DISKOMINFO BATAM

G20 INDONESIA 2022

BerAKHLAK
Berorientasi Pelayanan Akuntabel Kompeten Harmonis Loyal Adaptif Kolaboratif

PANDUAN PENANGANAN INSIDEN

WEB DEFACEMENT

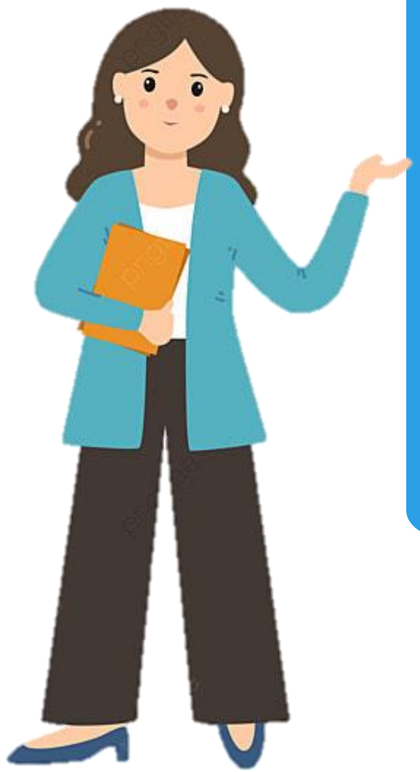
Dinas Komunikasi dan Informatika Kota Batam

DISKOMINFO BATAM

G20 INDONESIA 2022

BerAKHLAK
Berorientasi Pelayanan Akuntabel Kompeten Harmonis Loyal Adaptif Kolaboratif

PENDAHULUAN



Serangan Deface adalah bentuk tindakan peretasan yang menyerang website untuk mengubah tampilan website dan meninggalkan 'jejak' berupa pesan khusus

Selain mengganti tampilan, biasanya konten yang ada di dalamnya juga tak luput dari serangan para hacker, misalnya menghapus atau memodifikasi konten

TUJUAN

- Memastikan adanya sumber daya yang memadai untuk menangani insiden yang terjadi
- Menjamin pihak-pihak yang bertanggung jawab dalam penanganan insiden bekerja sesuai dengan tugas dan kewajiban masing-masing
- Menjamin aktivitas dari penanganan insiden dapat terkoordinasi dengan baik
- Melakukan pengumpulan informasi yang akurat
- Sharing pengetahuan dan pengalaman di antara anggota tim penanganan insiden
- Meminimalisir dampak dari insiden yang terjadi
- Mencegah adanya serangan lanjutan dan mencegah kerusakan agar tidak lebih meluas

