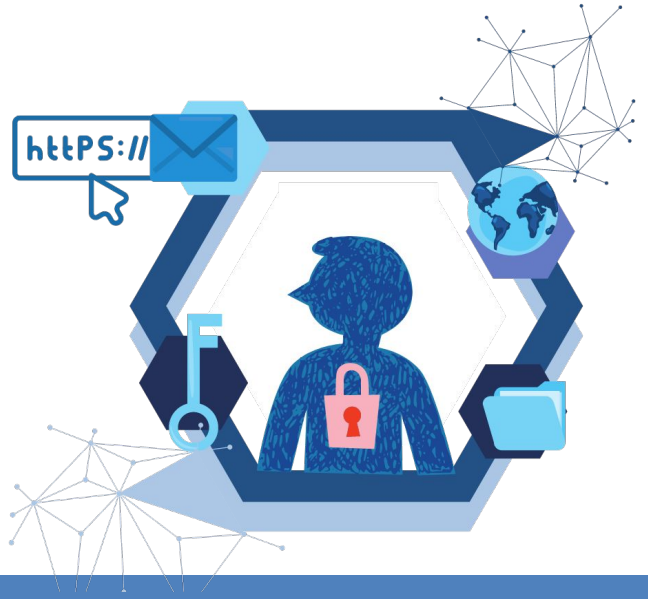
BADAN SIBER DAN SANDI NEGARA



KEBIJAKAN DATA PRIBADI DI PEMERINTAH PUSAT

DIREKTORAT OPERASI KEAMANAN SIBER

DEPUTI BIDANG OPERASI KEAMANAN SIBER DAN SANDI

JAKARTA, DESEMBER 2023

#JagaRuangSiber

BADAN SIBER DAN SANDI NEGARA

OUTLINE

1. Overview
2. Serba-Serbi Pelindungan Data Pribadi
3. Upaya Pelindungan Data Pribadi dari Pemerintah
4. Langkah Mitigasi dan Tips&Trick Melindungi Data Pribadi

BADAN SIBER DAN SANDI NEGARA

LANSKAP KAMSINAS TAHUN 2023

Malware - Ransomware

- Sebanyak 26 kasus indikasi serangan ransomware dan terdapat 991.571 aktivitas ransomware terdeteksi pada sensor monitoring selama tahun 2023*
- Indikasi sektor terdampak : ESDM, Perbankan dan Keuangan, Penegak Hukum, Pemerintahan, Kesehatan, Transportasi, Pendidikan, TIK, Pertahanan, dll.
- Ransomware yang menyerang : Luna Moth, WannaCry, Locky, LockBit, Darkside, Gandcrab, Troldesh, Ryuk, STOP, BlackCat (ALPHV), Hive, Vice Society, Medusa, dll.
- Berdasarkan Indonesia Honeynet Project milik BSSN, pada tahun 2022 ditemukan sebanyak **883.239 serangan malware** dengan **6.026 Malware unik**. Hingga Bulan November 2023*, Indonesia Honeynet Project BSSN telah menemukan **1.233.293 serangan malware** dengan **6.128 malware unik.**

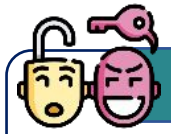
Data Breach

- **311** notifikasi Indikasi dugaan kebocoran data pada tahun 2022
- 272 notifikasi Indikasi dugaan kebocoran data pada tahun 2023*

Advanced Persistent Threat

Pada tahun 2022 tercatat sebanyak 4.393.935 serangan APT yang terdeteksi pada sensor monitoring. Beberapa Jenis APT meliputi APT41, Dark Pink, Turla, OceanLotus, Kimsuky, Winnti, Anchor, dan lain-lain. Sementara sampai dengan November 2023* tercatat 3.112.577 serangan APT yang terdeteksi pada sensor monitoring.

Social Engineering



Metode yang umum digunakan yaitu melalui phishing via Chat dengan menyebarkan file

- Undangan pernikahan.apk
- Ekspedisi paket
- Berbagai jenis tautan berbahaya lainnya.

Web Defacement

defacement yang terdeteksi:

2022	2023
885 situs pemerintah	175 website

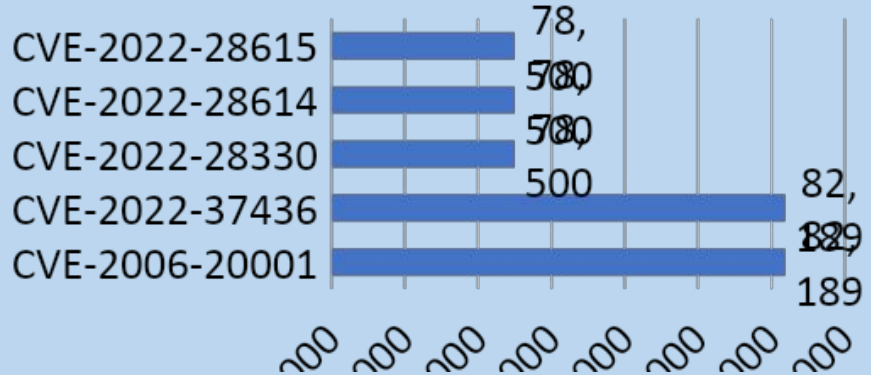
...umumnya juga berpotensi digunakan untuk tindak kejahatan lainnya oleh threat actor.

BADAN SIBER DAN SANDI NEGARA

LANSKAP KAMSINAS TAHUN 2023

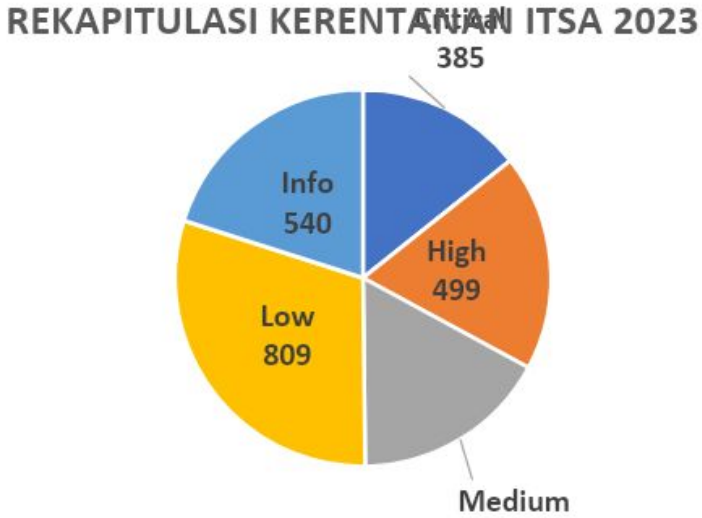
Vulnerability

TOP 5 CVE pada Sensor Monitoring 2023



- Berdasarkan hasil ITSA pada 131 Stakeholder di tahun 2023*, ditemukan 2.688 kerentanan dengan jumlah aplikasi sebanyak 626 aplikasi.

