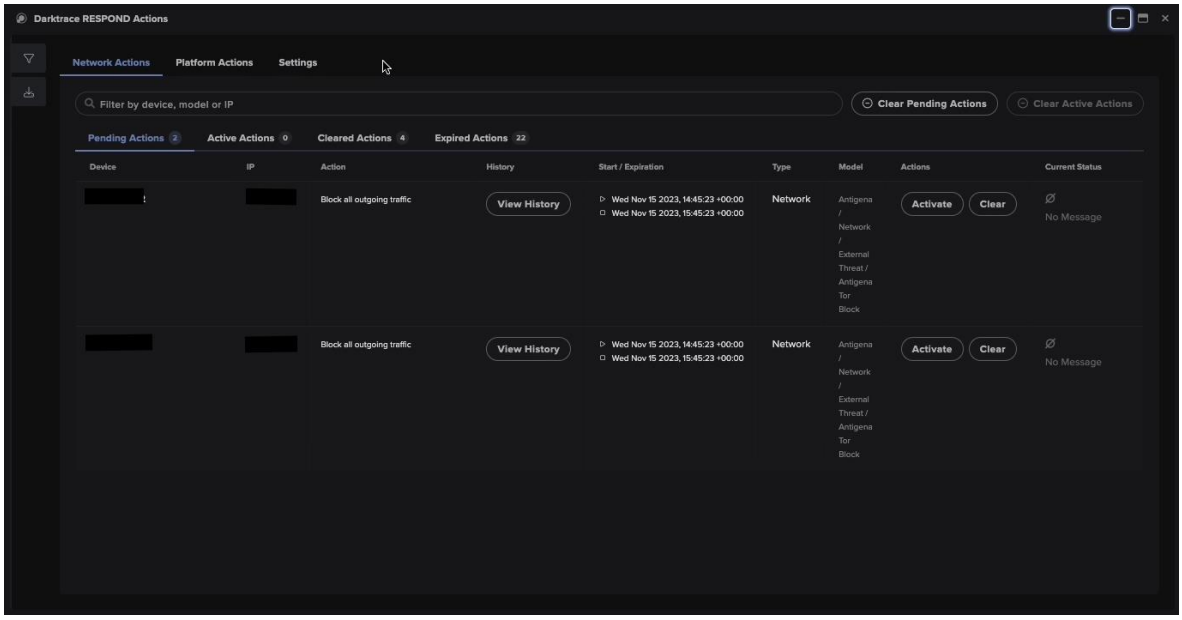
Respons ini bertujuan untuk memblokir lalu lintas jaringan yang masuk maupun keluar dari perangkat. Dengan menerapkan respons ini, maka perangkat yang terlibat tidak akan bisa mengakses maupun mengunduh informasi apapun pada jaringan. Tujuan dari penerapan insiden ini adalah untuk menghentikan potensi ancaman yang belum diketahui, memblokir penyebaran *malware*, serta pencegahan *ransomware* yang dapat mengenkripsi informasi pada perusahaan.

vi. *Enforce Pattern of Life*

Respons ini bertujuan untuk menerapkan pola perilaku dari perangkat. Dengan menerapkan respons ini, maka perangkat yang terlibat hanya diizinkan untuk berkomunikasi kepada sumber informasi yang dianggap normal oleh NDR Darktrace. Hal ini dilakukan untuk memastikan bahwa perangkat tersebut tidak dapat berkomunikasi dengan sumber yang berpotensi berbahaya, sehingga mengurangi risiko terjadinya serangan siber.

Walaupun sudah dilakukan respons insiden melalui NDR Darktrace, tim keamanan harus tetap melanjutkan proses manajemen insiden secepat mungkin. Hal ini dikarenakan respons insiden NDR Darktrace bersifat sementara atau langkah pencegahan utama. Ketika Penyerang sudah mendapatkan celah atau kerentanan pada perusahaan, maka dia akan mencari celah lainnya yang bisa mereka eksploitasi sehingga serangan yang mereka tetap berlanjut tanpa kita sadari. Hal ini dapat terus berlanjut sampai tim keamanan dapat memblokir salah satu *root cause* (akar permasalahan) insiden dapat terjadi.

Ketika sudah menerapkan Darktrace *Respond* pada suatu insiden, maka terdapat halaman yang menampilkan berbagai informasi yang berkaitan dengan Darktrace *Respond*. Pada halaman ini tim keamanan bisa mengontrol seluruh respond yang terdaftar. Berikut merupakan halaman utama Darktrace *Respond Action* NDR Darktrace yang dapat dilihat pada gambar 3.19.



Gambar 3.19 Halaman utama Darktrace *Respond Action* NDR Darktrace

Pada halaman utama Darktrace *Respond Action*, terdapat empat menu pilihan yang mengkategorikan status Darktrace Respon pada perangkat yang terindikasi. Dengan adanya empat menu ini, tim keamanan akan lebih mudah dalam mengetahui alur untuk respons pada insiden tersebut. Berikut merupakan status pada Darktrace Respond Action pada NDR Darktrace:

i. *Pending Action* pada dasarnya akan terisi ketika tim keamanan menerapkan *Human Confirmation Mode.* jika insiden respon tampil pada menu ini, hal ini mengindikasikan bahwa respons serangan tersebut belum berjalan sampai tim keamanan menekan aksi untuk jalankan respons serangan.

ii. *Active Action* menjelaskan bahwa aksi respons pada perangkat yang terlibat sedang berjalan. Ketika respons insiden sedang berjalan dan insiden tersebut sudah ditangani, maka tim keamanan bisa untuk mematikan respons serangan secara manual pada menu ini.

iii. *Cleared Action* menjelaskan terkait aksi respons yang sudah selesai. Pada menu ini, tim keamanan bisa untuk mengaktifkan kembali aksi respons dari perangkat yang terlibat.

iv. *Expired Action* memiliki fungsi seperti Riwayat respons yang sudah pernah dijalankan. Menu ini akan terisi secara otomatis apabila tidak ada aksi respons lanjutan pada menu *Cleared Action* dalam waktu beberapa hari. Namun, pada menu ini tetap dapat menjalankan respons yang sama kepada perangkat yang terlibat sebelumnya, jika terindikasi mengalami insiden yang serupa di masa depan.

b. *Reporting*

Pada saat terjadi sebuah insiden, tim keamanan perlu membuat laporan resmi sebagai dokumentasi terkait insiden yang terjadi. Laporan pada insiden harus memiliki informasi lengkap dari insiden tersebut agar bisa dijadikan sebagai referensi bagi perusahaan ketika terjadi insiden yang serupa. Laporan harus berisi berdasarkan informasi yang telah ditemukan maupun dilakukan pada fase maupun tahap sebelumnya. Untuk memperdalam informasi pada laporan, berikut merupakan informasi utama yang harus ada pada laporan insiden perusahaan:

i. Deskripsi Insiden

Laporan insiden harus memiliki rincian lengkap terkait insiden yang terjadi. Hal ini untuk menjelaskan kepada rekan tim keamanan lainnya tentang insiden apa yang terjadi pada waktu tersebut. Selain itu, laporan insiden harus menjelaskan waktu kejadian sampai waktu kejadian dapat ditanggulangi, sistem dan perangkat yang terpengaruh dari insiden tersebut, dan jenis dari insiden tersebut berdasarkan hasil dari fase *Validation* sebelumnya.

ii. Alur Pencegahan

Laporan insiden harus memiliki rincian terkait apa yang dilakukan tim keamanan dalam memitigasi serangan tersebut. Laporan ini harus memiliki uraian terkait langkah-langkah dalam merespons serangan seperti karantina perangkat dan tindakan yang diambil pada perangkat yang terlibat seperti menghapus malware dari perangkat tersebut.

iii. Hasil tindakan Respons

Laporan insiden harus ditutup dengan penilaian terhadap efektivitas langkah-langkah yang telah diambil oleh tim keamanan. Laporan harus memiliki informasi terkait hasil tindakan yang mencakup penilaian terhadap keberhasilan dalam mengatasi serangan serta dampak yang berhasil diredam atau diminimalkan sebagai hasil dari langkah-langkah yang telah dilaksanakan. Dengan demikian, laporan tidak hanya menjadi dokumentasi tentang peristiwa

yang terjadi, tetapi juga menjadi alat untuk mengevaluasi kinerja tim keamanan dalam menangani insiden tersebut.

3.2.4. *Remediation*

Fase *Remediation* adalah fase yang dimana tim keamanan melakukan tindakan memperbaiki dampak insiden dan mengembalikan sistem atau lingkungan yang terkena dampak ke keadaan normal dan aman. Selain itu, fase ini juga menjadi fase untuk memaksimalkan hasil pendeteksian dari NDR Darktrace dalam mendeteksi dan merespons serangan yang terjadi dimasa depan. Berikut merupakan langkah-langkah yang perlu dilakukan oleh tim keamanan pada fase *Remediation*:

a. Memonitoring Hasil Fase *Containment*

Setelah selesai melakukan fase *Containment*, tim keamanan perlu untuk untuk secara teratur untuk melakukan pemantauan pada perangkat yang terlibat. Tujuan dilakukannya adalah untuk memastikan bahwa insiden yang terjadi dapat tetap terkendali dan tidak menjadi masalah yang lebih serius. Melalui kegiatan pemantauan ini, tim keamanan dapat memutuskan perlu atau tidaknya langkah-langkah tindakan pencegahan lebih lanjut pada perangkat yang terlibat. Dengan demikian, monitoring tidak hanya berfungsi sebagai upaya pengendalian, tetapi juga sebagai sarana untuk meningkatkan proaktifitas dalam menjaga keamanan sistem.

