BADAN SIBER DAN SANDI NEGARA

BUKU PUTIH

MITIGASI INSIDEN SIBER
SAAT PANDEMI COVID-19

01

INSIDEN SIBER

DEFINISI

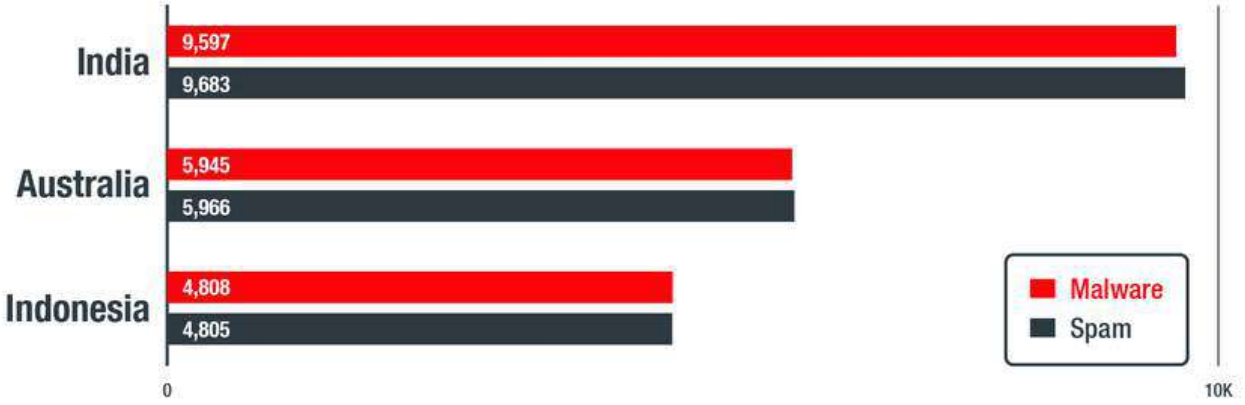
Insiden siber adalah kejadian yang mengganggu atau mengancam berjalannya Sistem Elektronik dan/atau pelanggaran kepatuhan terhadap kebijakan keamanan siber. Contoh insiden siber misalnya serangan virus, pencurian data (informasi pribadi, hak kekayaan intelektual perusahaan, dsb), pengubahan tampilan *website* secara tidak sah (*web defacement*), gangguan akses terhadap layanan elektronik, dsb.

TREN ANCAMAN SIBER SAAT PANDEMI COVID-19

Wabah *Corona Virus Disease* 2019 (COVID-19) yang terjadi di sebagian besar wilayah dunia saat ini dimanfaatkan oleh *threat actor* untuk menyebarkan *malware* (*virus, ransomware*, dsb) dan *spam email* ke banyak pihak. Berdasarkan informasi yang dirilis oleh penyedia layanan keamanan TrendMicro*, setidaknya terdeteksi lebih dari 200.000 kampanye penyebaran *malware* dan *spam* yang terjadi di seluruh dunia pada Q1 2020. Di Indonesia sendiri, terdeteksi setidaknya 4800 aktifitas kampanye serupa pada rentang waktu tersebut.

Sumber :
Developing Story: COVID-19 Used in Malicious Campaigns - https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains

02



Penyebaran *malware* dalam jumlah masif dan memanfaatkan keingintahuan masyarakat tentang COVID-19 sangat berpotensi menyebabkan intrusi secara tidak sah pada infrastruktur TI organisasi, kebocoran data sensitif, infeksi *malware* (*ransomware, virus,* dsb), atau insiden siber lainnya. Ditambah lagi, mayoritas karyawan yang saat ini bekerja secara dari rumah (*Work From Home*/WFH) berpotensi besar terpapar risiko ini karena tidak terhubung ke jaringan yang aman sebagaimana di jaringan korporat organisasi. Oleh karena itu, sangat penting bagi organisasi untuk mempersiapkan diri serta mengantisipasi terjadinya insiden siber terutama di saat pandemi COVID-19 saat ini.

