INCIDENT HANDLING DRILL EXERCISE

Mobile Phone Users

308,2 million (121% of population)

Smart Phone Users

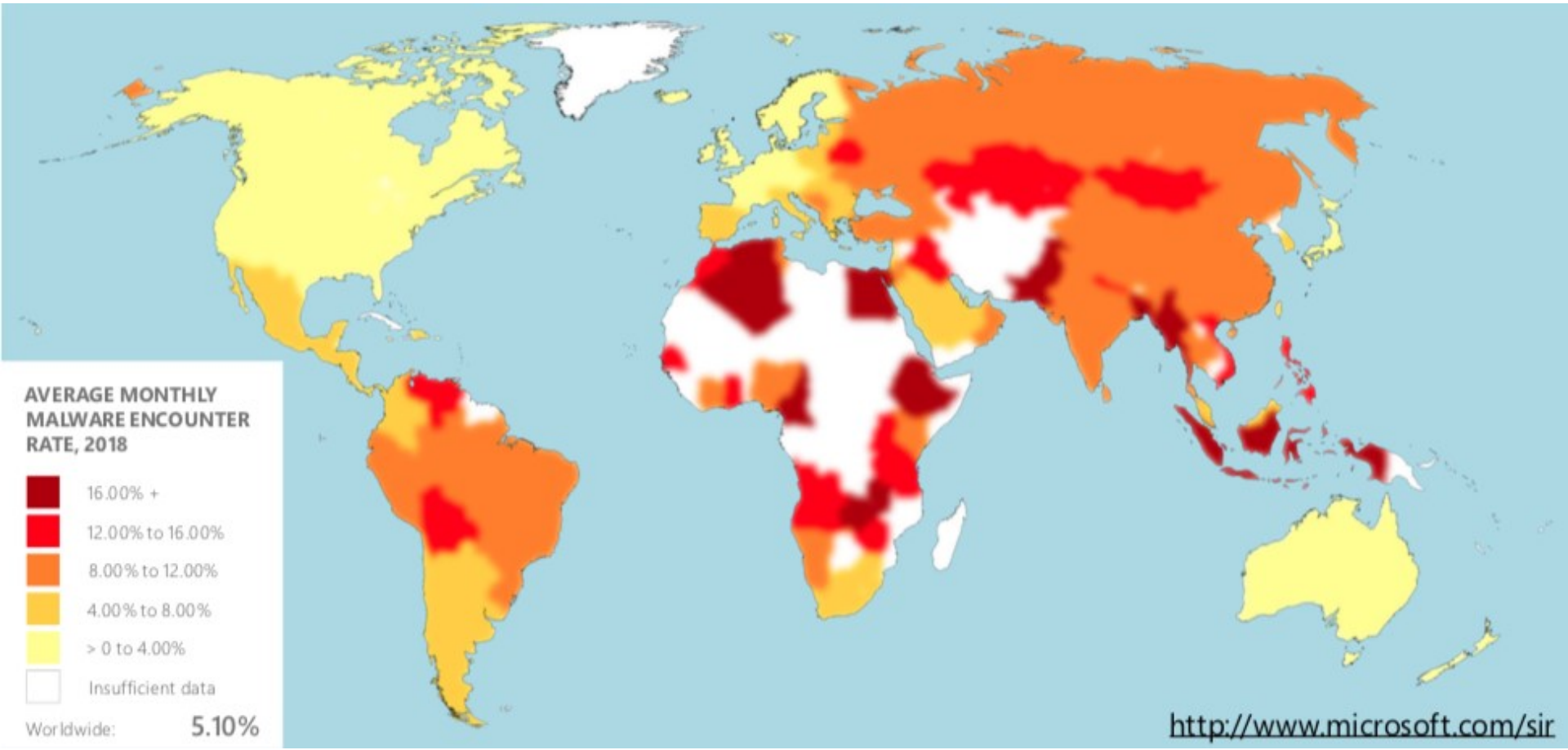
63,4 million (24,7 % of population)

Age Composition

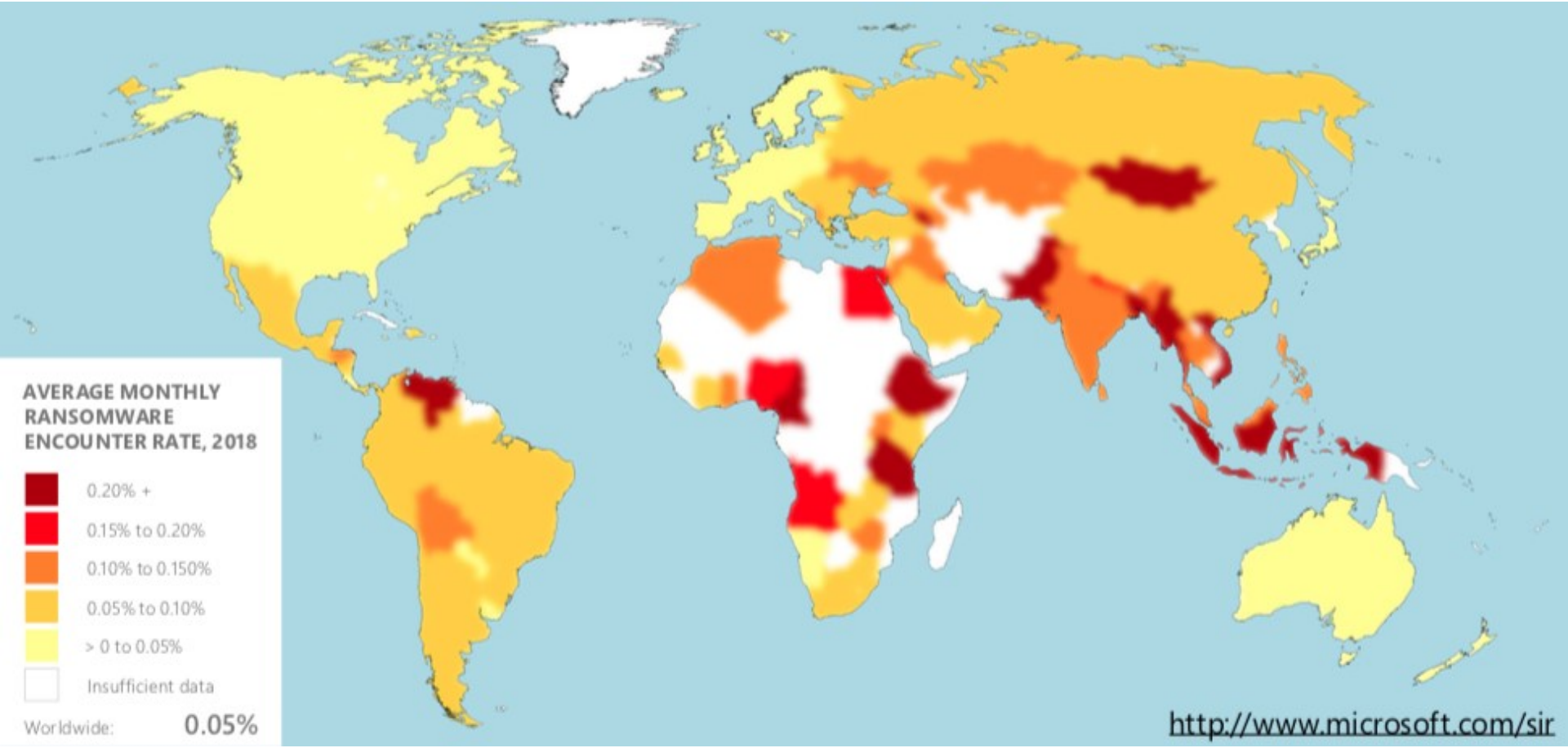
125 million people under the age of 35, potential targets of e-commerce


