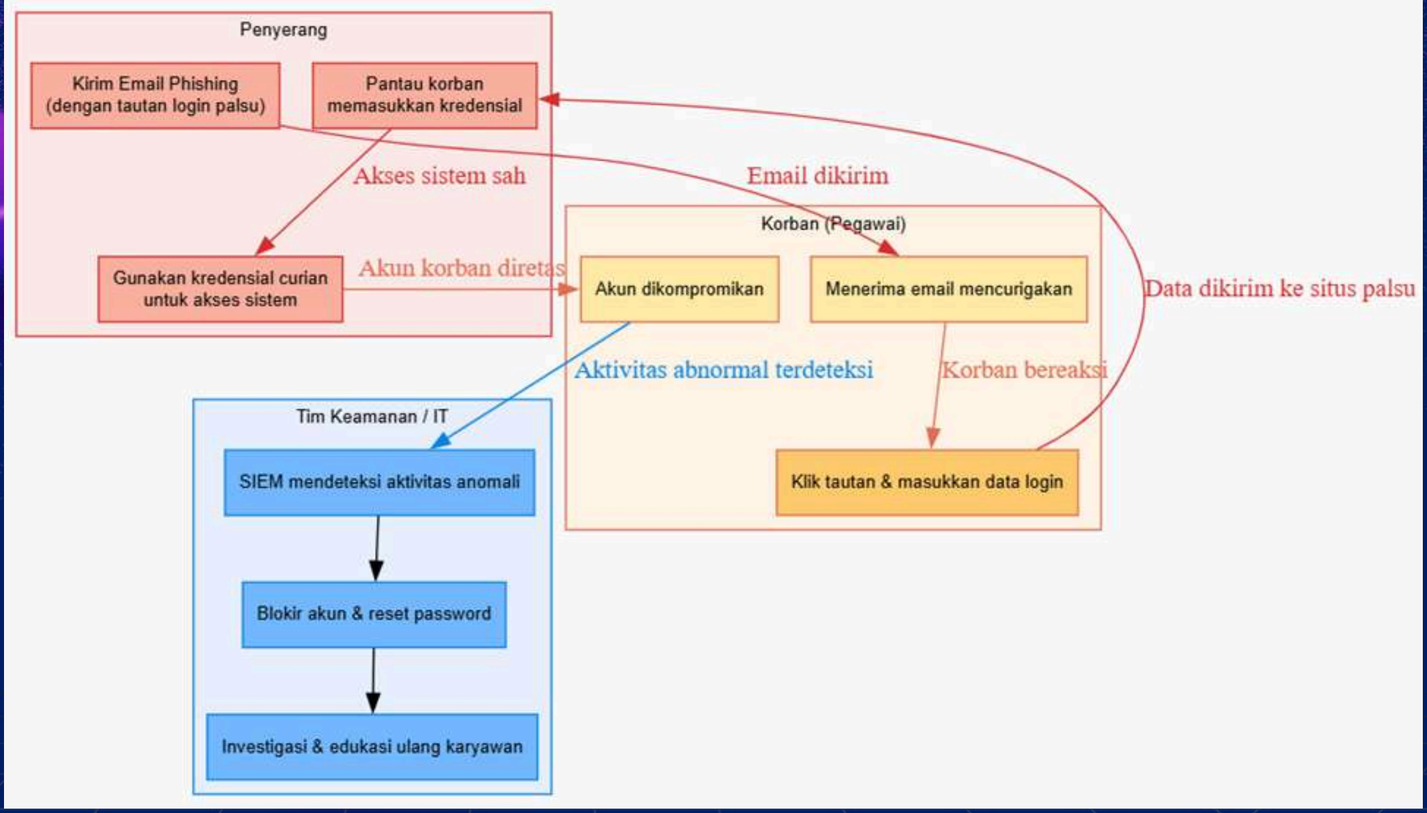

SISTEM
KEAMANAN
D4 TEKNIK INFORMATIKA 3A

PRESENTASI KELOMPOK 1

1. AFIFAH NAUFAL RAHMANI (714230026)
2. AHMAD KARTA NUGRAHA (714230035)
3. EFENDI SUGIANTORO (714230018)
4. GALUH SANJAYA PUTRA (714230067)
5. ANANDA RAKA ADITYA WILANGGA (714230023)