Penelusuran Kerentanan



TOP 3 Kerentanan

1. Information Disclosure
2. Weak Password Policy
3. Insecure Direct Object References (IDOR)

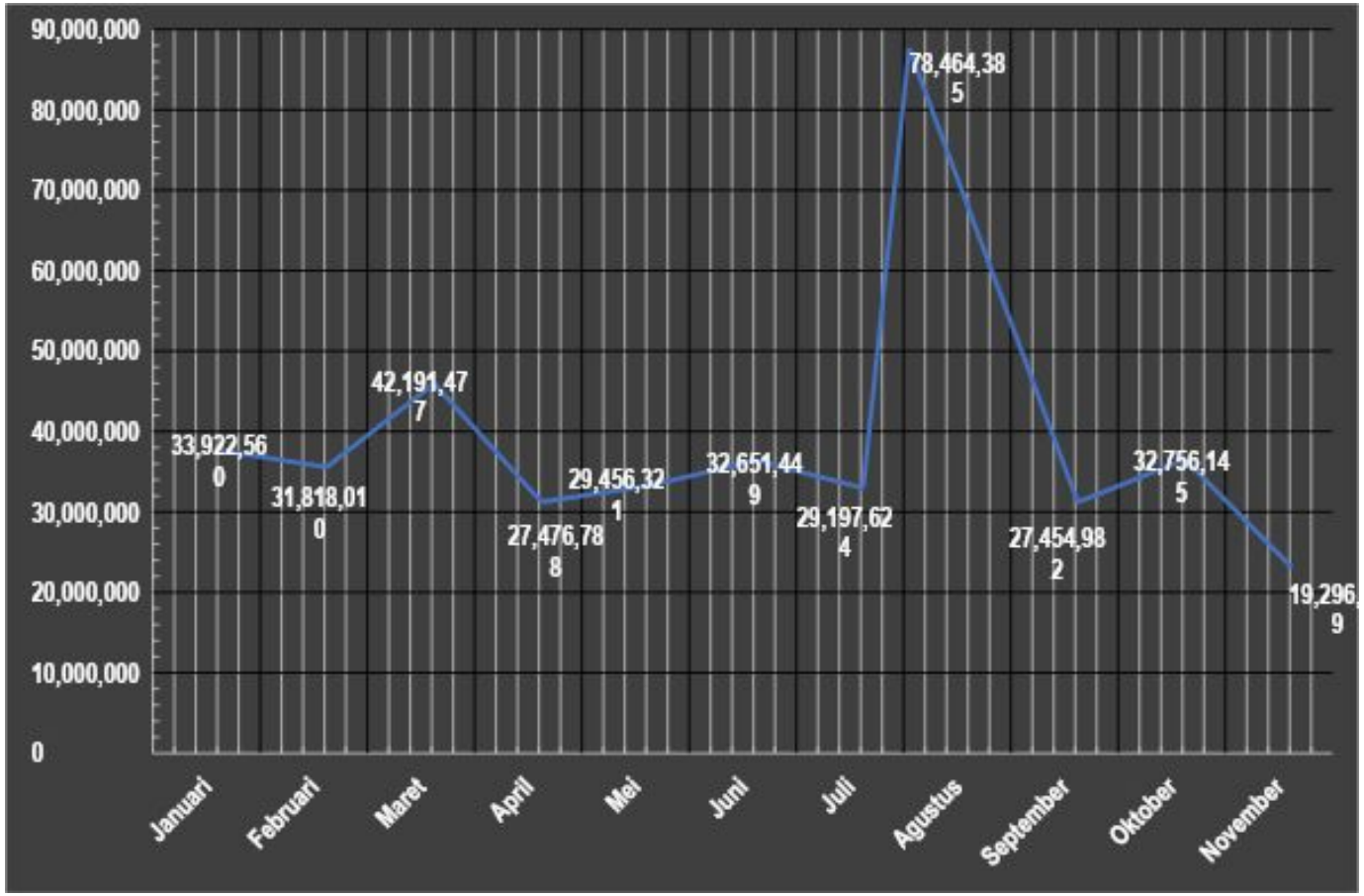
*) periode 1 Januari s.d. 30 November 2023

BADAN SIBER DAN SANDI NEGARA

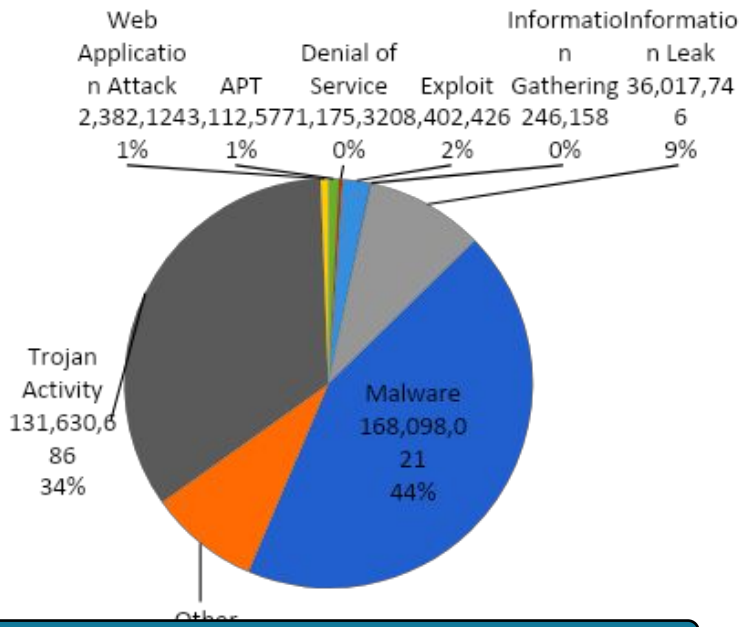
ANOMALI TRAFIK KEAMANAN SIBER NASIONAL

Periode 1 Januari s.d. 30 November 2023

Tercatat terdapat 384.686.180 Anomali Trafik pada 1 Januari s.d. 30 November 2023



KLASIFIKASI ANOMALI TRAFIK



TOP #3 – JENIS ANOMALI TRAFIK

43,70 168.098.021 MALWARE ACTIVITY

131.630.686 TROJAN ACTIVITY **34,22**

9,36 36.017.746 INFORMATION LEAK

48.939.727 LAINNYA **12,72**

BADAN SIBER DAN SANDI NEGARA

WEB DEFACEMENT

Kasus Insiden "Slot Gacor"

Web Defacement

Defacement adalah sebuah serangan terhadap website dengan cara mengganti konten website yang bertujuan untuk mengirimkan pesan tertentu/hacktivist. Serangan ini dapat dilakukan dengan memanfaatkan sebuah kelemahan dari sistem sehingga memungkinkan pelaku memiliki akses masuk hingga ke server dan memiliki kewenangan untuk mengganti atau menghapus konten suatu website. Terdapat berbagai metode untuk melakukan web defacement, cara yang sering dijumpai yaitu eksploitasi pada kerentanan plugins framework dan SQL Injection yang memungkinkan akses administratif.