INDONESIA SUMBER SERANGAN TERBANYAK
16,939 TOTAL INSIDEN WEBSITE
DOMAIN TERBANYAK DISERANG: GO.ID
2,885 LAPORAN PENGADUAN PUBLIK
122,435,215 TOTAL AKTIVITAS MALWARE
INDONESIA TARGET SERANGAN TERBANYAK
1,872 TOTAL INFORMASI CELAH KEAMANAN
PORT TERBANYAK DISERANG: 53
232,447,974
SERANGAN

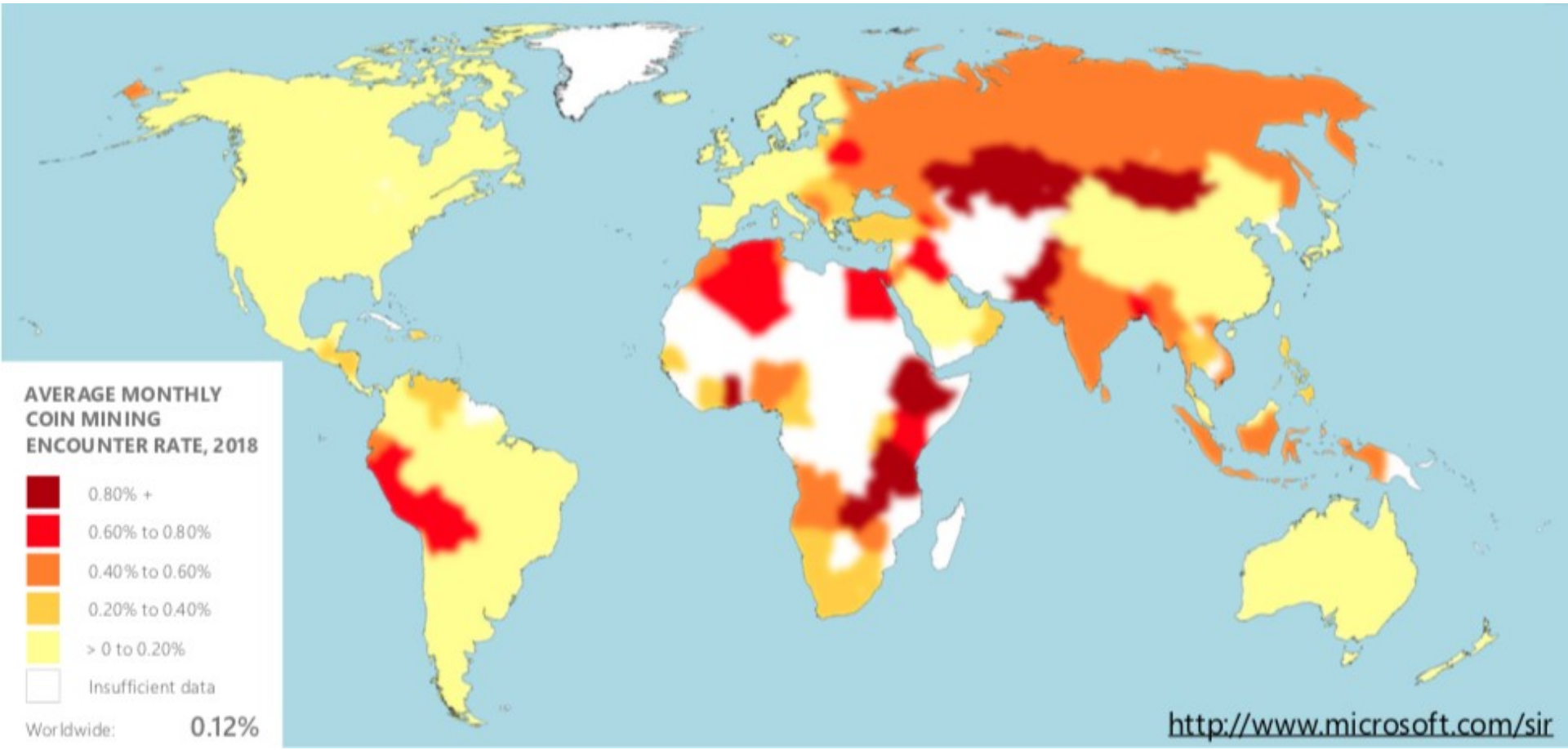
Penyebaran Malware



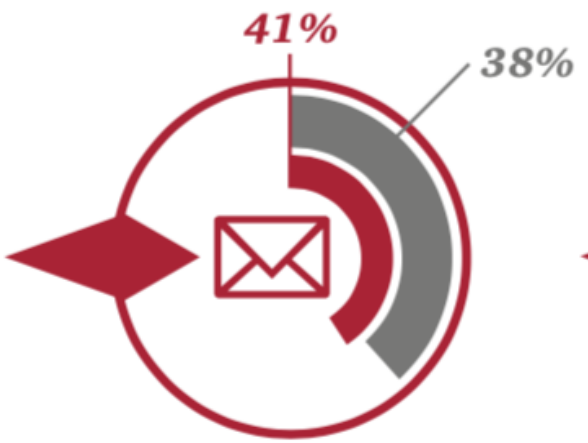
Penyebaran Ransomware



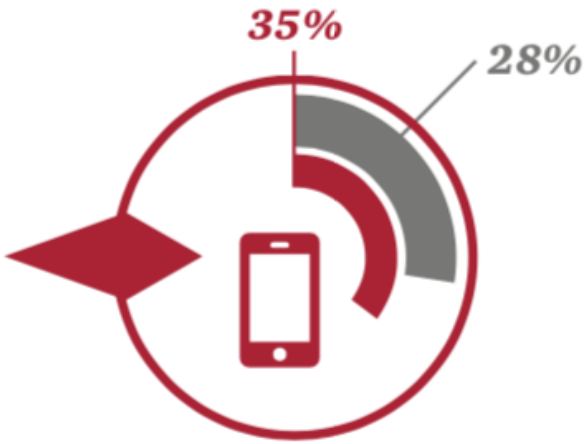
Penyebaran Crypto Mining



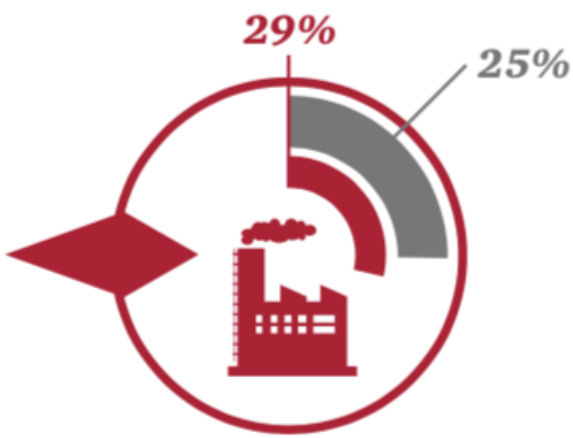
Top Vectors of Cyber Security Incidents



Phishing

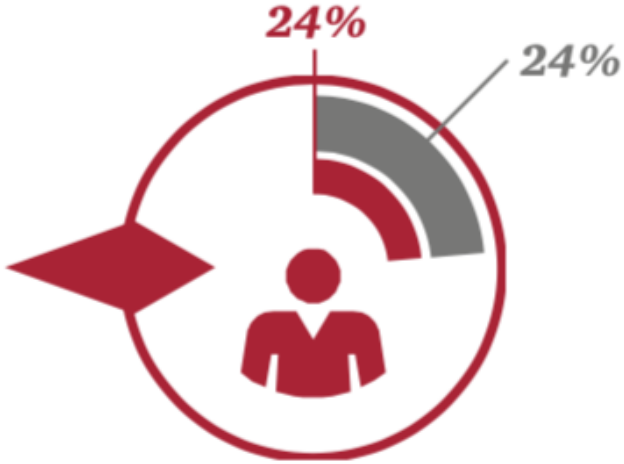


Mobile Device



Operational Technology

Financial Technology



Employee

Sumber: GSISS 2017

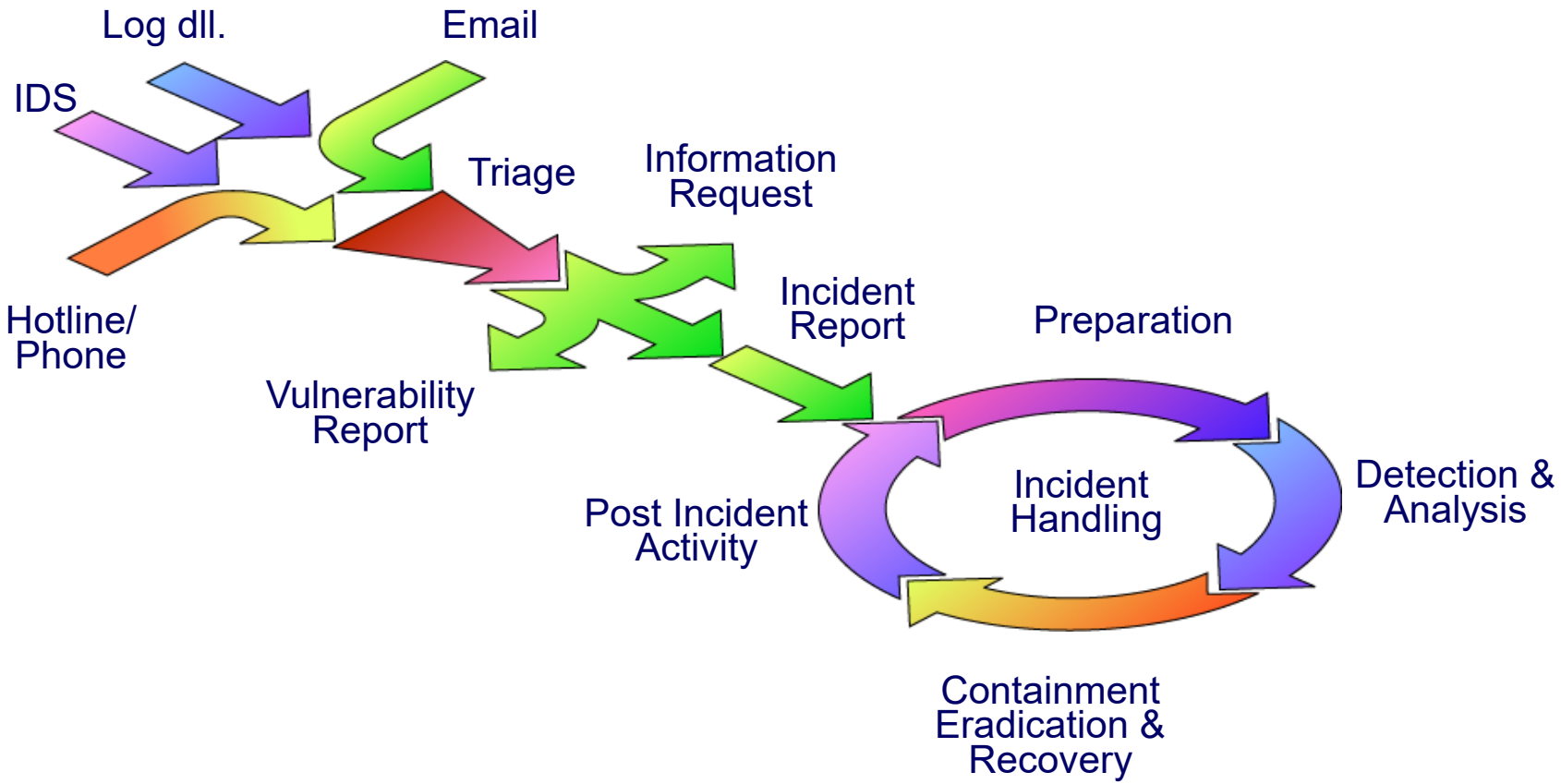
pwc

Cyber Kill Chain

Cyber Attack Life Cycle Phase	Description	Example
Recon(naissance)	The adversary identifies and investigates targets.	Web mining against corporate websites and online conference attendee lists.
Weaponize	The set of attack tools are packaged for delivery and execution on the victim's computer/network.	The adversary creates a trojanized Portable Document Format (PDF) file containing his attack tools.
Deliver	The packaged attack tool or tools are delivered to the target(s).	The adversary sends a spear phishing email containing the trojanized PDF file to his target list.
Exploit	The initial attack on the target is executed.	The targeted user opens the malicious PDF file and the malware is executed.
Control	The adversary begins to direct the victim system(s) to take actions.	The adversary installs additional tools on the victim system(s).
Execute	The adversary begins fulfilling his mission requirements.	The adversary begins to obtain desired data, often using the victim system as a launch point to gain additional internal system and network access.
Maintain	Long-term access is achieved.	The adversary has established hidden backdoors on the target network to permit regular reentry.

