BADAN SIBER &
SANDI NEGARA

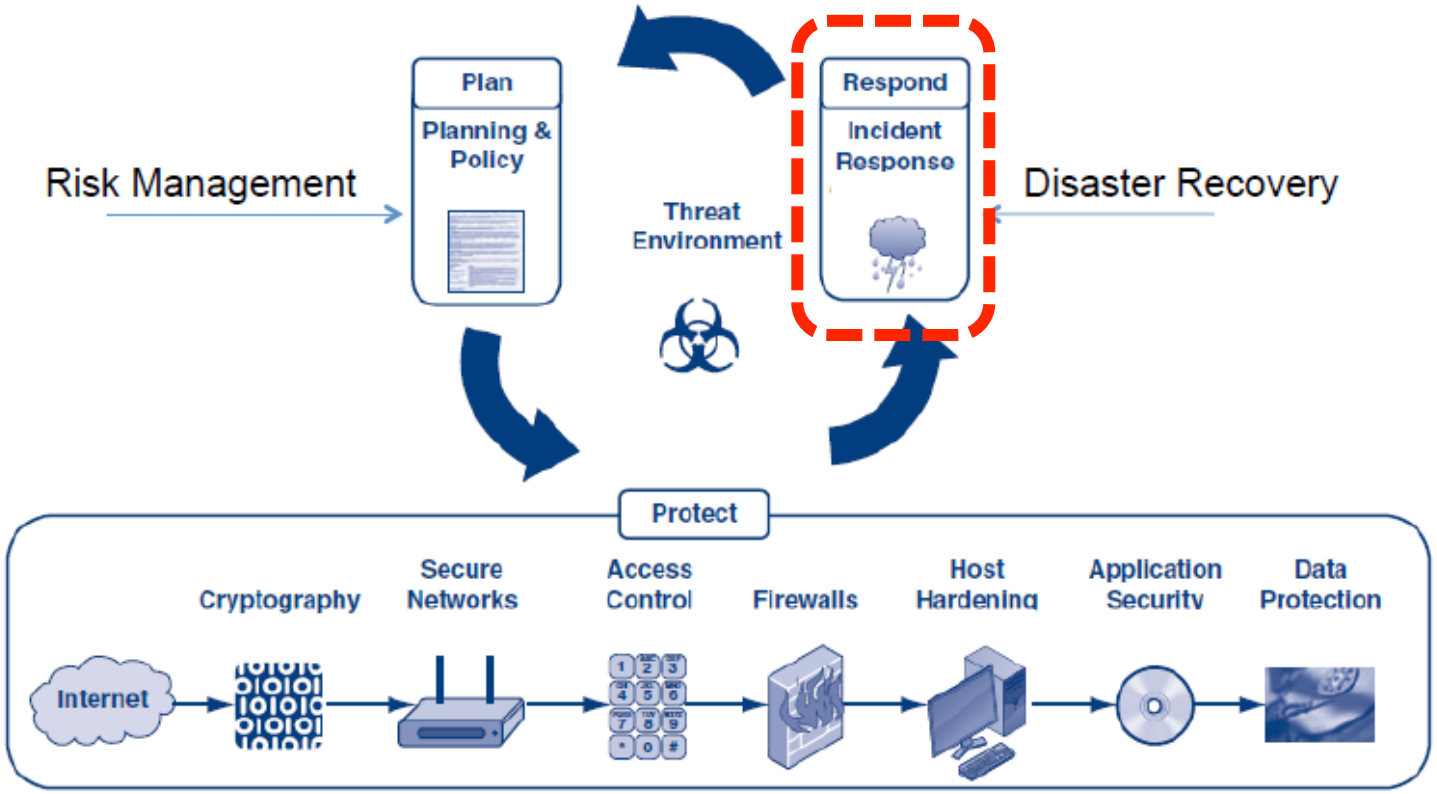
ASEAN-JAPAN ONLINE CYBER EXERCISE

Jakarta, 20 Juni 2019

Outline

- Pengantar
- Skenario ASEAN-Japan Cyber Exercise
- Persiapan Kegiatan

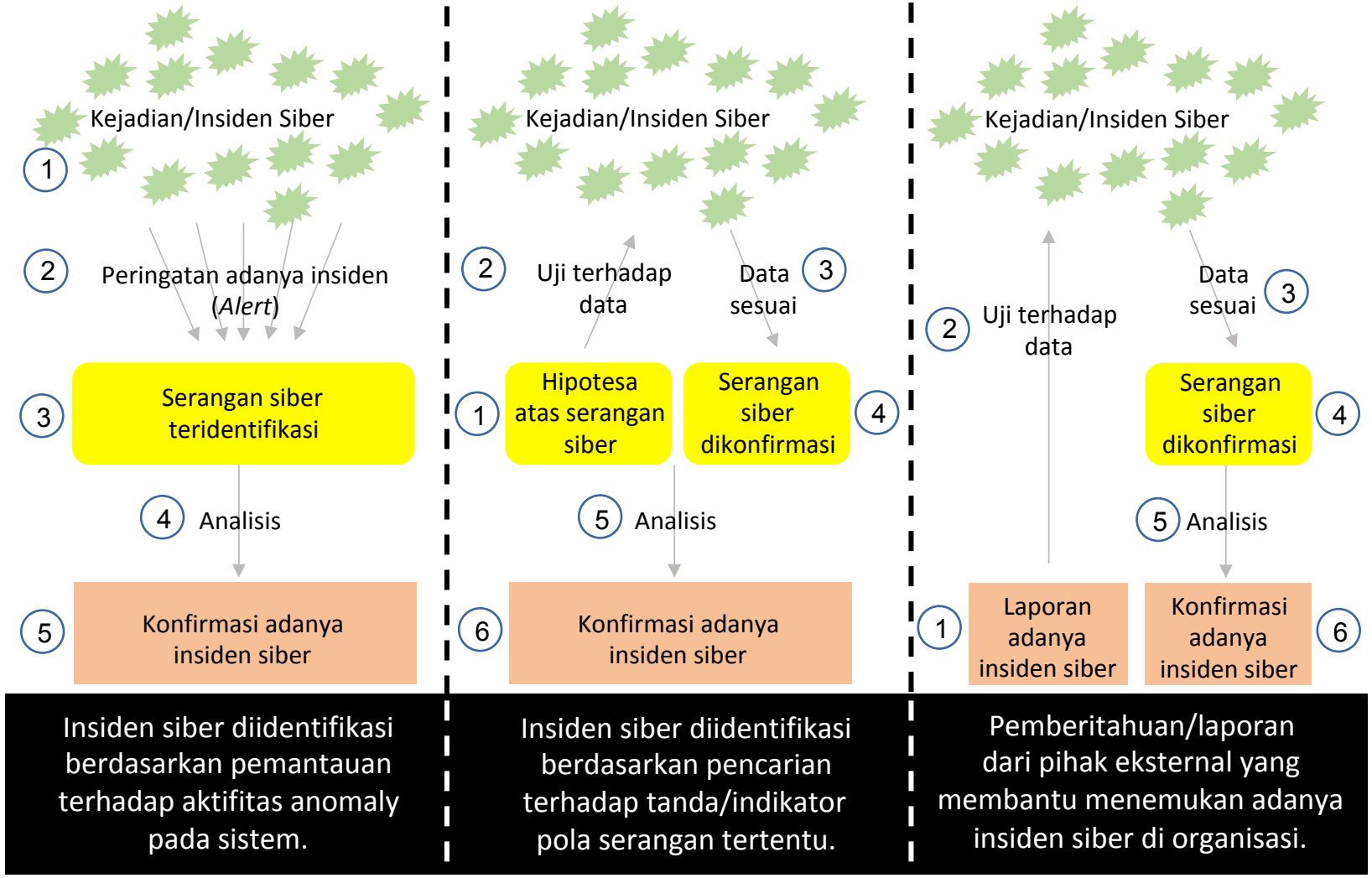
Urgensi Penanganan Insiden Siber *(Incident Handling)*



