STANDAR OPERASIONAL PROSEDUR *SECURITY OPERATION CENTER*

Dipersiapkan untuk:

PT Hutama Karya (Persero)

Inovasi Untuk Solusi

	SOP SOC Defend IT360 --- Document Document ver1.0 Release Date 10/01/2025 --- **DEFEND IT360** **OPERATION CENTER** **Graha Hyper** **Jl. Makaliwe Raya No. 24 – 24A** **Grogol Petamburan Jakarta – 11450** **P: +62 21 2939 3939**

DEFEND IT360	**STANDAR OPERASIONAL PROSEDUR** ***SECURITY OPERATION CENTER***	Nomor : Status Versi : 1.0 Tanggal Efektif : Subject : Standar Frekuensi : Internal

LEMBARAN PENGESAHAN

Dibuat Oleh,

No	Nama	Jabatan	Tanggal	Tanda Tangan
1.				
2.				

Ditinjau Oleh,

No	Nama	Jabatan	Tanggal	Tanda Tangan
1.				
2.				

Disetujui Oleh,

No	Nama	Jabatan	Tanggal	Tanda Tangan
1.				
2.				

REVISI/PERUBAHAN

No	Tanggal	No. Revisi	Ringkasan Perubahan

DAFTAR DISTRIBUSI

No	Perusahaan Penerima
1	PT Data Enkripsi Informasi Teknologi (DEFEND IT360)
2	PT HUTAMA KARYA

DAFTAR ISI

1. PENDAHULUAN

Keamanan informasi merupakan aspek penting dalam menjaga keberlangsungan bisnis dan melindungi data perusahaan dari berbagai ancaman siber. Insiden keamanan dapat berdampak pada operasional, reputasi, dan kepatuhan terhadap regulasi yang berlaku. Oleh karena itu, diperlukan prosedur standar yang dapat memastikan setiap insiden ditangani secara sistematis dan efektif.

SOP ini disusun sebagai panduan bagi tim keamanan informasi dalam menangani insiden keamanan yang terjadi di lingkungan PT Defend IT360. Prosedur ini mencakup tahapan identifikasi, klasifikasi, respons, investigasi, pemulihan, serta pelaporan insiden guna meminimalkan dampak yang ditimbulkan dan meningkatkan ketahanan sistem terhadap ancaman di masa depan.

2. TUJUAN

Dokumen ini bertujuan untuk memberikan panduan standar dalam menangani insiden keamanan informasi di lingkungan PT Defend IT360 agar respons insiden dilakukan secara cepat, efektif, dan sesuai dengan peraturan yang berlaku.

3. RUANG LINGKUP

SOP ini berlaku untuk semua insiden keamanan informasi yang terjadi di lingkungan operasional PT Defend IT360, termasuk ancaman siber, kebocoran data, akses tidak sah, malware, dan serangan lainnya.

4. REFERENSI

a) ISO/IEC 27001 – *Information Security Management System*
b) ISO/IEC 27035 - *Information Security Incident Management*
c) NIST Special Publication 800-61 - *Computer Security Incident Handling Guide*
d) UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi
e) CIS Controls - *Security Best Practices for Incident Handling*

5. DEFINISI ISTILAH

Untuk memahami istilah yang digunakan dalam pedoman ini, berikut adalah beberapa definisi penting:

a) **Security Operational Center (SOC)**: Pusat kendali keamanan yang bertanggung jawab atas pemantauan, deteksi, respons, dan pencegahan ancaman siber.

b) **SIEM (Security Information and Event Management)**: Sistem yang mengumpulkan dan menganalisis log untuk mendeteksi ancaman keamanan.

c) **Firewall:** Perangkat atau sistem yang mengontrol lalu lintas jaringan berdasarkan aturan keamanan yang telah ditetapkan.

d) **IDS/IPS (Intrusion Detection/Prevention System):** Sistem yang mendeteksi dan mencegah intrusi dalam jaringan.

e) **Endpoint Detection & Response (EDR):** Teknologi keamanan yang memonitor dan merespons ancaman pada perangkat akhir (endpoint).