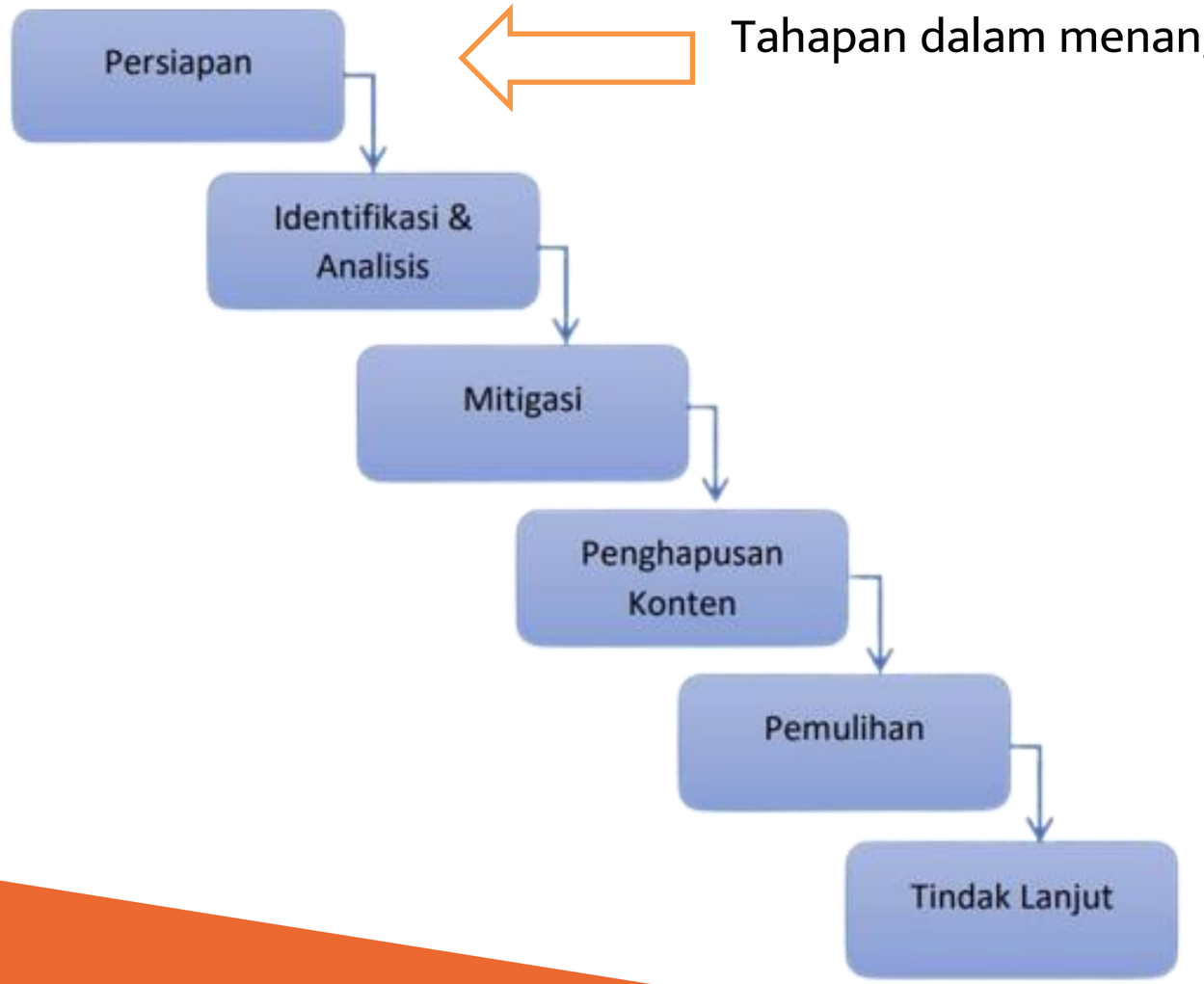
RUANG LINGKUP

Prosedur standar penanganan insiden ini berisi langkah-langkah yang harus diambil apabila terjadi insiden web defacement, yang dimulai dari tahap persiapan sampai dengan tahap pembuatan laporan dari penanganan insiden. web defacement dapat terjadi pada semua halaman web, baik milik sektor pemerintah, infrastruktur informasi kritikal nasional dan ekonomi digital

Prosedur standar penanganan insiden ini dapat dijadikan acuan bagi semua individu atau tim yang bertindak sebagai penanggung jawab/administrator dari suatu web server

PROSEDUR PENANGANAN WEB DEFACEMENT

Tahapan dalam menangani insiden



PERSIAPAN

1

Pembentukan tim penanganan insiden perlu dilakukan baik berasal dari institusi yang mengalami insiden (internal) atau juga bisa berasal dari luar institusi (eksternal) jika memang sangat diperlukan

2

Menyiapkan dokumen yang dibutuhkan dalam proses penanganan insiden. Dokumen ini antara lain adalah :

- Standar Operation Procedure
- Form-form yang akan digunakan : form penanganan insiden, form chain of custody
- Gambaran diagram terbaru yang menggambarkan hubungan antar komponen-komponen aplikasi yang membangun website (web server, aplikasi web, para user, diagram network)
- Dokumentasi dari sistem operasi, aplikasi, protokol dan anti virus yang terdapat pada web server

3

Lakukan koordinasi insiden dengan tim yang dapat menangani secara teknis, koordinasi dengan tim CSIRT ataupun Point of Contact untuk mendapatkan informasi tambahan dalam penanangan insiden

PERSIAPAN

4

Menyimpan bukti insiden antara lain screenshot insiden web defacement, log server ataupun log perangkat pendukung server. Jika menemukan file yang mencurigakan dapat dilakukan pendokumentasian file tersebut. Untuk kegiatan forensik, dapat juga dilakukan proses imaging baik seluruh storage server ataupun memori (RAM) yang digunakan