"Slot Gacor"

'Situs Slot Gacor' adalah istilah yang berasal dari komunitas permainan online Indonesia, Pada dasarnya, 'situs slot gacor' mengacu pada situs web slot online yang dianggap memiliki mesin slot dengan frekuensi kemenangan yang lebih tinggi. Web defacement belakangan ini marak terjadi pada situs milik pemerintah dan pendidikan, terutama web defacement judi online. Dampak nyata dari web defacement judi online yaitu situs menampilkan halaman judi online. Salah satu alasan hal tersebut banyak menyasar situs milik pemerintah dan pendidikan diindikasikan sebagai cara untuk menghindari situs di-block oleh pihak berwenang.

Dampak Insiden

Kepercayaan Masyarakat akan meragukan keamanan dan keandalan situs pemerintah, serta kemampuan pemerintah dalam melindungi data sensitif dan informasi publik.

Availability Defacement dapat menyebabkan gangguan pada layanan yang disediakan oleh situs pemerintah serta dapat menyebabkan ketidaknya ketidakpuasan masyarakat terhadap pemerintah.

Reputasi Tampilan halaman judi online yang tidak pantas atau ilegal pada situs pemerintah akan menciptakan kesan negatif terhadap integritas.

BADAN SIBER DAN SANDI NEGARA

REKAPITULASI PENANGANAN INSIDEN JUDI ONLINE

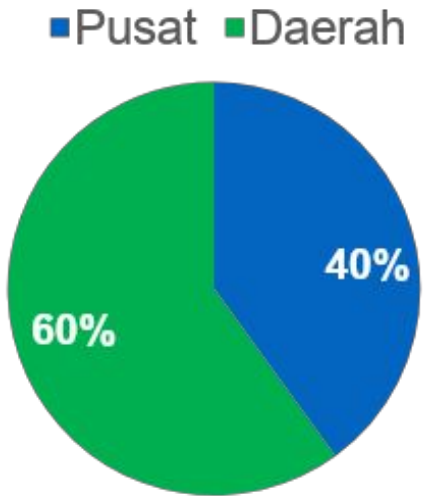
Periode 1 Januari s.d. 30 November 2023

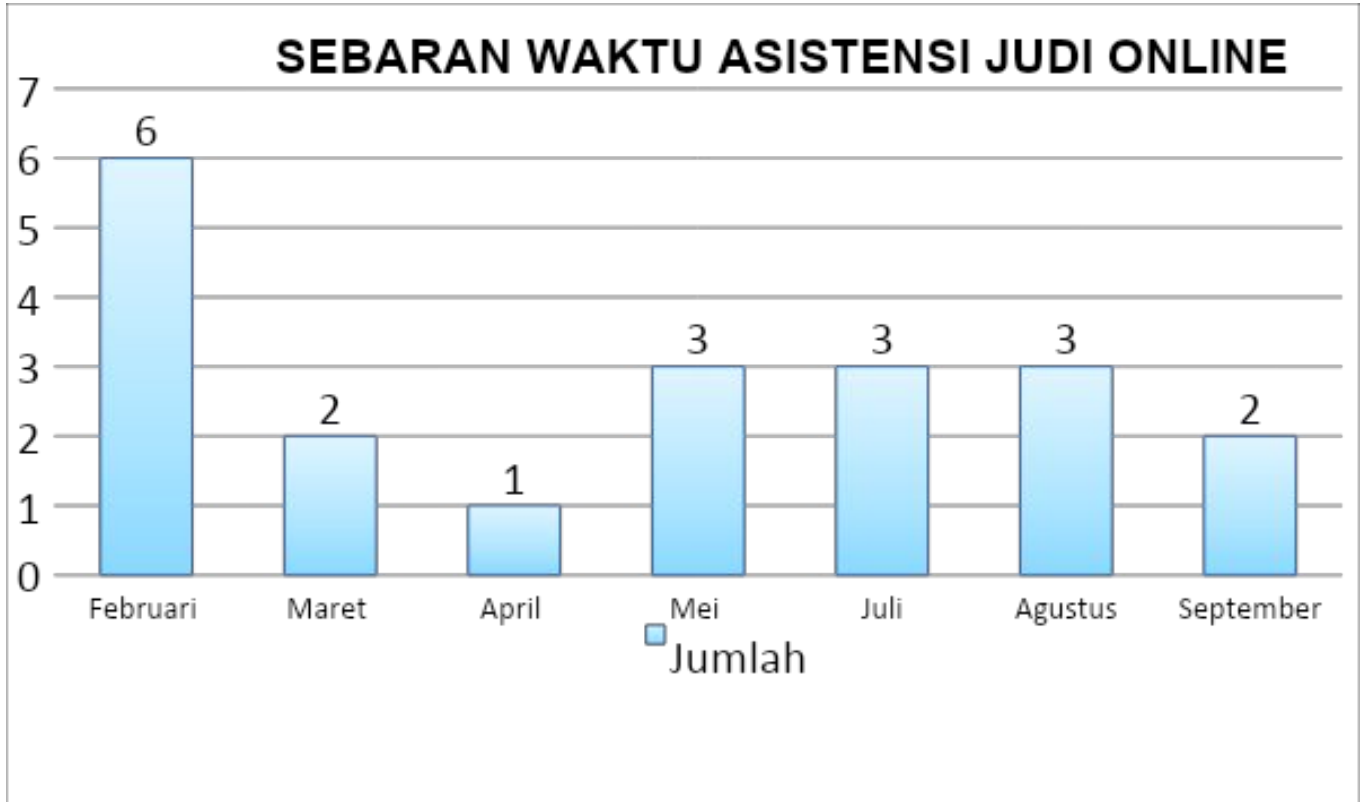
20
ASISTENSI PENANGAN INSIDEN JUDI ONLINE

8
SEKTOR PEMERINTAH PUSAT

12
SEKTOR PEMERINTAH DAERAH

Persentase penanganan insiden judi online BERDASARKAN SEKTOR





APA SIH PELINDUNGAN DATA PRIBADI ?