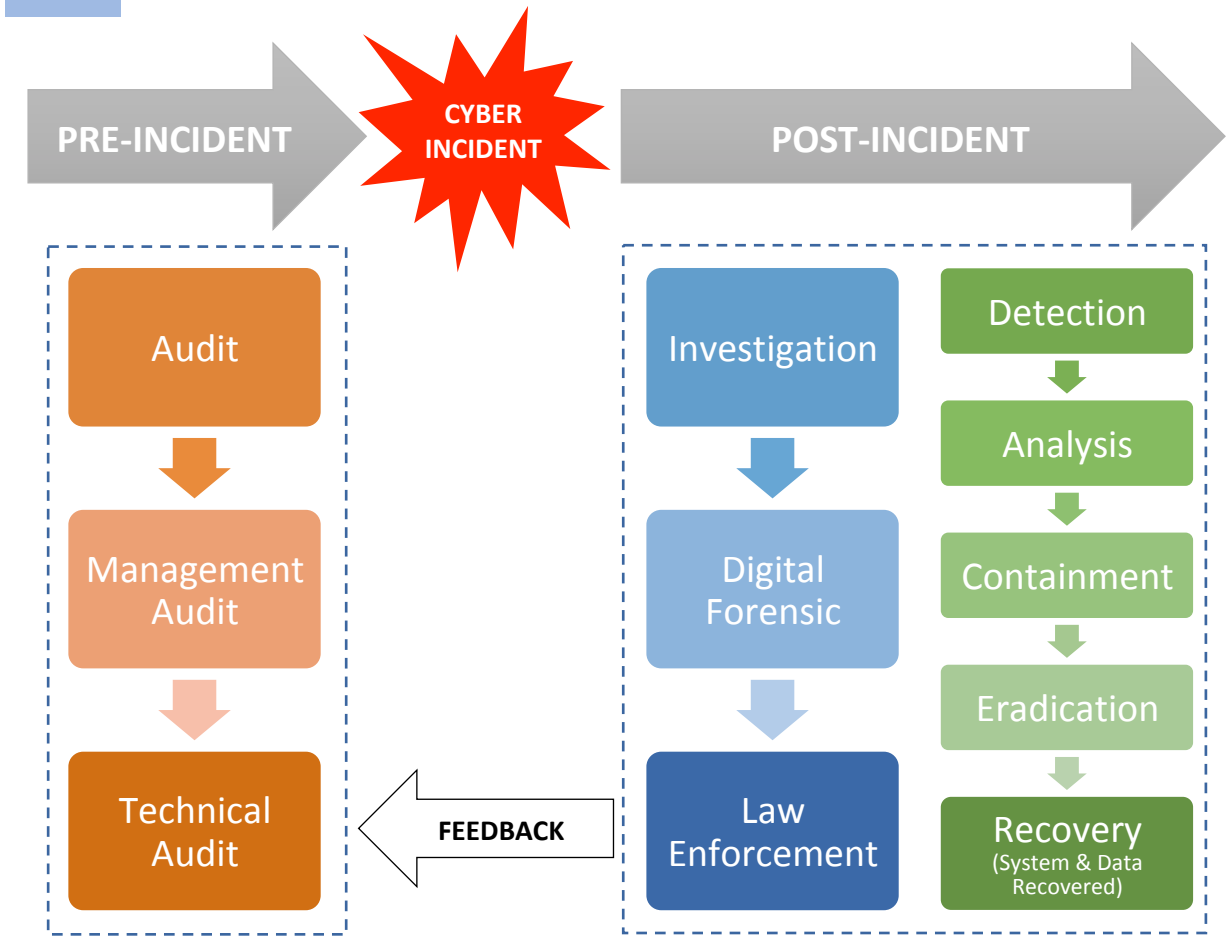
Proses/tindakan untuk merespon insiden siber secara sistematis, dengan tujuan :

- **Meminimalisasi kerugian** sebagai akibat dari pencurian informasi atau gangguan dari layanan;
- Menggunakan informasi yang diperoleh selama penanganan insiden, sebagai **langkah perbaikan** & persiapan penanganan insiden di kemudian hari;
- **Mempersiapkan langkah hukum** sebagai akibat dari insiden yang terjadi (jika diperlukan).