PENTINGNYA KESIAPAN ORGANISASI

Kebijakan dan prosedur terkait implementasi TI di organisasi perlu disesuaikan dengan situasi dan kondisi saat ini, terutama untuk memastikan keamanan siber di organisasi saat sebagian besar pegawai melaksanakan WFH atau *teleworking*.

MENGAPA ORGANISASI PERLU BERSIAP MENGHADAPI INSIDEN SIBER?

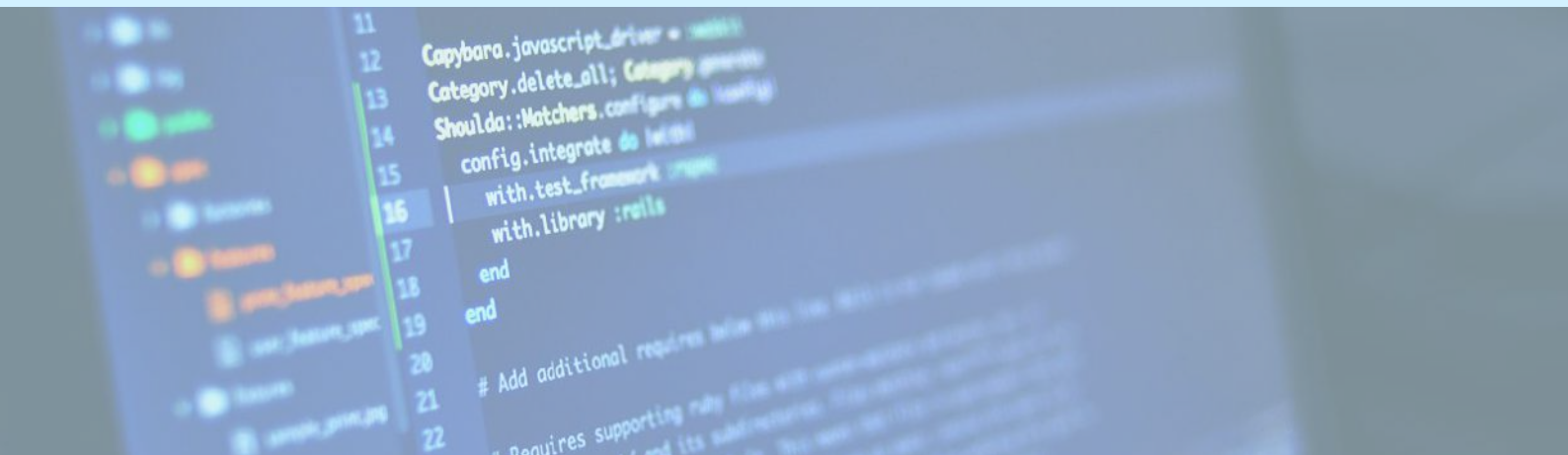
- Meminimalisasi kerugian sebagai akibat dari pencurian informasi atau gangguan dari layanan dan mencegah insiden siber berkembang lebih luas dan berimplikasi pada kerugian yang lebih besar;
- Sesegera mungkin memulihkan sistem dan data elektronik yang terdampak insiden sehingga organisasi dapat melanjutkan proses bisnis dan kegiatannya;
- Menggunakan informasi yang diperoleh selama penanganan insiden, sebagai langkah perbaikan dan persiapan penanganan insiden di kemudian hari;
- Menyimpan bukti kejadian dan mempersiapkan langkah hukum sebagai akibat dari insiden yang terjadi (jika diperlukan).

04

Semakin meningkatnya ketergantungan organisasi terhadap teknologi informasi, dan semakin kompleks serta meningkatnya jumlah serangan siber, maka organisasi perlu memiliki 3 elemen penting berikut sebagai langkah mempersiapkan diri saat insiden siber terjadi.

