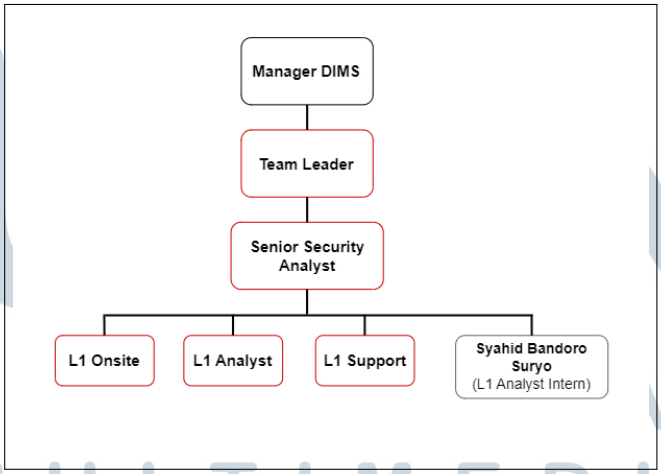
BAB 3
PELAKSANAAN KERJA MAGANG

3.1 Kedudukan dan Koordinasi

Selama menjalani program magang di PT Defender Nusa Semesta, posisi ditempatkan dalam tim analis keamanan tingkat pertama (*L1 Security Analyst*) yang bertanggung jawab dalam mendukung operasional *Security Operations Center* (SOC) melalui aktivitas *security monitoring*. Pemantauan dilakukan secara langsung dengan menganalisis data keamanan menggunakan sistem yang disediakan oleh perusahaan. Dalam pelaksanaannya, kegiatan magang dipandu oleh *buddy* yang menjabat sebagai *Senior Security Analyst* (SSA). Koordinasi juga dilakukan bersama rekan satu *shift* untuk memastikan operasional SOC berjalan secara efektif. Selain tim analis, struktur tim juga mencakup bagian SDM dan *system administrator* yang tergabung dalam satu unit bernama *DIMS (Defenxor Intelligence Managed Security)*, yang dipimpin oleh Bapak Andi Wahyudi sebagai *Team Leader*. Struktur organisasi *DIMS* yang menggambarkan posisi dalam tim dapat dilihat pada Gambar 3.1, yang menunjukkan hierarki dan jalur koordinasi yang berlaku selama masa magang berlangsung.



Gambar 3.1. Struktur *DIMS (Defenxor Intelligence Managed Security)*

Struktur organisasi *DIMS* menempatkan *Manager DIMS* pada posisi tertinggi dengan tanggung jawab memimpin keseluruhan operasional *Security Operations Center*. Di bawahnya, *Team Leader* berperan aktif dalam mengoordinasikan kegiatan harian untuk memastikan proses *security monitoring* berjalan dengan baik. Dalam pelaksanaan tugas, apabila terjadi kebuntuan, diskusi awal dilakukan

bersama rekan satu *shift*. Jika permasalahan tidak dapat diselesaikan, maka dilakukan eskalasi kepada *Senior Security Analyst* sesuai klien yang ditangani. Apabila *Senior Security Analyst* juga tidak dapat memberikan solusi, maka eskalasi diteruskan ke *Team Leader*, dan jika masih belum terselesaikan, akan dilanjutkan hingga ke *Manager DIMS*. Setiap *Senior Security Analyst* juga bertindak sebagai penghubung antara *Defenxor* dan klien, serta menangani insiden yang memerlukan penanganan lebih lanjut. Secara struktural, posisi analis dalam SOC terbagi menjadi tiga kategori, yaitu *L1 Onsite Analyst* yang bertugas di lokasi klien, *L1 Analyst* yang melakukan pemantauan dari kantor pusat *Defenxor*, dan *L1 Support* yang menjembatani komunikasi antara tim SOC dan klien.

3.2 Tugas yang Dilakukan

Tugas utama yang dilakukan selama pelaksanaan magang berfokus pada aktivitas *security monitoring* terhadap sistem milik klien secara *real-time*. Pemantauan dilakukan melalui platform yang menampilkan *case*, yaitu kumpulan *alert* yang telah difilter menggunakan *rule* yang disusun oleh *Senior Security Analyst* (SSA). Proses analisis difokuskan terlebih dahulu pada tingkat *case* untuk memastikan efisiensi dan akurasi dalam mendeteksi aktivitas mencurigakan. Jika tidak ditemukan indikasi ancaman pada level *case*, analisis akan dilanjutkan ke tingkat *alert* individual guna menelusuri potensi insiden tersembunyi.

Setiap potensi insiden yang terdeteksi akan dianalisis untuk mengidentifikasi jenis ancaman, penyebab, serta kemungkinan dampaknya terhadap sistem. Hasil analisis kemudian disusun dalam bentuk notifikasi insiden yang dikirim kepada klien. Notifikasi tersebut berisi informasi teknis terkait insiden, sistem yang terdampak, serta rekomendasi mitigasi yang dapat dilakukan. Dalam beberapa kasus, notifikasi disertai permintaan konfirmasi kepada klien untuk memastikan apakah aktivitas yang terdeteksi merupakan aktivitas yang sah (*authorized*) atau tidak.

Selain notifikasi harian, tugas lainnya adalah membantu penyusunan laporan bulanan yang merangkum seluruh insiden keamanan yang terjadi dalam periode satu bulan. Laporan ini berisi rekapitulasi insiden, tren ancaman, serta saran peningkatan keamanan sistem, dan disusun sebagai bahan presentasi yang akan disampaikan oleh *Senior Security Analyst* kepada klien masing-masing.

Seluruh aktivitas tersebut dilaksanakan di ruang kerja SOC, yaitu ruang terbatas dengan akses terkontrol yang dirancang untuk mendukung monitoring

sistem selama 24/7. Lingkungan kerja ini mengikuti standar keamanan informasi ISO 27001, termasuk pelarangan penggunaan perangkat pribadi, pengawasan aktivitas kerja, serta pengaturan hak akses personel.