f) **Threat Intelligence:** Informasi yang dikumpulkan untuk memahami dan mengantisipasi ancaman siber.

g) **Insiden Keamanan Informasi:** Kejadian yang dapat membahayakan kerahasiaan, integritas, atau ketersediaan informasi perusahaan.

h) **Incident Responder:** Personel yang bertugas menangani insiden keamanan siber.

i) **Security Analyst:** Analis keamanan yang mengevaluasi ancaman dan anomali dalam sistem.

j) **Threat Intelligence Analyst:** Analis yang mengumpulkan dan menganalisis data ancaman siber.

k) **CSIRT (Computer Security Incident Response Team):** Tim khusus yang menangani insiden keamanan dalam organisasi.

l) **SOC Engineer:** Teknisi yang bertanggung jawab atas pengelolaan infrastruktur SOC.

m) **PIC Customer:** Penanggung jawab pihak pelanggan dalam hal ini adalah PT Hutama Karya (Persero)

n) **Service Level Agreement:** Kesepakatan tingkat layanan antara penyedia jasa layanan dengan pengguna layanan.

o) **SIEM (Security Information and Event Management)**: Sistem yang mengumpulkan dan menganalisis log untuk mendeteksi ancaman keamanan.

p) **Firewall:** Perangkat atau sistem yang mengontrol lalu lintas jaringan berdasarkan aturan keamanan yang telah ditetapkan.

q) **IDS/IPS (Intrusion Detection/Prevention System):** Sistem yang mendeteksi dan mencegah intrusi dalam jaringan.

r) **Endpoint Detection & Response (EDR):** Teknologi keamanan yang memonitor dan merespons ancaman pada perangkat akhir (endpoint).

s) **Threat Intelligence:** Informasi yang dikumpulkan untuk memahami dan mengantisipasi ancaman siber.

t) **Insiden Keamanan Informasi:** Kejadian yang dapat membahayakan kerahasiaan, integritas, atau ketersediaan informasi perusahaan.

u) **Incident Responder:** Personel yang bertugas menangani insiden keamanan siber.

v) **Security Analyst:** Analis keamanan yang mengevaluasi ancaman dan anomali dalam sistem.

w) **Threat Intelligence Analyst:** Analis yang mengumpulkan dan menganalisis data ancaman siber.

x) **CSIRT (Computer Security Incident Response Team):** Tim khusus yang menangani insiden keamanan dalam organisasi.

y) **SOC Engineer:** Teknisi yang bertanggung jawab atas pengelolaan infrastruktur SOC.

z) **PIC Customer:** Penanggung jawab pihak pelanggan dalam hal ini adalah PT Hutama Karya (Persero)

aa) **Service Level Agreement:** Kesepakatan tingkat layanan antara penyedia jasa layanan dengan pengguna layanan.

6. TUGAS DAN TANGGUNG JAWAB

Setiap anggota tim SOC memiliki peran yang spesifik dalam memastikan keamanan perusahaan: **a)** ***SOC Manager***

- Berkomunikasi dengan pemangku kepentingan; berfungsi sebagai titik kontak organisasi untuk insiden penting dan insiden yang meningkat;
- Memastikan anggota tim SOC bekerja sama erat di dalam dan di luar fungsi SOC;

- Pastikan fungsi SOC memberikan aktivitas deteksi dan respons ancaman sebagaimana ditentukan;
- Terus memantau efektivitas solusi deteksi dan respons insiden dan memberikan masukan perbaikan kepada tim Arsitektur dan Teknik SOC;
- Pastikan tim SOC memberikan dukungan sesuai dengan SLA/KPI yang disepakati; dan
- Pimpinan Operasional dan Analis akan memastikan tim operasi SOC mendapatkan serah terima yang tepat selama pengenalan layanan baru.

b) *Security Analyst* (T1)