We can’t prepare for every Possibility

Incident Response Life Cycle



- pentingnya konstituen
- pengalaman pelapor insiden
- dampak insiden
- tingkat keparahan (*severity*)
- batasan waktu.

Mengkonfirmasi, mengkategorikan, ruang lingkup, dan memprioritaskan dugaan insiden siber

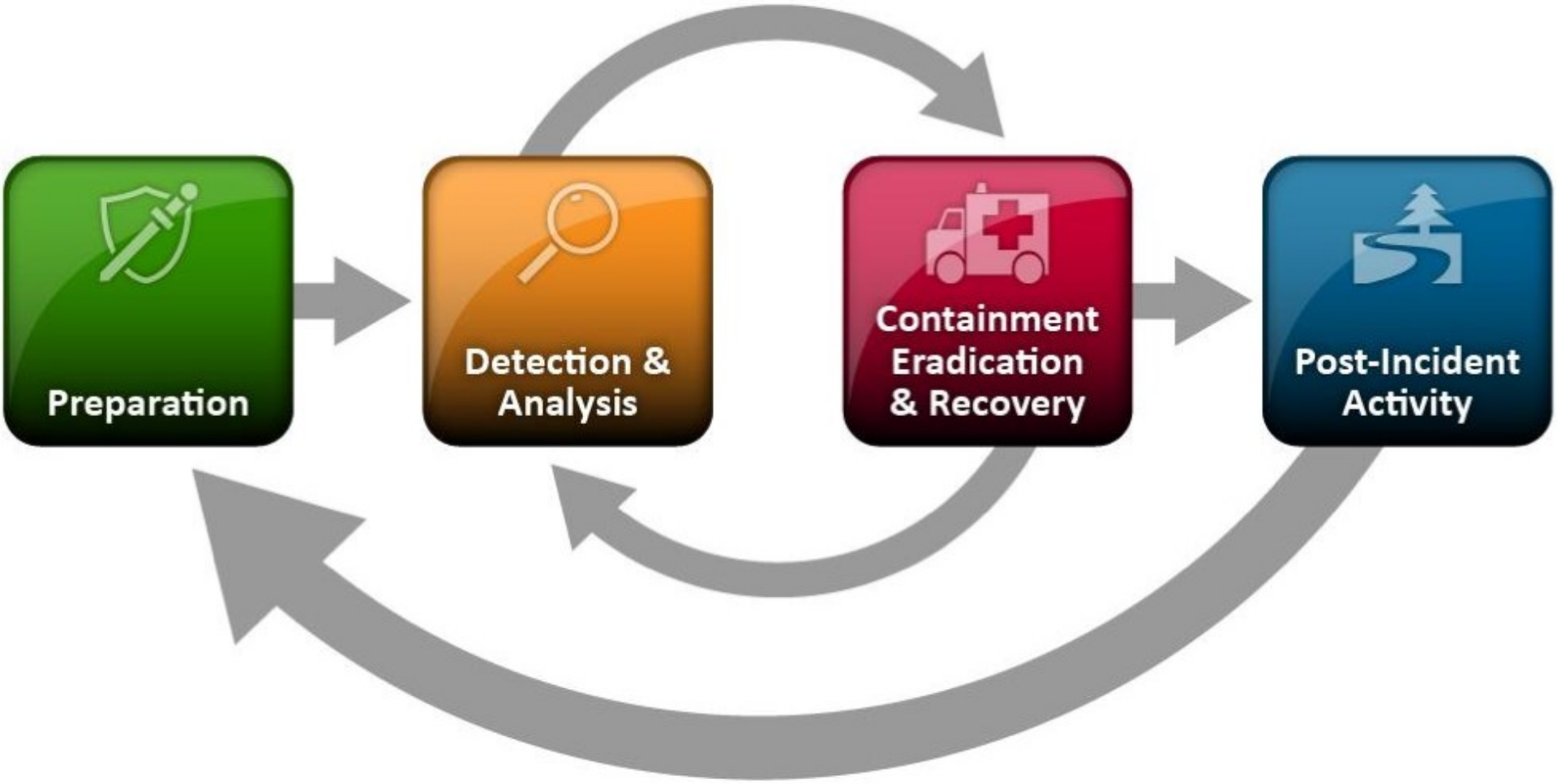
Tingkat Keparahan (Severity)

1. Potensi jumlah pihak yang terkena dampak:
   Seberapa besar produktivitas dipengaruhi oleh insiden ini?
   1. Kurang dari 1% sistem; kurang dari 1% tenaga kerja = 1
   2. Lebih dari 1%, tapi kurang dari 10% dari sistem; lebih dari 1%, tapi kurang dari 10% dari tenaga kerja = 2
   3. Lebih dari 10% dari sistem; lebih dari 10% tenaga kerja = 3
2. Kemungkinan eskalasi meluas:
   Apakah insiden ini berpotensi menyebar ke sistem yang belum terpengaruh?
   1. Minimal = 1
   2. Moderate = 2
   3. High = 3
3. Kemiripan:
   Apakah insiden ini terjadi di masa lalu; apakah ada pengalaman dalam mengurangi insiden ini?
   1. Terlihat biasa = 1
   2. Kadang terjadi = 2
   3. Jarang = 3
4. Potensi kerusakan atau kerugian
   Seberapa mahal akibat dampak insiden yang terjadi, baik dari kerugian produksi maupun biaya mitigasi?
   1. Rendah = 1
   2. Sedang = 2
   3. Tinggi = 3