Cara Mengidentifikasi Insiden Siber



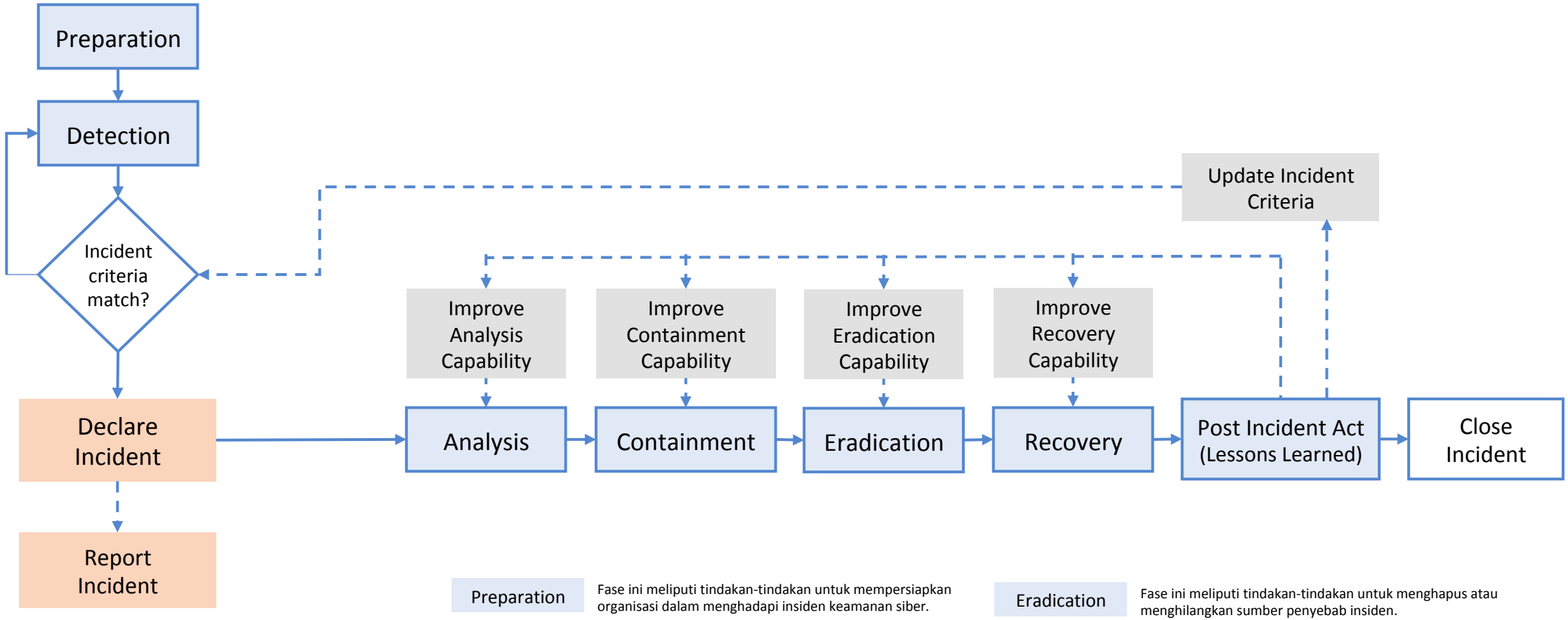
Insiden & Tindakan Kriminal di Ranah Siber



PENANGANAN TINDAKAN KRIMINAL DI RANAH SIBER

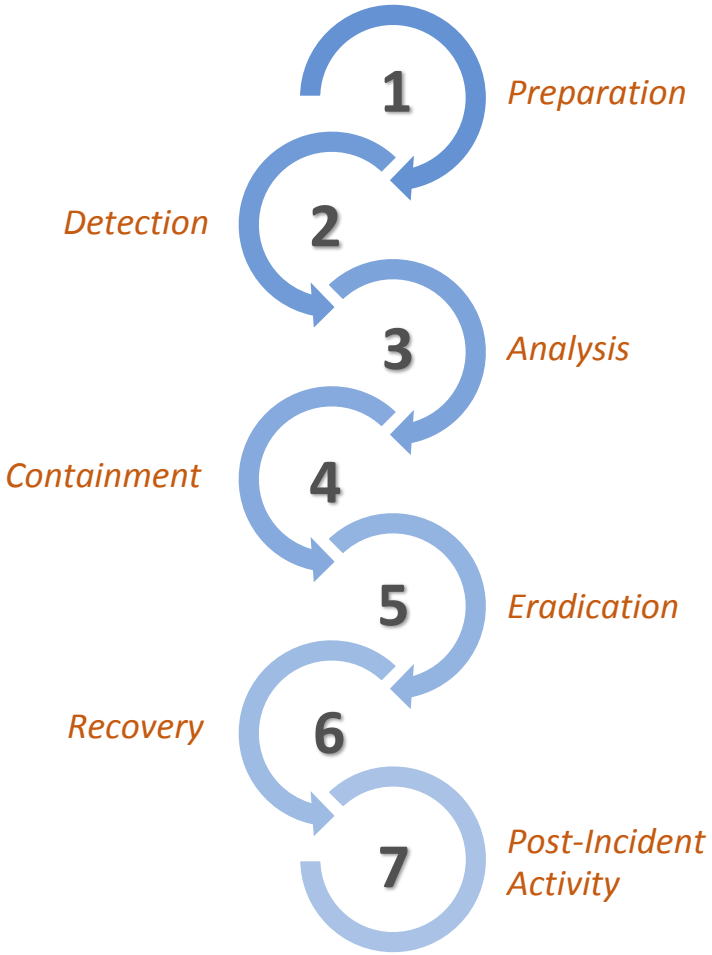
- **Cyber Crime (Cyber Incident)**
  - Computer/smartphone as tools and/or target.
  - Example : Carding, Malware/Ransomware, Web defacement, etc.
- **Computer-Related Crime**
  - Any type of crime with computer/ smartphone as evidence.
  - Example : Hoax, Ujaran kebencian, dsb.