- T1 melakukan monitoring dan triage security alerts yang bersumber dari aset-aset TI yang termonitor dalam system monitoring SOC Hutama Karya;
- T1 melakukan investigasi awal insiden keamanan informasi;
- T1 mengoperasikan SIEM yang digunakan di Hutama Karya;
- Memberikan dukungan kepada tim lain saat terjadi insiden keamanan informasi;
- T1 ikut aktif dalam koordinasi dan komunikasi dengan tim terkait penanganan insiden;
- T1 melakukan pencatatan security register dari kegiatan monitoring;
- T1 melakukan dokumentasi dan pengelolaan tiket SOC Hutama Karya sebagai bagian dari pelaporan;
- Tanggung jawab dalam kegiatan operasional T1 meliputi: ○ Mengisi catatan security register setiap shift, mencatat alert yang terjadi, statistik insiden, eskalasi dan penanganan insiden
  - Mengisi laporan kegiatan monitoring setiap shift, catatan aktivitas operasional SOC, pengelolaan ticket, follow up insiden, dan handover shifting
  - Supporting dalam penyusunan laporan-laporan lain yang ditugaskan berkaitan kegiatan security monitoring

c) *Security Analyst* (T2)

- T2 memastikan event dan alert T1 Monitoring ditangani tepat waktu, menggunakan pelaporan dan sesuai dengan matrik dan SLA yang berlaku;
- T2 melakukan investigasi, dan analisa lanjutan terhadap event dan alert yang di eskalasi oleh T1 Monitoring;
- T2 melakukan supervisi kepada T1 Monitoring untuk meningkatkan deteksi dini terhadap event yang dicurigai sebagai anomali dan ancaman cyber;

- T2 melakukan tinjauan terhadap efektivitas threshold/aturan/kebijakan use case dalam sistem monitoring SOC PT Hutama Karya (Persero);
- T2 melaporkan dokumentasi, investigasi, dan analisa root cause setiap insiden untuk dilakukan eskalasi pada T3 Incident Response;
- Tanggung jawab T2 sebagai leader dalam operasional kegiatan SOC memiliki tanggung jawab meliputi:
  - Memastikan laporan bisa di deliver dengan baik seperti : laporan monitoring setiap shift, absensi, ticketing, eskalasi dan follow up insiden, laporan harian, mingguan, bulanan dan tahunan
  - Memastikan SLA SOC dapat tercapai sesuai dengan ketentuan yang telah ditetapkan
    o Memastikan koordinasi dari level paling bawah sampai dengan level manajemen atas dapat berjalan dengan baik
  - T2 memberikan masukan berupa *cybersecurity advisory* dan akan berdiskusi lebih lanjut untuk melakukan *recovery* bilamana diberikan akses dan wewenang untuk melakukan pemulihan layanan

d) *Incident Response* (T3)

- T3 merespon dan menganalisa risiko dan dampak setiap insiden yang dieskalasi T2;
- T3 melakukan analisa strategi dan rencana penanganan dan pemulihan pasca terjadinya insiden;
- T3 membuat analisa dan rekomendasi efektivitas pengendalian keamanan berkaitan insiden;
- T3 memberikan arahan untuk T1 dan T2 serta memberikan rekomendasi-rekomendasi kepada tim terkait di Perusahaan pasca penanggulangan insiden;
- T3 Incident Response berperan sebagai *Subject Matter Expert* (SME) dalam melakukan pendampingan proses identifikasi, proteksi, deteksi, respon, dan recovery insiden; dan
- Tanggung jawab lain T3 Incident Response meliputi: Memberikan laporan penanganan insiden, analisa perbaikan, rekomendasi dan arahan untuk meningkatkan pengendalian cyber security di Pegadaian.