Pedoman Prioritas Severity

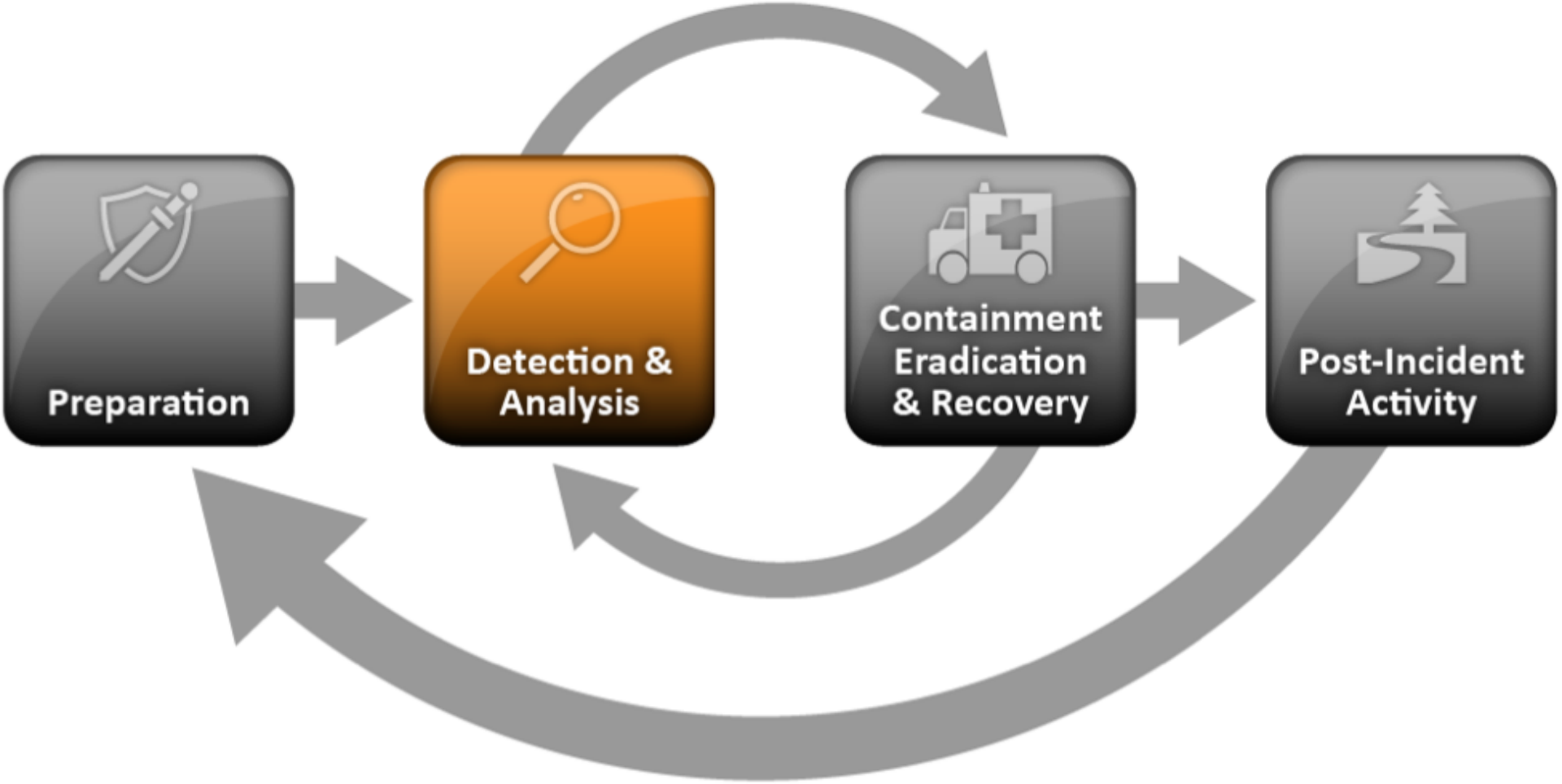
Pedoman Prioritas	Skor	Tindakan Awal	Containment Goal
Severity Severe: Dampak severity terhadap organisasi	13-15	Segera	**ASAP**
Severity High: Kehilangan layanan utama	11-12	Segera	**<24 jam**
Severity Medium: Beberapa dampak terhadap sebagian dari organisasi	8-10	Dalam 4 jam	**<72 jam**
Severity Low: Dampak kecil pada sebagian kecil organisasi	**5-7**	**Dalam 24 jam**	**<7 hari**

INCIDENT HANDLING



Preparation

- Menjaga dan meningkatkan kemampuan respons insiden siber
- Preparing to Handle Incident
  - Incident Handler Communications and Facilities
  - Incident Analysis Hardware and Software
  - Incident Analysis Resources
  - Incident Mitigation Software
- Preventing Incidents
  - Risk Assessments
  - Host Security
  - Network Security
  - Malware Prevention
  - User Awareness and Training