BADAN SIBER DAN SANDI NEGARA

PELINDUNGAN DATA PRIBADI

UU RI No. 27 Tahun 2022
tentang Pelindungan Data

"Keseluruhan upaya untuk melindungi Data Pribadi dalam rangkaian pemrosesan Data Pribadi guna menjamin hak konstitusional subjek Data Pribadi"

- **UNDANG-UNDANG NOMOR 11 TAHUN 2008**
  tentang Informasi dan Transaksi Elektronik
- **NOMOR 19 TAHUN 2016**
  tentang Perubahan Atas UU Nomor 11 Tahun 2008

PERPRES NO. 95 TAHUN 2018
Sistem Pemerintah Berbasis Elektronik

PERATURAN BSSN NO. 4 TAHUN 2021
Pedoman manajemen keamanan sistem informasi sistem pemerintah berbasis elektronik dan standar teknis prosedur keamanan SPBE

BADAN SIBER DAN SANDI NEGARA

PELINDUNGAN DATA PRIBADI

UU RI No. 27 Tahun 2022
tentang Pelindungan Data

Keputusan Menkopolhukam Nomor 96 Tahun 2022
tentang pembentukan Satuan Tugas Pelindungan Data

SATGAS PELINDUNGAN DATA PRIBADI (PDP)

- Melakukan asesmen, pendataan, verifikasi, pemantauan, dan manajemen risiko terhadap penyelenggaraan sistem informasi untuk menghindari penyalahgunaan data
- Melakukan respons dan mitigasi insiden secara cepat terhadap penyalahgunaan data
- Merekomendasikan saran perbaikan teknis dan/atau nonteknis untuk meningkatkan pengamanan data
- Merekomendasikan penegakan hukum terhadap penyalahgunaan data
- Melakukan komunikasi publik yang efektif kepada masyarakat
- Melakukan evaluasi terhadap pelaksanaan kegiatan Satgas Pelindungan Data

BADAN SIBER DAN SANDI NEGARA

PELINDUNGAN DATA PRIBADI

1 *Vulnerability Assessment* (VA)

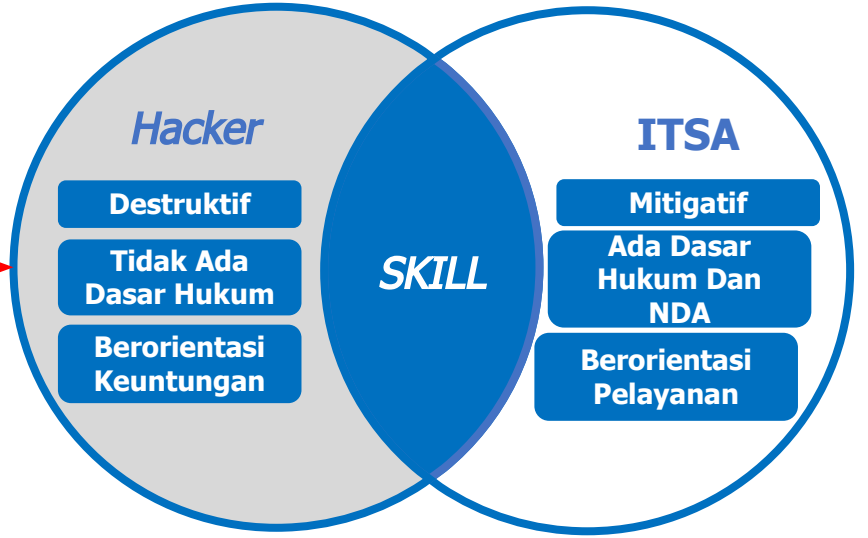
VA adalah **proses identifikasi, evaluasi, dan klasifikasi tingkat kerentanan keamanan** pada sebuah jaringan komputer, sistem, aplikasi, atau bagian lain di ekosistem IT berdasarkan risiko yang dapat ditimbulkan.

2 *Information Technology Security Assessment* (ITSA)

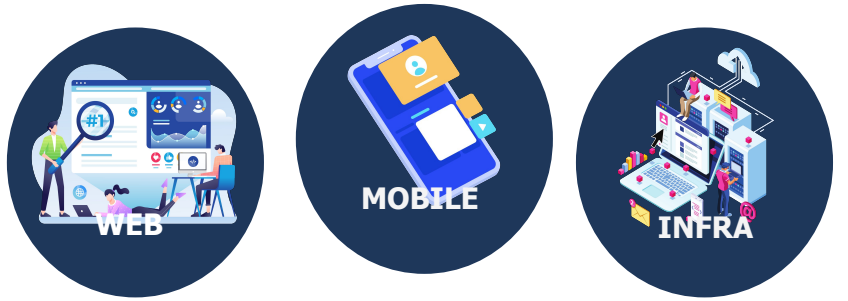
ITSA adalah **pengujian yang dilakukan dengan mengeksploitasi kelemahan atau kerentanan sistem elektronik** yang dapat mengakibatkan hilangnya informasi, pendapatan, reputasi dari pihak internal atau eksternal yang menyebabkan kerugian bagi organisasi.

3 *Hardening*

Hardening adalah **proses perbaikan celah keamanan** yang ditemukan dari hasil IT Security Assessment dengan memberikan himbauan teknis kepada pengelola.



OBJEK LAYANAN



BADAN SIBER DAN SANDI NEGARA

PELINDUNGAN DATA PRIBADI

1 *Vulnerability Assessment* (VA)

VA adalah **proses identifikasi, evaluasi, dan klasifikasi tingkat kerentanan keamanan** pada sebuah jaringan komputer, sistem, aplikasi, atau bagian lain di ekosistem IT berdasarkan risiko yang dapat ditimbulkan.

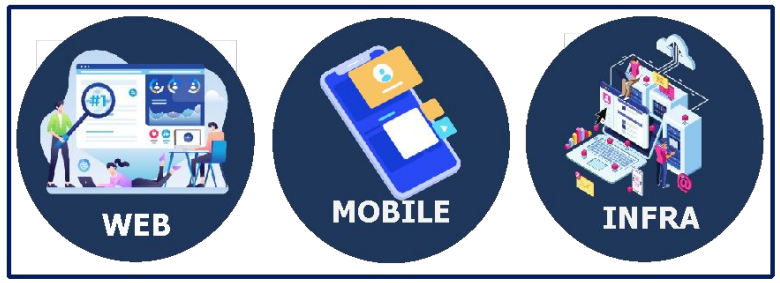
2 *Information Technology Security Assessment* (ITSA)

ITSA adalah **pengujian yang dilakukan dengan mengeksploitasi kelemahan atau kerentanan sistem elektronik** yang dapat mengakibatkan hilangnya informasi, pendapatan, reputasi dari pihak internal atau eksternal yang menyebabkan kerugian bagi organisasi.

3 *Hardening*

Hardening adalah **proses perbaikan celah keamanan** yang ditemukan dari hasil IT Security Assessment dengan memberikan himbauan teknis kepada pengelola.