Prosedur Penanganan Insiden Siber

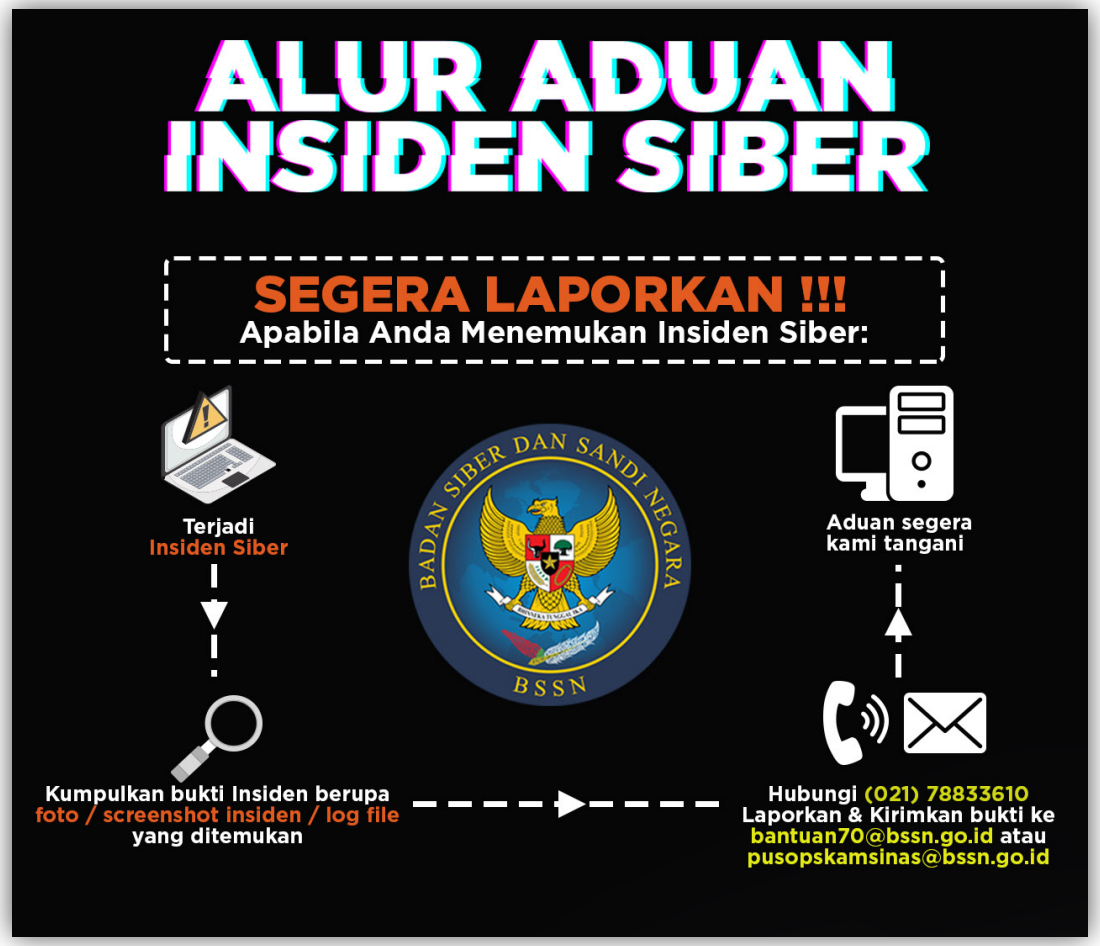


Preparation	Fase ini meliputi tindakan-tindakan untuk mempersiapkan organisasi dalam menghadapi insiden keamanan siber.
Detection	Fase ini meliputi tindakan-tindakan untuk mengidentifikasi dan melakukan verifikasi terhadap insiden keamanan siber yang terjadi.
Analysis	Fase ini meliputi tindakan-tindakan 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.

Petunjuk Teknis Penanganan Insiden Siber
(Incident Response Playbook)



Pelaporan Insiden Siber



Cyber Exercise

- Latihan terkait keamanan siber yang diperuntukkan bagi staf pelaksana di bidang Teknologi Informasi atau Administrator yang bertanggung jawab dalam operasional keamanan siber dan/atau penanganan insiden siber.
- Bentuk kegiatan :
  - Table Top Exercise – Paper-driven exercise with injects scripted by exercise planners and **delivered via paper (cards/discussion)**
  - Hybrid - Paper injects with **some live scenarios** facilitated by a Red Team for realism (probes, scans, e-mail spoofing, etc.)
  - Full Live - Exercise plan incorporates **real scenarios** and injects into the exercise. Paper injects only used to stimulate if necessary.
- Pelaksanaan Cyber Exercise oleh BSSN
  - National Cyber Exercise (National Cyber-X)
  - Government Cyber Exercise (Government Cyber-X)
  - Critical Information Infrastructure Cyber Exercise (CII Cyber-X)

ASEAN-Japan Cyber Exercise

TUJUAN

- Meningkatkan kerjasama dan berbagi informasi (*information sharing*) di bidang keamanan siber antar negara anggota ASEAN dan Jepang, serta institusi-institusi yang terlibat dalam pelaksanaan Cyber Exercise.

SASARAN

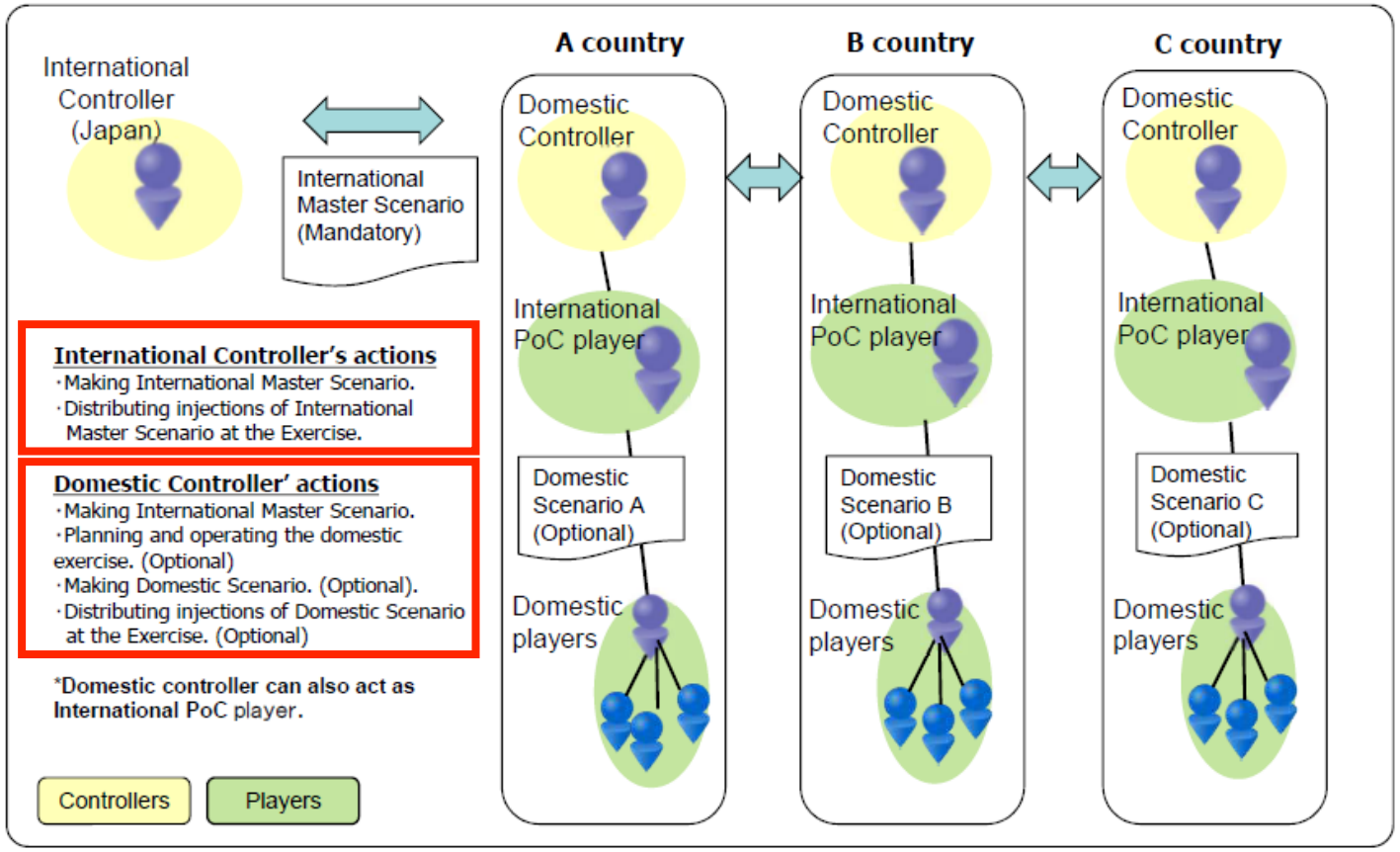
1. Meningkatkan **kapabilitas dan kesiapan** dalam koordinasi penanggulangan insiden keamanan siber di tingkat nasional pada setiap negara ASEAN.
2. Membangun metode komunikasi untuk **berbagi informasi** secara aman antara para peserta dan antar negara ASEAN.
3. Terjalinnya **kerja sama dan komunikasi** yang baik antar negara ASEAN dan Jepang dalam keamanan siber.