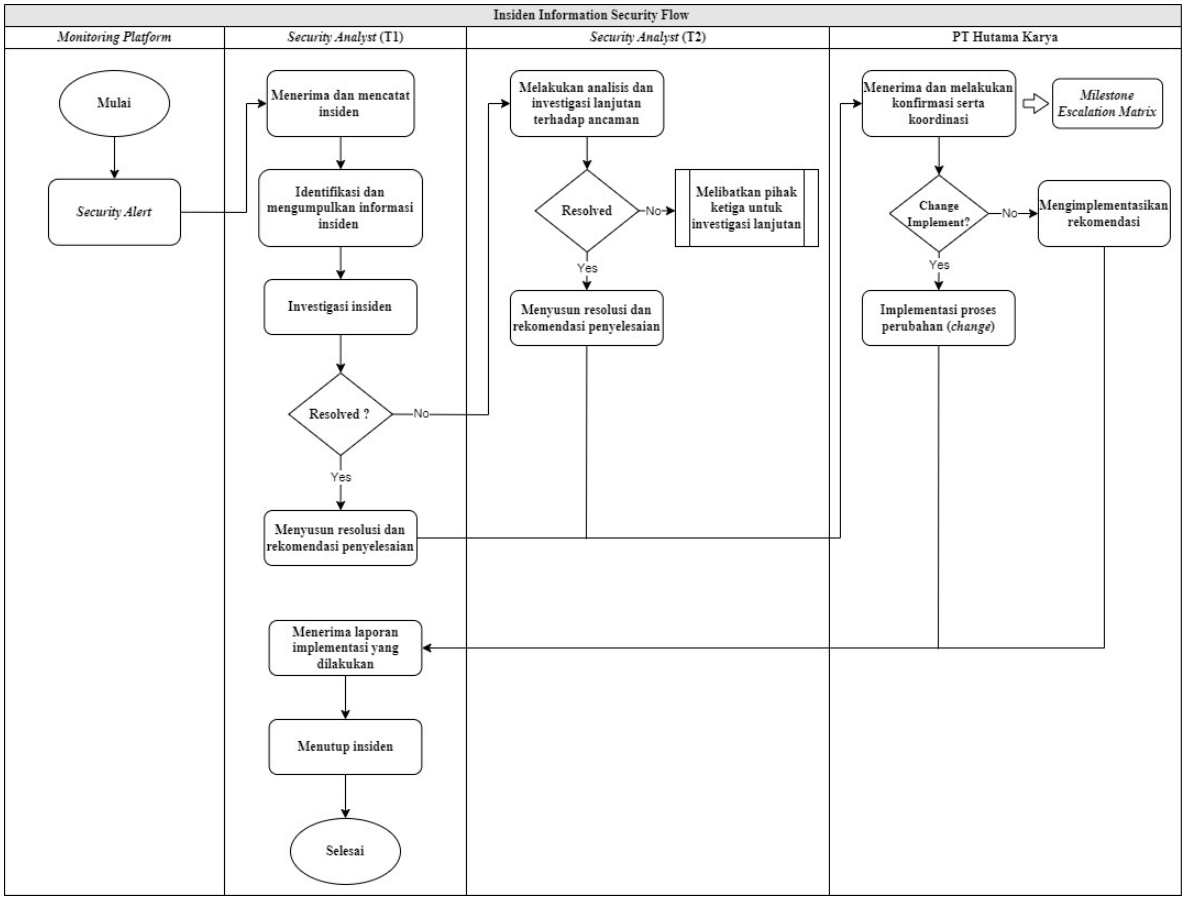
e) *PIC Customers* (PT Hutama Karya)

- Menerima rekomendasi dari Security Analyst (T1, T2);
- Melakukan konformasi terhadap rekomendasi dari Security Analyst (T1, T2);

- Melakukan perubahan configurasi jika terdapat rekomendasi dari Security Analyst (T1, T2)
- Meminta konfirmasi kepada Security Analyst terkait hasil implementasi yang sudah dilakukan.

7. ALUR INSIDEN KEAMANAN OPERASIONAL SOC

Insiden keamanan informasi dapat terjadi kapan saja dan memiliki dampak yang beragam terhadap organisasi. Oleh karena itu, diperlukan prosedur yang jelas dan sistematis untuk memastikan bahwa setiap insiden dapat ditangani dengan cepat dan efektif. Prosedur ini mencakup serangkaian langkah yang harus diikuti oleh tim keamanan dalam mengidentifikasi, mengklasifikasikan, merespons, menganalisis, memulihkan, dan mengevaluasi insiden keamanan. Dengan adanya prosedur yang terstruktur, organisasi dapat meminimalkan risiko, mengurangi dampak, serta meningkatkan ketahanan sistem terhadap ancaman keamanan di masa depan.