OBJEK LAYANAN



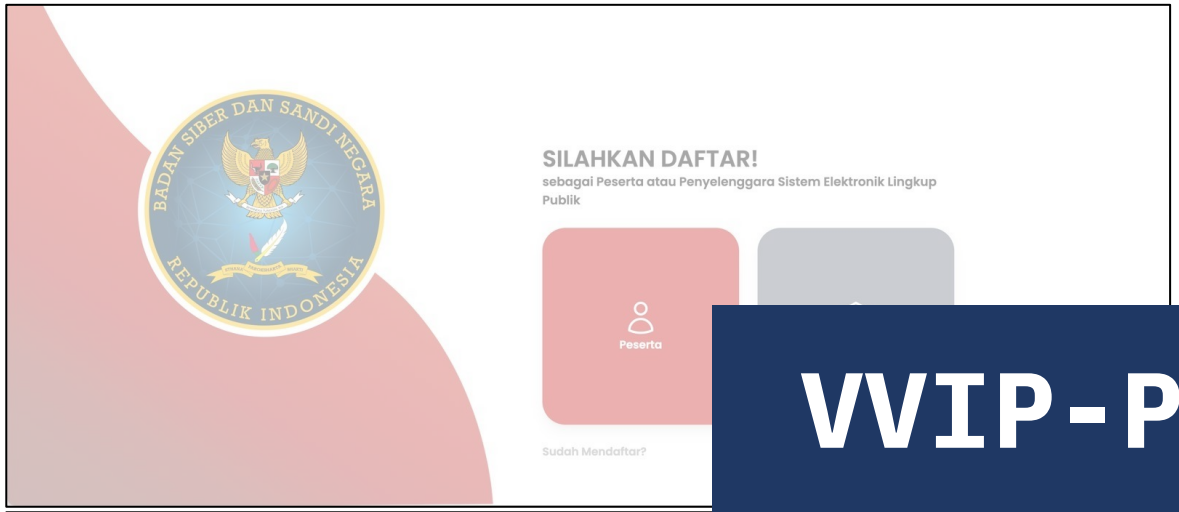
LAYANAN YANG DIBERIKAN

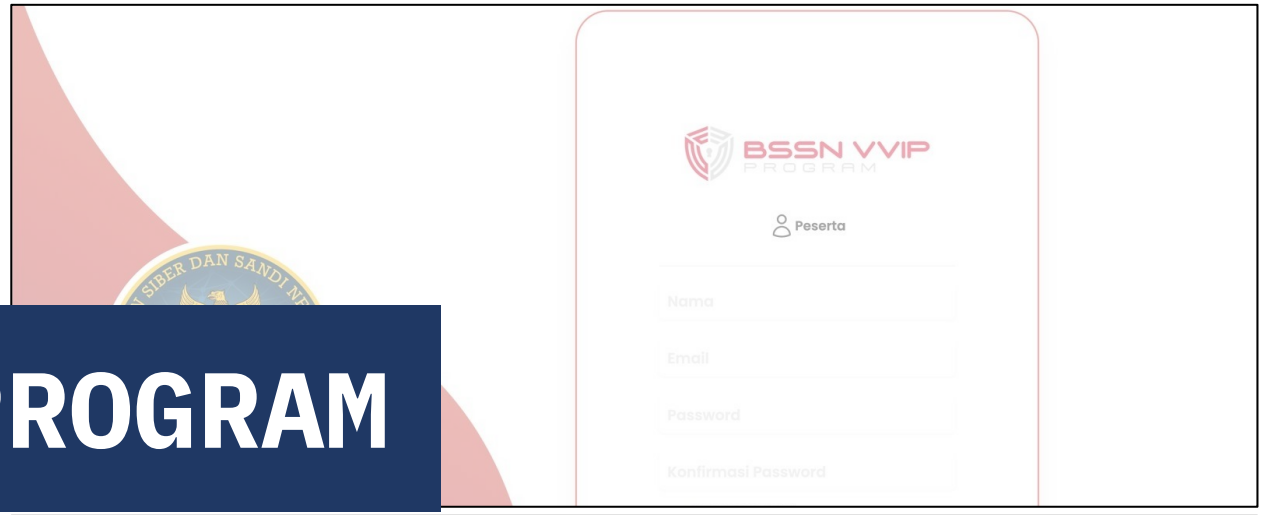
LAYANAN PROTEKSI KARYA MANDIRI

XDR *SERVER & ENDPOINT*

BADAN SIBER DAN SANDI NEGARA

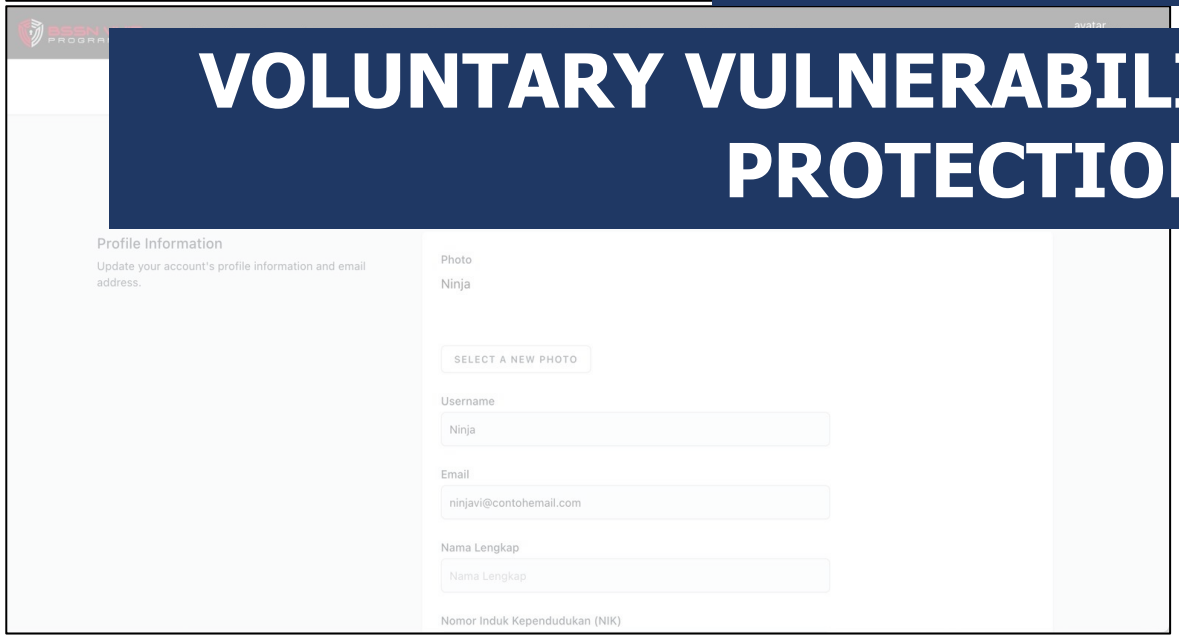
PELINDUNGAN DATA PRIBADI

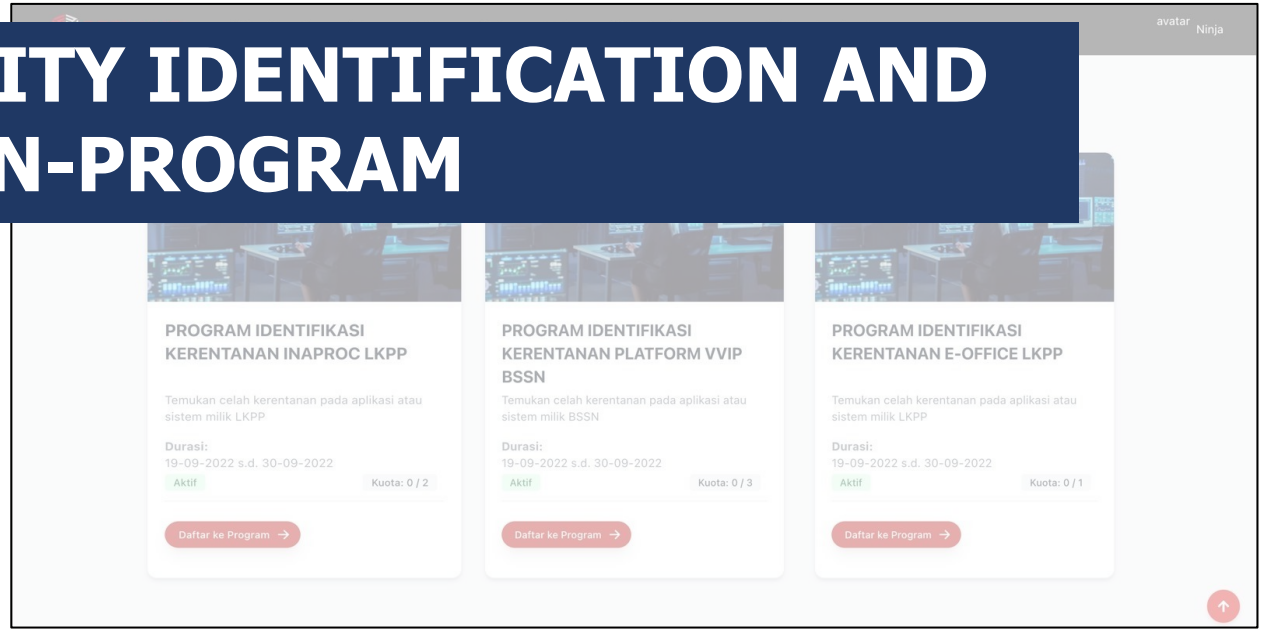




VVIP-PROGRAM

VOLUNTARY VULNERABILITY IDENTIFICATION AND PROTECTION-PROGRAM





BADAN SIBER DAN SANDI NEGARA

PELINDUNGAN DATA PRIBADI

VVIP-PROGRAM

Peraturan Kepala Badan Siber Dan Sandi Negara Nomor 5 Tahun 2023

tentang Penyelenggaraan Program Identifikasi Kerentanan Dan Proteksi Secara Sukarela

"Program identifikasi kerentanan dan proteksi secara sukarela diselenggarakan oleh Badan Siber dan Sandi Negara bekerja sama dengan Penyelenggara Sistem Elektronik Lingkup Publik dan Pengidentifikasi serta Pemberi Rekomendasi Keamanan"

PROGRAM IDENTIFIKASI (PENCARIAN KERENTANAN)

PROGRAM PROTEKSI (PERBAIKAN CELAH KEAMANAN DAN HARDENING)

PROGRAM PUBLIK

1. Program yang bisa diikuti oleh seluruh peserta
2. Tidak terdapat batasan siapa saja yang bisa mengikuti Program Publik

PROGRAM PRIVAT