5

Menentukan tempat (ruangan) untuk menangani insiden baik kegiatan rapat tim maupun kegiatan analisis insiden

6

Menyiapkan tool dan media yang dibutuhkan untuk menangani insiden. Tools yang dapat disiapkan antara lain Scanning Tools, Forensic Tools, dan Monitoring Tools. Media dapat berupa storage external

IDENTIFIKASI DAN ANALISIS

1. Memeriksa file-file yang bersifat statis, apakah terjadi perubahan dan kapan perubahan itu terjadi. Memeriksa semua link yang ada pada halaman web (src, meta, css, script)

2. Memeriksa semua log file. File log yang dapat diperiksa antara lain Error Log, Acces Log, Database Log, Auth Log, Install Log, Event Log, Firewall Log, IDS/IPS Log, Switch/Roater Log

3. Memeriksa folder pada website yang bersifat publik (akses write, biasanya untuk menyimpan file upload) untuk indikasi file backdoor, malware, trojan, atau maliciuous file lainnya

4. Memeriksa kembali kode sql yang digunakan pada web aplikasi, apakah terdapat bug pada code tersebut. Memeriksa pada implementasi fitur Login/Logout, Koneksi Database, dan Menampilkan Isi Database

IDENTIFIKASI DAN ANALISIS

5

Memeriksa version setiap aplikasi/library yang digunakan. Pastikan versi web server, versi aplikasi dan versi database

6

Memastikan setiap koneksi yang terhubung ke server tersebut

7

Memeriksa layanan/service yang sedang berjalan. Periksa semua port yang terbuka, periksa cronjob (service otomatis harian), periksa last login untuk user, periksa history

8

Dalam melakukan tahapan ini, tools yang dapat digunakan antaran lain: Nmap, Nikto, Accunetic, Nessus

DISKOMINFO BATAM

MITIGASI

01 Perlu dilakukan pembangunan website sementara agar publikasi informasi pada website tetap berjalan. Atau dapat juga dilakukan pembangunan site under maintenance

02 Lakukan backup sistem, untuk keperluan forensik ataupun untuk mengumpulkan bukti-bukti insiden

03 Pembatasan akses terhadap sumber serangan yang ditemukan antara lain sumber IP, sumber port, serta akun user yang digunakan oleh penyerang

G20 INDONESIA 2022 BerAKHLAK

PENGHAPUSAN KONTEN DAN PEMULIHAN

PENGHAPUSAN KONTEN

Setelah ditemukan aplikasi ataupun file yang bersifat malicious, maka tahap selanjutnya adalah melakukan penghapusan konten tersebut

Adapun tahapannya sebagai berikut:

1. Lakukan hapus file malicious, antara lain :
   file defacement, file backdoor, file rootkit ataupun file malware

2. Lakukan uninstall aplikasi yang ditemukan sebagai aplikasi malicious

PENGHAPUSAN KONTEN DAN PEMULIHAN

PEMULIHAN

Pada tahap ini bertujuan untuk memulihkan kembali halaman web kepada keadaan semula

Prosedur yang dapat dilakukan sebagai berikut:

1. Mengaktifkan (me-restore) file-file yang telah di-backup. File dapat berupa file pada web server, file database
2. Lakukan update/upgrade/patch semua aplikasi yang digunakan pada web server. Jika menggunakan CMS, update versi web aplikasi, plugins, themes yang digunakan. Jika menggunakan API dapat melakukan update library yang digunakan. Selain itu perlu dilakukan update rules pada konfigurasi keamanan yang digunakan
3. Lakukan automatic updates pada setiap aplikasi yang digunakan
4. Lakukan pembaruan seluruh akun yang digunakan baik pada sistem operasi, web aplikasi
5. Lakukan hardening server ataupun aplikasi yang digunakan seperti memasang Web Application Firewall (WAF), memasang aplikasi antidefacement (DotDefender, Nagios, Webguard)
6. Pisahkan antara file web server dengan file database pada partisi yang digunakan

DISKOMINFO BATAM

G20 INDONESIA 2022

BerAKHLAK
Berorientasi Pelayanan Akuntabel Kompeten Harmonis Loyal Adaptif Kolaboratif

TINDAK LANJUT

Lakukan uji keamanan web server dan aplikasi, serta membuat evaluasicdan rekomendasi