3.3 Uraian Pelaksanaan Magang

Berikut uraian semua kegiatan selama yang dilakukan dalam pelaksanaan Magang di PT Defender Nusa Semesta sebagai Security Analyst dalam Tabel 3.1.

Tabel 3.1. Pekerjaan yang dilakukan tiap minggu selama pelaksanaan kerja magang

Minggu Ke -	Pekerjaan yang dilakukan
1-2	1. Melakukan Onboarding dan self-learning materi Security+. 2. Melakukan presentasi dan diskusi mengenai materi Security+.
3-4	1. Mempelajari sistem yang akan digunakan saat operasional SOC. 2. Mempelajari contoh-contoh case sekaligus melakukan analisa terhadap case. 3. Mempresentasikan hasil analisis case.
5	1. Review semua yang telah dipelajari selama sebulan terakhir. 2. Setup User untuk operasional pada ruangan SOC
6	First week operasional, *late shift*. Mendapatkan mayoritas *alarm* dan *case* mengenai *web attack dan web scanning*. Melakukan analisis dan notifikasi, serta *Security Device Availability Monitoring* di dalam SOC.
7	*Mid shift* operasional. Mendapatkan mayoritas *alarm* dan *case* mengenai *bruteforce* atau *audit internal*. Melakukan analisis dan mulai menangani permintaan klien, serta *Security Device Availability Monitoring* di dalam SOC.
Lanjutan pada halaman berikutnya	

Minggu Ke -	Pekerjaan yang dilakukan
8	*Early shift* operasional. Mendapatkan mayoritas *alarm* dan *case* mengenai *malware*. Melakukan analisis dan menangani permintaan klien, serta *Security Device Availability Monitoring* di dalam SOC.
9	*Late shift* operasional. Shift dijalankan pada hari libur Idul Fitri. Mendapatkan mayoritas *alarm* dan *case* yang berasal dari eksternal. Melakukan analisis, serta *Security Device Availability Monitoring* di dalam SOC.
10	*Mid shift* operasional. Mendapatkan mayoritas *alarm* dan *case* yang berasal dari eksternal. Melakukan analisis dan mulai melakukan *daily report*, serta *Security Device Availability Monitoring* di dalam SOC.
11	*Early shift* operasional. Mendapatkan mayoritas *alarm* dan *case* mengenai *web attack dan web scanning*. Melakukan analisis dan mulai melakukan *daily report*, serta *Security Device Availability Monitoring* di dalam SOC.
12	*Late shift* operasional. Mendapatkan mayoritas *alarm* dan *case* yang berasal dari eksternal. Melakukan analisis, serta *Security Device Availability Monitoring* di dalam SOC.
13	*Mid shift* operasional. Mendapatkan mayoritas *alarm* dan *case* mengenai *audit internal*. Melakukan analisis dan mulai membantu pengerjaan *monthly report* untuk salah satu *customer*
14	*Early shift* operasional. Monitoring secara rutin dan melakukan *daily report*, serta *Security Device Availability Monitoring* di dalam SOC.
15	*Late shift* operasional. Monitoring secara rutin dan menangani permintaan klien, serta *Security Device Availability Monitoring* di dalam SOC.
16	*Mid shift* operasional. Mendapatkan mayoritas *alarm* dan *case* mengenai *credential leak*. Melakukan analisis dan menangani permintaan klien.

3.3.1 Workflow *Security Monitoring* dan *Incident Response* oleh *L1 Analyst*

Sebagai analis keamanan tingkat pertama (L1), peran utama dalam kegiatan operasional *Security Operations Center* (SOC) adalah melakukan pemantauan sistem klien secara *real-time* melalui platform *Security Information and Event Management* (SIEM), serta merespons insiden dengan memberikan analisis awal terhadap aktivitas yang terindikasi mencurigakan. Proses ini merupakan bagian dari strategi *security monitoring* dan *incident response* yang dijalankan oleh tim SOC untuk menjaga keamanan siber klien.

Pemantauan dilakukan berdasarkan *case*, yaitu kumpulan *alert* yang telah difilter oleh *rule* yang dibuat oleh *Senior Security Analyst* (SSA). Setiap *case* dianalisis untuk mengidentifikasi indikasi ancaman, baik dari log *endpoint*, *firewall*, maupun perangkat keamanan lainnya. Jika tidak ditemukan anomali dalam *case*, maka analisis dapat dilanjutkan hingga ke tingkat *alert* individual.

Apabila ditemukan indikasi insiden, L1 Analyst bertugas menyusun *notifikasi insiden* sebagai bentuk respons awal. *Notifikasi* ini mencakup ringkasan teknis, sistem terdampak, indikator yang ditemukan, serta saran tindakan mitigasi. Dalam konteks *incident response*, *notifikasi* ini menjadi dokumentasi awal untuk proses eskalasi dan penanganan lanjutan oleh tim yang lebih senior.