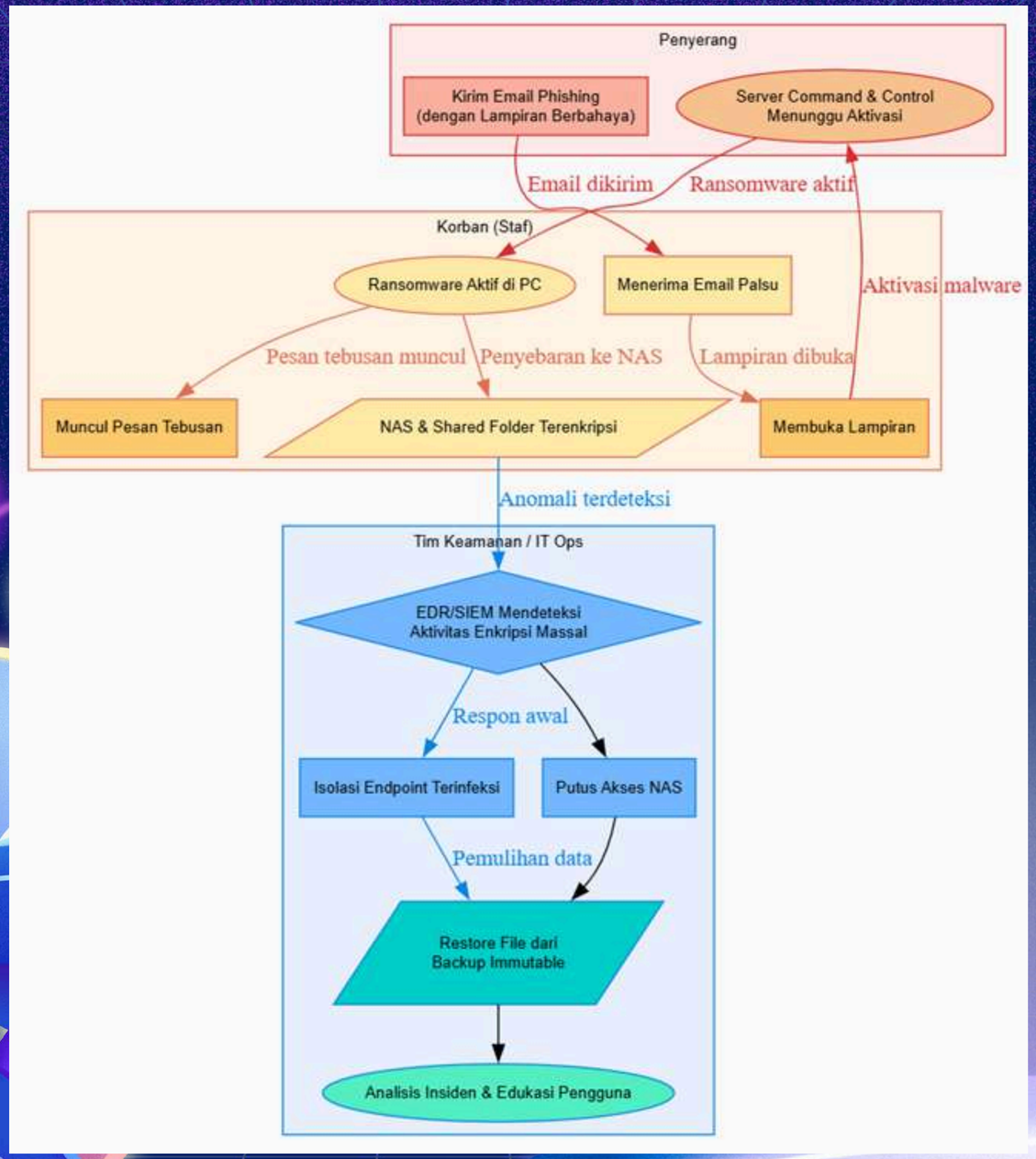
PHISHING EMAIL



Contoh Seorang pegawai menerima email yang tampak resmi dari vendor perusahaan. Karena terburu-buru, ia mengklik tautan dan memasukkan kredensial pada halaman login palsu. Akun tersebut digunakan penyerang untuk mengakses data internal dan mengekspor informasi pelanggan. Kejadian ini menimbulkan risiko kebocoran data dan menurunkan kepercayaan pengguna terhadap sistem.