Memetakan kerentanan yang ditemukan, baik rentan terhadap serangan SQL Injection, atau sudah deprecated/usangnya versi aplilkasi yang digunakan

Membuat semua dokumentasi dan laporan terkait kegiatan dan waktu yang dibutuhkan pada proses incident handling yang telah dilakukan

Menuliskan tools apa saja yang digunakan dalam membatu proses incident handling

1

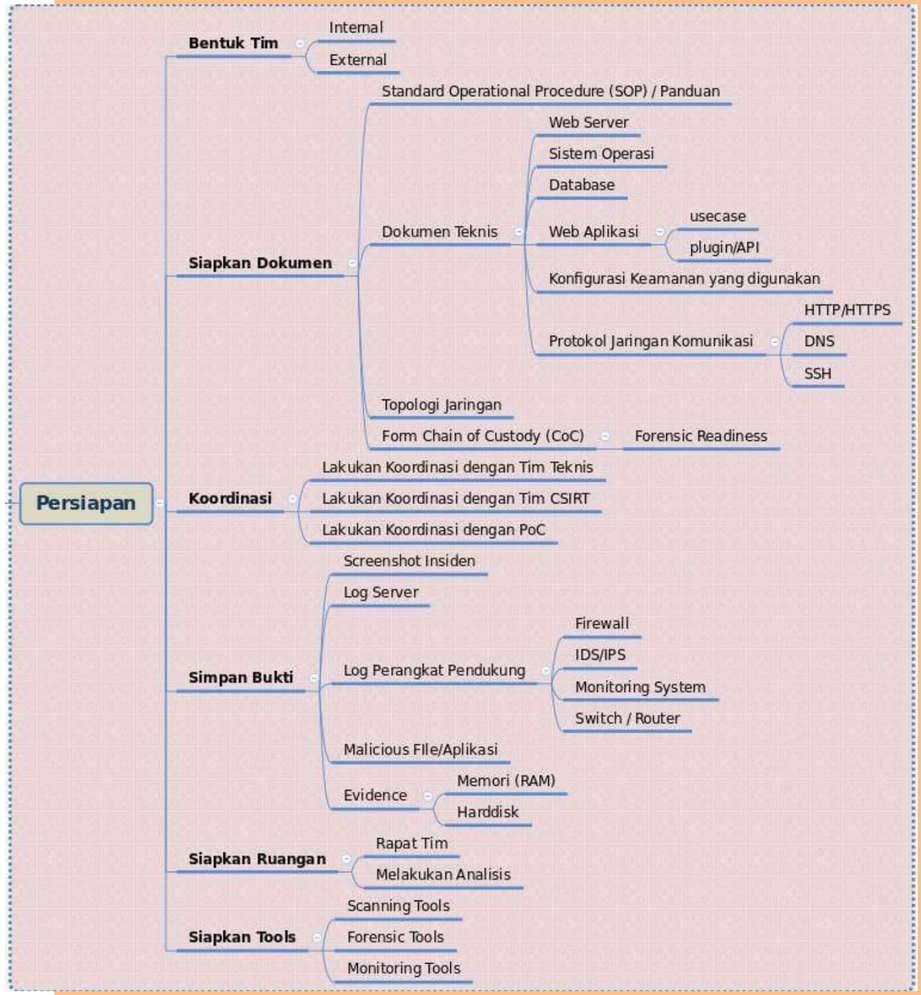
Menuliskan bukti-bukti yang ditemukan, hal ini terkait dengan proses hukum kedepannya

Memberikan analisa dan penjelasan apa yang harus dilakukan sehingga insiden serupa tidak terulang kembali