1. Program yang hanya bisa diikuti oleh peserta tertentu
2. Peserta yang dipilih untuk mengikuti Program Privat akan dikirimi undangan

APRESIASI & SANKSI

UPAYA PELINDUNGAN DATA PRIBADI KITA SEBAGAI PERSEORANGAN BAGAIMANA YA ?

BADAN SIBER DAN SANDI NEGARA

IMBAUAN MENJAGA KEAMANAN DATA PRIBADI

Sebelum Liburan

- Melakukan back up data perkantoran maupun data pribadi.
- Memastikan tidak ada perangkat elektronik yang terhubung dengan arus listrik.
- Menyimpan barang berharga dalam berankas ataupun tempat penyimpanan yang aman dan yang telah disediakan.
- Pastikan meja kerja bersih sebelum meninggalkan kantor.

Saat Liburan

- Hati-hati dalam mengambil dan membagikan konten pribadi seperti foto/video/data diri lainnya.
- Hindari menggunakan jaringan Wi-Fi publik yang tidak aman.
- Jangan mengklik tautan yang mencurigakan atau mengunduh lampiran dari sumber yang tidak dikenal.

DON'T KNOW! KASIH NO!

- Minimalisir barang berharga yang dibawa, dan pastikan selalu dalam pengawasan.
- Jangan berbagi data pribadi dengan sembarang orang.
- Lakukan riset dan gunakan agen perjalanan terpercaya untuk menghindari penipuan saat liburan.