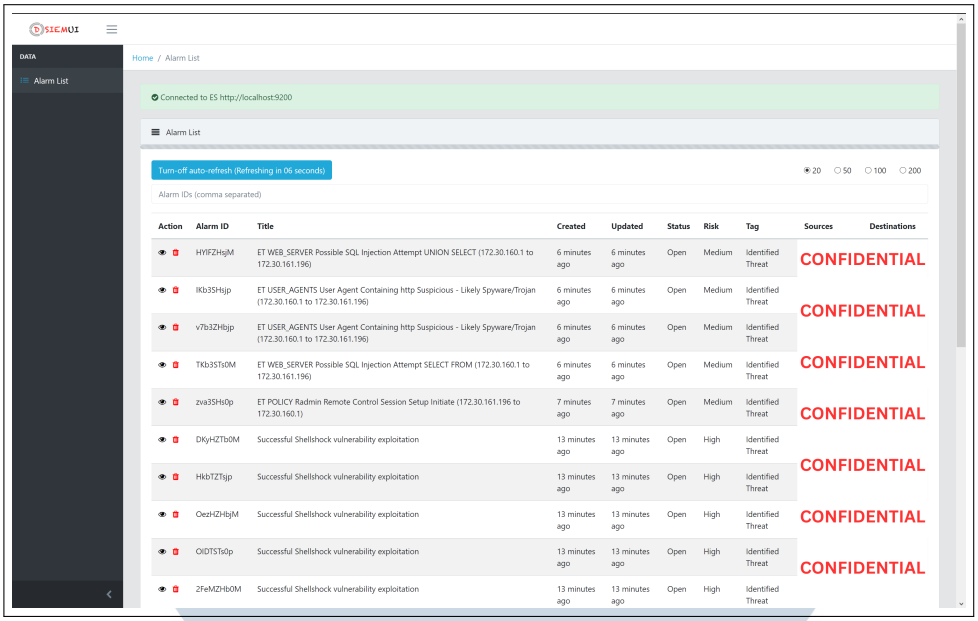
Dengan menjalankan proses ini secara konsisten, L1 Analyst berperan sebagai garda depan dalam mendeteksi dan merespons potensi insiden siber, sekaligus memastikan bahwa prosedur kerja yang dijalankan telah sesuai dengan standar keamanan yang berlaku di lingkungan PT *Defender Nusa Semesta*.

A Deteksi Alarm pada Sistem Monitoring

Tahapan awal dalam proses *security monitoring* dimulai ketika sistem mendeteksi adanya aktivitas yang mencurigakan berdasarkan *rule* atau pola tertentu yang telah dikonfigurasi sebelumnya. Deteksi ini dilakukan secara otomatis oleh *Security Information and Event Management* (SIEM), yang memantau log dari berbagai perangkat dalam infrastruktur klien.

Salah satu platform yang digunakan untuk pemantauan adalah DSIEM, sebuah SIEM berbasis *open-source* yang dikembangkan oleh Defenxor. DSIEM menyajikan daftar *alarm* hasil korelasi log dan pemicu *rule* dalam format tabel, yang berisi informasi penting seperti waktu kejadian, tingkat risiko, nama *rule* yang aktif, serta sistem atau perangkat yang terpengaruh. Gambar 3.2 menunjukkan

tampilan DSIEM yang memuat daftar *alarm* dengan *rule* yang terpicu.



Gambar 3.2. Tampilan *alarm list* pada DSIEM.

Tingkat risiko pada DSIEM ditentukan secara otomatis berdasarkan perhitungan yang menggabungkan tingkat *priority* dari *rule* yang terpicu dengan *asset value* dari perangkat terdampak. Nilai aset tersebut dikategorikan berdasarkan segmentasi IP yang mencerminkan sensitivitas dan kepentingan sistem yang dipantau. Dengan pendekatan ini, sistem dapat mengklasifikasikan *alarm* secara lebih akurat, sehingga memudahkan tim analis dalam menentukan prioritas penanganan.

Selain DSIEM, SOC juga menggunakan platform lain seperti Wazuh yang terintegrasi dengan Opensearch atau Elasticsearch. Di sistem ini, *alarm* ditampilkan dalam *dashboard* keamanan yang menyajikan detail serupa dan mendukung proses analisis secara interaktif.

Perlu dicatat bahwa tidak semua *alarm* menandakan insiden yang valid. Oleh karena itu, setiap *alarm* harus melalui tahap analisis terlebih dahulu untuk menentukan apakah mengindikasikan ancaman nyata atau hanya merupakan *false positive*. Proses ini merupakan titik awal dari tahapan *detection and analysis* dalam siklus *incident response*.

B Referensi *Playbook* dan Treatment Khusus Klien

Setiap klien memiliki perlakuan khusus yang disesuaikan dengan kebutuhan dan karakteristik sistem mereka. Perbedaan ini mencakup topologi jaringan, fokus keamanan yang menjadi perhatian utama (*concern*), serta daftar *whitelist* terhadap *event* tertentu seperti alamat IP, pengguna, atau domain yang telah dianggap sah. Seluruh informasi ini tercatat dalam *playbook*, yaitu dokumen prosedural yang berfungsi sebagai panduan teknis dalam menangani insiden.

Playbook memuat rincian terkait sistem klien, termasuk daftar aset, segmentasi jaringan berdasarkan sensitivitas, dan kebijakan respons terhadap jenis ancaman tertentu. Informasi ini menjadi acuan awal dalam proses analisis, guna membantu menentukan apakah suatu *alarm* menunjukkan potensi ancaman atau berasal dari aktivitas yang telah diketahui dan diizinkan.

Sebagai contoh, jika terdapat aktivitas komunikasi dari sebuah IP eksternal, analis dapat merujuk pada *playbook* untuk memverifikasi apakah IP tersebut sudah termasuk dalam daftar *whitelist* klien. Hal serupa juga berlaku untuk trafik antarsegmen jaringan yang melintasi batas komunikasi yang tidak umum; *playbook* akan memberikan panduan apakah hal tersebut tergolong anomali atau termasuk dalam aktivitas yang telah disetujui.

Perubahan *treatment* khusus oleh klien juga diakomodasi dengan dua pendekatan. Jika perubahan bersifat jangka pendek atau hanya berlaku sementara, maka informasi tersebut akan dicatat dalam *handover notes* yang disampaikan oleh tim shift sebelumnya. Sementara untuk perubahan yang bersifat jangka panjang atau permanen, pembaruan akan dimasukkan langsung ke dalam *playbook*, dan tetap dicantumkan dalam *handover notes* selama minimal satu minggu sebagai pengingat tambahan antar shift.