ELEMEN KE-1 : RENCANA PENANGANAN INSIDEN SIBER

Organisasi perlu memiliki rencana penanganan insiden siber yang komprehensif (biasanya berupa peraturan, pedoman, atau prosedur). Rencana tersebut setidaknya mencakup bagaimana mempersiapkan tim/unit di organisasi untuk menangani insiden siber, mekanisme untuk mencegah penyebarluasan insiden (isolasi insiden), mengidentifikasi tingkat keparahan yang ditimbulkan, menghilangkan sumber penyebab insiden, memulihkan sistem beserta data yang terdampak, sampai dengan evaluasi pembelajaran untuk mencegah insiden serupa terulang di kemudian hari.



05

ELEMEN KE-2 : TIM PENANGANAN INSIDEN SIBER

Sumber daya manusia memiliki peran sangat penting dalam proses penanganan insiden. Keberadaan tim atau unit yang menangani saat terjadi insiden siber sangat penting agar organisasi mempunyai kemampuan menghadapi insiden siber secara responsif. Peran dalam tim penanganan insiden siber sebaiknya terdiri dari beberapa unsur, misalnya sebagai berikut:

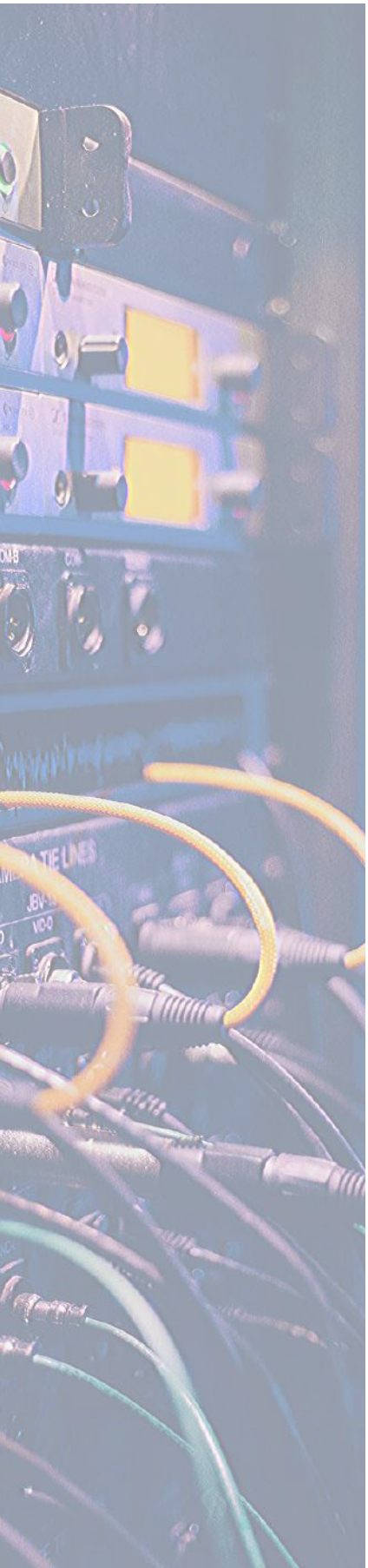
- Kepala tim penanganan insiden siber (*incident response team manager*);
- Analis keamanan siber (*cybersecurity analyst*);
- Peneliti ancaman keamanan siber (*threat researcher*);
- Petugas penanganan awal terhadap bukti digital (*digital evidence first responder*);
- Koordinator komunikasi (*communications lead*).

Untuk mendukung investigasi pasca terjadinya insiden siber (misal, diperlukan langkah penegakan hukum pasca terjadinya insiden siber), peran yang diperlukan antara lain:

- Analis forensik digital (*digital forensic analyst*)
- Perwakilan divisi hukum (*legal representation*).

Setiap unsur dalam tim harus memahami tugas dan perannya dengan baik untuk untuk kelancaran dan efektifitas proses penanganan insiden, utamanya dalam meredam insiden siber yang terjadi sehingga tidak meluas ke komponen sistem lainnya.