Pelaksanaan Cyber Exercise

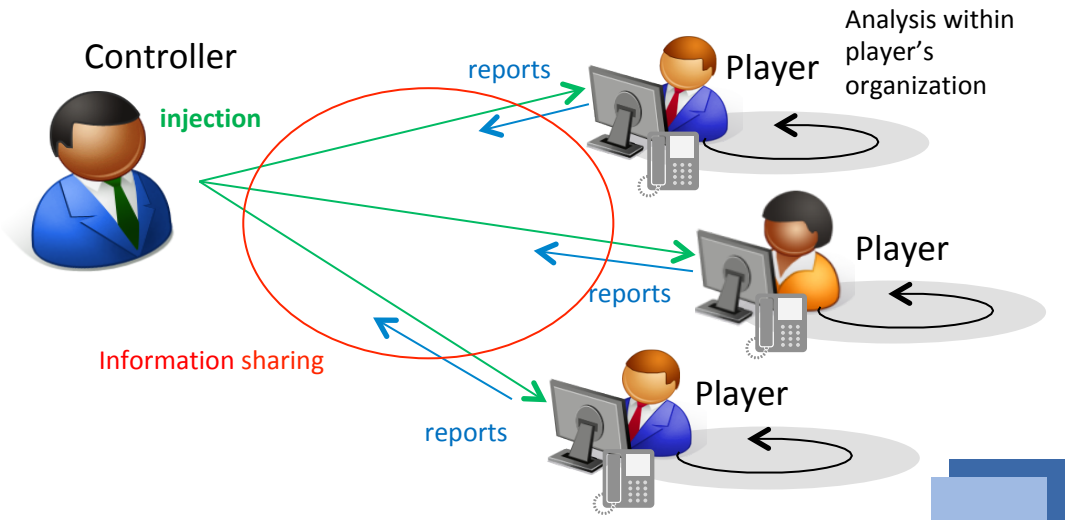
NATIONAL CYBER EXERCISE
2019

KEGIATAN DRILL TEST
PADA SEKTOR INFRASTRUKTUR INFORMASI KRITIKAL NASIONAL
2018

Peserta Kegiatan (ASEAN-Jepang)



1. Indonesia
2. Brunei
3. Cambodia
4. Japan
5. Laos
6. Myanmar
7. Malaysia
8. Philippines
9. Singapore
10. Thailand
11. Viet Nam



Peserta Kegiatan (Indonesia)

1. Badan Siber dan Sandi Negara
    1. National CSIRT - International PoC Player
    2. Government CSIRT (Gov-CSIRT) - Domestic Controller
2. Kementerian Energi dan Sumber Daya Mineral
3. Kementerian Pertahanan
4. Kementerian Pendidikan dan Kebudayaan
5. Kementerian Sosial
6. Kejaksaan Agung
7. Kantor Staf Presiden
8. Lembaga Ilmu Pengetahuan Indonesia
9. Lembaga Administrasi Negara
10. Lembaga Kebijakan Pengadaan Pemerintah
11. Pemerintah Daerah Khusus Ibukota Jakarta
12. Pemerintah Daerah Istimewa Yogyakarta
13. Pemerintah Daerah Jawa Barat
14. Pemerintah Kota Palembang
15. Pemerintah Kabuten Oku

Skenario ASEAN-Japan Cyber Exercise
Deskripsi Umum Skenario

- Kasus yang diangkat berdasarkan kejadian insiden siber yang aktual.
- Dibagi ke dalam 2 tahap :
  - STAGE 1 : Studi kasus atas insiden *web redirection*.
  - STAGE 2 : Studi kasus serangan siber secara masif berupa *distributed denial of service*.
- Dalam mengatasi permasalahan yang diangkat pada kasus, Peserta bekerjasama dan melakukan praktek berbagi informasi keamanan siber berupa :
  - Mengirimkan status/keadaan keamanan siber pada institusi masing-masing;
  - Mengirimkan laporan singkat atas kejadian insiden siber yang dihadapi.
- Tanggapan atas setiap kasus dikirim melalui media yang ditentukan (email).

Skenario ASEAN-Japan Cyber Exercise

Tahapan Skenario

STAGE 1

1. Jepang mengidentifikasi bahwa terdapat beberapa kejadian pengunjung situs/ website institusi pemerintah diarahkan (*redirect*) ke toko online palsu.

2. Sumber/penyebab dari kejadian *web redirection* teridentifikasi, namun diketahui bahwa banyak pihak yang telah mengakses toko online palsu tersebut.