Dengan merujuk pada *playbook* dan memahami *treatment* khusus dari masing-masing klien, proses analisis insiden dapat dilakukan secara lebih akurat, efisien, dan konsisten, sekaligus meminimalkan risiko kesalahan interpretasi antar analis.

C Validasi Alarm melalui Peninjauan Log

Setelah melakukan referensi terhadap *playbook*, tahap selanjutnya dalam proses *security monitoring* adalah melakukan peninjauan terhadap data log untuk memvalidasi alarm yang telah terdeteksi. Langkah ini bertujuan untuk memastikan

apakah alarm yang muncul benar-benar mencerminkan aktivitas mencurigakan atau hanya merupakan *false positive*.

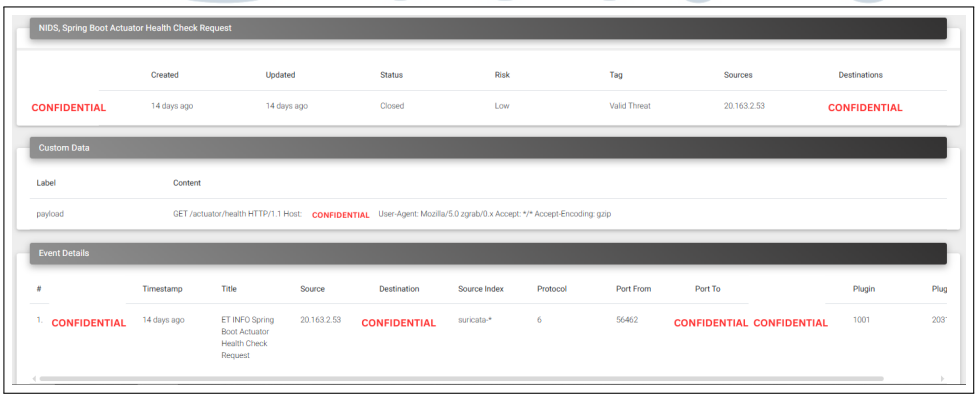
Peninjauan log dilakukan dengan memanfaatkan platform seperti *Opensearch* atau *Elasticsearch*, yang telah mengkonsolidasikan berbagai sumber log dari sistem klien. Informasi penting seperti alamat IP sumber dan tujuan, jenis event, *event ID*, sistem terdampak, serta waktu kejadian menjadi acuan utama dalam proses analisis.

Langkah analisis ini tidak hanya berfokus pada satu perangkat saja, tetapi mempertimbangkan keseluruhan konteks topologi dan segmentasi jaringan milik klien. Hal ini penting untuk menghindari kesalahan dalam mengklasifikasikan insiden, terutama ketika alarm muncul dari aktivitas yang sah namun tidak terdaftar dalam *whitelist*.

Validasi ini dilakukan secara berurutan dan terstruktur, mengikuti alur kerja yang telah ditetapkan oleh tim SOC. Dengan pendekatan sistematis ini, analis dapat menilai dengan lebih akurat apakah alarm yang muncul benar-benar menunjukkan indikasi ancaman siber atau tidak.

C.1 Analisis Awal terhadap Alarm Terkonfirmasi

Setelah sebuah *alarm* berhasil terkonfirmasi dan naik menjadi *case*, langkah awal yang dilakukan adalah menganalisis informasi dasar yang disediakan oleh sistem monitoring untuk memahami karakteristik dan potensi risiko awal. Pada kasus ini, alarm yang muncul berasal dari rule *NIDS, Spring Boot Actuator Health Check Request*, yang menunjukkan adanya permintaan akses terhadap endpoint `/actuator/health` pada aplikasi berbasis Spring Boot. Endpoint ini sering menjadi target dalam fase awal serangan karena dapat mengungkapkan status dan konfigurasi aplikasi.



Gambar 3.3. Tampilan *alarm* pada DSIEM.

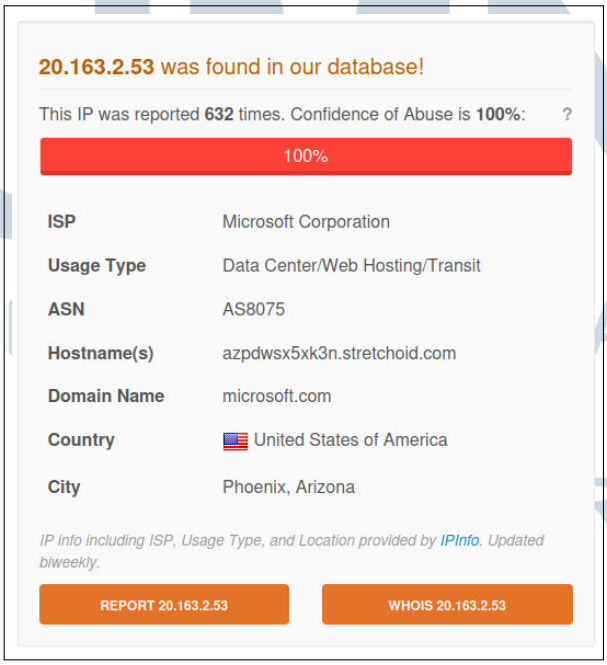
Informasi awal yang ditampilkan oleh DSIEM pada Gambar 3.3 mencakup *timestamp*, alamat IP sumber dan tujuan, nama rule yang terpicu, serta tingkat risiko dari aktivitas yang terdeteksi. Dalam kasus ini, rule yang terpicu adalah *Spring Boot Actuator Health Check Request*, yang menandakan bahwa sistem mendeteksi adanya permintaan ke endpoint aplikasi dan perlu diverifikasi karena dapat dimanfaatkan oleh pihak tidak bertanggung jawab.