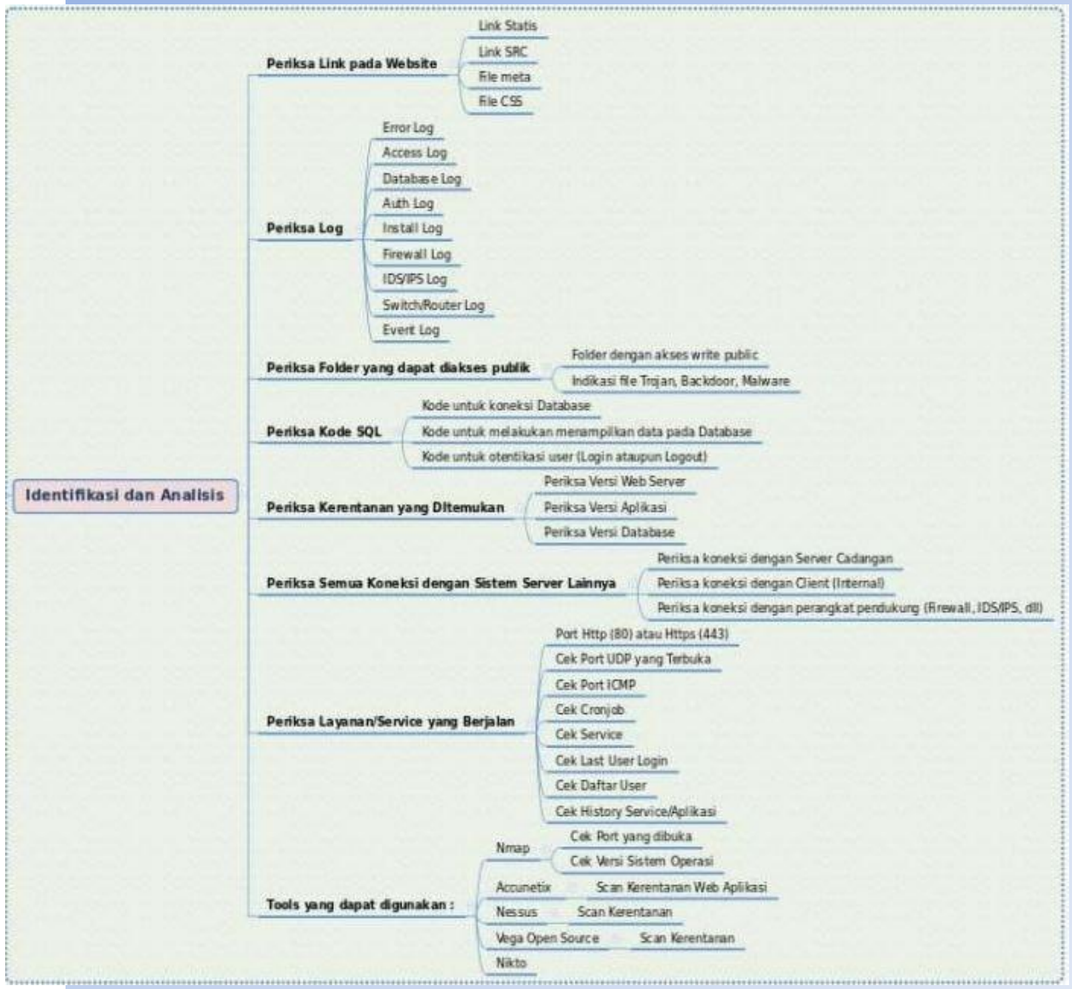
Membuat evaluasi dan rekomendasi

LAMPIRAN I - BAGAN PENANGANAN INSIDEN

A. TAHAP PERSIAPAN



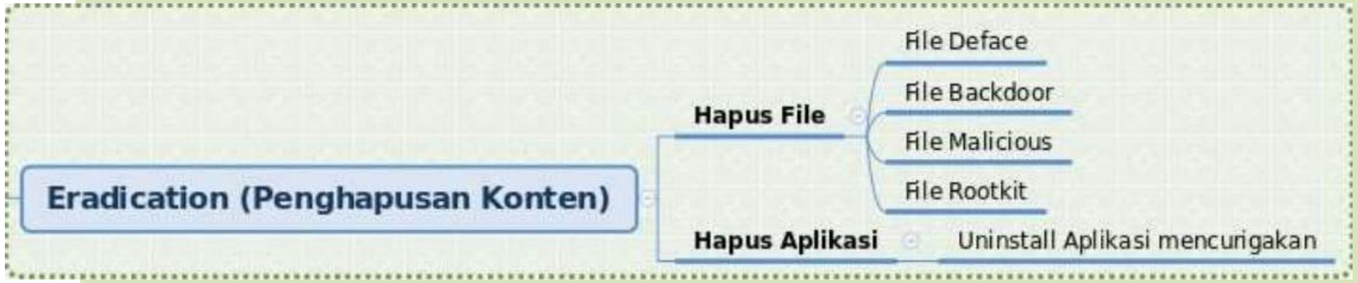
B. TAHAP IDENTIFIKASI DAN ANALISIS