Sesuai dengan penjelasan sebelumnya, langkah respons insiden NDR Darktrace bersifat sementara karena hanya bertujuan untuk mengganggu aktifitas percobaan serangan yang lebih jauh. Maka dari itu, tim keamanan harus monitoring terkait hasil yang sudah dilakukan pada fase containment sampai akar permasalahan dari insiden dapat ditemukan dan kasus manajemen insiden ditutup atau dinyatakan selesai.

b. Membuat *Recommendation Action*

Recommendation Action sebuah penentuan langkah-langkah yang harus diambil untuk mengendalikan insiden dan meminimalkan dampaknya. Dengan adanya *Recommendation Action*, tim keamanan akan lebih mudah dalam mengendalikan insiden, mencegah penyebaran serangan lebih lanjut, memulihkan keamanan dengan lebih cepat dan efektif, dan berupaya untuk memastikan serangan yang serupa tidak terjadi lagi dimasa depan. Berikut merupakan a informasi yang harus ada pada *Recommendation Action* pada insiden siber:

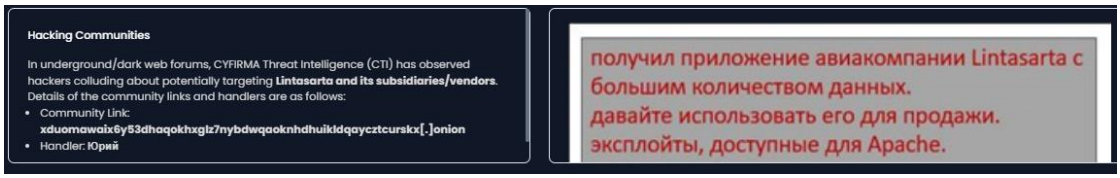
i. Rekomendasi Perbaikan

Ketika pada fase *Detection*, kemungkinan besar tim keamanan dapat menemukan kerentanan yang digunakan oleh *Threat Actor* yang menjadi akar penyebab insiden dapat terjadi. Untuk itu, maka tim keamanan harus melakukan aksi serta mendokumentasikan terkait langkah yang diambil pada perbaikan dari kerentanan tersebut.

Pada kasus yang terjadi di lintasarta, tim keamanan mengambil kesimpulan bahwasannya insiden terjadi dikarenakan ada salah satu port yang krusial yang terbuka pada salah satu domain di Lintasarta. Port yang terbuka adalah port 22 yang sengaja dibuka oleh tim keamanan namun mereka lupa untuk menutup kembali. Port ini merupakan port protokol *Secure Shell* (SSH) yang digunakan untuk administrasi jaringan yang aman, transfer file, dan operasi *remote command-line*.

Hal ini juga diperkuat dengan bantuan teknologi *Threat Intel* yang digunakan Lintasarta. *Threat intel* sendiri adalah teknologi yang bekerja dari sisi luar perusahaan. Sehingga teknologi ini akan memberikan informasi tentang kerentanan yang mungkin bisa dieksploitasi oleh penyerang dikarenakan kesalahan konfigurasi atau kelalaian pada tim keamanan dari internal perusahaan atau isntansi.

Pada *Threat Intel*, ternyata terdapat informasi yang dimana ada salah satu *threat actor* dari Rusia yang bernama FIN7. Dari informasi tersebut bertuliskan bahwa Threat Actor ini memberikan informasi kerentanan yang mereka dapatkan dari Lintasarta ke forum *Dark Web*. Informasi tersebut adalah mereka mendapatkan celah kerentanan pada domain Lintasarta yang dimana disana terdapat banyak data-data penting perusahaan. Berikut merupakan bukti informasi yang ditangkap Threat intel terkait insiden yang terjadi yang dilihat pada gambar 3.20.



Gambar 3.20 Informasi Insiden yang ditangkap *Threat Intel*

Pada informasi dari gambar 3.20, jika diartikan ke bahasa indonesia dapat dibaca menjadi ”Mendapatkan aplikasi dari Lintasarta dengan data penting yang banyak. mari kita gunakan untuk berjualan. Eksploitasi tersedia untuk Apache”. Dari informasi ini, tim keamanan langsung mengambil langkah tindakan lebih lanjut terhadap domain yang teridentifikasi agar insiden yang terjadi tidak berulang dari akar permasalahan yang sama.

Untuk tindakan utama yang diambil adalah menutup port tersebut. Namun, untuk memastikan insiden seperti ini dapat dihindari dengan lebih baik lagi. Tim keamanan menerapkan metode ”*IP Regional Lock*”, metode ini merupakan suatu tindakan pencegahan yang dimana domain-domain penting yang digunakan Lintasarta hanya dapat diakses dan diperlihatkan hanya jika perangkat tersebut terkoneksi dengan IP indonesia atau menggunakan VPN (*Virtual Private Network*) dari Indonesia.

Selain itu, tim keamanan juga melakukan pemeriksaan update *patch* dari sistem maupun alat keamanan dari Lintasarta. Setelah dilakukan tindakan perbaikan dan pembaruan *patch* keamanan, insiden atau koneksi serupa dengan insiden tidak teridentifikasi kembali oleh NDR Darktrace sehingga langkah penutupan *root cause* (akar permasalahan) kerentanan yang dieksploitasi dapat dibilang sukses.

Untuk memastikan kerentanan yang dikarenakan *open port* ini, tim keamanan tetap mencari informasi *open port* dari semua domain Lintasarta secara berkala. Sebenarnya open port ini dapat dilihat dengan teknologi *Threat Intel*. Namun, karena sistem ada kemungkinan celah yang dilewatinya, maka pencarian *open port* tetap dilakukan secara manual di Lintasarta untuk beberapa kasus Domain.

Dari permasalahan pencarian *open port* ini, tim keamanan tidak dapat melakukan pencarian informasi secara langsung menggunakan NMAP atau *tools scanning* lainnya. Hal ini dikarenakan perusahaan menengah dan besar menggunakan WAF (*Web Application Firewall*), sehingga memberikan informasi palsu pada saat kita mencari informasi dari suatu domain jika kita tidak tahu IP sebenarnya dari domain tersebut.

Hal inilah yang menjadi tantangan baru lagi dalam pencarian informasi, sehingga pada saat tersebut penulis diberikan sebuah tugas untuk melakukan validasi dari suatu port walaupun perusahaan tersebut menggunakan WAF pada *environment* mereka. Berikut merupakan syntax yang bertujuan untuk mengetahui open port pada suatu domain yang menggunakan WAF yang dapat dilihat pada tabel 3.1.

Tabel 3.1 *Syntax* validasi *Open Port*

Port	*Service*	*Syntax*
21	FTP	`ftp <IP>`
22	SSH	`ssh <IP TARGET>`
23	Telnet	`nmap -n -sV -Pn --script "*telnet* and safe" -p 23 <IP>`
25	SMTP	`nmap --script smtp-* -p 25 <IP>`
67/68	DHCP	`nmap -sU --script broadcast-dhcp-discover -p 67,68 <target-ip>`
80	HTTP	`http:// <IP TARGET>`
110	POP3	`nmap --script "pop3-capabilities or pop3-ntlm-info" -sV -p 110 <IP>`
123	NTP	`nmap -sU -sV --script "ntp* and (discovery or vuln) and not (dos or brute)" -p 123 <IP>`
135/539	RPC	`rpcclient -k <ip> atau rpcclient -W WORKGROUP -U username <target-ip>`
137	NetBIOS	`nmblookup -A <IP>`
143/993	IMAP	`nmap -p143,993 -sV --script=banner <IP TARGET>`
161	SNMP	`sudo nmap -sU -p 161 --script snmp-* <IP>`

389/636	LDAP	`nmap -n -sV --script "ldap* and not brute" -p 389,636 <DOMAIN>`
		
		`ldapsearch -x -b "dc=idola,dc=net,dc=id" "*" -H ldap://<IP> -D "cn=admin,dc=idola,dc=net,dc=id" -W`

443	HTTPS	`https:// <IP TARGET>`
444	SNPP	`https:// <IP TARGET>:444`
445	SMB	`nmap --script=smb2-security-mode -p 445 <IP>`
465	SMTP	`openssl s_client -crlf -connect <DOMAIN>:465 atau nmap --script smtp-* -p 465 <IP>`
1900	UPnP	`nmap -sU --script upnp-info -p 1900 <ip>`

2082/2083	CPanel	`nmap -A -p 2083 <DOMAIN TARGET> -sV`
		
		`<DOMAIN TARGET>:2083`

3306	MySQL	`nmap -sV -p 3306 --script mysql-audit,mysql-databases,mysql-dump-hashes,mysql-empty-password,mysql-enum,mysql-info,mysql-query,mysql-users,mysql-variables,mysql-vuln-cve2012-2122 <IP>`
		
		`mysql -h <DOMAIN> -u root@localhost`

3128	Proxy	`curl --proxy http://<IP>:3128 http://<IP>`
		
		`http://<ip>:3128/`

3389	RDP	`nmap --script "rdp-enum-encryption or rdp-vuln-ms12-020 or rdp-ntlm-info" -p 3389 <IP>`
4369	EPMD	`nmap -sV -Pn -n -T4 -p 4369 --script epmd-info <IP>`
5222	XMPP	`nmap --script=xmpp-info --script-args xmpp-ino.alt_server_name=value,xmpp-info.no_starttls=value -p 5222 <DOMAIN>`

Port	*Service*	*Syntax*
5432	PostgreSQL	`nmap -sV <IP> -p 5432`
5601	Elastic	`https://<ip>:5601`
5672	AMQP	`nmap -sV -Pn -n -T4 -p 5672 --script amqp-info <IP>`

5985/5986	WinRM	`nmap -p5985,5986 -sV <IP>`
		
		`http://<ip>:5985 dan https://<IP>:5986`

6001	X11	`nmap -sV --script x11-access -p 6001 <IP>`
6668	IRC	`nmap -sV --script irc-botnet-channels,irc-info,irc-unrealircd-backdoor -p 6668 <IP>`
6443	ArcGIS	`curl -k -v -H "Authorization: Bearer <jwt-token>" https://<IP>:6443/api/v1/namespaces/default/pods/`
7071	Oracle	`https://<DOMAIN>:7071`
7080	OPUtils	`https://<DOMAIN>:7080`
8200	Trivnet1	`http://<ip>:8200`

8443	Secure Web	`curl -i <DOMAIN TARGET>:8443`
		
		`https://<IP>:8443`

9200	CONNX	`https://<DOMAIN>:9200`

Dalam pembuatan dokumentasi rekomendasi perbaikan, informasi yang terdapat dalam Tabel 3.1 juga disertakan di dalamnya untuk memberikan panduan yang komprehensif kepada tim keamanan. Penambahan informasi ini bertujuan untuk memudahkan proses validasi apabila suatu saat diidentifikasi adanya insiden yang disebabkan oleh kasus Open Port di masa depan. Dengan menyertakan data dari Tabel 3.1, diharapkan tim keamanan dapat dengan lebih efektif untuk mengidentifikasi, menganalisis, dan menanggulangi insiden yang mungkin muncul.

ii. Alur pencegahan yang Efektif dan Efisien

Walaupun sudah melakukan rekomendasi perbaikan, bukan berarti membuat potensi serangan yang serupa menjadi tidak mungkin. Hal ini dikarenakan kerentanan pada sistem perusahaan dapat saja terjadi secara sengaja maupun tidak sengaja. Untuk itu, tim keamanan harus melakukan analisis mendalam untuk menentukan langkah mitigasi dan respons dari insiden yang serupa di masa depan. Hal ini bertujuan, untuk pengambilan langkah pencegahan yang efektif dan efisien sehingga membuat potensi kerugian serangan yang seminimal mungkin.