Alamat IP sumber diketahui berasal dari eksternal dan memiliki reputasi buruk berdasarkan basis data *threat intelligence*. Fakta ini menjadi indikasi awal bahwa aktivitas tersebut berpotensi merupakan bagian dari aktivitas berbahaya dan bukan trafik sah dari sistem internal.

Tahapan ini berfungsi sebagai fondasi untuk menentukan arah investigasi lebih lanjut sebelum masuk ke proses pencarian log, korelasi lintas perangkat, dan pengambilan keputusan terhadap insiden.

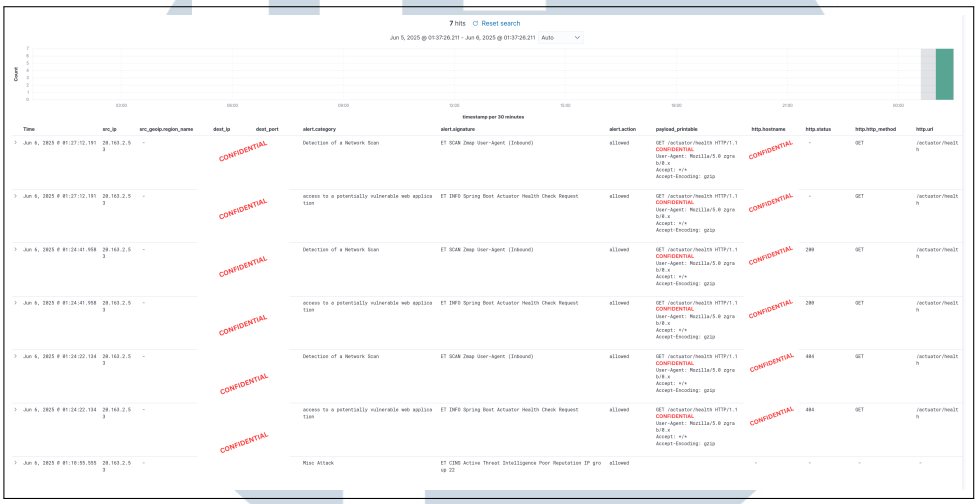
C.2 Investigasi Log Suricata Berdasarkan Alarm Awal

Setelah dilakukan analisis awal terhadap *alarm*, langkah selanjutnya adalah melakukan pencarian log yang relevan untuk memperkuat indikasi insiden. Dalam kasus ini, pencarian dilakukan terhadap log Suricata yang berfungsi sebagai *Network Intrusion Detection System* (NIDS), dengan fokus pada aktivitas dari IP eksternal `20.163.2.53` yang memiliki reputasi buruk.



Gambar 3.4. Reputasi IP `20.163.2.53` pada AbuseIPDB.

Pencarian dilakukan menggunakan parameter *source IP* yang diperoleh dari alarm, dan menghasilkan tujuh event log dalam kurun waktu sekitar 10 menit. Payload yang digunakan konsisten, yaitu `GET /actuator/health HTTP/1.1`, dengan *User-Agent* mencurigakan (`Mozilla/5.0 zgrab/0.x`), yang mengindikasikan kemungkinan aktivitas pemindaian otomatis.



Gambar 3.5. Log Suricata menunjukkan request `/actuator/health` dari IP `20.163.2.53`.

Meskipun endpoint yang diminta sama, yaitu `/actuator/health`, log mencatat bahwa permintaan diarahkan ke *hostname* yang berbeda-beda. Hal ini menunjukkan bahwa aktor eksternal kemungkinan menargetkan beberapa layanan yang dihosting secara terpisah, memperkuat dugaan adanya aktivitas pemindaian sistematis terhadap layanan Spring Boot yang terbuka di internet.

Dua *signature rule* terpicu dalam proses ini, yaitu:

1. *ET SCAN Zmap User-Agent (Inbound)* dengan kategori *Detection of a Network Scan*
2. *ET INFO Spring Boot Actuator Health Check Request* dengan kategori *Access to a Potentially Vulnerable Web Application*

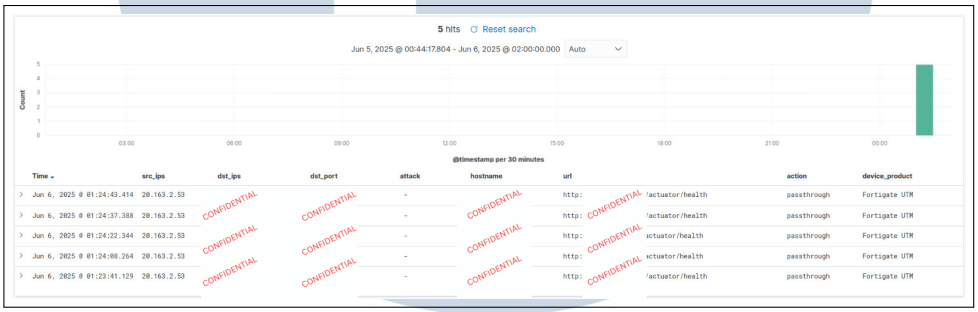
Status HTTP pada log menunjukkan bahwa beberapa akses mendapat respons `200` dari server tujuan, yang menandakan bahwa endpoint tersebut memang aktif dan memberikan respons. Hal ini memperkuat indikasi bahwa layanan Spring Boot dengan endpoint `/actuator/health` dapat diakses secara terbuka dari luar jaringan internal.

Informasi ini menjadi dasar untuk melanjutkan ke tahap berikutnya, yaitu korelasi log lintas perangkat seperti FortiGate UTM dan F5 ASM, guna mengetahui

apakah terdapat indikasi upaya lanjutan seperti eksploitasi, *brute force*, atau transfer data yang mencurigakan.