06



ELEMEN KE-3 : ALAT BANTU

Perangkat atau alat bantu untuk proses penanganan insiden siber beragam tergantung kebutuhan dan jenis insiden siber yang dialami. Umumnya, alat bantu dalam mendeteksi, menganalisis dan remediasi atas suatu insiden siber yakni *system log*, Netflow, *security information and event management* (SIEM), antivirus atau perangkat *endpoint security*, dsb.

Jenis Perangkat/ Alat Bantu	Tujuan	Contoh Produk/ Teknologi
Security Information and Event Management (SIEM)	▪ Mengumpulkan dan mengagregasikan data *log* pada infrastruktur TI organisasi, yang mencakup aplikasi, perangkat *server*, jaringan dan perangkat-perangkat keamanan. ▪ Menyediakan informasi tentang peringatan, insiden, dan informasi terkait keamanan TI lainnya.	ELK, Security-Onion, IBM QRadar, AlienVault USM
Intrusion Detection Systems (IDS) - *Network & Host-based*	Mendeteksi adanya percobaan intrusi secara tidak sah, aktifitas mencurigakan, atau bentuk serangan siber lainnya. Biasanya menggunakan *baseline* atau *attack signature* untuk proses pendeteksian, berupa *host-based intrusion detection system* (HIDS), atau *network-based intrusion detection system* (NIDS).	Snort, Suricata, BroIDS, OSSEC
Netflow Analyzers	Mendapatkan informasi lalu lintas data aktual pada *border gateway* dan dalam jaringan, melacak aktifitas atau aliran data tertentu pada jaringan, dan menganalisis protokol yang digunakan pada jaringan.	ntop, NfSen, Nfdump
Availability Monitoring	Gangguan ketersediaan layanan atau aplikasi dapat menjadi indikator awal adanya suatu insiden siber. Aplikasi pemantauan ketersediaan (*availability monitoring*) dapat memberikan informasi tentang *uptime* dari setiap komponen infrastruktur termasuk aplikasi dan perangkat *server*, sehingga membantu administrator mengidentifikasi permasalahan sebelum berdampak ke organisasi.	Nagios
Vulnerability Scanners	Memindai kerentanan potensial pada aset TI organisasi. Berdasarkan hasil pemindaian, akan diketahui titik-titik kerentanan potensial beserta rekomendasi untuk perbaikannya.	OpenVAS, Nessus