STAGE 2

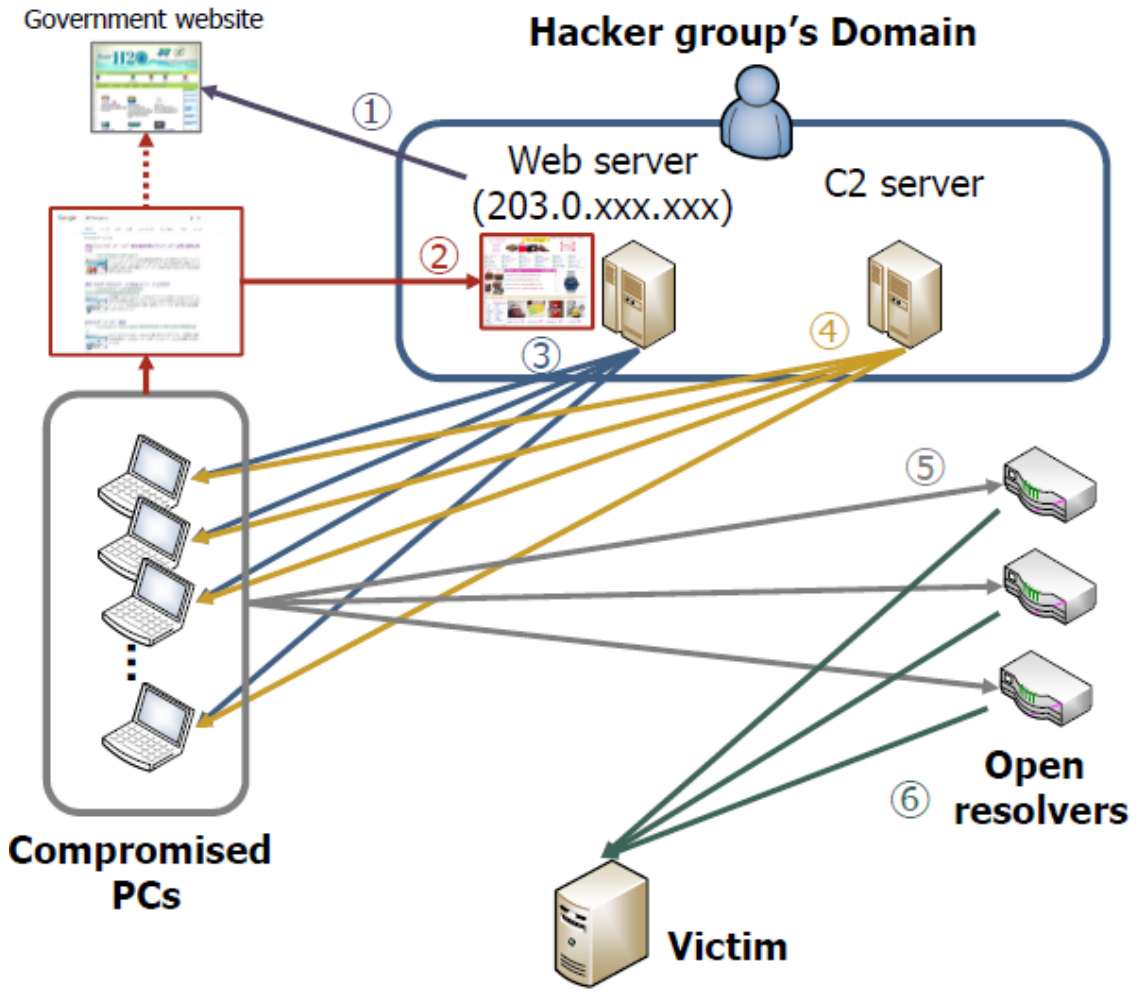
3. Terjadi kegagalan konektifitas jaringan yang diidentifikasi disebabkan oleh serangan *distributed denial of service* (DDoS). Walaupun serangan tersebut telah berhenti, investigasi atas kasus tersebut masih berjalan.

4. Negara yang mengalami kejadian serangan DDoS (Singapura) berbagi informasi ttg bagaimana metode mitigasi serangan DDoS tersebut berikut sumber/penyebab serangan tsb.

5. Akar permasalahan atas kasus *web redirection* (Stage 1) berhasil diketahui. Setiap negara saling berbagi informasi ttg metode mitigasi berikut dg informasi lainnya.

Skenario ASEAN-Japan Cyber Exercise

Gambaran Teknis Serangan Siber pada Skenario (1)