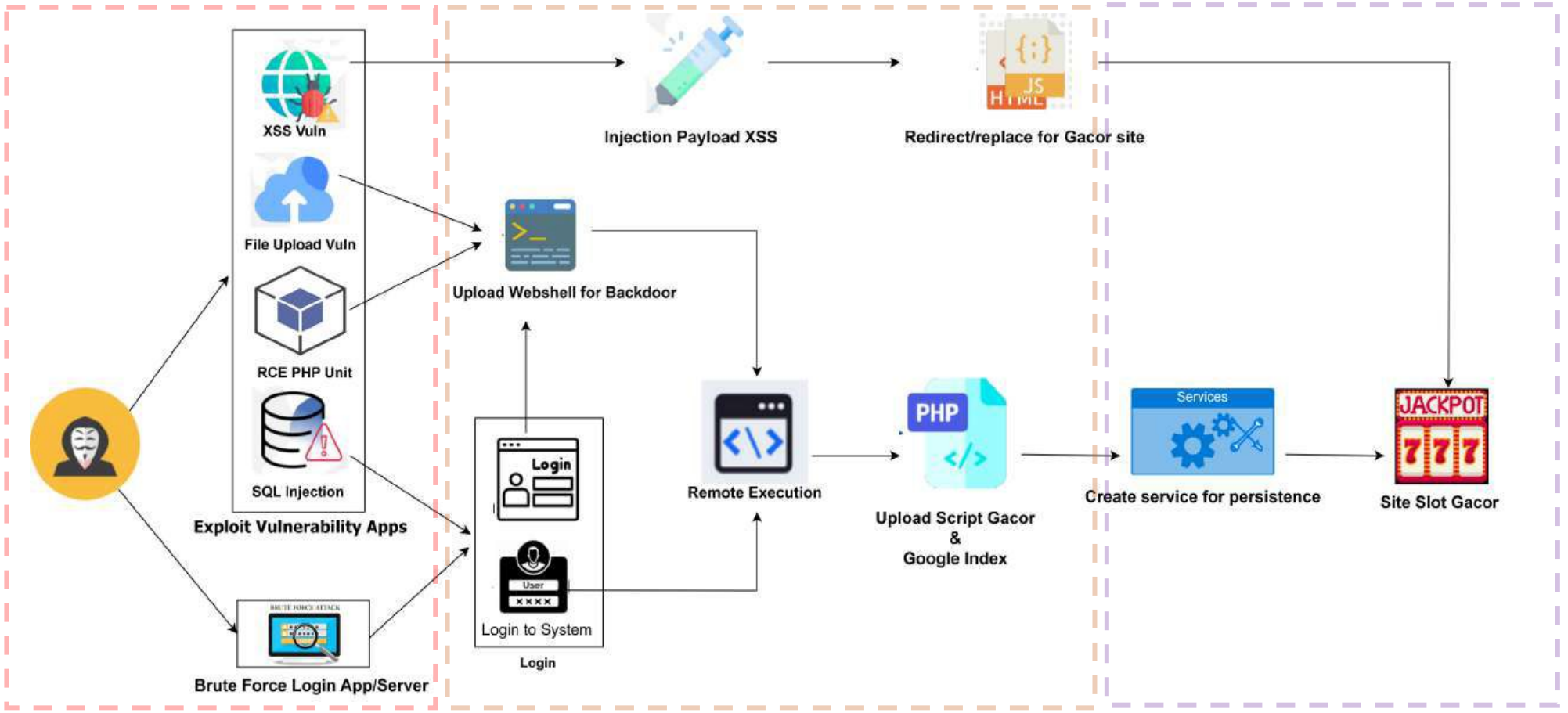
Setelah Liburan

- Periksa barang-barang dan data pribadi yang disimpan.
- Lakukan scanning menggunakan tools antivirus / antimalware sebelum menggunakan kembali perangkat.

BADAN SIBER DAN SANDI NEGARA

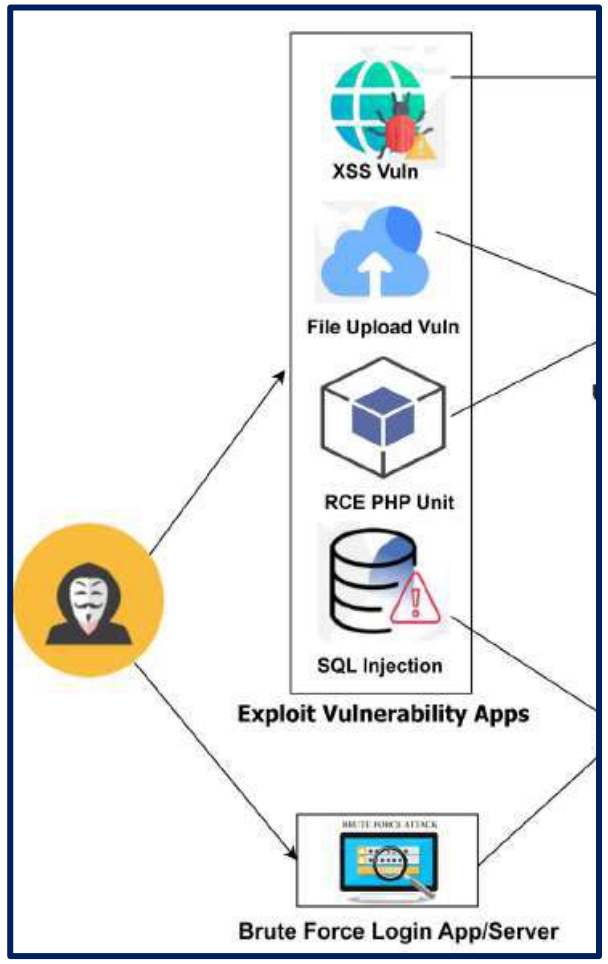
ALUR PENYERANGAN

Alur serangan merupakan suatu metode atau jalan yang digunakan oleh penyerang untuk melancarkan serangan. Alur serangan menggambarkan cara penyerang memanfaatkan kelemahan atau celah dalam sistem untuk memperoleh akses tidak sah terhadap sistem



BADAN SIBER DAN SANDI NEGARA

ALUR PENYERANGAN



1 *Initial Acces*

Initial access melibatkan upaya dalam memanfaatkan kerentanan dan kesalahan pada konfigurasi untuk dapat masuk kedalam sistem. Web defacement judi online diidentifikasi memanfaatkan **Exploit Vulnerability Apps** dan **Brute Force Attack** untuk masuk ke dalam sistem.

Contoh *Exploit Vulnerability Apps*		Contoh *Brute Force Attack*
XSS	*File Upload*	*Brute Force Login*
PHP *Unit*	*SQL Injection*	

BADAN SIBER DAN SANDI NEGARA

ALUR PENYERANGAN

2 *Execution*

Penyerang melakukan aktivitas pada server untuk melakukan penyisipan script judi online

Contoh Aktifitas yang Dilakukan

Remote Execution

- Penyerang memanfaatkan *backdoor* yang telah tertanam pada server untuk melakukan *Remote Code Execution.*

Upload *Script* Judi *Online* dan Google *Index*

- Penyerang akan melakukan modifikasi pada file .htaccess untuk mengizinkan beberapa file webshell untuk dapat diekseskusi pada folder yang telah ditentukan.

3 *Persistence*

Penyerang melakukan mekanisme persistence untuk memastikan akses mereka terhadap server korban tetap tersedia

Contoh Aktifitas yang Dilakukan

Penyisipan *Backdoor/Webshell*

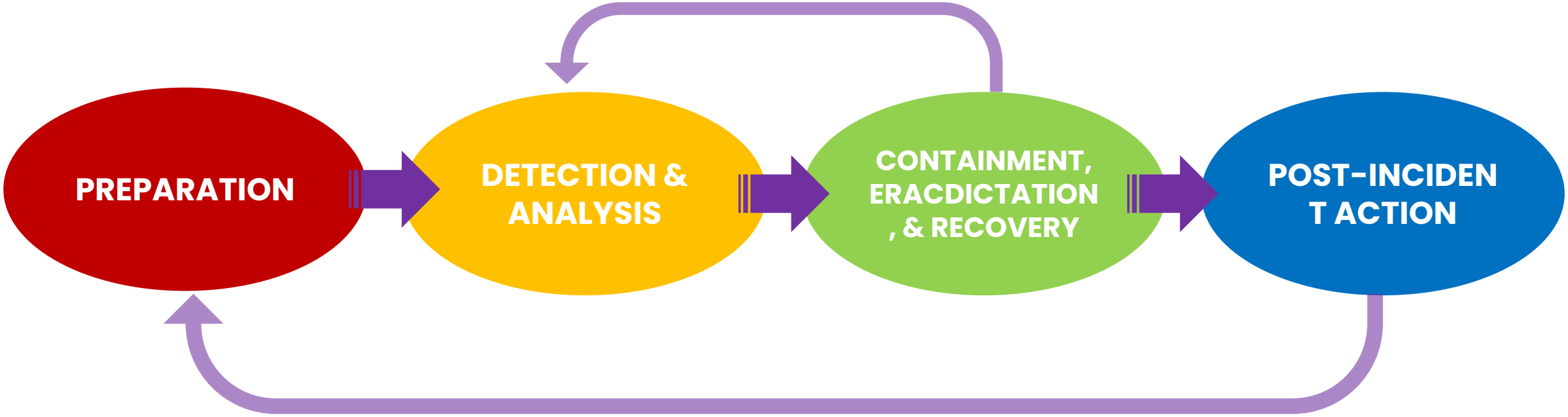
- Penyerang memanfaatkan *webshell* sebagai pintu untuk masuk ke server. Beberapa *webshell* yang sering ditemukan antara lain **Lzt.zip.gz.txt.php, Mad.php, b374k.php, dan alfa.php.**

Pembuatan *Process* dan *Service*

- Penyerang melakukan serangan *persistence* dengan membuat *process* dan *service* berjalan terus menenus untuk memastikan bahwa tampilan judi *online* tidak dapat dihapus.