Pada alur pencegahan dari kasus sebelumnya, tim keamanan membuat alur yang kurang lebih sama dengan alur pencegahan pada fase *containment* sebelumnya. Untuk hal yang berbeda adalah tim keamanan lebih merincikan kriteria dari serangan tersebut. Tujuan

dilakukan hal ini adalah membantu dalam memastikan serangan yang terjadi di masa depan sama dengan insiden yang saat ini terjadi, sehingga mereka tidak perlu melakukan konfirmasi dari sumber eksternal pada fase validation, yang dimana tahap inilah yang paling banyak memakan waktu dalam melakukan manajemen insiden yang baru saja terjadi.

Setiap Alur pencegahan final yang dibuat Lintasarta, akan diberikan label yang sesuai dengan kriteria MITRE ATT&CK yang ditemukan sebelumnya. Tujuan dilakukan hal ini adalah untuk mempermudah tim keamanan dalam menemukan berkas alur pencegahan yang dibutuhkan dengan cepat pada saat insiden yang serupa karena banyaknya insiden yang sudah dimitigasi dan dilakukan verifikasi Perusahaan Lintasarta.

c. Konfigurasi hasil deteksi dan respons NDR Darktrace

Setelah tim keamanan sudah memastikan bahwa serangan sudah diatasi dengan baik, maka tim keamanan dapat mengambil langkah lebih lanjut untuk mendapatkan hasil deteksi yang optimal dari NDR Darktrace. Berdasarkan hasil dari yang didapatkan pada fase *Validation*, tim keamanan perlu untuk meningkatkan serta memperbaiki hasil dari pendeteksian dari NDR Darktrace.

Pada kasus sebelumnya, setelah dilakukan verifikasi bahwa ancaman adalah valid (*True-Positive*) dan dilakukan penutupan akar permasalahan yang menjadi celah kerentanan perusahaan yang dieksploitasi oleh penyerang, tim keamanan melakukan penentuan otomatisasi dari respon NDR Darktrace. Terdapat dua poin yang dilakukan konfigurasi pada respons NDR Darktrace pada insiden tersebut.

Poin awal yang dilakukan konfigurasi untuk membuat *respon state* pada insiden yang serupa menjadi *Force Autonomous Action*. Aksi ini berguna untuk membuat kriteria insiden yang serupa akan dilakukan respon otomatis selama 24 jam, sehingga pada waktu jam bekerja NDR Darktrace akan tetap melakukan respons otomatis.

Hal ini dilakukan untuk mengurangi resiko kerugian dan tersebarnya informasi melalui *Dark Web* terkait kerentanan yang ditemukan penyerang pada perusahaan Lintasarta. Serta aktivitas ini biasanya hanya dilakukan oleh orang-orang tertentu, sehingga NDR Darktrace akan mengetahui orang tersebut berkat bantuan *Self-Learning AI* yang dapat memahami alur kebiasaan penggunaan pada jaringan yang dimonitoringnya dan jika emang perlu dilakukan oleh orang baru, orang tersebut bisa menghubungi tim keamanan agar diberikan akses untuk terhubung ke proxy server perusahaan tanpa dilakukan respons oleh NDR Darktrace.

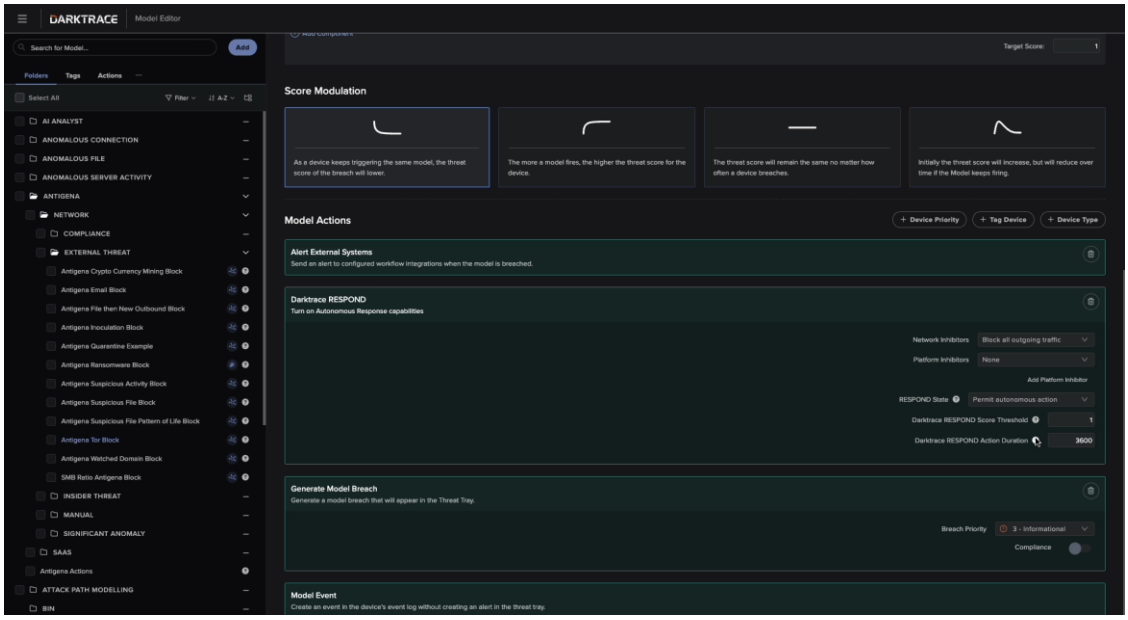
Untuk poin selanjutnya yang dilakukan konfigurasi adalah *Darktrace Respond Action Duration*. Aksi ini berguna untuk mengatur waktu berjalannya respons yang dilakukan NDR Darktrace kepada perangkat tersebut. Fitur respons NDR Darktrace bersifat tidak permanen, sehingga pada beberapa waktu respons insiden akan dimatikan secara otomatis oleh NDR Darktrace.

Pada kasus insiden, tim keamanan menetapkan waktu dilakukan respons insiden menjadi waktu maksimal respons yang bisa dilakukan NDR Darktrace, yaitu selama 10.800 detik (tiga jam). Alasan dibuat menjadi waktu maksimal adalah memberi waktu bagi tim keamanan ketika mereka tidak menyadari adanya ancaman pada malam hari, serta untuk memberikan waktu tim keamanan dalam melakukan validasi dari ancaman tersebut. Perlu diingat bahwa walaupun respons NDR Darktrace bersifat tidak permanen, namun aksi respons yang bisa dilakukan NDR Darktrace dapat dilakukan berulang kali pada perangkat yang sama.

Untuk penjelasan terkait konfigurasi yang perlu dilakukan tim keamanan terhadap respons yang dilakukan NDR Darktrace. Berikut merupakan poin-poin yang perlu diperbaiki oleh tim keamanan guna untuk meningkatkan hasil pendeteksian dan respons NDR Darktrace berdasarkan hasil dari fase *Validation*:

i. Pada Pendeteksian *True-Positive*

Pada saat insiden tersebut dinyatakan valid, tim keamanan dapat menyesuaikan konfigurasi pada pendeteksian NDR Darktrace untuk jenis insiden yang serupa. Tujuan dilakukan konfigurasi ini adalah untuk meningkatkan waktu dalam merespons insiden sehingga dapat meminimalkan kerugian yang lebih jauh lagi. Dalam mengatasi permasalahan ini, tim keamanan dapat mengubah hasil deteksi dan respons dengan menggunakan fitur yang disediakan NDR Darktrace. Berikut merupakan menu ubah respons NDR Darktrace yang dapat dilihat pada gambar 3.21.



Gambar 3.21 Menu ubah respons NDR Darktrace

Pada saat mengubah Tindakan respons ketika NDR Darktrace mendeteksi sebuah ancaman, terdapat beberapa menu pilihan yang dapat disesuaikan. Berikut merupakan beberapa maksud dari setiap aksi yang dapat dilakukan oleh tim keamanan untuk mengubah aksi respons NDR Darktrace:

- *Network Inhibitors* berguna untuk menentukan langkah respons terkait koneksi jaringan yang akan diterapkan kepada perangkat yang terlibat.
- *Platform Inhibitors* berguna untuk menghentikan atau menghambat akses ke platform yang dituju perangkat tersebut.
- *Respond State* berguna untuk menentukan Langkah respon otomatis dari insiden tersebut. Menu ini memberikan tiga opsi, yaitu *Force Human Action* yang bermaksud untuk melakukan konfirmasi kepada tim keamanan terlebih dahulu sebelum menjalankan tindakan respons, *Force Autonomous Action* yang bertujuan untuk menjalankan aksi respon secara langsung ketika terjadi peringatan serangan tersebut, dan *Permit Autonomous Action* yang bertujuan untuk menjalankan aksi respon berdasarkan konfigurasi respon otomatis yang telah dikonfigurasi sebelumnya.
- *Darktrace Respond Score Threshold* berguna untuk menentukan prioritas respon dari insiden tersebut. Semakin kecil angka dari respond scorenya maka akan

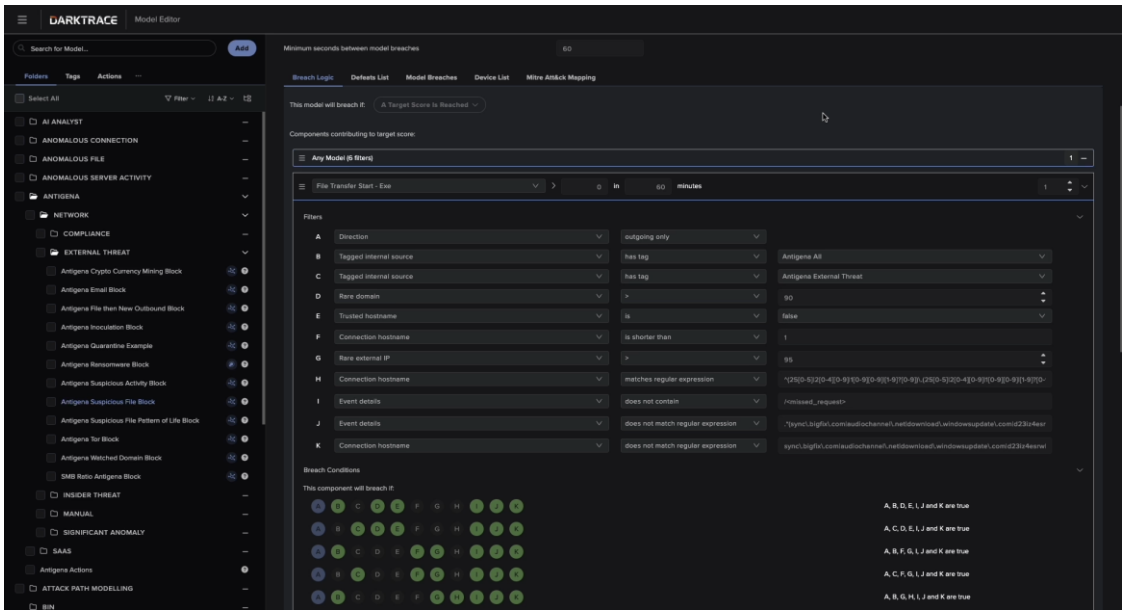
semakin cepat dilakukan tindakan respon ketika terjadi peringatan insiden tersebut.