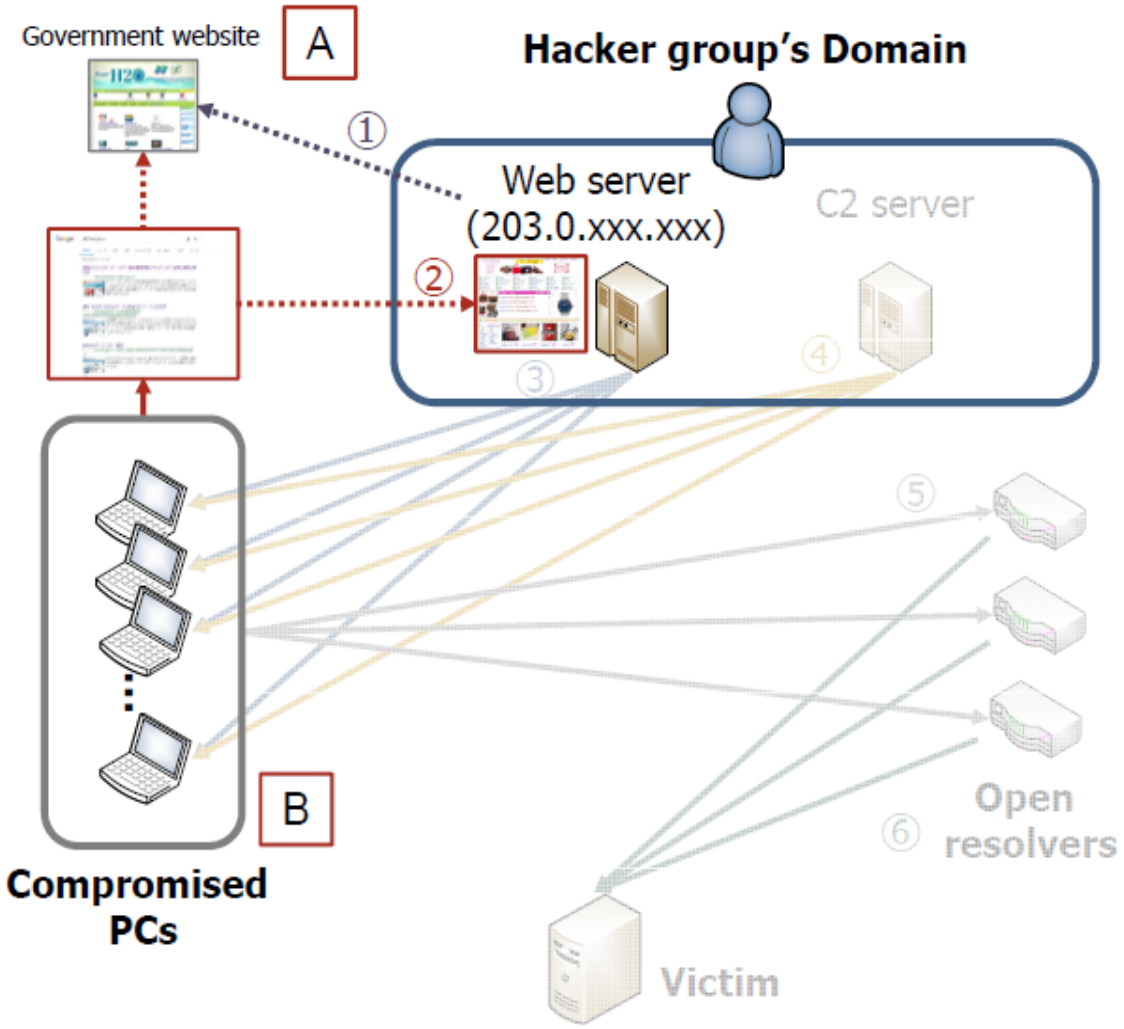


Tahapan Serangan Siber

1. Sekelompok grup hacker berhasil menyisipkan kode/skrip secara tidak sah ke dalam situs/website institusi pemerintah, yang menyebabkan pengunjung situs tersebut di-*redirect* ke situs toko online palsu.
2. Selain itu, saat pengunjung *search engine* mencari toko online, ditemukan bahwa toko online tersebut beralamat pada domain website suatu institusi pemerintah.
3. Grup hacker (pelaku serangan siber) memasang perangkat (secara tidak sah) Remote Access Trojan/RAT (missal, JBiFrost) ke PC yang mengakses toko online palsu.
4. Command and Control (C2, server pengendali yang dipasang oleh grup hacker) mengendalikan dari jarak jauh setiap PC yang terinfeksi RAT.
5. PC yang terinfeksi mengirimkan paket-paket jaringan yang dipalsukan ke server Open DNS Resolver, yang ditujukan ke komputer korban sebagai target serangan (paket jaringan yang dipalsukan berisi alamat IP dari target serangan).
6. Setelah menerima paket *request* (permintaan) dari PC-PC yang terinfeksi, DNS Resolver mengirimkan paket *response* (balikan) ke alamat IP korban (target serangan). Saat komputer korban menerima paket response tsb, karena volume paket yang sangat besar, maka berakibat pada Denial of Service.

Skenario ASEAN-Japan Cyber Exercise

Gambaran Teknis Serangan Siber pada Skenario (2)

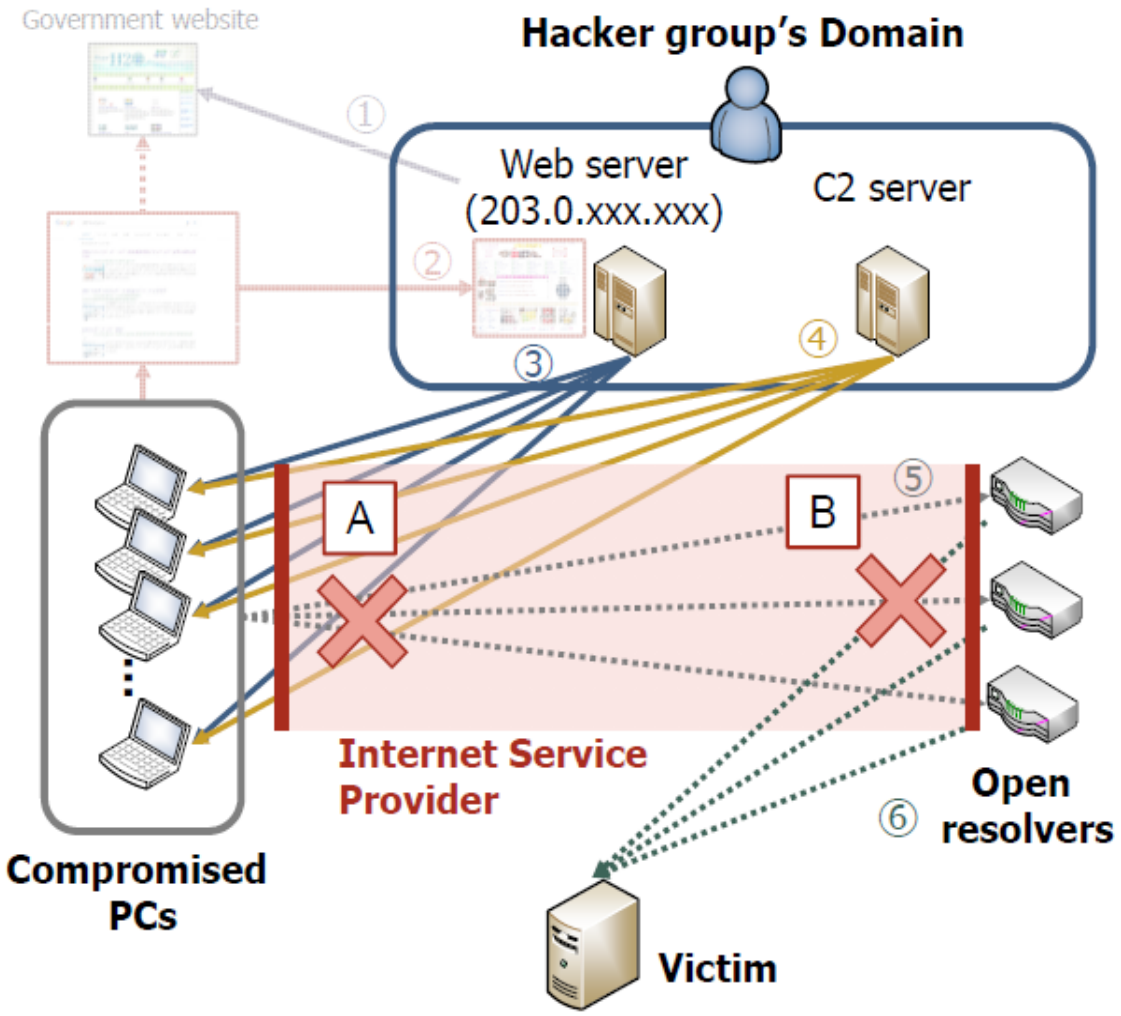


Penanganan dan Penangkalan Serangan Siber

1. Penanganan kasus *web redirection* tersebut dapat dilakukan dengan memasang versi terbaru dari aplikasi Content Management System (CMS), sistem operasi dan aplikasi lainnya yang digunakan untuk menjalankan web server. Selain itu, kode/skrip yang disisipkan secara tidak sah ke dalam website tsb juga harus dihapus.
2. Bagi pengguna (pengunjung website), mitigasi perlu dilakukan untuk mencegah infeksi malware saat membuka website yang compromised (terpasang kode/skrip yang disisipkan secara tidak sah). Pemblokiran terhadap website yang compromised dapat dilakukan untuk mencegah penyebaran malware lebih lanjut. Selain itu, pastikan bahwa perangkat anti-virus, sistem operasi dan aplikasi lainnya diperbarui dengan versi paling mutakhir.