Alur proses ini menggambarkan penanganan insiden keamanan informasi di PT Hutama Karya, melibatkan tiga pihak utama: Monitoring Platform, Security Analyst (T1), dan Security Analyst (T2):

1. Proses dimulai ketika Monitoring Platform mendeteksi adanya potensi insiden keamanan dan mengirimkan Security Alert.
2. Security Analyst (T1) menerima alert tersebut, mencatat insiden, dan mulai mengidentifikasi serta mengumpulkan informasi terkait insiden tersebut.
3. Security Analyst (T1) melakukan investigasi awal untuk memahami sifat dan dampak insiden.
   - Jika insiden dapat diselesaikan pada tahap ini (Resolved? Yes), Security Analyst (T1) menyusun resolusi dan rekomendasi penyelesaian.
   - Jika insiden memerlukan investigasi lebih lanjut (Resolved? No), proses berlanjut ke Security Analyst (T2).

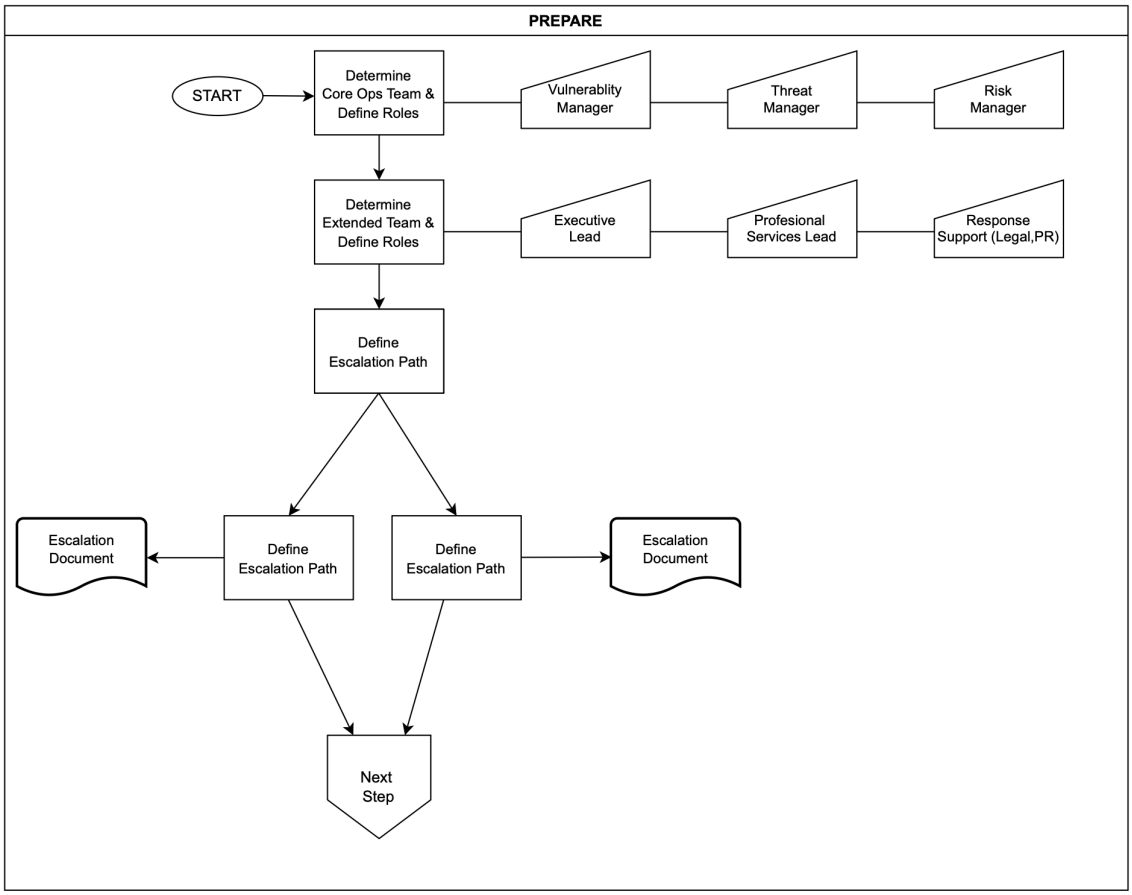
4. Security Analyst (T2) melakukan analisis dan investigasi lanjutan terhadap ancaman, termasuk kemungkinan melibatkan pihak ketiga jika diperlukan.
    - Jika insiden dapat diselesaikan (Resolved? Yes), Security Analyst (T2) menyusun resolusi dan rekomendasi penyelesaian.
    - Jika insiden memerlukan perubahan pada sistem, Security Analyst (T2) berkoordinasi dengan PT Hutama Karya.
5. PT Hutama Karya menerima informasi dari Security Analyst (T2), melakukan konfirmasi dan koordinasi internal.
    - Jika rekomendasi memerlukan perubahan sistem (Change Implement? Yes), PT Hutama Karya mengimplementasikan proses perubahan (change).
    - Jika tidak diperlukan perubahan (Change Implement? No), PT Hutama Karya langsung mengimplementasikan rekomendasi.
6. Security Analyst (T1) menerima laporan implementasi dari PT Hutama Karya.
7. Setelah menerima laporan implementasi, Security Analyst (T1) menutup insiden.
8. Proses penanganan insiden selesai.