- *Darktrace Respond Action Duration* berguna untuk menjelaskan rentang waktu berjalannya aksi respons dari insiden. Satuan dari waktunya adalah *Second* (detik), sehingga jika dimasukkan angka 3600 mengindikasikan bahwa aksi respons ancaman akan berjalan selama satu jam.

Setiap tindakan konfigurasi yang dilakukan pada *rules* serangan dalam sistem NDR Darktrace akan secara otomatis disimpan dan disesuaikan oleh sistem. Selain itu, konfigurasi yang dilakukan akan dipelajari oleh NDR Darktrace guna untuk diterapkan pada sebuah *rules* serangan baru, jika NDR mempelajari bahwa ada potensi anomali yang kurang lebih serupa di masa depan.

ii. Pada Pendeteksian *False-Positive*

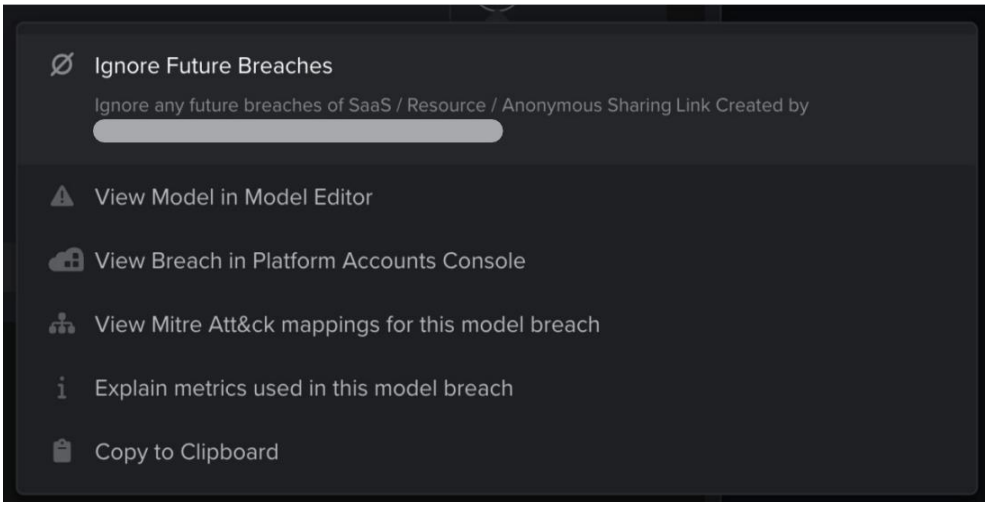
Ketika hasil pendeteksian yang dideteksi oleh NDR Darktrace berupa peringatan palsu, terdapat beberapa langkah yang perlu dilakukan oleh tim keamanan agar kejadian tersebut tidak terjadi kembali di masa depan. Salah satu langkahnya yaitu, tim keamanan dapat mengubah *rule* pendeteksian NDR Darktrace agar sesuai dengan ancaman yang dapat mungkin terjadi pada kategori serangan tersebut. Berikut merupakan menu mengubah rule pendeteksian NDR Darktrace yang dapat dilihat pada gambar 3.22.



Gambar 3.22 Menu mengubah *rule* NDR Darktrace

Pada menu ubah rule, tim keamanan dapat menambahkan dan mengurangkan rule pada pendeteksian insiden tersebut. Selain itu juga, NDR Darktrace membuat Breach Condition yang bertujuan untuk menentukan rule apa saja yang harus terpenuhi untuk menghidupkan alarm peringatan adanya insiden. Pada Breach Condition, terdapat tiga warna untuk penentuan pengkategorian rule, yaitu untuk warna biru mengkategorikan bahwa semua kolom Breach condition harus memenuhi persyaratan tersebut tanpa terkecuali pada barisnya, pada warna hijau mengindikasikan bahwa insiden harus memenuhi pada poin tersebut, dan warnah abu-abu mengindikasikan bahwa insiden harus tidak memenuhi pada poin tersebut.

Selain dapat mengubah pendeteksian pada suatu insiden, NDR Darktrace juga dapat menerapkan whitelist pada jenis insiden tersebut. *Whitelist* merupakan daftar-daftar yang berisi kegiatan yang diizinkan atau dianggap aman oleh sistem sehingga tidak akan menimbulkan peringatan ancaman (Doe J, 2023). Untuk menu whitelist, tim keamanan dapat mencarinya di fitur *Model Breach* pada menu *Three Idots Icon*. Berikut merupakan menu untuk menerapkan whitelist pada NDR Darktrace yang dapat dilihat pada gambar 3.23.



Gambar 3.23 Menu *Whitelist* pada NDR Darktrace

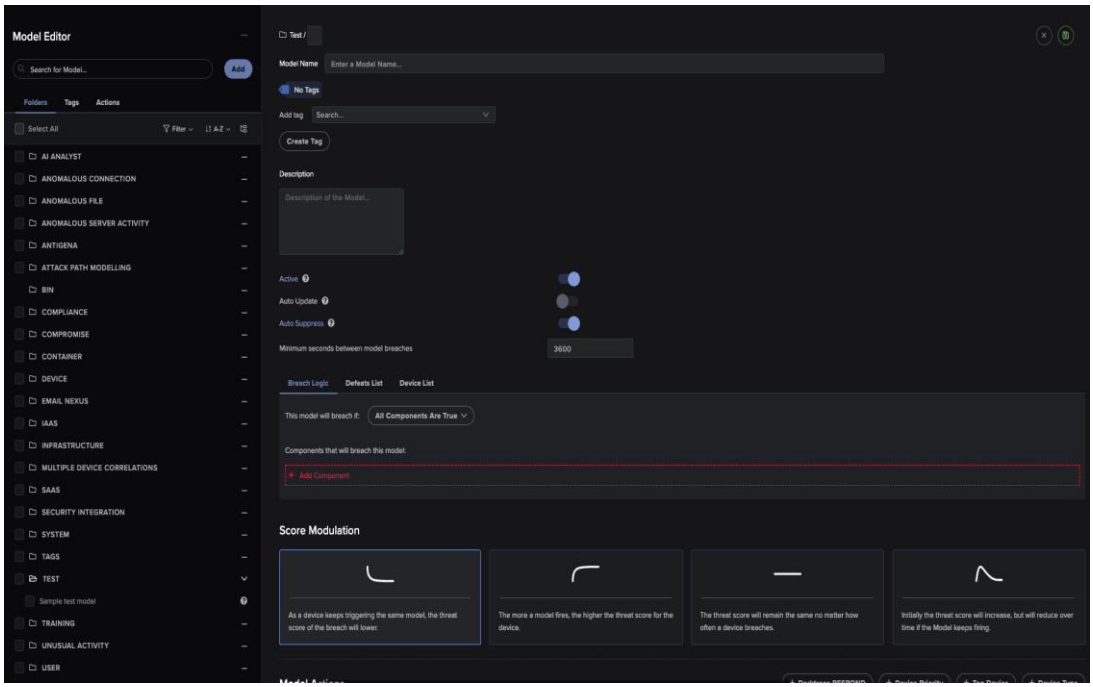
iii. Pada Pendeteksian *False-Negative*

Dalam konteks keamanan siber, tidak ada satupun teknologi yang dapat memberikan perlindungan menyeluruh. Hal ini juga berlaku untuk NDR Darktrace, yang meskipun canggih, masih memiliki keterbatasan dalam mendeteksi semua jenis ancaman yang mungkin mengancam aset vital perusahaan. Oleh karena itu, sangat penting bagi perusahaan untuk menggunakan alat keamanan lainnya agar dapat membangun pertahanan yang lebih kuat dan menyeluruh. Sebagai alat pendukung NDR, beberapa teknologi yang sering digunakan

termasuk Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), Firewalls, dan Network Traffic Analysis (NTA).

Dengan menerapkan teknologi yang berguna sebagai alat pendukung NDR, perusahaan dapat memperluas cakupan deteksi dan meningkatkan kemampuan respons terhadap insiden keamanan di tingkat jaringan, sehingga menciptakan lapisan pertahanan yang lebih komprehensif dan efektif dalam melindungi aset penting dari berbagai kemungkinan serangan.

Selain itu, untuk mengatasi keterbatasan dalam deteksi oleh NDR Darktrace, Terdapat fitur yang memungkinkan tim keamanan untuk mengembangkan dan mengimplementasikan model deteksi serta respons secara manual. Fitur ini sangat vital karena memberikan kesempatan kepada tim keamanan untuk menyesuaikan sistem deteksi sesuai dengan ancaman spesifik yang dihadapi perusahaan, sehingga dapat memperkuat keamanan secara keseluruhan serta meningkatkan efektivitas dari NDR Darktrace dalam mengidentifikasi dan merespons ancaman. Fitur ini dapat diakses melalui menu *Model Editor* yang ditampilkan pada gambar 3.24, yang mana memfasilitasi pengguna dalam merancang dan menerapkan strategi keamanan yang lebih adaptif dan target yang sesuai dengan kebutuhan perusahaan.