Skenario ASEAN-Japan Cyber Exercise

Gambaran Teknis Serangan Siber pada Skenario (3)



Penanganan dan Penangkalan Serangan Siber

Saat suatu paket data IP dimana alamat sumbernya (*source address*) bukan merupakan alamat IP yang dikelola di internal jaringan tsb kemudian dikirim ke luar jaringan, maka dapat diidentifikasi bahwa alamat sumber tersebut dipalsukan. Koneksi paket data tersebut sebaiknya diblokir. Mekanisme ini dikenal dengan nama BCP38 [IETF RFC 2827].

Referensi Terkait dengan Skenario yang Diangkat

STAGE 1 | Web Redirection

- In February 2019, Drupal disclosed a vulnerability which by exploiting it is possible to remotely execute a malicious PHP code. As a countermeasure, it was released that updating to the latest version that modified the vulnerability.
  - https://www.drupal.org/sa-core-2019-003
- In February 2019, RIPS Technologies disclosed a vulnerability on WordPress that enables remote code execution, and then CVEs were allocated for the vulnerability found. It was recommended to update to the latest version.
  - https://blog.ripstech.com/2019/wordpress-image-remote-code-execution/
- In June 2018, Japan Cybercrime Control Center (JC3) and Anti-Phishing Working Group (APWG) published a report aimed at minimizing the threat of fake stores and reducing the number of victims that fake store websites compromise.
  - https://www.jc3.or.jp/about/pdf/JC3_APWG_Revealed_Threat_of_Fake_Store.pdf

STAGE 2 | DDoS Attack

- In the report of the US NCCIC published in November 2018, a RAT (Remote Access Tool) called JBiFrost has been exploited many times in recent cyber incidents, and there exist possibilities that it is exploited as a botnet for information leakage and DDoS attack.
  - https://www.us-cert.gov/ncas/alerts/AA18-284A
- In February 2019, ENISA posted that the number of new DDoS attack patterns targeting ISPs has been increasing. It exploits DNS's open resolver across hundreds of IP addresses to avoid detection. ENISA continues to recommend to avoid the open resolver.
  - https://www.enisa.europa.eu/publications/info-notes/dns-ddos-attack-protections
- Moreover, February 1, 2019 is a special day called DNS Flag Day. The worldwide DNS service providers collaborate to remove the evasion function of EDNS (Extension mechanisms for DNS) from this day.
  EDNS is an extension function enabling UDP transmission etc. of messages larger than 512 bytes. Until now, there has been existing a workaround solution even if incorrect EDNS equipment is detected.
  - https://www.us-cert.gov/ncas/current-activity/2019/01/30/MS-ISAC-Releases-Advisory-DNS-Flag-Day

TAHAPAN		DESKRIPSI	WAKTU
Start		Jepang (International Controller) mengirimkan email notifikasi untuk menandakan bahwa kegiatan dimulai.	**14.00**
STAGE 1	**Injection 1**	Jepang mengirimkan informasi bahwa terdapat kasus *web redirection* pada beberapa situs/website institusi pemerintah. Pengunjung situs web institusi pemerintah dibelokkan ke situs-situs took online palsu.	**14.01**
	Injection 2	Thailand memberitahukan informasi perihal kerentanan (*vulnerability*) yang menyebabkan kasus *web redirection* pada beberapa situs/ website institusi pemerintah (eksploitasi thd kerentanan pada CMS Drupal versi 8.5.x sebelum 8.5.11 dan Drupal versi 8.6.x sebelum 8.6.10).	**14.20**
	Injection 3	Jepang memberitahukan beberapa negara telah memperbaiki situs/website yang rusak (terdampak insiden *web redirection*), namun situs-situs toko online palsu masih banyak yang aktif dan diketahui bahwa banyak pihak yang telah mengakses toko online palsu tersebut.	**14.35**
	Injection 4	Indonesia melakukan investigasi terhadap salah satu website pemerintah yang terdampak insiden. Waktu kejadian *hacking* thd salah satu website pemerintah diidentifikasi berdasarkan investigasi *log file* pada web server.	**14.45**
STAGE 2	**Injection 5**	Terjadi kegagalan koneksi jaringan dalam skala besar pada institusi pemerintah di Singapura. Walaupun serangan tersebut telah berhenti, investigasi atas kasus tersebut masih berjalan.	**15.00**
	Injection 6	Kelompok *hacker* bernama Anti-AJ Society melancarkan ancaman melalui media Twitter, bahwa kelompok tsb akan melakukan serangan siber skala besar berupa Distributed Denial of Service ke negara-negara ASEAN.	**15.00**
	Injection 7	Saat ini terjadi serangan siber skala besar berupa Distributed Denial of Service (DDoS) di negara-negara ASEAN termasuk Indonesia. Setiap entitas saling berbagi informasi metode penanganan serangan tersebut melalui media selain internet (*conference call*).	**15.15**
	Injection 8	Thailand melakukan investigasi terhadap kasus serangan DDoS yang ditujukan ke Singapura (Injection 5). Berdasarkan hasil investigasi bersama dengan ISP pada Thailand, diungkap bahwa sumber serangan DDoS adalah *malware* berupa Remote Access Trojan/RAT bernama JBiFrost.	**15.55**
	Injection 9	Malaysia melakukan analisis lanjutan terhadap *malware* berupa Remote Access Trojan/RAT yang diberikan oleh Thailand. Ditemukan bahwa insiden *web redirection* yang sebelumnya terjadi (STAGE 1) berkaitan dengan kejadian serangan DDoS yang telah terjadi di ASEAN dimana aktor pelaku serangan adalah kelompok *hacker* Anti-AJ Society.	**16.05**
	Injection 10	Kelompok *hacker* Anti-AJ Society ditangkap. Setiap negara merilis berita (*press release*) perihal perkembangan situasi keamanan siber yang terjadi, penangkapan grup *hacker* Anti-AJ Society, dan bahwa situasi keamanan siber kembali terkendali.	**16.20**

Persiapan Pelaksanaan Kegiatan
Informasi Pengiriman & Uji Komunikasi Email

- Gunakan frase **[Latihan Latihan Latihan]** pada Subject & Email Header untuk setiap email yang dikirim.
- Rata-rata waktu ± 15 menit untuk penyelesaian setiap kasus.
- Persiapan kegiatan :

Diskusi seputar kasus skenario yang diangkat (tanya-jawab)	11.30 WIB
Uji komunikasi (email)	13.00 WIB
Diskusi seputar kasus skenario yang diangkat *(lanjutan)*	13.30 WIB
Pelaksanaan kegiatan ASEAN-Japan Cyber Exercise	14.00 WIB

- Seluruh kirim/terima email berasal dan ditujukan ke alamat berikut (sebaiknya dimasukkan dalam Contact List untuk kemudahan) :

gulih.pemerintah@bssn.go.id

BADAN SIBER &
SANDI NEGARA

SEKIAN