Catatan:

- Milestone Escalation Matrix: Dokumen ini digunakan sebagai panduan dalam menentukan eskalasi insiden di internal PT Hutama Karya jika diperlukan.
- Proses ini memastikan bahwa setiap insiden keamanan ditangani secara sistematis dan efektif, dengan kolaborasi antara tim keamanan dan pihak terkait di PT Hutama Karya.

8. PLAYBOOK RESPON MALWARE

f) *Prepare*



Tahap ini memastikan organisasi siap menangani insiden siber dengan mendefinisikan peran, tanggung jawab, jalur eskalasi, dan dokumen pendukung.

1. Menentukan Tim Operasional Inti & Mendefinisikan Peran
    - Meliputi SOC Analyst L1, SOC Analyst L2, Incident Responder, Threat Hunter, dan IR Manager.
    - Menetapkan tanggung jawab utama dan cadangan.
    - Menentukan SLA untuk setiap peran dalam penanganan insiden.
2. Menentukan Tim Ekstended & Mendefinisikan Peran

    Tim tambahan yang terlibat ketika insiden memiliki dampak lebih besar:
    - Executive Lead: Pengambil keputusan strategis.
    - Professional Services Lead: Konsultan atau tim eksternal jika diperlukan.

- Response Support (Legal/PR): Menangani aspek hukum dan komunikasi publik.