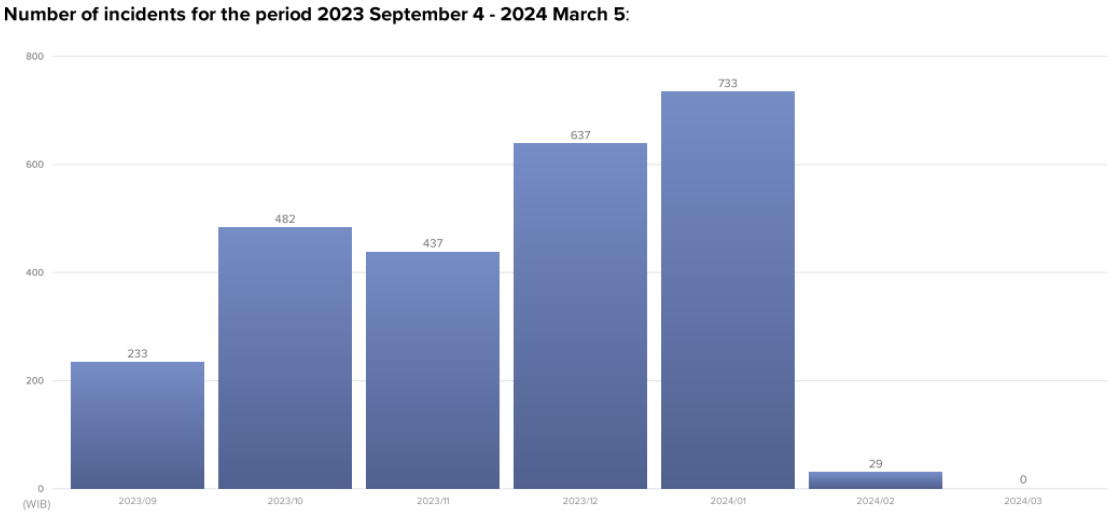


Gambar 3.24 Menu Pembuatan Model NDR Darktrace

3.2.5. Hasil Percobaan Manajemen insiden

Setelah menjelaskan terkait alur manajemen insiden serta menunjukkan bukti efektivitas dari rangkaian langkah manajemen insiden yang dibuat oleh penulis kepada tim yang mengoperasikan NDR Darktrace. Tim keamanan mulai menerapkan langkah-langkah manajemen insiden tersebut pada bulan februari agar bisa diterapkan dalam melakukan mitigasi ancaman pada kasus insiden kedepannya yang dideteksi oleh NDR Darktrace.

Setelah penerapan manajemen insiden pada NDR Darktrace, terjadi perubahan signifikan dalam pendeteksian dan pengendalian anomali jaringan perusahaan lintasarta. Hal ini dapat dilihat melalui grafik jumlah insiden yang berhasil dimitigasi oleh NDR Darktrace. Berikut merupakan tampilan grafik mitigasi insiden NDR Darktrace yang dapat dilihat pada gambar 3.25.



Gambar 3.25 Grafik Mitigasi Insiden NDR Darktrace

Pada gambar 3.25, dapat dilihat adanya ketimpangan data yang cukup jauh. Ketimpangan terjadi karena pada bulan September adalah waktu NDR Darktrace baru digunakan oleh perusahaan, sehingga NDR Darktrace mempelajari alur operasional perusahaan pada waktu tersebut. Oleh karena itu, hasil mitigasi insiden pada bulan tersebut relatif rendah dibandingkan bulan-bulan berikutnya.

Pada bulan Oktober – Januari, terdapat lonjakan yang signifikan. pada periode ini, manajemen insiden NDR Darktrace belum diterapkan. Hal ini disebabkan oleh beberapa faktor, seperti perlunya pembuatan dokumen pengadaan barang agar bisa dikomersilkan serta penentuan alur manajemen insiden yang tepat. Selain itu, periode ini digunakan untuk menguji kinerja NDR Darktrace dalam merespons insiden secara otomatis tanpa adanya manajemen insiden.

Pada bulan Februari, setelah dikembangkannya manajemen insiden dan dicoba untuk diterapkan, terdapat perubahan yang signifikan pada NDR dalam mendeteksi dan merespons insiden. Hal ini membuktikan bahwa insiden respons yang menerapkan manajemen insiden diimplementasikan dengan baik pada teknologi NDR Darktrace.

BAB 4
REFLEKSI PELAKSANAAN MAGANG

4.1. Relevansi Akademik

Selama pelaksanaan kegiatan magang, terdapat banyak kesenjangan yang telah dipelajari selama masa perkuliahan dengan penerapannya selama magang. Ilmu akademik yang penulis dapatkan merupakan referensi selama pembelajaran melalui perkuliahan dan pembelajaran melalui kegiatan studi independen MSIB di perusahaan Metrodata Academy pada tanggal 16 Februari 2023 – 30 Juni 2023.

Kesenjangan yang menjadi masalah utama adalah kurang updatenya informasi dalam dunia akademik dengan informasi yang sudah digunakan oleh berbagai perusahaan atau instansi saat ini dalam konteks keamanan siber. Karena kesenjangan ini, membuat penulis harus mempelajari banyak informasi terbaru secara independen agar bisa bekerja secara optimal dalam proses pelaksanaan magang.

Kesenjangan pertama adalah kurang updatenya dalam pembahasan teknologi keamanan yang digunakan. Selama pelaksanaan magang, teknologi yang penulis pernah pelajari dan gunakan adalah *Network Detection and Response* (NDR), *Endpoint Detection and Response* (EDR), *Threat Intelligence*, *Digital Forensic* (DFIR), dan *Management Center* untuk teknologi *Digital Forensic*.

Dari semua teknologi yang sudah disebutkan, tiga dari lima teknologi tersebut merupakan teknologi yang tidak pernah disinggung atau dipelajari selama masa perkuliahan. Kesenjangan ini membuat proses magang agak terhambat, karena untuk menunjang dalam penggunaan teknologi tersebut, penulis harus setidaknya belajar selama dua bulan lebih agar bisa memahami fungsi dan kegunaan dari teknologi tersebut secara lebih baik.

Selanjutnya, tidak adanya dalam kurikulum akademik terkait pembahasan mengenai perusahaan pengembang teknologi keamanan yang beroperasi secara global. Penjelasan mengenai perusahaan-perusahaan ini sangat penting karena mereka memainkan peranan krusial dalam ekosistem keamanan siber. Hal ini sangat relevan terutama di Indonesia, karena saat ini belum ada perusahaan yang aktif dalam mengembangkan teknologi keamanan siber. Pemahaman yang lebih mendalam tentang perusahaan-perusahaan pengembang ini akan membantu mahasiswa dalam memahami keunggulan dan kelemahan dari berbagai alat keamanan yang digunakan oleh perusahaan atau instansi di seluruh dunia.

Setelah itu terdapat kesenjangan pada pembelajaran tentang berbagai *tolls* yang digunakan oleh *Script Kiddies* dalam dunia akademik. *Script Kiddies* sendiri adalah individu yang menggunakan program dan skrip/*payload* yang telah dibuat oleh orang lain untuk melakukan kegiatan atau percobaan penyerangan cyber, tanpa memahami secara mendalam cara kerjanya.

Pendidikan akademik seringkali lebih berfokus pada pengajaran penggunaan *tools* keamanan siber yang sederhana dan mudah digunakan. Memang, *Tools* yang dipelajari emang efektif dalam melakukan percobaan serangan pada sebuah *website dummy* yang disediakan. Akan tetapi, penerapan teknik-teknik yang diajarkan ini menjadi sangat sulit, bahkan bisa dibilang mustahil, jika dicoba terapkan pada *website* yang asli. Hal ini dikarenakan pada *website* yang asli memiliki sistem keamanan yang jauh lebih kompleks dan matang.

Pada kasus nyatanya, tim keamanan menggunakan *tools* keamanan siber yang lebih kompleks dan canggih, seperti Burp Suite, Metasploit, wireshark, dan lainnya dalam mendukung pekerjaannya sebagai *red team* dalam melakukan *manual penetration system* (Pentest) . Tools ini digunakan oleh tim keamanan karena tools dapat digunakan dalam berbagai kasus, mulai dari *website dummy* sampai *website* asli.

Dan kesenjangan terakhir terdapat pada metodologi terkait manajemen insiden yang penulis gunakan sebagai tugas akhir. Selama proses pembelajaran, terdapat beberapa metodologi yaitu ”*6- Step Incident Handling*” yang dikembangkan oleh SANS *Institute*, ”*Computer Security Incident Handling Guide*” yang dikembangkan oleh NIST800-61, dan ”*Good Practise Guide for Incident Management*” yang dikembangkan oleh ENISA.

Faktanya, perusahaan atau instansi mayoritas mengimplementasikan metodologi ”*Computer Security Incident Handling Guide*” yang dikembangkan oleh NIST800-61 sebagai acuan utama. Hal ini umumnya dikarenakan perusahaan akan mengembangkan dan menyesuaikan metodologi tersebut agar lebih sesuai dengan pemahaman dan kebutuhan spesifik tim keamanan mereka.

Dari kesenjangan yang dijelaskan sebelumnya, dapat disimpulkan masih banyak kesenjangan ilmu dalam akademik dengan kegiatan magang sebagai *Blue Team* maupun *Red Team*. Dari permasalahan tersebut membuat penulis lebih banyak belajar secara independen selama kegiatan magang. Hal ini dilakukan penulis agar dapat mendukung pekerjaan yang diberikan serta mempermudah penulis dalam berbicara serta berkonsultasi kepada mentor magang dan teman kerja di Lintasarta.

4.2. Pembelajaran Magang

Pembelajaran dari pengalaman yang penulis peroleh selama menjalani magang di perusahaan PT. Aplikanusa Lintasarta di bidang keamanan siber mencakup aspek-aspek berikut:

4.2.1. Manfaat Magang

Selama melaksanakan kegiatan magang di Lintasarta kurang lebih enam bulan, terdapat banyak manfaat serta pelajaran didapatkan oleh penulis, yang dimana hal ini sangat membantu penulis dalam mempersiapkan diri pada lingkungan profesional. Lintasarta memberikan kesempatan kepada seluruh peserta magang untuk melakukan pekerjaan yang sesuai dengan yang dilakukan oleh para pekerja kontrak maupun tetap. Berikut adalah beberapa manfaat magang yang penulis peroleh diantaranya:

a. Pemahaman Teknologi keamanan siber dengan lebih baik

Teknologi keamanan memiliki jenis yang sangat banyak dan akan terus berkembang setiap tahunnya. Berkat kesempatan magang, penulis dapat mempelajari banyak jenis teknologi keamanan dengan bertanya kepada rekan kerja satu divisi serta penulis juga diberikan kesempatan untuk mengoperasikan beberapa jenis teknologi keamanan yang digunakan perusahaan. Selain itu, dengan diberikannya kesempatan untuk mengikuti pelatihan, penulis jadi dapat lebih dalam memahami lebih dalam untuk menggunakan beberapa teknologi keamanan.