07

TIPS PENTING SAAT PENANGANAN INSIDEN SIBER

PANTAU SECARA CERMAT SETIAP ANOMALI

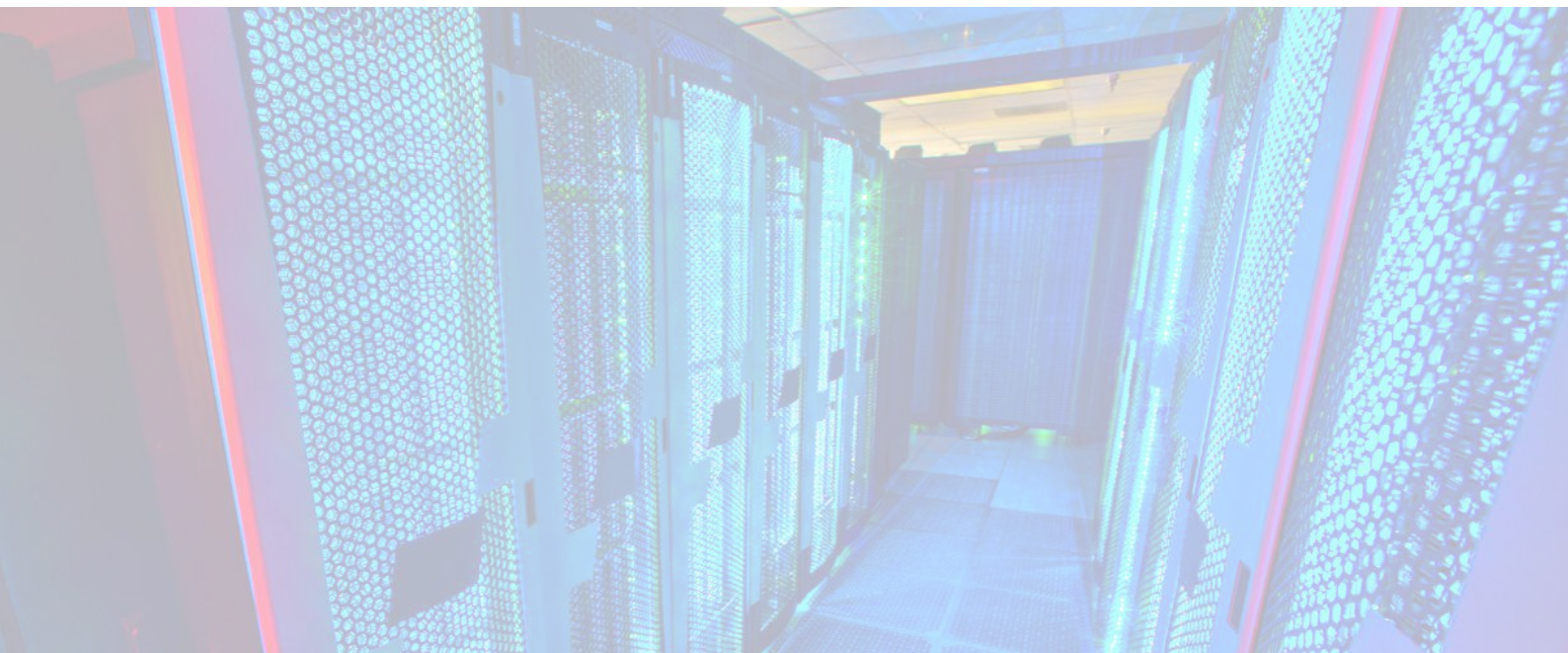
Deteksi terhadap suatu pelanggaran keamanan atau insiden siber tidak dapat sepenuhnya mengandalkan perangkat atau alat bantu. Analisis dari tim atau personil keamanan sangat dibutuhkan untuk menganalisis lebih lanjut aktifitas-aktifitas anomali yang berkaitan, menentukan dampaknya serta langkah apa yang perlu diambil untuk mengamankan aset informasi penting organisasi. Berikut ini beberapa hal penting yang perlu dipantau secara rutin oleh tim keamanan siber di organisasi.

- Anomali lalu lintas data. Akses terhadap aset sensitif dan koneksi aplikasi/*server* yang digunakan secara internal biasanya memiliki volume yang relatif stabil. Jika ditemukan peningkatan secara tiba-tiba atau akses pada waktu yang tidak biasa, maka perlu segera diperiksa.

- Akses tanpa izin/tidak sah terhadap suatu informasi. Akun khusus (misal, Administrator) memiliki akses ke lebih banyak informasi dan sistem dibandingkan akun pegawai lainnya. Akun-akun tersebut perlu dipantau secara cermat, serta perhatikan juga perubahan atau peningkatan status hak akses (*privilege*) di akun pegawai normal.

- *File* mencurigakan dan penggunaan sumber daya komputasi secara berlebihan. Jika terjadi peningkatan kinerja memori dan CPU di luar normal, maka bisa jadi ini merupakan indikator terdapat seseorang yang secara ilegal memanfaatkan aset komputer organisasi untuk kepentingannya, atau indikator pelanggaran keamanan lain seperti kebocoran data.

Perangkat keamanan siber mutakhir seperti *Entity and User Behavioral Analytics* (UEBA) dapat meng-otomasi proses-proses di atas dan mengidentifikasi anomali perilaku pengguna atau akses terhadap *file-file* yang sensitif. Pemanfaatan perangkat tersebut akan membantu dalam mendeteksi adanya insiden secara lebih awal dan mengurangi beban tim keamanan di organisasi.