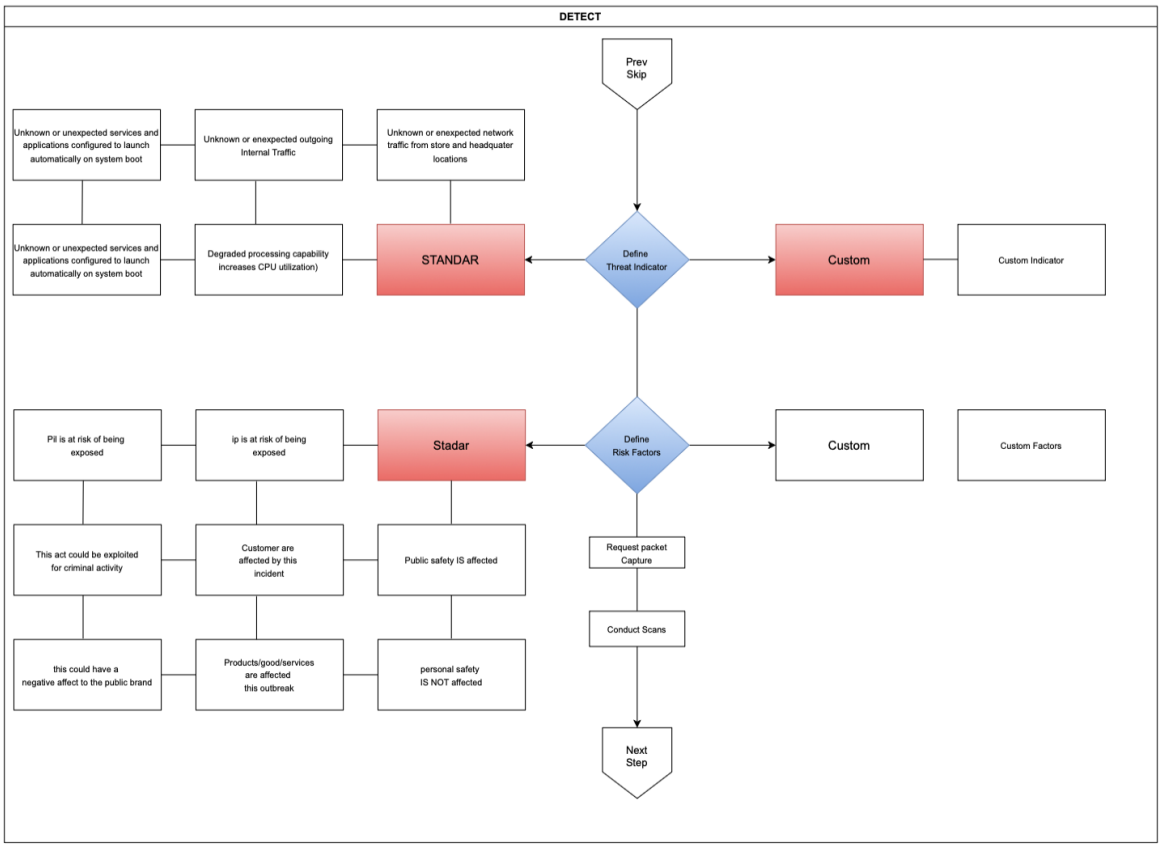
3. Subject Matter Experts (SME)
    - Vulnerability Manager: Mengevaluasi kerentanan terkait insiden.
    - Threat Manager: Memvalidasi IOC/TTP ancaman.
    - Risk Manager: Menilai tingkat risiko dan dampak bisnis.
4. Menentukan Jalur Eskalasi

    Menjelaskan bagaimana insiden naik dari L1 ke L2, L2 ke L3, hingga ke manajemen jika diperlukan. Termasuk:
    - Kriteria eskalasi
    - Kontak person
    - Media komunikasi
5. Dokumen Eskalasi

    Dokumen formal berisi:
    - Direktori kontak
    - Diagram proses eskalasi
    - SLA untuk setiap tahapan eskalasi
6. Lanjut ke Tahap Detect

    Menandakan organisasi siap masuk ke fase deteksi ancaman.

g) *Detect*



Tahap ini bertujuan mengidentifikasi aktivitas anomali atau berbahaya, mengkategorikannya, dan memahami faktor risiko yang mungkin ditimbulkan.

1. Mengidentifikasi Indikator Ancaman (Threat Indicators)

A. Indikator Standar:

- Layanan atau aplikasi tidak dikenal berjalan otomatis saat boot.
- Lalu lintas keluar internal yang tidak biasa.
- Lalu lintas antar lokasi kantor yang tidak biasa.
- Penggunaan CPU meningkat akibat proses mencurigakan.

B. Indikator Khusus (Custom):

- IOC internal perusahaan.
- Pola ancaman yang spesifik untuk lingkungan organisasi.

2. Mengidentifikasi Faktor Risiko (Risk Factors)

A. Faktor Risiko Standar:

- Risiko terekspos nya PII.
- Risiko terekspos nya IP (intellectual property).
- Potensi eksploitasi untuk aktivitas kriminal.
- Dampak terhadap reputasi publik.
- Gangguan layanan/produk.
- Dampak terhadap keselamatan publik.

B. Faktor Risiko Khusus (Custom):

- Dampak bisnis internal.
- Risiko kepatuhan (GDPR, PDPA, ISO27001).
- Risiko industri tertentu.
- Risiko operasional yang unik.