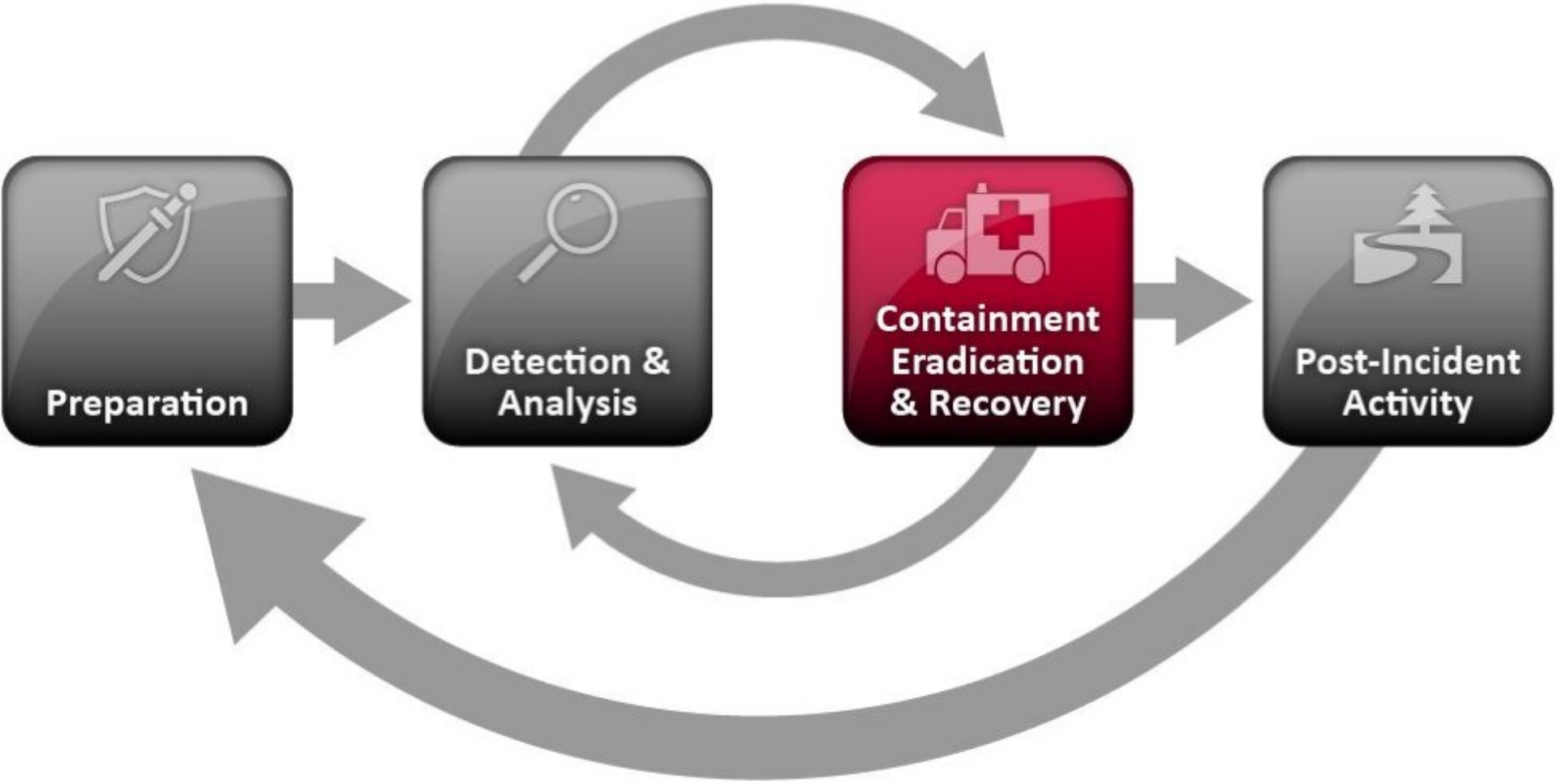

Preparation
Detection & Analysis
Containment Eradication & Recovery
Post-Incident Activity

Analisis Insiden

- Profile Networks dan Systems
- Memahami Normal Behaviors
- Membuat Kebijakan Log Retention
- Melakukan Event Correlation
- Menggunakan Informasi Internet
- Menjalan Packet Sniffers
- Mencari bantuan jika perlu

Identifikasi Vector Serangan

Sumber	Keterangan
	Monitor Infrastruktur Sistem
IDS/IPS	Signature alerts, anomalous patterns, known attacks
SIEM	Event Correlation and log aggregation services
Anti Virus	Deteksi malware, virus, spam/phishing related files, Email dll
FIM	File Integrity Monitor deteksi perubahan pada file systems
	LOG
System	Sistem Operasi, Storage, dll.
Aplikasi	Web, Database: Event, Error dll
Network	Firewall, Router, Switch, Load Balancer
	Informasi Publik
Vulnerability	Common Vulnerably and Exploit
Web Hacker	Zone-H, exploit-db, paste-bin dll


Preparation
Detection & Analysis
Containment Eradication & Recovery
Post-Incident Activity

Containment Strategy

- Meminimalkan kehilangan, pencurian data/informasi, atau gangguan layanan
- Membatasi dampak serangan meluas
- Service availability (*putus jaringan, matikan web, dll*)
- Waktu, resources, efektifitas strategi

  (*partial containment, full containment*)
- Durasi solusi (*emergency workaround 3 jam, 1 hari, permanent solution*)

Pengumpulan Informasi Insiden

- Identifikasi informasi serangan (*lokasi, serial number, model number, hostname, MAC addresses, IP addresses dll*)
- Name, title, and phone number of each individual who collected or handled the evidence during the investigation
- Time and date (*including time zone*) of each occurrence of evidence handling
- Locations where the evidence was stored