SPEAR-PHISHING → CREDENTIAL ATTACK → **SOCIAL ENGINEERING ATTACK**

RANSOMWARE



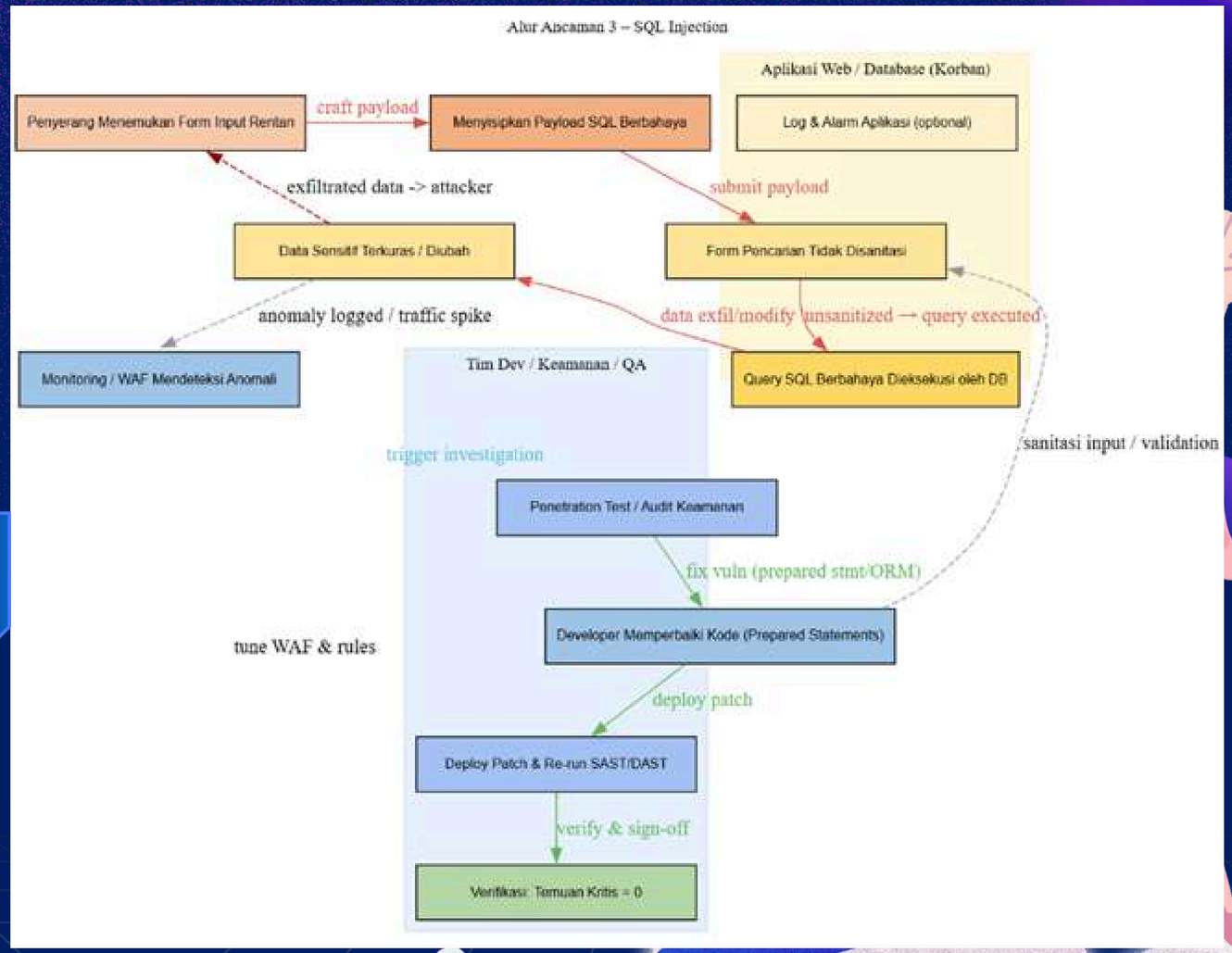
Seorang staf membuka lampiran berbahaya dari email yang dikira dokumen pekerjaan. Ransomware langsung mengenkripsi file di perangkat dan menyebar ke folder bersama di **NAS**. Seluruh dokumen proyek menjadi tidak dapat diakses, menghambat operasional perusahaan dan berpotensi menghapus backup penting yang belum terpisah dengan baik.