Faktanya, setiap teknologi keamanan terbaru yang ada saat ini mayoritas merupakan evolusi dari teknologi keamanan tradisional yang memiliki kegunaan dan fungsi yang sama. Hal ini berlaku juga pada NDR yang dimana teknologi ini merupakan evolusi dari teknologi *Intrusion Prevention System* (IPS) dan *Network Traffic Analysis* (NTA) yang merupakan evolusi dari teknologi *Intrusion Detection System* (IDS). teknologi tersebut memiliki peran dan fungsi yang kurang lebih sama yaitu mendeteksi dan melindungi perusahaan atau instansi dalam serangan melalui jaringan internet.

Selama kegiatan magang, penulis diminta untuk mencari berbagai macam perbedaan dari teknologi NDR dengan teknologi yang memiliki peran yang kurang lebih sama. Tujuan Lintasarta memerintahkan untuk membuat perbandingan ini adalah agar dapat mencari perbedaan terkait kekurangan dan keunggulan dari setiap teknologi.

Pada kasus perbandingan pertama, penulis diminta untuk mencari perbedaan antara NDR dan NTA. Kasus pertama ini menjadikan pijakan utama penulis dalam memahami apa itu NDR dan bagaimana cara kerjanya. Tugas ini merupakan tugas pertama yang berkaitan dengan tugas utama yang diberikan oleh mentor kepada penulis. Berikut merupakan perbedaan dari NTA dan NDR yang dapat dilihat pada tabel 4.1.

Tabel 4.1 Perbedaan Antara NTA dan NDR

Fitur	NTA	NDR
Fokus	Berfokus pada mendeteksi tren, pola, dan anomali ancaman keamanan.	Berfokus untuk mendeteksi, menginvestigasi dan merespons ancaman keamanan secara *real-time*.
Teknik	Menggunakan *Static Analytics*, *Behavioral Analytics*, dan *Pattern Analytics*.	Menggunakan *Automation response*, *Behavioral Analytics,* dan *Threat Intelligence*.
Tujuan	Memberikan visibilitas yang lebih baik pada traffic jaringan yang dimonitoring.	Melakukan respons serangan berdasarkan anomali yang dideteksi dengan cepat dan efektif.
Kebutuhan	Untuk mendukung teknologi tradisional dalam mendeteksi serangan yang tidak dapat dideteksinya.	Mendukung perusahaan atau instansi dalam merespons serangan yang berpotensi agar tidak memberikan kerugian.
Kemampuan	Dapat mendeteksi anomali dari suatu jaringan untuk memperkaya informasi dan dapat diintegrasi dengan SIEM dan teknologi keamanan lainnya.	Dapat mendeteksi serangan anomali pada jaringan dan merespons anomali tersebut secara otomatis dari teknologi secara langsung. Serta dapat diintegrasikan dengan teknologi lainnya seperti SIEM jika diperlukan.

Di Lintasarta, kedua teknologi ini digunakan dalam melindungi aset penting perusahaan dan dijadikan layanan untuk diberikan kepada pelanggan. Kedua teknologi ini dipisahkan oleh Lintasarta berdasarkan tim atau kelompok tim keamanan yang ada. Hal ini dilakukan karena bedanya tugas dan peran yang diberikan oleh NDR dan NTA.

Pada kasus NTA, teknologi ini dimasukkan kedalam paket jika calon klien ingin berlangganan SIEM kepada Lintasarta. Alasan dimasukkan ke dalam paket SIEM adalah karena tugasnya yang hanya mendeteksi serangan pada jaringan, sehingga teknologi ini dapat mendukung dan memperkaya log informasi yang dipelajari oleh SIEM dan akan dilakukan respons serangan secara otomatis oleh teknologi SOAR jika perusahaan atau instansi tersebut menggunakannya.

Pada kasus NDR, teknologi ini masuk kepada paket khusus berlangganan NDR saja. Hal ini dikarenakan fungsinya yang sudah cukup lengkap, yaitu dapat melakukan deteksi, investigasi, dan respons serangan secara otomatis maupun manual dari teknologi NDR itu sendiri. Serta pada kasus di Lintasarta, NDR akan digunakan oleh tim khusus yang hanya melakukan monitoring pada teknologi *Detection and Response*, seperti NDR dan EDR.

Untuk kegiatan perbandingan kedua adalah melakukan perbandingan antara NDR dengan IPS. Hal ini dilakukan untuk untuk mencari perbedaan utama antara keduanya karena IPS adalah salah satu teknologi keamanan utama yang digunakan oleh perusahaan atau instansi dalam melindungi aset mereka pada lingkungan jaringan. Berikut merupakan tabel perbedaan antara IPS dan NDR yang dapat dilihat pada tabel 4.2.

Tabel 4.2 Perbedaan Antara IPS dan NDR

Fitur	IPS	NDR
Definisi	Sistem keamanan tradisional yang beroperasi di jaringan untuk mendeteksi dan mencegah serangan berdasarkan aturan atau *signature* dari informasi serangan yang sudah terjadi sebelumnya.	Sistem keamanan modern yang menggunakan metode berbasis perilaku dengan analitik canggih, pembelajaran mesin, dan AI untuk mendeteksi, menganalisis, dan merespon ancaman keamanan dalam jaringan secara *real-time*.
Fokus	Mendeteksi dan melakukan respons serangan berdasarkan rules serangan yang telah dimasukkan atau terdaftar pada teknologi.	Mendeteksi dan melakukan respons serangan berdasarkan anomali dari penggunaan suatu perusahaan atau instansi yang dimonitoring.
Metode Pendeteksian	Berbasis aturan dan *signature* untuk mengidentifikasi dan menghalangi serangan.	Menggunakan analisis perilaku, analitik canggih, dan korelasi untuk mendeteksi ancaman yang tidak sesuai dengan pola lalu lintas normal yang dipelajari NDR itu sendiri atau biasa disebut *Behavioral-Based*.
Respons Ancaman	Dapat melakukan blokir atau karantina jaringan pada suatu perangkat dan diintegrasikan dengan firewall untuk pencegahan serangan terpadu.	Menggunakan metode TCP Reset dalam melakukan respons, sehingga memberikan opsi respons yang lebih beragam kepada suatu perangkat menggunakan alat dari NDR secara langsung.

Fitur	IPS	NDR
Kemampuan Adaptasi	Pembaruan *rules* pada *Signature rules* bergantung kepada perusahaan yang mengembangkan teknologi IPS itu sendiri.	Pembaruan *rules* pada *Behavioral-Based* akan dilakuan secara *real-time* selama teknologi NDR dapat membaca setiap log aktivitas dari perusahaan atau instansi.
Keunggulan	Efektif dalam mendeteksi dan merespons serangan yang sudah dikenal dan harganya yang tergolong murah dari teknologi serupa lainnya, membuat IPS berguna sebagai jantung perlindungan pada tingkat jaringan setelah firewall.	Efektif dalam mendeteksi berbagai macam potensi serangan termasuk serangan *Zero-day*, serta NDR dapat Memberikan visibilitas yang luas terhadap aktivitas jaringan, memungkinkan identifikasi dan analisis perilaku yang mencurigakan secara mendetail.
Keterbatasan	Teknologi ini tidak efektif dalam mendeteksi dan merespons serangan *zero-day*, karena rules dari serangan tersebut tidak terdaftar pada teknologi IPS itu sendiri.	Teknologi ini tidak dapat berfungsi pada bulan awal pemasangan, Hal ini dikarenakan NDR memerlukan waktu untuk mempelajari alur aktivitas dari perusahaan atau instansi sebelum dia dapat membuat rules serangan dibuat secara otomatis. Serta, karena besarnya modal yang harus dikeluarkan untuk penggunaan teknologi NDR membuat tidak semua perusahaan atau instansi dapat atau mau menggunakan teknologi ini.

Walaupun NDR dapat melakukan tugas deteksi dan respons lebih baik daripada IPS. Faktanya, teknologi NDR tidak dapat menggantikan fungsi dan tugas dari IPS secara keseluruhan. Hal ini dikarenakan NDR hanya mengandalkan pendeteksian *Behavioral-Based* yang hanya mendeteksi anomali serangan, sehingga ada kemungkinan beberapa serangan yang bisa dideteksi IPS dapat terlewat oleh teknologi NDR dan membuat celah pada deteksi serangan.

Pada saat menjalani magang, penulis dapat kesempatan untuk mengikuti kegiatan *NDR Enabling*. Kegiatan ini diikuti oleh beberapa perwakilan karyawan Lintasarta dengan beberapa tim pengembang dari Darktrace secara daring dengan tujuan untuk memastikan tidak adanya kesalah pahaman dari tim Lintasarta terkait fitur-fitur yang ada pada NDR Darktrace. Pada kegiatan tersebut, tim dari Darktrace menjelaskan bahwa NDR tidak dimaksudkan untuk menggantikan tugas IPS; sebaliknya, kedua teknologi ini seharusnya bekerja sama agar bisa saling melengkapi dalam menutup celah deteksi serangan yang terjadi.

Dari pembahasan NDR ini, penulis tidak hanya mendapatkan pemahaman dari satu teknologi saja, melainkan dapat tiga ilmu yang berharga karena membahas NDR beserta ada beberapa pemahaman dari teknologi yang tidak bersangkutan dengan NDR seperti, EDR, *Threat intel*, *Digital Forensic* (DFIR), *NGFW*, *NGAV*, dan lain sebagainya. Pengalaman ini sangat membantu penulis dalam memperluas wawasan tentang bagaimana teknologi-teknologi keamanan jaringan bekerja secara komplementer. Serta Pengetahuan ini tidak hanya meningkatkan kemampuan teknis penulis, tetapi juga memperkuat kemampuan penulis dalam berkomunikasi dan berkolaborasi dengan berbagai pihak dalam lingkungan kerja yang dinamis.

b. Memahami Masih Pentingnya SDM Dalam Konteks *Cybersecurity*

Karena semakin majunya dunia teknologi, membuat semua aspek dalam dunia IT menjadi maju secara signifikan. Hal ini juga berlaku pada konteks keamanan siber, yang dimana mayoritas teknologi yang ada saat ini sudah dapat melakukan deteksi dan respons serangan secara mandiri.