C.3 Korelasi Log pada Perangkat Keamanan Fortigate dan F5 ASM

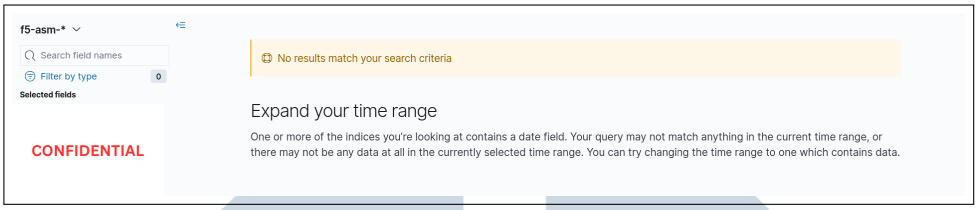
Setelah melakukan analisis lanjutan terhadap alarm yang muncul pada sistem Network Intrusion Detection System (NIDS) Suricata, dilakukan proses korelasi dengan log dari perangkat keamanan lain, yaitu Fortigate dan F5 ASM. Tujuan dari korelasi ini adalah untuk memverifikasi konsistensi peristiwa yang terjadi serta mengidentifikasi sejauh mana serangan atau aktivitas mencurigakan berhasil melewati lapisan keamanan lainnya.



Gambar 3.6. Log dari Fortigate menunjukkan aktivitas akses ke URL `/actuator/health`.

Berdasarkan gambar log dari perangkat Fortigate Gambar 3.6, ditemukan lima entri log yang menunjukkan adanya akses dari IP sumber yang sama, yaitu `20.163.2.53`. Jalur URL yang diakses adalah `/actuator/health`, yang juga merupakan payload yang terdeteksi oleh Suricata. Hal menarik yang ditemukan dalam korelasi ini adalah perbedaan pada *alamat IP tujuan (destination IP)* yang dicatat oleh Fortigate dibandingkan dengan Suricata.

Jika pada log Suricata terlihat bahwa destination IP merupakan IP internal, maka pada log Fortigate, IP tujuan merupakan IP publik atau eksternal. Perbedaan ini terjadi karena perbedaan posisi perangkat dalam arsitektur jaringan. Fortigate sebagai perangkat edge firewall mencatat koneksi sebelum dilakukan translasi jaringan (NAT), sedangkan Suricata yang berada di belakang firewall melihat koneksi setelah NAT dilakukan. Dengan demikian, Fortigate mencatat akses ke IP eksternal, sementara Suricata mencatat IP internal yang sesungguhnya menjadi tujuan akhir koneksi. Hal ini menunjukkan bahwa koneksi benar-benar diteruskan dari edge firewall menuju server internal.



Gambar 3.7. Hasil pencarian log pada F5 ASM.

Selanjutnya, dilakukan pencarian pada log perangkat F5 ASM menggunakan IP sumber yang sama, namun hasil pencarian menunjukkan bahwa tidak ditemukan log yang relevan seperti pada Gambar 3.7. Ada beberapa kemungkinan penyebab dari kondisi ini:

1. Trafik tidak diteruskan menuju F5, bisa karena tidak ada konfigurasi virtual server atau NAT dari Fortigate ke F5 yang menangani request tersebut.
2. Trafik memang tidak melewati F5 karena diarahkan ke backend server yang tidak berada di bawah proteksi F5.
3. Permintaan HTTP ke `/actuator/health` tidak dianggap mencurigakan oleh F5 sehingga tidak dicatat dalam log. Hal ini dapat terjadi jika URL tersebut tidak termasuk dalam security policy atau tidak memicu signature apapun pada F5 ASM.
4. Waktu pencarian pada F5 tidak sesuai atau tidak mencakup rentang waktu yang sama dengan temuan dari perangkat lainnya.

Kondisi ini menggarisbawahi pentingnya pemahaman terhadap posisi fisik dan logis dari setiap perangkat dalam jaringan, serta bagaimana setiap perangkat mencatat lalu lintas yang berbeda tergantung pada titik pengamatannya. Korelasi seperti ini sangat penting untuk memastikan bahwa proses investigasi tidak hanya bergantung pada satu sumber log, melainkan menyusun potongan informasi dari berbagai perangkat untuk mendapatkan gambaran menyeluruh dari insiden yang terjadi.

D Drafting dan Pengiriman Notifikasi

Setelah seluruh bukti *log* dan hasil korelasi dari berbagai perangkat terkumpul, tahap berikutnya adalah penyusunan notifikasi insiden yang akan disampaikan kepada pihak klien. Tujuan dari proses ini adalah untuk mengomunikasikan hasil

analisis secara jelas dan terstruktur, serta memberikan saran tindakan untuk mitigasi lebih lanjut.