LAMPIRAN EMAIL → EKSEKUSI MALWARE → ENKRIPSI FILE LOKAL → PENYEBARAN KE **NETWORK SHARE** → PERMINTAAN TEBUSAN.

SQL INJECTION

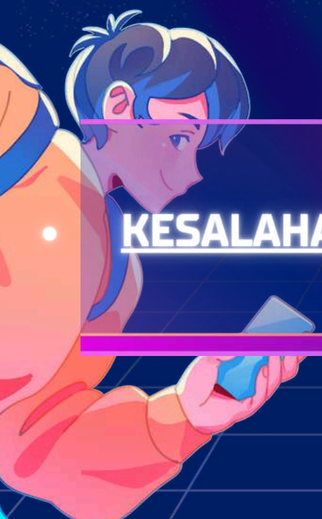
Form pencarian di situs web perusahaan tidak divalidasi dengan benar. Penyerang menyisipkan kode SQL berbahaya dan berhasil menampilkan data sensitif pengguna. Dalam beberapa kasus, serangan juga dapat mengubah isi database dan menyebabkan kerusakan data yang berdampak pada keandalan layanan.

INPUT TIDAK DISANITASI → QUERY SQL BERBAHAYA DIJALANKAN → DATA BOCOR ATAU DIMODIFIKASI → **WAF**

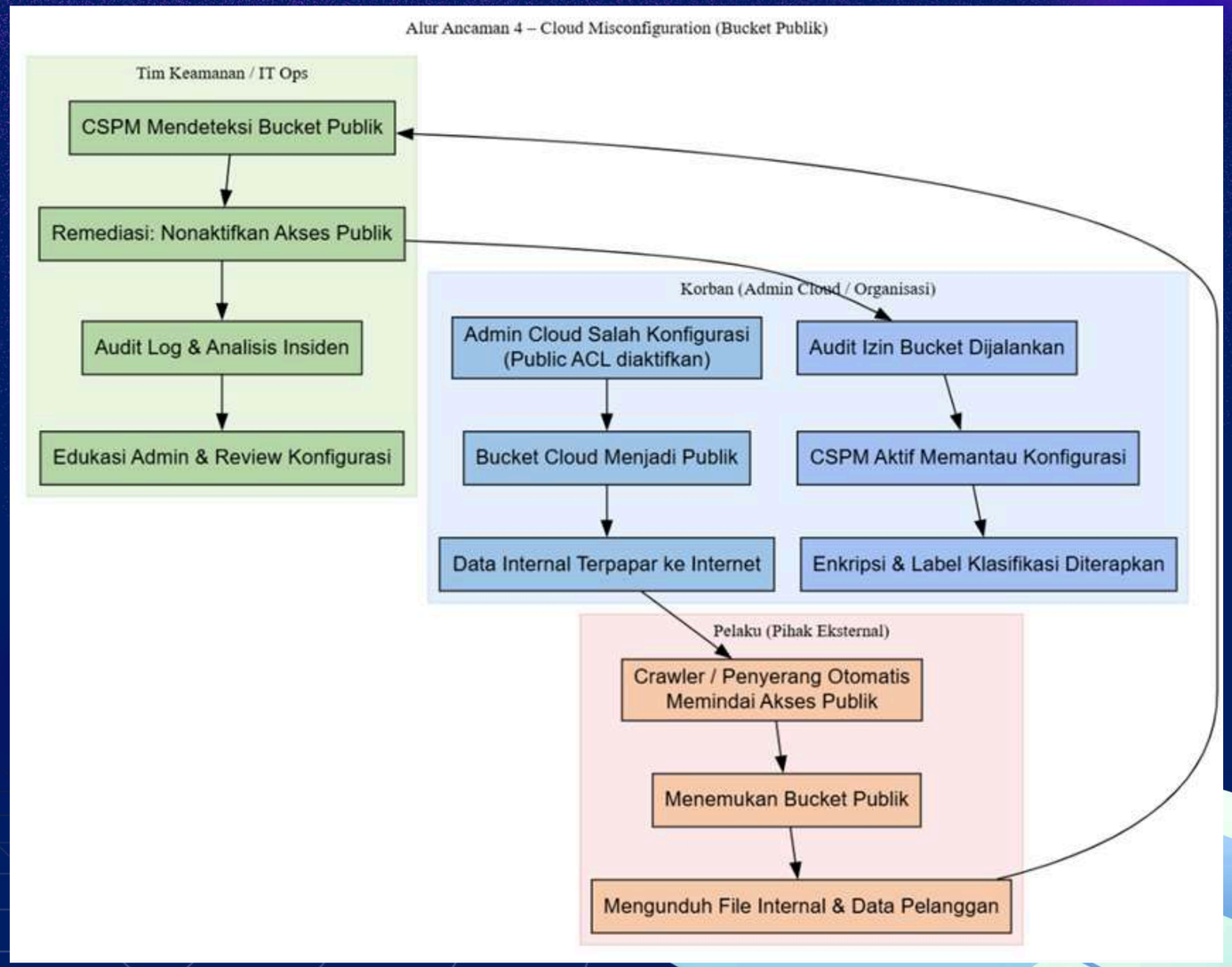


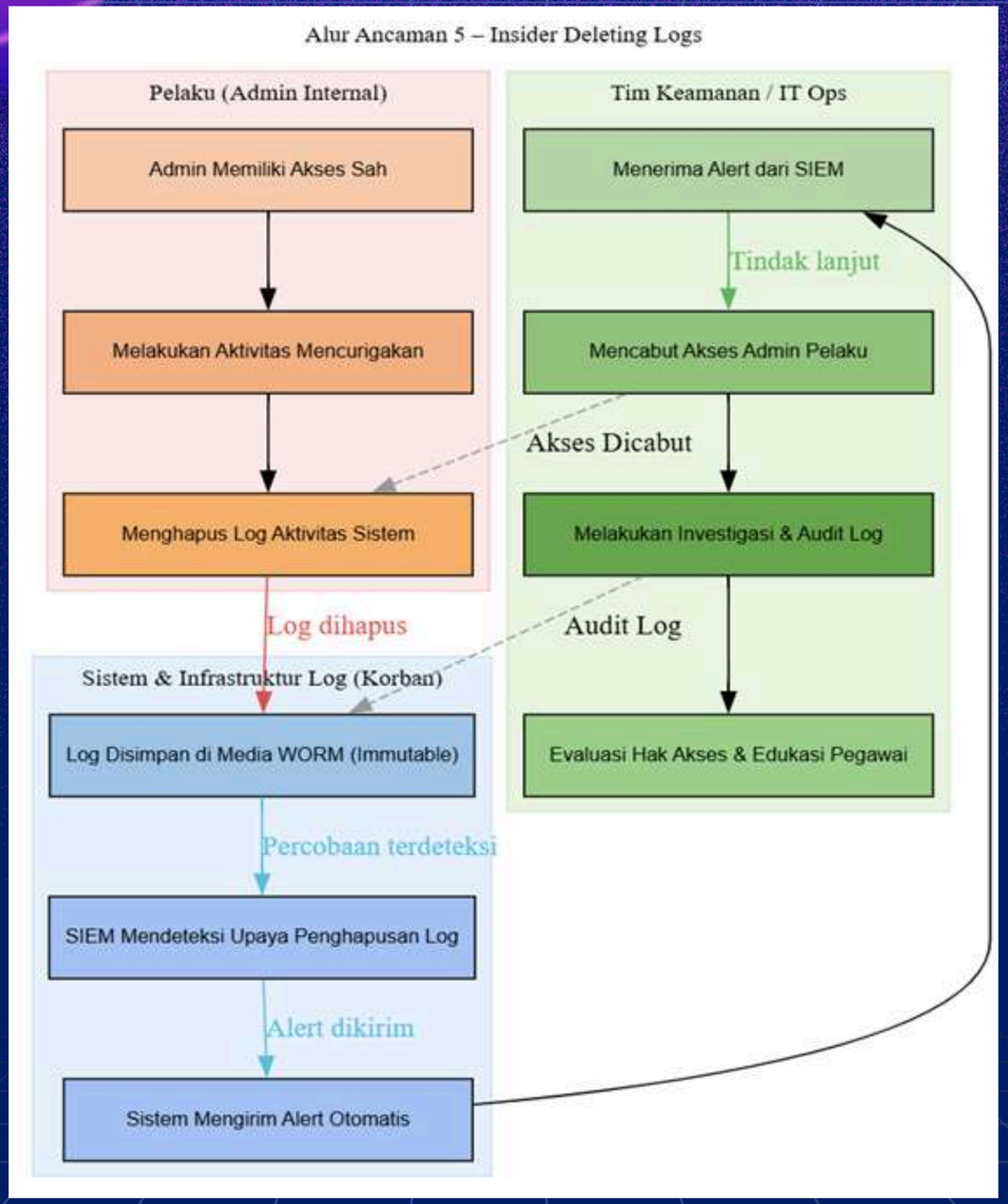
CLOUD MISCONFIGURATION (BUCKET PUBLIK)