Namun selama melaksanakan kegiatan magang, penulis menyimpulkan bahwa manusia tetap menjadi salah satu faktor yang harus ada dalam konteks keamanan siber saat ini. Keberadaan dan peran manusia sangat penting karena mereka tidak hanya bertindak sebagai pengguna akhir yang harus dilindungi, tetapi juga sebagai pelaksana dan pengelola sistem keamanan itu sendiri. Tanpa adanya kesadaran, pengetahuan, dan kepatuhan dari manusia terhadap protokol keamanan, teknologi secanggih apapun tidak akan mampu memberikan perlindungan yang optimal.

Alasan utama diperlukan manusia dalam keamanan siber adalah karena teknologi keamanan tradisional maupun modern saat ini masih banyak memberikan hasil peringatan palsu (*False-Negative*). Permasalahan ini membuat perusahaan atau instansi tidak dapat hanya mengandalkan teknologi keamanan yang ada saat ini dalam melindungi aset penting mereka tanpa bantuan dari manusia yang ahli di bidang keamanan siber.

Bagi tim keamanan, permasalahan *false-negative* menjadi tantangan bagi mereka untuk bisa diatasi. Terdapat banyak dampak negatif jika permasalahan ini tidak segera diatasi, salah satunya yaitu hilangnya kewaspadaan tim keamanan jika ada insiden yang valid (*True-Negative*). Permasalahan ini terjadi karena tim keamanan seringkali terbebani dengan jumlah peringatan palsu yang tinggi yang mereka deteksi dan analisis. Akibatnya, hal ini dapat mengarah pada persiapan yang kurang optimal dalam menghadapi ancaman nyata, karena sumber daya yang terbatas terbuang pada insiden yang tidak relevan.

Pada kasus NDR Darktrace, setiap respons serangan dapat dikategorikan menjadi dua aksi, yaitu aksi respons otomatis dan aksi respons dengan konfirmasi manusia. Pada kategori aksi respons dengan konfirmasi manusia, setiap permintaan perizinan respons serangan akan masuk kedalam halaman '*pending action'*. Permintaan tersebut akan terus menumpuk jika tim keamanan tidak segera mengambil aksi yang perlu dilakukan. Untuk aksi yang bisa dilakukan tim keamanan adalah menjalankan aksi respons atau menghapus aksi respons.

Karena banyaknya kasus *false-negative* yang terjadi pada waktu tersebut, membuat permintaan aksi menjadi sangat banyak. Hal ini menyebabkan penundaan dalam waktu respons, yang pada gilirannya meningkatkan waktu yang diperlukan untuk mengatasi ancaman secara efektif. Permasalahan ini membuat tim keamanan mengalami kesulitan dalam mengelola dan memprioritaskan tindakan yang kritis. Untungnya semua insiden valid dapat teratasi pada waktu tersebut, akan tetapi tetap ada potensi risiko kerusakan yang lebih besar di masa depan akibat serangan yang tidak teratasi jika permasalahan *false-negative* ini tidak segera diatasi.

Dari permasalahan tersebut, maka manusia yang berperan sebagai tim keamanan harus dapat mencari solusi dalam mengatasi *false-positive*. Salah satu cara efektif dalam mengatasi permasalahan ini adalah dengan menerapkan langkah manajemen insiden respons pada setiap teknologi keamanan. Dengan langkah ini, setiap kejadian dapat diinvestigasi secara mendalam, memastikan bahwa tindakan yang diambil berdasarkan analisis yang akurat dan tepat, dan memastikan teknologi keamanan dapat mendeteksi dan merespons insiden yang valid di masa depan, sehingga dapat mengurangi risiko kesalahan dalam mengidentifikasi ancaman yang sebenarnya tidak ada. Implementasi proses ini tidak hanya meningkatkan efektivitas sistem keamanan, tetapi juga memperkuat kepercayaan dan keamanan informasi bagi perusahaan atau instansi.

c. Gambaran Tugas Dalam Lingkungan Profesional

Berkat peran Lintasarta yang merupakan sebuah perusahaan berperan sebagai penyedia jasa Teknologi Informasi. Penulis dapat mempelajari alur pekerjaan antara perusahaan penyedia jasa (Vendor) dan pengguna layanan (*End User*). Serta penulis juga memahami dinamika interaksi antara penyedia jasa (vendor) dan pengguna layanan (end user) dalam konteks keamanan siber.

Selain itu, dengan mengamati terkait cara tim keamanan Lintasarta dalam mengimplementasikan protokol keamanan siber dan kolaborasi antara tim keamanan dalam mengamankan aset perusahaan lintasarta sendiri dan instansi lainnya telah membuka wawasan penulis terkait bagaimana teknologi keamanan dapat diintegrasikan dalam setiap aspek operasional bisnis. Dari sini penulis belajar tentang berbagai ancaman siber yang dapat mengganggu operasi bisnis dan cara efektif untuk mengatasinya tanpa mengganggu operasional bisnis perusahaan dalam skala besar. Serta dengan diberinya kesempatan dalam melakukan pelatihan pada beberapa teknologi yang digunakan, penulis dapat memahami tentang pentingnya keberlanjutan dan adaptasi dalam strategi keamanan siber dalam melindungi aset dan data perusahaan atau instansi.

Lebih lanjut, dengan kesempatan berpartisipasi dalam rapat mingguan divisi untuk berdiskusi tentang strategi keamanan selanjutnya dan sesi brainstorming memberikan wawasan baru bahwa pentingnya komunikasi dan kolaborasi dalam menyelesaikan tugas bersama dan mengatasi permasalahan yang dialami setiap individu. Pengalaman ini tidak hanya meningkatkan pengetahuan teknis penulis tetapi juga memperkuat kemampuan analitis dan strategis dalam menghadapi masalah keamanan siber yang dinamis.

Secara keseluruhan, pengalaman ini memperkaya pemahaman penulis tentang pentingnya keamanan siber dalam bisnis modern dan bagaimana penyedia jasa keamanan seperti Lintasarta memainkan peran kunci dalam mengamankan infrastruktur TI dari perusahaan-perusahaan klien mereka. Ini menegaskan betapa pentingnya memiliki kerangka kerja keamanan yang kuat dan responsif dalam menjaga integritas dan keandalan sistem informasi.

d. Validasi Pemahaman

Terkadang, informasi yang didapatkan selama belajar mandiri dapat menimbulkan kesalahpahaman yang membingungkan. Namun, Dengan mengikuti magang penulis dapat memvalidasi pemahaman tersebut dengan mentor dan rekan kerja di divisi yang sama. Melalui interaksi langsung ini, penulis dapat memperoleh wawasan praktis yang lebih mendalam, menerima umpan balik konstruktif, serta belajar dari pengalaman dan pengetahuan profesional yang lebih berpengalaman.

Melalui pengalaman magang ini, penulis tidak hanya memperbaiki pemahaman yang salah dari pemahamanan yang sudah dipelajari sebelumnya, tetapi juga mendapatkan peluang untuk mengeksplorasi aspek-aspek baru dalam teknologi keamanan yang belum penulis ketahui atau pelajari. Melalui pemaparan langsung terhadap proyek-proyek nyata dan pemberian solusi dalam mengatasi insiden keamanan yang terjadi memperluas cara pemikiran penulis dalam menerapkan pemikiran kritis dan solutif dalam setiap tugas yang diberikan.

Dan pengalaman ini mengajarkan penulis tentang pentingnya kegigihan dan fleksibilitas dalam dunia kerja. Seringkali, penulis dihadapkan pada masalah yang tidak memiliki solusi yang jelas, sehingga memaksa penulis untuk berinovasi dan mencari pendekatan baru. Pembelajaran ini tidak hanya meningkatkan kemampuan teknis penulis, tetapi juga membantu dalam mempersiapkan diri untuk menghadapi dan menavigasi tantangan yang tak terduga dengan percaya diri dan kreativitas.

e. Memperluas koneksi

Dengan diberikannya kesempatan untuk melakukan pekerjaan secara kolaboratif dan mengikuti pelatihan di luar perusahaan, penulis dapat memperluas koneksi dengan orang-orang yang memiliki minat dan tujuan karir yang sama. Serta hal ini juga memperluas pemahaman penulis dalam mengetahui orang-orang yang berperan penting dalam dunia keamanan siber dari indonesia maupun luar negeri. Dengan koneksi yang penulis dapatkan selama magang, hal ini tidak hanya bermanfaat untuk pengembangan karir jangka panjang, tetapi juga dapat membuka peluang baru seperti kolaborasi proyek, referensi pekerjaan, dan berbagi pengetahuan.

Hal ini didapatkan penulis pada kesempatan mengikuti kegiatan pelatihan Cyfirma, EDR Eset, NDR NDR Darktrace, NDR Vectra, dan MDR Cyberreason. Dengan keterlibatan penulis dalam kegiatan pelatihan ini tidak hanya membantu penulis dalam mendapatkan koneksi baru, tetapi juga membantu dalam mendapatkan pengalaman berharga yang memperkaya kemampuan profesional penulis. Interaksi rutin dengan profesional dari berbagai latar belakang dalam pelatihan dan proyek kolaboratif memperkenalkan penulis pada perspektif dan pendekatan baru dalam menyelesaikan masalah. Keahlian dan wawasan yang penulis peroleh dari mereka telah membuka pandangan tentang berbagai kemungkinan karir dan memperkuat kemampuan adaptasi dalam lingkungan kerja yang dinamis.

Serta dengan kesempatan dalam mengikuti kegiatan diskusi dan pertukaran ide selama mengikuti pelatihan, membantu penulis dalam meningkatkan kepercayaan diri untuk berkontribusi secara aktif. Pada kegiatan ini penulis diajak untuk menyampaikan pendapat, memberikan umpan balik, dan berpartisipasi dalam proses pengambilan keputusan, yang semuanya penting untuk pertumbuhan profesional. Keterampilan ini tidak hanya berharga untuk karir penulis saat ini, tetapi juga untuk ambisi profesional masa depan yang di mana kepemimpinan dan inisiatif menjadi kunci kesuksesan.

4.2.2. Tantangan dan Hambatan Magang

Selama proses pelaksanaan kegiatan magang, terdapat berbagai kendala, hambatan, dan tantangan yang muncul sehingga mengganggu kelancaran dalam proses pelaksanaan. Kondisi ini membuat beberapa proses magang menjadi terhambat sehingga penulis harus melakukan berbagai pekerjaan secara tidak konsisten. Meskipun demikian, penulis masih dapat menyelesaikan semua pekerjaan dengan baik.