BADAN SIBER DAN SANDI NEGARA

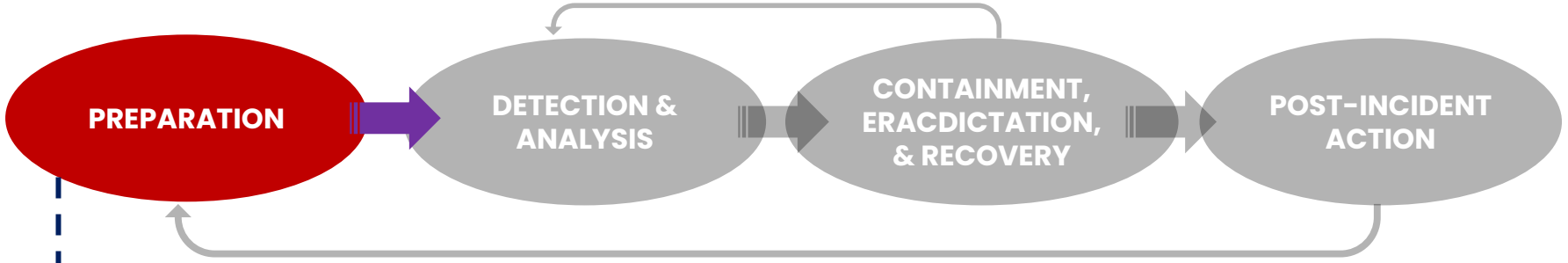
LANGKAH PENANGANAN INSIDEN



Sumber: Computer Security Incident Handling Guide NIST 800-52

BADAN SIBER DAN SANDI NEGARA

LANGKAH PENANGANAN INSIDEN



Tahap persiapan kebijakan, prosedur, teknologi, dan sumber daya manusia yang dibutuhkan saat melakukan respon cepat terhadap insiden

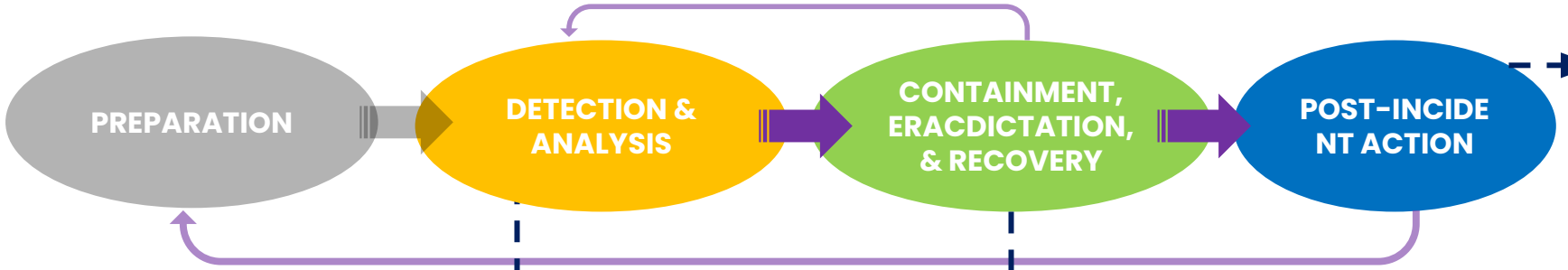
Hal-hal yang perlu disiapkan:

1. Pembentukan Tim Tanggap Insiden
2. Penyiapan Dokumen Legal
3. Koordinasi dengan Pihak Terkait
4. Penyiapan ***Jump Kit*** untuk penanganan insiden
5. Melakukan Identifikasi Aset Terdampak

JUMP KIT PENANGANAN INSIDEN		
Evidence Collection	Computer Forensics	IoC Scanner
dd	FTK Imager	ThorLite
FTK imager	Autopsy	Yara Rules
KAPE	Volatility	Redline

BADAN SIBER DAN SANDI NEGARA

LANGKAH PENANGANAN INSIDEN



Pemilik aset melakukan pemeliharaan serta pemantauan keamanan secara berkala untuk memastikan serangan lanjutan tidak terjadi

Tahapan berulang yang dilakukan guna mendeteksi kemungkinan adanya malicious file, backdoor, atau webshell pada sistem dan melakukan analisis untuk mendapatkan *root cause* insiden

Langkah-Langkah yang dilakukan:

1. Pengumpulan dan akuisis barang bukti digital
2. *Scanning* server terdampak
3. Pengecekan *Command and Center* (CnC)
4. Pengecekan mekanisme *presistent*
5. Pencarian *malicious/suspicious file*
6. Analisis barang bukti digital yang telah dikumpulkan

Upaya penghentian penyebaran serangan, penghilangan secara penuh ancaman yang ada pada aset terdampak, dan pengembalian aset terdampak ke kondisi normal

Langkah-Langkah yang dilakukan:

1. Pengarsipan dan penghapusan *malicious/suspicious file* yang ditemukan
2. Modifikasi file .htaccess
3. Penerapan pembatasan akses pada server terdampak
4. Pengecekan mekanisme *presistent*
5. Penghentian proses dan layanan yang berbahaya dan mencurigakan
6. Proses *hardening* sistem dan server

BADAN SIBER DAN SANDI NEGARA

LANGKAH MITIGASI

1. Aktifkan *landing page* pada halaman yang terkena insiden *webdefacement*
2. Lakukan analisis dan *malware* dan *vulnerability scanning*
3. Lakukan *patching*, penghapusan *malware*, dan penggantian *password* secara berkala
4. Lakukan *recovery* website dan notifikasi kepada seluruh *user* untuk meningkatkan keamanan
5. Menghapus *indexing* Google menggunakan Google *search console*

BADAN SIBER DAN SANDI NEGARA

“(Ingatlah) Kechilafan Satu Orang Sahaja Tjukup Sudah Menjebabkan Keruntuhan Negara”

MAYJEN TNI DR. ROEBIONO KERTOPATI (1914 - 1984)

BAPAK PERSANDIAN REPUBLIK INDONESIA