Admin cloud secara tidak sengaja mengatur izin bucket penyimpanan menjadi publik untuk memudahkan akses. Tanpa disadari, file internal dan data pelanggan dapat diakses oleh siapa pun di internet. Situasi ini mengakibatkan potensi kebocoran informasi penting dan ancaman reputasi bagi organisasi.



KESALAHAN KONFIGURASI → BUCKET MENJADI PUBLIK → **CSPM.**





INSIDER DELETING LOGS

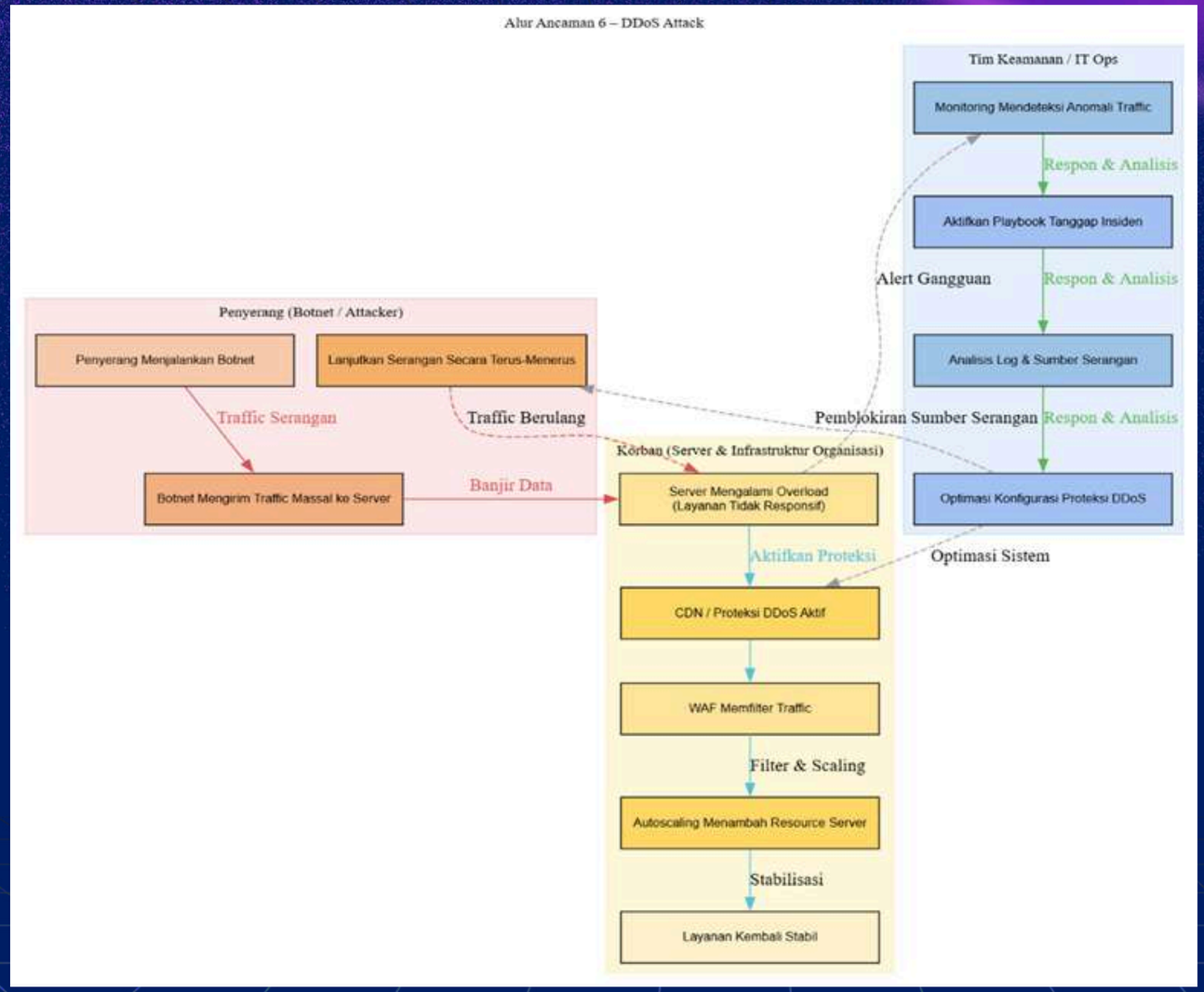
Pegawai dengan akses admin mencoba menutupi tindakannya dengan menghapus log aktivitas sistem. Akibatnya, jejak digital insiden hilang dan proses investigasi menjadi sulit dilakukan. Jika dibiarkan, hal ini dapat mengganggu integritas bukti audit dan menurunkan kepercayaan terhadap keamanan internal perusahaan.

AKSES SAH → HAPUS LOG → **WRITE ONCE READ MANY (WORM).**

DDOS ATTACK

Situs utama organisasi diserang dengan lalu lintas besar dari botnet sehingga pengguna sah tidak dapat mengakses layanan. Serangan ini menyebabkan gangguan operasional selama beberapa jam dan menurunkan reputasi perusahaan di mata pelanggan.

BOTNET → MENGIRIM TRAFFIC BESAR → SERVER OVERLOAD → LAYANAN TIDAK RESPONSIF.



KESIMPULAN

Keenam ancaman siber yang dibahas — phishing email, ransomware, SQL injection, cloud misconfiguration, insider deleting logs, dan DDoS attack — menggambarkan bahwa serangan dapat terjadi pada berbagai lapisan, mulai dari manusia, aplikasi, hingga jaringan. Setiap serangan memiliki karakteristik dan dampak yang berbeda, namun semuanya mengancam aspek utama keamanan informasi, yaitu kerahasiaan, integritas, dan ketersediaan data. Karena itu, upaya perlindungan harus dilakukan secara menyeluruh melalui edukasi pengguna, pengamanan sistem dan database, konfigurasi cloud yang tepat, serta pemantauan aktivitas jaringan secara berkelanjutan. Pendekatan keamanan yang terintegrasi akan membantu organisasi menjaga keandalan dan ketahanan sistem digital dari berbagai bentuk ancaman.

KING RENDY

TERIMA KASIH