Kendala yang pertama adalah kendala dengan laptop digunakan selama kegiatan magang. Hal ini dikarenakan tingginya mobilitas mentor dan beberapa rekan kerja yang dimana mereka sering membawa laptop mereka ke berbagai tempat karena kebutuhan pekerjaan. Akan tetapi, penulis memiliki laptop yang memiliki baterai yang cukup boros dan seringkali di beberapa tempat tidak memiliki fasilitas untuk mengisi daya. Oleh permasalahan tersebut, penulis harus mencatat semua kegiatan yang dilakukan di luar kantor dengan smartphone terlebih dahulu. Dan jika terdapat tugas yang perlu dilakukan selama berkomunikasi di luar kantor, penulis harus kembali ke kantor untuk melaksanakan tugas tersebut. Kondisi ini membuat penulis harus memastikan bahwa semua informasi penting telah dicatat dengan baik menggunakan smartphone. Hal ini berguna untuk mengantisipasi jika tugas-tugas mendesak harus segera diselesaikan setelah kembali ke kantor.

Untuk kendala selanjutnya adalah sistem pembagian informasi pekerjaan yang hanya dapat diakses oleh karyawan yang menggunakan email perusahaan. Hal ini membuat penulis tidak dapat langsung melihat daftar tugas atau memperbarui status pekerjaan yang telah diselesaikan. Sebagai akibatnya, penulis harus secara rutin berkonsultasi dengan mentor setiap kali menyelesaikan tugas. Ketergantungan ini seringkali memperlambat proses kerja karena harus menunggu konfirmasi dan arahan selanjutnya dari mentor. Kendala ini tidak hanya menghambat efisiensi kerja, tetapi juga membatasi kemampuan penulis untuk bekerja secara mandiri dan proaktif dalam mengelola tugas-tugas yang diberikan.

Untuk kendala terakhir yang dialami adalah berkaitan dengan kebutuhan akan akun khusus untuk mengakses beberapa teknologi keamanan, seperti Lintasarta VPN. Namun, pendaftaran untuk Lintasarta VPN membutuhkan penggunaan email resmi dari Lintasarta, yang dimana email resmi tidak dapat diakses oleh penulis sebagai peserta magang.

Kendala ini berlaku kepada teknologi NDR Darktrace sebagai tugas utama yang diberikan oleh Lintasarta kepada penulis. Sebagai solusi atas kendala ini, mentor telah membantu dengan meminjamkan laptopnya kepada penulis pada saat kasus di kantor dan melakukan akses *remote desktop* ke laptop mentor menggunakan fitur yang ada pada Microsoft Teams. Dengan bantuan ini, memungkinkan penulis untuk mengakses teknologi keamanan seperti NDR Darktrace dalam menyelesaikan tugas-tugas yang diberikan secara efektif. Namun, ketergantungan dengan *remote desktop* memberikan kendala tersendiri, yang dimana hal ini memberikan *lagging* yang parah pada saat digunakan, sehingga mengganggu efektivitas penggunaannya pada saat melakukan pekerjaan secara *Work From Home* (WFH).

Melalui semua kendala ini, sebenarnya tetap memberikan manfaat yang dirasakan penulis selama magang. Efek positif yang diberikan dapat berupa baiknya komunikasi antara penulis dengan mentor dan rekan kerja satu divisi. Kendala-kendala yang dihadapi memaksa penulis untuk selalu berkomunikasi secara intensif, sehingga membentuk hubungan kerja yang lebih kuat dan efisien. Komunikasi yang baik ini tidak hanya memperlancar proses kerja, tetapi juga memperkaya pengalaman belajar penulis dengan pengetahuan praktis yang tidak terdapat dalam buku atau teori.

Selain itu dengan kendala tersebut, penulis juga mendapatkan kesempatan untuk memahami lebih dalam tentang pentingnya fleksibilitas dan berpikir cepat dalam lingkungan kerja yang dinamis. Hal ini tidak hanya membantu dalam mengatasi hambatan saat ini, tetapi juga menyiapkan penulis untuk tantangan serupa di masa depan di dunia kerja yang sebenarnya. Magang ini, meskipun penuh dengan tantangan, telah menjadi platform yang solid untuk pengembangan profesional dan personal, memberikan penulis perspektif baru tentang bagaimana industri beroperasi dan apa saja yang dibutuhkan untuk berhasil dalam karir.

Dari kendala-kendala yang penulis alami selama magang justru dapat menjadi motivasi penulis untuk lebih proaktif dalam mencari solusi dan alternatif, tidak hanya bergantung pada sumber daya yang tersedia, tetapi juga menciptakan cara-cara kreatif untuk mengoptimalkan sumber daya tersebut. Dengan demikian, magang ini tidak hanya tentang mempelajari aspek teknis pekerjaan, tetapi juga tentang membangun karakter dan etos kerja yang kuat, yang akan berguna jauh melampaui periode magang ini.

BAB 5
PENUTUP

5.1. Kesimpulan

Berdasarkan pembuatan manajemen insiden siber pada teknologi NDR Darktrace yang telah dikerjakan selama proses kegiatan magang, dapat ditarik beberapa kesimpulan sebagai berikut:

a. Dengan mengambil langkah manajemen insiden yang tepat, perusahaan dapat mengurangi risiko keamanan dan menjaga keandalan operasional pada sistem mereka, sehingga dapat membantu memelihara kepercayaan pelanggan dan reputasi perusahaan.
b. Manajemen Insiden dapat membantu tim keamanan dalam memandu *Self-Learning AI* NDR Darktrace dengan memberikan wawasan dan data yang diperlukan untuk memahami pola serangan dengan lebih baik. Wawasan yang dimaksud dapat berupa analisis mendalam terhadap serangan sebelumnya, identifikasi tanda-tanda awal ancaman, dan penyusunan strategi respons yang efektif.
c. Setelah diterapkannya proses manajemen insiden siber pada teknologi NDR Darktrace, didapatkan hasil yang cukup memuaskan. Hal ini didasari dengan ketika percobaan pada insiden yang terdeteksi oleh NDR Darktrace. Ketika diterapkannya metodologi ini, maka didapatkan informasi penting berupa akar permasalahan dari serangan, respon serangan tanpa menyebabkan kerugian pada perangkat yang tidak terlibat, dan pengatasan serangan sebelum mengakibatkan kerugian lebih lanjut.

5.2. Saran

Berikut merupakan saran yang sekiranya diperlukan dalam pembuatan manajemen insiden siber:

a. Memiliki pemahaman tentang beberapa teknologi keamanan yang serupa dengan yang akan dikembangkan. pada dasarnya, teknologi keamanan terbaru adalah evolusi dari teknologi keamanan sebelumnya. Oleh karena itu, dengan pahamnya dengan teknologi serupa, maka dapat mempermudah dalam pembuatan langkah manajemen insiden siber.

b. Dengan membantu dalam melakukan analisis insiden dan melakukan simulasi penanganan insiden, dapat membantu dalam mempelajari cara kerja suatu teknologi keamanan. Hal ini dapat membantu dalam mencari alur dalam mengatasi sebuah insiden yang paling efektif dan efisien.

DAFTAR PUSTAKA

Ahmad, A., Desouza, K., Maynard, S., Naseer, H., & Baskerville, R. (2019). How integration of cyber security management and incident response enables organizational learning. *Journal of the Association for Information Science and Technology*, *71*. https://doi.org/10.1002/asi.24311

Al-Rushdan, H., Shurman, M., Alnabelsi, S. H., & Althebyan, Q. (2019). Zero-day attack detection and prevention in software-defined networks. *Proceedings - 2019 International Arab Conference on Information Technology, ACIT 2019*, 278–282. https://doi.org/10.1109/ACIT47987.2019.8991124

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). *Computer Security Incident Handling Guide : Recommendations of the National Institute of Standards and Technology*. https://doi.org/10.6028/NIST.SP.800-61r2

Darktrace. (n.d.). *Top AI Cyber Security Company | About Darktrace*. Retrieved May 6, 2024, from https://darktrace.com/company

Darktrace Academy. (n.d.-a). *Darktrace Respond/Network*. Retrieved May 7, 2024, from https://customerportal.darktrace.com/education/main?video=428

Darktrace Academy. (n.d.-b). *Threat Visualizer Part 1 - Familiarization*. Retrieved May 7, 2024, from https://customerportal.darktrace.com/education/videos

Denny S, Suhiindra S, & Syah M B S. (2017). IPS. *Academia*.

D'hoinne, J., & Smith, N. (2022). *Market Guide for Network Detection and Response*.

Doe J. (2023). Whitelisting in Cybersecurity: A Comprehensive Review. *Cybersecurity Journal*.

Gartner. (n.d.). *Network Detection and Response Market Guide* . Retrieved March 10, 2024, from https://www.gartner.com/reviews/market/ network-detection-and-response

MITRE. (n.d.). *MITRE ATT&CK®*. Retrieved May 14, 2024, from https://attack.mitre.org/

Muhtadi, A. F., Budiono, A., Almaarif, A., & Kom, S. (2019). *Analisis Dampak Malware Terhadap Trafik Jaringan dengan Teknik Deteksi Behavior-based Analysis of The Impact of Malware on Network Traffic With Behavior-based Detection Techniques*.

Prakash, D. S. (2023). *Zero-day Vulnerabilities*.

Vira, C., Kaliu, M., Mawengkang, A., Reimon Batmetan, J., Pendidikan, J., Informasi, T., Komunikasi, D., & Teknik, F. (2022). *ANALISIS MANAJEMEN INSIDEN IT PADA SISTEM INFORMASI AKADEMIK UNIVERSITAS NEGERI MANADO*.

LAMPIRAN

Surat Keterangan Telah Selesai Melaksanakan Magang

lintasarta
empowering your future

SURAT KETERANGAN
No. : 009/LA/02020/2024

PT. Aplikanusa Lintasarta, dengan ini menerangkan :

Nama : **Bintang Ananda**

Institusi : **Universitas Islam Indonesia**

Jurusan : **Informatika**

Telah melaksanakan & menyelesaikan Magang atau Kerja Praktek di PT. Aplikanusa Lintasarta di Cybersecurity Solution per tanggal 15 September 2023 s/d 05 Maret 2024. Selama dalam melaksanakan Magang atau Kerja Praktek yang bersangkutan dapat melaksanakan tugas-tugasnya dengan baik dan penuh tanggung jawab.

Demikian surat keterangan ini dibuat, untuk digunakan sebagaimana mestinya.

Jakarta, 05 Maret 2024

Talent Acquisition
Senior Manager

lintasarta

ANNISA NURAINI TAHIR

Menara Thamrin 12 th Floor
Jl. MH Thamrin Kav. 3
Jakarta 10250 Indonesia
+6221 230 2345
+6221 230 3883
info@lintasarta.co.id
www.lintasarta.net