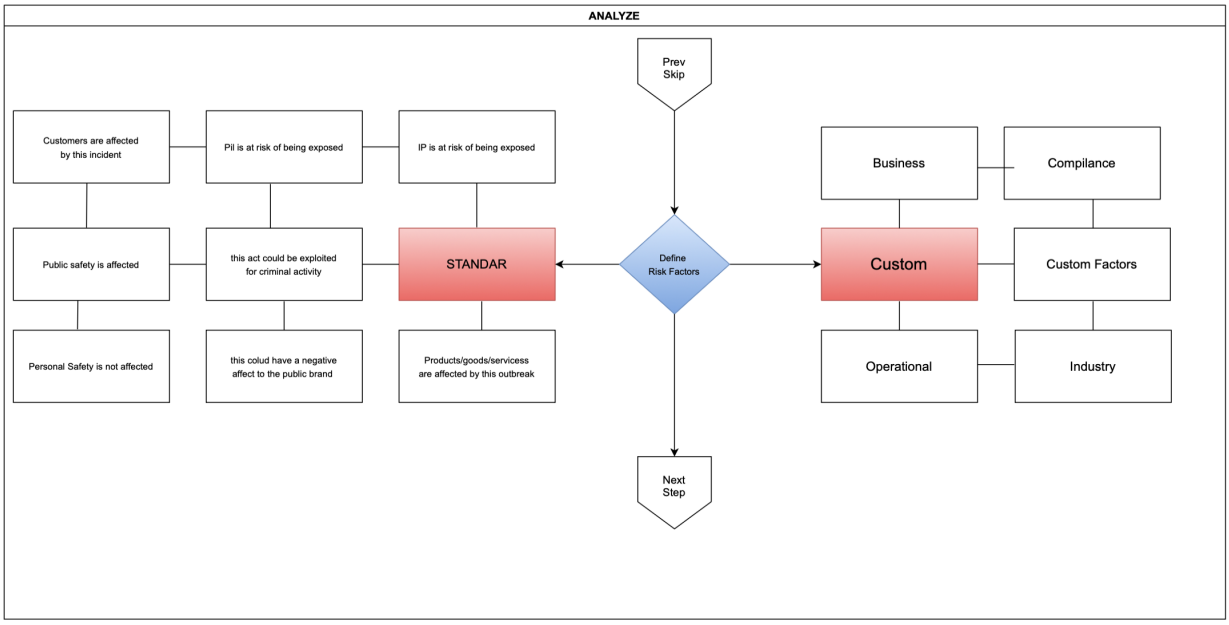
3. Tindakan Tambahan

- Melakukan packet capture untuk analisis jaringan.
- Melakukan pemindaian (AV scan, hunting IOC, scanning kerentanan).

4. Lanjut ke Tahap Analyze

Setelah indikator dan faktor risiko dikumpulkan, proses berlanjut ke analisis lebih dalam.

h) *Analyze*



Tahap ini memvalidasi apakah suatu insiden benar terjadi, menilai tingkat keparahan, dan menentukan tindakan selanjutnya.

1. Penilaian Faktor Risiko (Standar)

Meliputi:

- Dampak terhadap pelanggan.
- Dampak terhadap keselamatan publik.
- Risiko kebocoran data (PII, IP).
- Potensi penyalahgunaan kriminal.
- Kerusakan reputasi bisnis.
- Gangguan pada layanan/produk organisasi.

2. Penilaian Faktor Risiko (Custom)

Meliputi:

- Dampak operasional internal.
- Risiko kepatuhan terhadap regulasi tertentu.
- Risiko yang berkaitan dengan industri.

- Ketergantungan pada infrastruktur kritikal.

3. Menentukan Tingkat Keparahan & Eskalasi

Berdasarkan analisa:

- Menentukan tingkat keparahan (Low, Medium, High, Critical).
- Menentukan apakah IR Team perlu diaktifkan.
- Mengeskalasi ke manajemen bila dibutuhkan.
- Menetapkan langkah respons (containment, eradication, pemberitahuan).