09

GUNAKAN PENDEKATAN TERPUSAT

Kumpulkan informasi dari perangkat-perangkat keamanan dan sistem TI lainnya, serta simpan pada lokasi terpusat, misalnya pada perangkat *Security Information and Event Management* (SIEM). Gunakan informasi tersebut untuk membuat lini waktu kejadian, menganalisis keterhubungan antara satu *event* dengan *event* lainnya, dan menginvestigasi suatu insiden.

Pendekatan terpusat juga dapat digunakan untuk mengatur respon otomatis pada perangkat-perangkat keamanan TI, jika diperlukan langkah atau respon cepat terhadap suatu *event* dan insiden yang dinilai kritis. Untuk menerapkannya, gunakan teknologi misalnya *Security Orchestration, Automation and Response* (SOAR). SOAR memungkinkan dilakukannya metode analitik berdasarkan informasi yang dikumpulkan dari perangkat-perangkat keamanan yang ada, lalu mengatur *trigger* atau *threshold* yang sesuai dan mengaktifkan respon otomatis pada perimeter-perimeter keamanan (seperti *firewall* dan *intrusion prevention system*).

10

TIDAK MENGGUNAKAN ASUMSI

Saat melakukan investigasi, sebaiknya tidak membuat asumsi-asumsi tentang adanya suatu *event* atau insiden tertentu. Alih-alih menggunakan asumsi, buatlah semacam prosedur singkat yang dapat diverifikasi dan dievaluasi. Sebagai contoh, “Jika terdapat peringatan (*alert*) X pada perangkat Y, maka *event* Y seharusnya terjadi dalam jarak waktu yang dekat”. Buat prosedur-prosedur singkat tersebut berdasarkan pengalaman Anda dan tim, misalnya dalam mengkonfigurasi jaringan, membangun perangkat lunak, mengelola sistem, dsb dan gunakan sudut pandang dari seorang *threat actor*.

ABAIKAN KEJADIAN YANG TIDAK MUNGKIN

Saat melakukan investigasi atas suatu kejadian insiden, ada banyak kemungkin-kemungkinan yang terjadi dan mungkin kita tidak tahu persis informasi apa yang perlu kita cari. Dalam kondisi ini kita dapat mengabaikan kejadian-kejadian yang dapat dijelaskan secara logis. Setelah itu, kita dapat fokus pada kejadian-kejadian yang tidak biasa (anomali) atau belum terdapat penjelasan, misalnya :