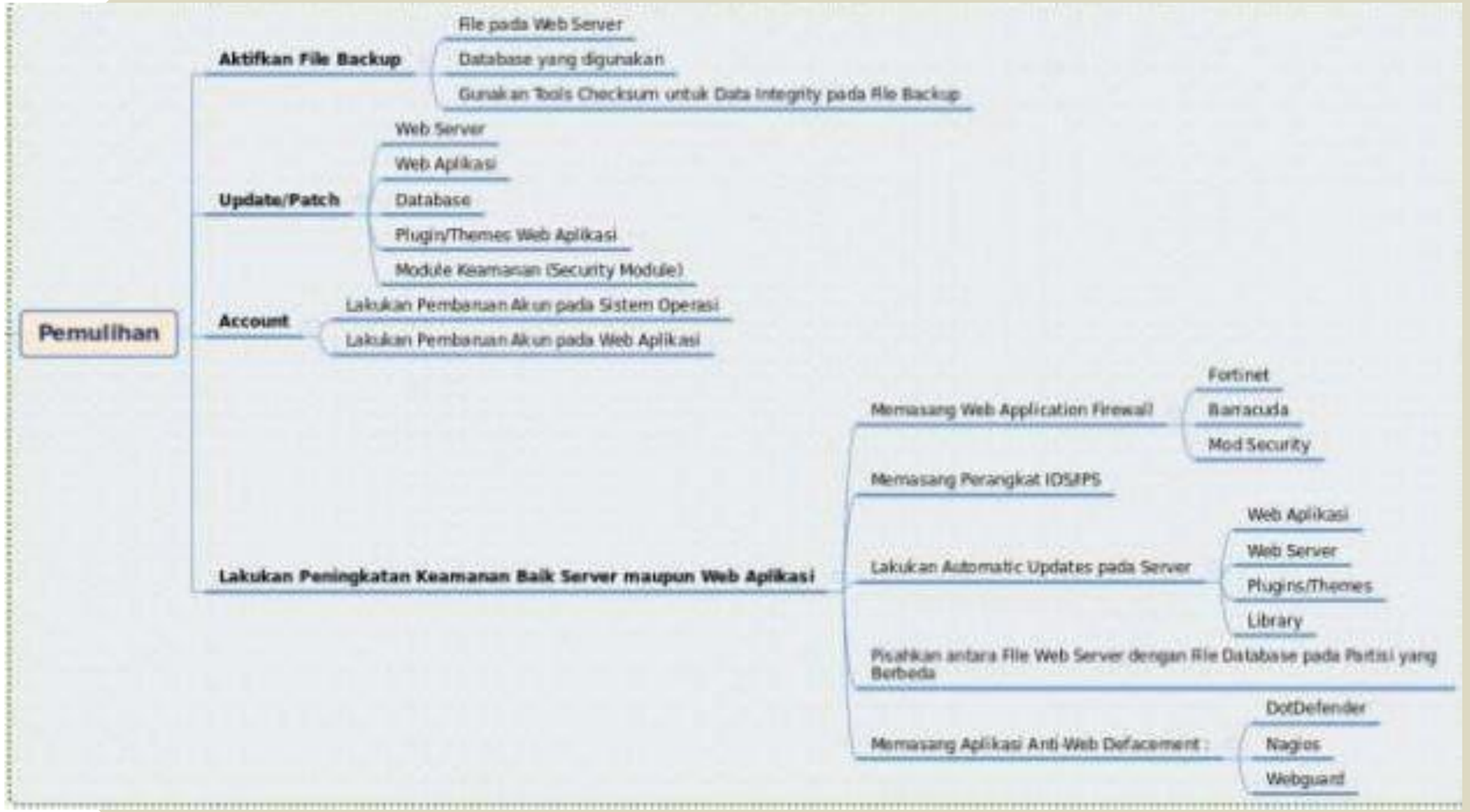
LAMPIRAN I - BAGAN PENANGANAN INSIDEN

C. TAHAP MITIGASI

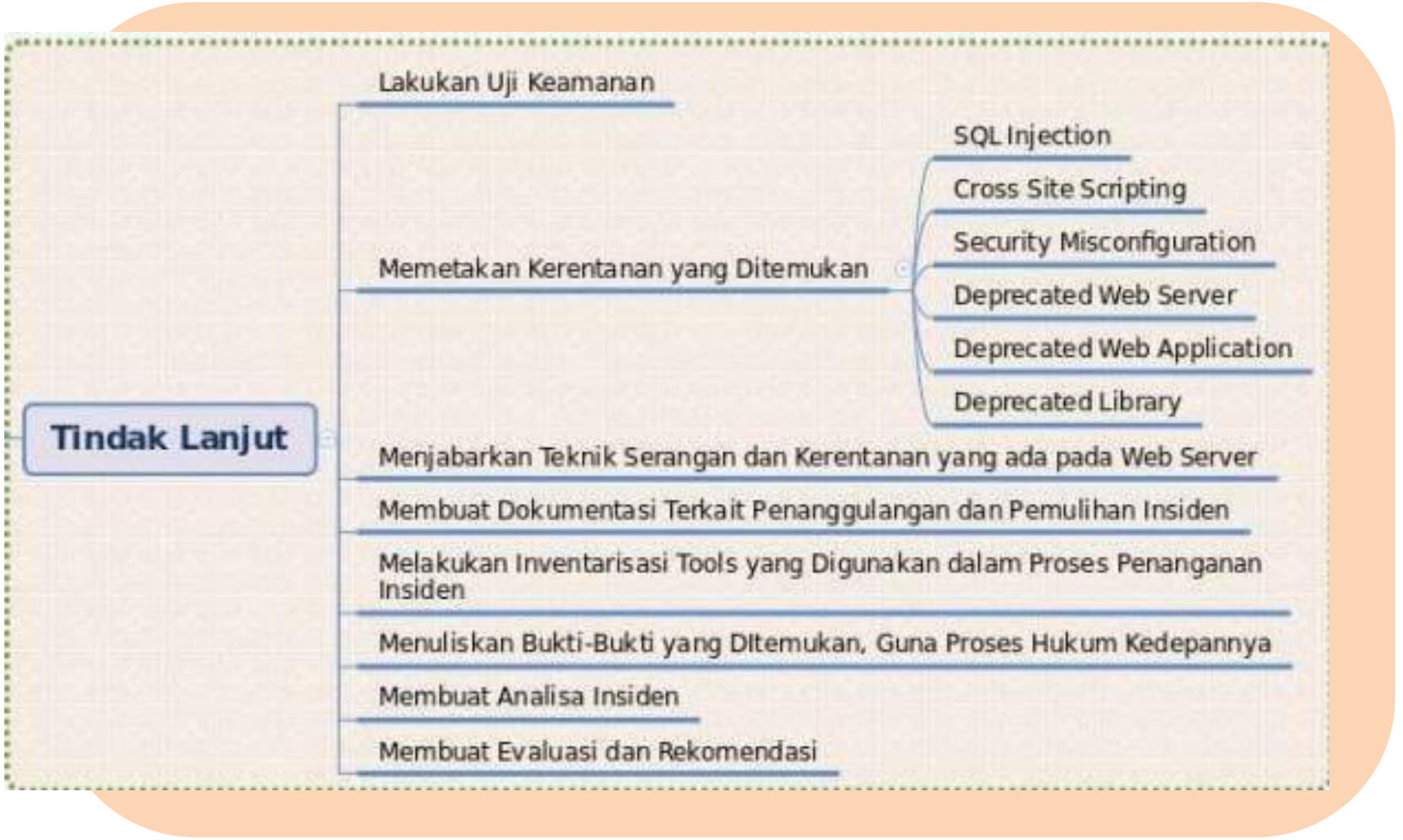
D. TAHAP PENGHAPUSAN KONTEN



E. TAHAP PEMULIHAN



F. TAHAP TINDAK LANJUT



DISKOMINFO BATAM

G20 INDONESIA 2022

BerAKHLAK
Berorientasi Pelayanan Akuntabel Kompeten Harmonis Loyal Adaptif Kolaboratif

PANDUAN PENANGANAN INSIDEN

WEB DEFACEMENT

Dinas Komunikasi dan Informatika Kota Batam