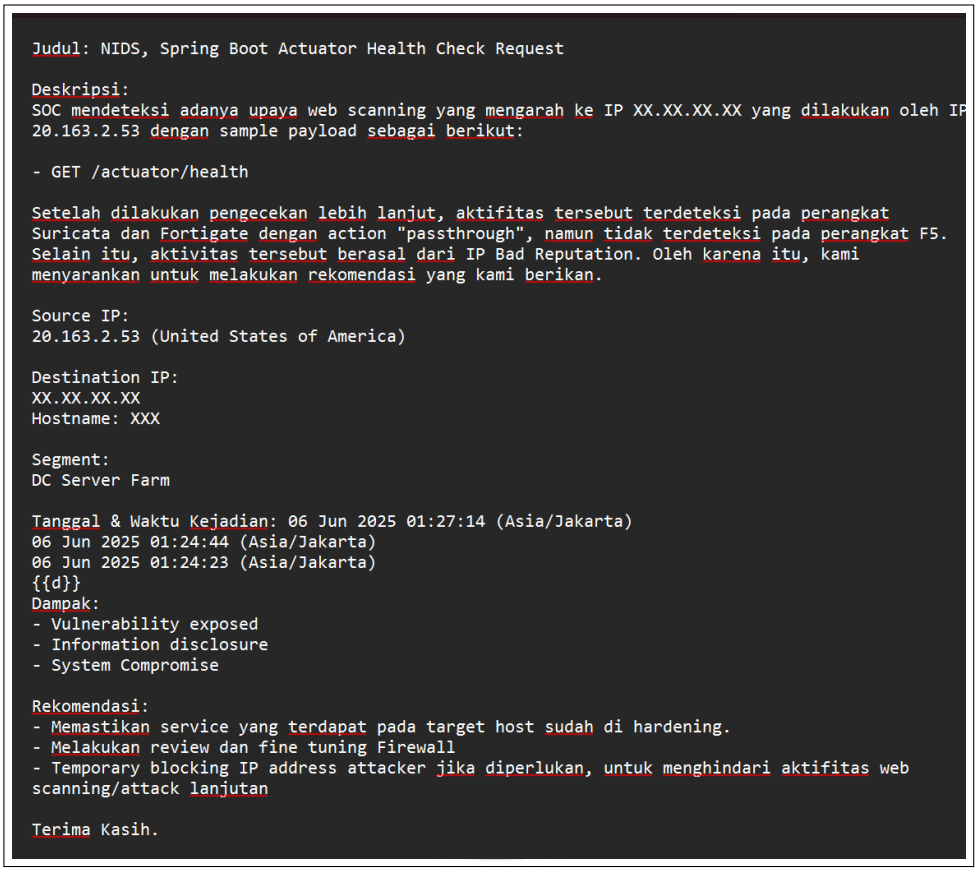
Notifikasi disusun mengikuti format standar yang berlaku di lingkungan operasional, dengan komponen-komponen utama sebagai berikut:

1. Incident Title / Summary
2. Alert Trigger Source (misalnya: IDS, Firewall, WAF, Proxy)
3. Detection Time
4. Deskripsi Singkat Aktivitas
5. Affected / Asset Details
6. Indicators of Compromise (IOC) (seperti IP, domain, hash, atau URL)
7. Log Highlights (cuplikan *log* yang relevan untuk mendukung analisis)
8. Impact Assessment jika aktivitas berlanjut atau tidak ditindaklanjuti
9. Recommendation (tindakan mitigasi yang disarankan kepada klien)

Struktur ini dirancang agar tetap fleksibel namun informatif, serta mudah dipahami oleh tim klien yang memiliki latar belakang teknis berbeda-beda. Oleh karena itu, bahasa yang digunakan bersifat profesional dan netral, serta menghindari penggunaan istilah teknis berlebihan kecuali benar-benar dibutuhkan.

Sebelum dikirimkan, setiap draf notifikasi akan melalui proses pengecekan ulang untuk memastikan tidak terdapat kesalahan dalam penulisan, analisis, maupun interpretasi data. Pengecekan ini sangat krusial karena kesalahan pengiriman notifikasi tidak hanya dapat menimbulkan kesalahpahaman dengan klien, tetapi juga dapat berdampak fatal terhadap reputasi perusahaan, termasuk potensi kehilangan kepercayaan dan kredibilitas sebagai penyedia layanan keamanan siber.

Setelah disusun dan dinyatakan valid, notifikasi akan dikirimkan melalui sistem internal yang telah terintegrasi dengan jalur komunikasi resmi, seperti email dan aplikasi Signal. Preferensi kanal pengiriman setiap klien telah dikonfigurasi sebelumnya, sehingga sistem secara otomatis akan menyesuaikan pengiriman sesuai preferensi masing-masing tanpa perlu intervensi manual.



```
Judul: NIDS, Spring Boot Actuator Health Check Request

Deskripsi:
SOC mendeteksi adanya upaya web scanning yang mengarah ke IP XX.XX.XX.XX yang dilakukan oleh IP
20.163.2.53 dengan sample payload sebagai berikut:

- GET /actuator/health

Setelah dilakukan pengecekan lebih lanjut, aktifitas tersebut terdeteksi pada perangkat
Suricata dan Fortigate dengan action "passthrough", namun tidak terdeteksi pada perangkat F5.
Selain itu, aktivitas tersebut berasal dari IP Bad Reputation. Oleh karena itu, kami
menyarankan untuk melakukan rekomendasi yang kami berikan.

Source IP:
20.163.2.53 (United States of America)

Destination IP:
XX.XX.XX.XX
Hostname: XXX

Segment:
DC Server Farm

Tanggal & Waktu Kejadian: 06 Jun 2025 01:27:14 (Asia/Jakarta)
06 Jun 2025 01:24:44 (Asia/Jakarta)
06 Jun 2025 01:24:23 (Asia/Jakarta)
{{d}}
Dampak:
- Vulnerability exposed
- Information disclosure
- System Compromise

Rekomendasi:
- Memastikan service yang terdapat pada target host sudah di hardening.
- Melakukan review dan fine tuning Firewall
- Temporary blocking IP address attacker jika diperlukan, untuk menghindari aktifitas web
scanning/attack lanjutan

Terima Kasih.
```

Gambar 3.8. Contoh draf notifikasi.

Dengan sistem pengiriman yang terintegrasi dan terdokumentasi, proses komunikasi insiden dapat dilakukan dengan cepat, akurat, dan tetap terjaga konsistensinya pada berbagai kanal komunikasi yang digunakan.

E Eskalasi atau Ticketing Internal

Jika dari hasil investigasi ditemukan bahwa insiden memerlukan penanganan teknis lanjutan, seperti pemblokiran IP, pembatasan akses jaringan, atau verifikasi sistem di sisi infrastruktur, maka proses dilanjutkan ke tahap eskalasi melalui sistem *ticketing* internal.