Eradication

Menghilangkan ancaman

Reimaged

Malware/Artifacts removed

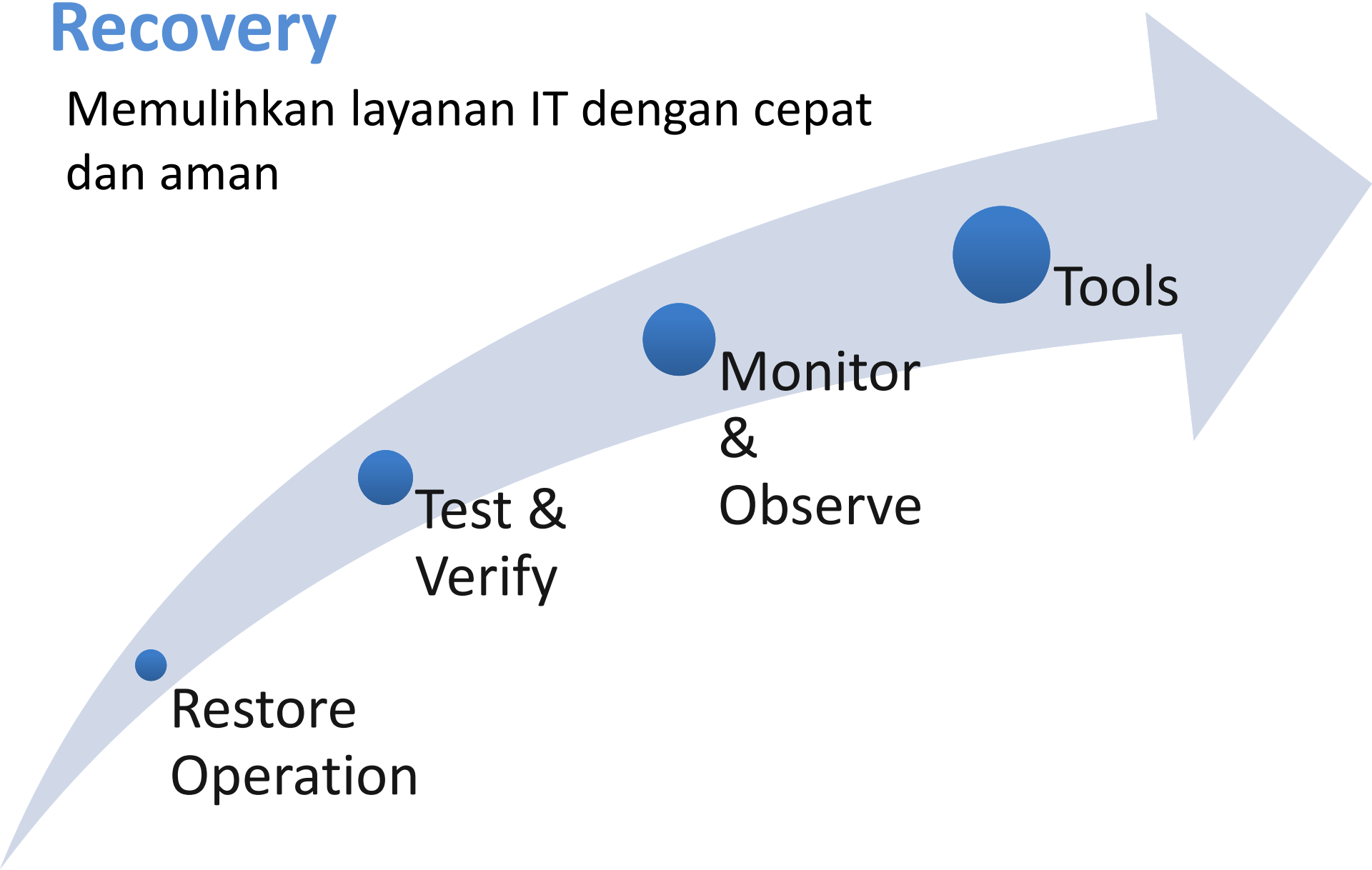
Hardened

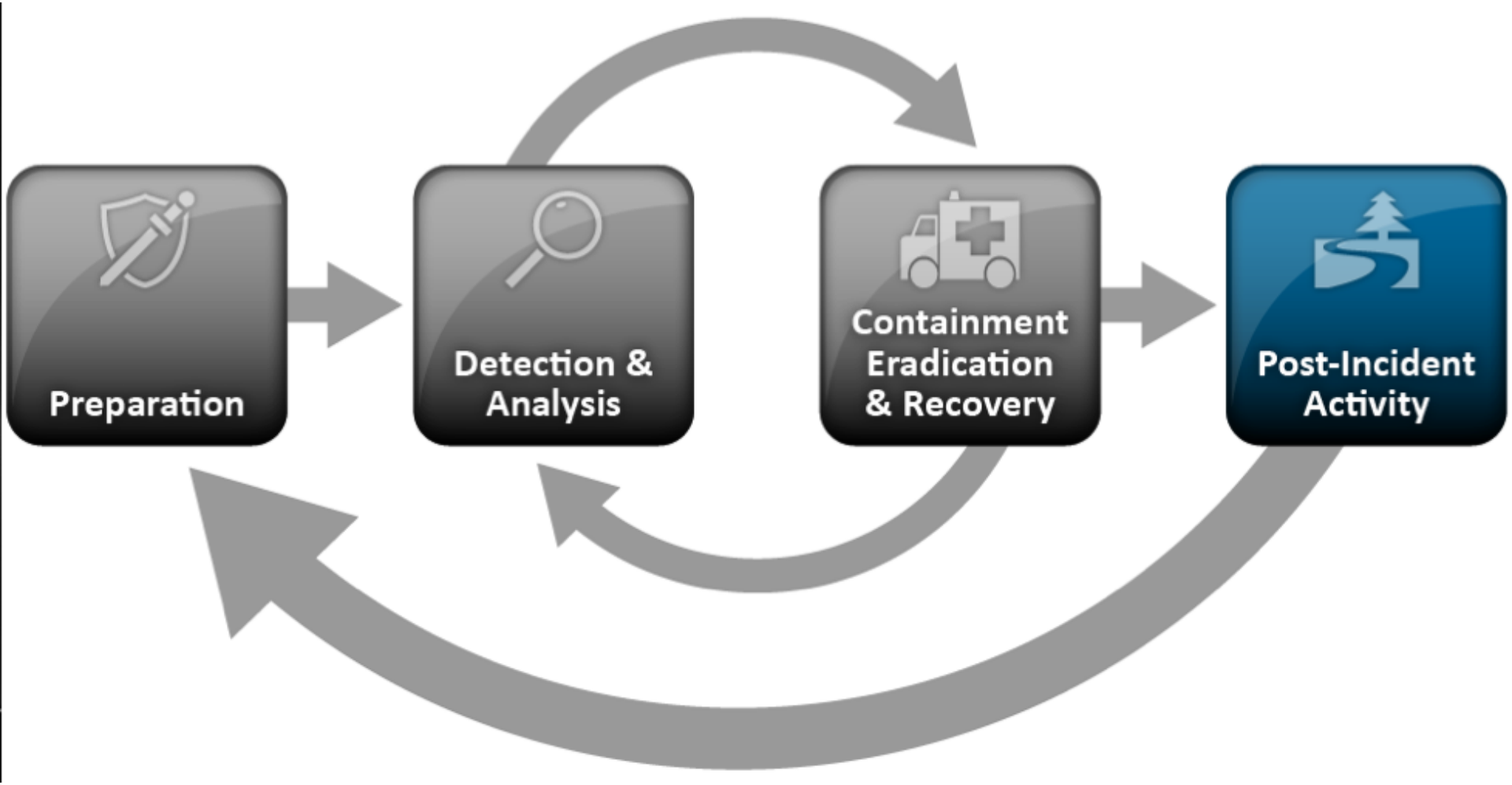
Patched

Countermeasure

Recovery

Memulihkan layanan IT dengan cepat dan aman




Preparation
Detection & Analysis
Containment Eradication & Recovery
Post-Incident Activity