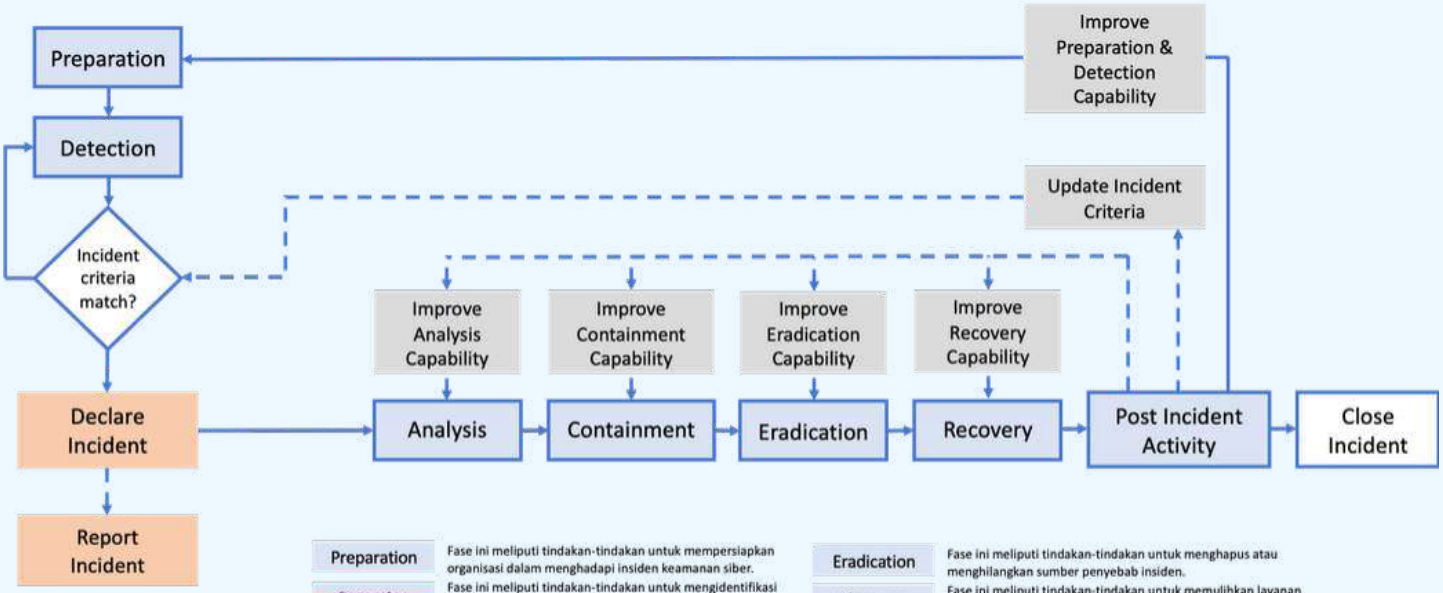
- Adanya perubahan volume lalu lintas data yang signifikan (naik/turun drastis dibandingkan normal);
- Adanya permasalahan akses ke fungsi administratif (*administration role*) ke aplikasi;
- Adanya permasalahan kinerja di jaringan yang mempengaruhi akses ke situs korporat atau aplikasi internal organisasi;
- Adanya perubahan pada konten, *layout* atau tata letak pada situs *web* korporat, namun tidak terdokumentasi/tercatat perubahannya;
- dsb.

11

LAKUKAN EVALUASI PASCA INSIDEN SIBER

Lakukan pemantauan secara berkelanjutan terhadap sistem Anda untuk mengantisipasi aktifitas-aktifitas anomali dan memastikan *threat actor* tidak berhasil masuk kembali. Kemudian lakukan tinjauan dan evaluasi pasca insiden untuk mencari solusi atas permasalahan yang dialami selama pelaksanaan penanganan insiden siber di organisasi.

ALUR HIDUP PENGELOLAAN INSIDEN SIBER



Preparation	Fase ini meliputi tindakan-tindakan untuk mempersiapkan organisasi dalam menghadapi insiden keamanan siber.
Detection	Fase ini meliputi tindakan-tindakan untuk mengidentifikasi dan melakukan verifikasi terhadap insiden keamanan siber yang terjadi.
Analysis	Fase ini meliputi tindakan-tindakan untuk menelaah dan menentukan jenis, skala dan dampak dari insiden yang terjadi.
Containment	Fase ini meliputi tindakan-tindakan untuk mencegah penyebarluasan insiden ke komponen sistem atau layanan TI lainnya.
Eradication	Fase ini meliputi tindakan-tindakan untuk menghapus atau menghilangkan sumber penyebab insiden.
Recovery	Fase ini meliputi tindakan-tindakan untuk memulihkan layanan dan data yang terganggu atau terdampak oleh insiden.
Post Incident Activity	Fase ini meliputi tindakan-tindakan dalam mengevaluasi hasil pembelajaran dalam penanganan insiden dan kendali keamanan yang diperlukan dalam mendeteksi serta mencegah insiden serupa di kemudian hari.

BADAN SIBER DAN SANDI NEGARA

Jl. Harsono RM No.70, Ragunan,
Jakarta Selatan
12550

Website : https://bssn.go.id
Telepon : (021) 780 5814
Aduan Siber : bantuan70@bssn.go.id
Email : humas@bssn.go.id