Tiket dibuat oleh analis SOC dengan mencantumkan informasi insiden secara ringkas namun lengkap, termasuk referensi notifikasi yang telah dikirimkan, kronologi kejadian, hasil analisis, perangkat atau aset yang terdampak, serta rekomendasi tindakan teknis. Prioritas penanganan disesuaikan berdasarkan tingkat risiko (*severity*) dari insiden.

Di lingkungan operasional PT Defender Nusa Semesta, proses ini dilakukan

dengan melibatkan tim SDM yang juga memiliki peran dalam pengelolaan akses sistem internal. Tim SOC akan menyampaikan permintaan melalui tiket yang telah dikonfigurasi ke jalur eskalasi SDM, terutama untuk tindakan seperti pemblokiran IP yang dianggap berisiko berdasarkan hasil analisis.

Sistem *ticketing* memastikan bahwa tiket disampaikan ke pihak yang tepat secara otomatis, dan memfasilitasi dokumentasi semua aktivitas yang terkait dengan insiden secara terpusat. Dalam beberapa kasus, tim yang menerima tiket dapat memberikan *update* atau hasil tindak lanjut langsung pada tiket yang sama, memastikan transparansi dan koordinasi antar tim tetap terjaga.

3.3.2 Security Device Availability Monitoring

Selain memantau aktivitas keamanan dan alarm dari sistem log, proses monitoring di SOC juga mencakup pengawasan terhadap status dan ketersediaan perangkat keamanan yang terpasang di sisi klien. Aktivitas ini dikenal sebagai *system availability monitoring*, yang bertujuan untuk memastikan bahwa seluruh komponen seperti endpoint agent, firewall, intrusion detection system (IDS/NIDS), serta log forwarder tetap aktif dan mengirimkan data secara konsisten.

Di lingkungan PT Defender Nusa Semesta, proses ini dilakukan menggunakan platform Grafana, yang menyajikan visualisasi dashboard mengenai status perangkat secara *real-time*. Dalam dashboard tersebut, status perangkat dapat ditampilkan dalam bentuk indikator seperti `Up`, `Down`, atau `No Data`, yang membantu analis untuk mengidentifikasi perangkat yang bermasalah atau tidak aktif.

Grafana juga digunakan untuk melakukan pemantauan terhadap Dedicated Security Appliance (DSA), yaitu perangkat khusus yang digunakan oleh klien sebagai endpoint log forwarding utama. Melalui pemantauan ini, SOC dapat dengan cepat mengetahui apabila DSA mengalami gangguan atau dalam kondisi `Down`, sehingga potensi kehilangan data log dapat segera diantisipasi.

Jika perangkat terpantau tidak merespons, berhenti mengirimkan log, atau mengalami gangguan konektivitas dalam jangka waktu tertentu, kondisi tersebut akan ditandai sebagai potensi insiden operasional dan perlu ditindaklanjuti lebih lanjut. Salah satu contoh adalah apabila perangkat firewall Fortigate pada sisi klien tidak mengirimkan log seperti biasa atau terpantau `Down`, maka SOC akan melakukan investigasi awal dan meneruskan informasi ini melalui sistem ticketing internal.

Tiket akan dikirimkan kepada tim sysadmin untuk dilakukan pengecekan langsung terhadap perangkat tersebut, baik dari sisi konektivitas, konfigurasi, maupun layanan yang berjalan. Tindakan ini bertujuan untuk mengembalikan fungsi monitoring secara optimal dan menghindari hilangnya visibilitas terhadap ancaman keamanan.

Dengan adanya sistem ini, system availability monitoring menjadi bagian krusial dalam menjaga kesinambungan visibilitas keamanan, sehingga potensi ancaman dapat terus diawasi secara efektif tanpa adanya celah akibat perangkat yang tidak aktif.

3.4 Kendala dan Solusi yang Ditemukan

Selama proses kegiatan magang di PT Defender Nusa Semesta, terdapat beberapa kendala yang muncul dalam pelaksanaan tugas monitoring, analisis, dan komunikasi tim. Berikut ini adalah kendala-kendala tersebut:

1. Setiap klien memiliki konfigurasi perangkat keamanan dan sistem monitoring yang berbeda-beda, sehingga menyebabkan variasi pada tampilan antarmuka, format *log*, serta alur analisis yang harus diikuti.
2. Tingkat sensitivitas dan fokus keamanan yang berbeda antar klien dapat memperlambat proses investigasi dan menyebabkan kebingungan dalam menentukan apakah suatu aktivitas perlu dinotifikasi.
3. Tahapan seperti penyusunan *notifikasi* dan pemantauan perangkat memerlukan ketelitian dan pemahaman teknis. Minimnya pengalaman langsung dapat menyebabkan kesalahan atau kelalaian.

Berikut merupakan solusi yang ditemukan pada saat proses kegiatan kerja magang:

1. Disarankan untuk membaca *playbook* masing-masing klien secara menyeluruh serta mempelajari topologi sistem yang digunakan. Pemahaman awal terhadap infrastruktur klien akan memudahkan dalam proses identifikasi dan analisis *log*.
2. Selain mengacu pada *playbook*, berdiskusi dengan anggota tim dapat membantu memahami preferensi klien secara lebih efektif. Komunikasi antar *shift* juga perlu ditingkatkan melalui penyusunan *handover notes* yang jelas agar proses kerja tetap konsisten.

3. Komunikasi intensif dalam tim sangat penting, baik dalam bentuk diskusi langsung maupun sesi tanya jawab. Selain itu, mempelajari dokumentasi *notifikasi* sebelumnya dapat menjadi acuan untuk memahami struktur laporan dan pola insiden yang sering terjadi.

UMN
UNIVERSITAS
MULTIMEDIA
NUSANTARA