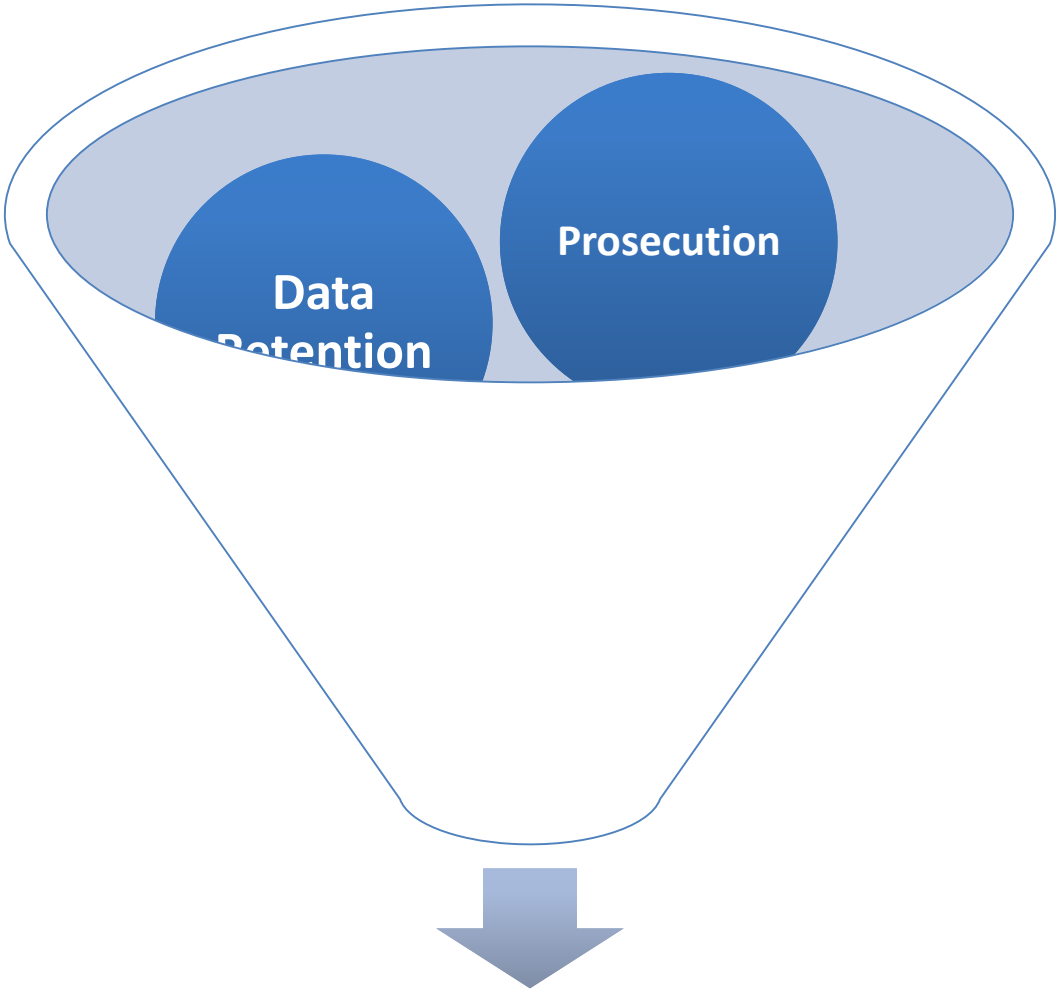
Post Incident Activity

Menilai respons untuk menangani insiden di masa depan dengan lebih baik melalui pemanfaatan laporan, belajar dari pengalaman dan kegiatan setelah tindakan, selain mitigasi kelemahan yang dieksploitasi untuk mencegah insiden serupa terjadi di masa depan

Lesson Learned

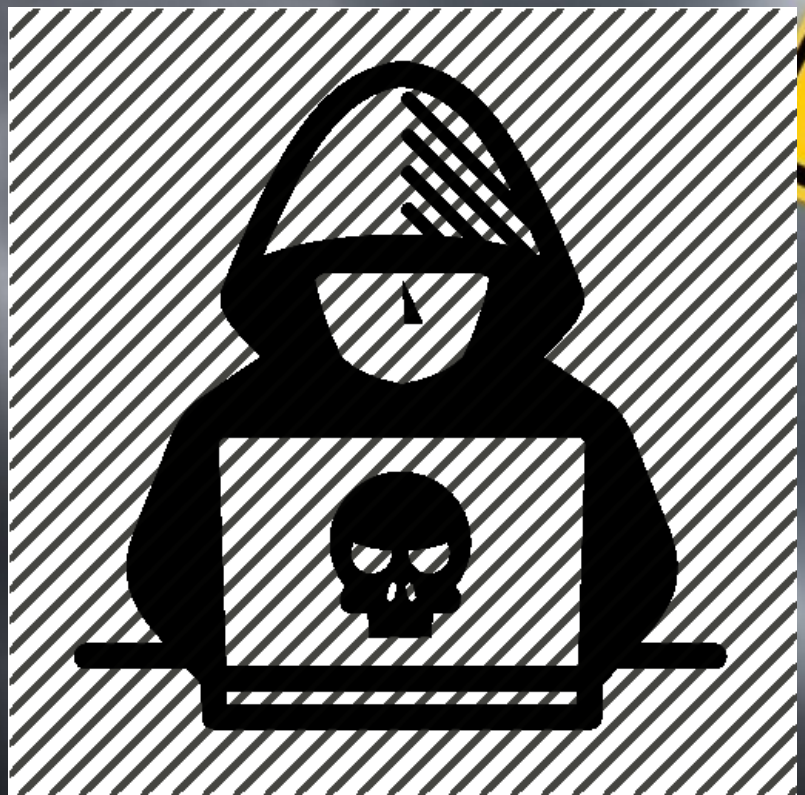
- Kapan insiden pertama kali terdeteksi dan oleh siapa?
- Ruang lingkup insiden.
- Bagaimana strategi containment eradication dan recovery?
- Bagian mana CSIRT dapat bekerja effective, dan yang perlu ditingkatkan?

Evidence Retention



Retention Policy

Cyber Security Incident Drill



Mengapa perlu incident drill?

- Kita tidak ingin menentukan proses selama krisis
  - drill memperbaiki incident response planning
  - drill memperbaiki disaster recovery planning
  - drill memperbaiki business continuity planning
- Merupakan security best practice
  - semua organisasi harus melakukan, hampir semua organisasi komersial sudah melakukan
  - Beberapa industri tertentu, merupakan kewajiban
- Kita tidak memiliki *real incidents* yang bisa dipelajari

ALUR ADUAN
INSIDEN SIBER

Segera laporkan !!!

apabila anda menemukan insiden siber

Terjadi
insiden siber

Kumpulkan bukti insiden berupa foto / screenshot insiden / log file yang ditemukan

BADAN SIBER DAN SANDI NEGARA
BSSN

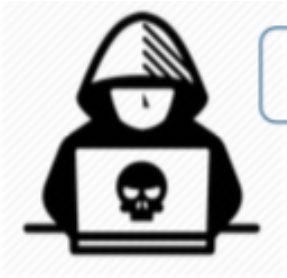
Aduan segera kami tangani

Hubungi (021) 78833610

Laporkan & Kirimkan bukti ke
bantuan70@bssn.go.id atau
pusopskamsinas@bssn.go.id

PUSAT KONTAK SIBER

Pusat Operasi Keamanan Siber Nasional BSSN



Terjadi insiden siber

Pusops

Injeksi 1

Reply

Reply

Peserta

Forwarding

Gov-CSIRT

Rekomendasi

Reply

Hint

Laporan

Komunikasi skenario drill test

REAL FROM: Kemenhub(kemenhub@mail.drillbssn.go.id)
REAL TO: GOV-CSIRT (govcsirt@mail.drillbssn.go.id
REAL CC: Pusopskamsinas (pusops@mail.drillbssn.go.id)
****

Dengan hormat…
Mohon bantuan untuk penanganan insiden…

…

Terima kasih…

****

Latihan Latihan Latihan BSSN – Gov-CSIRT Drill Test 2019