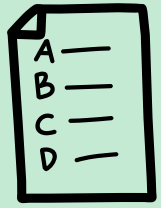
DIGITAL FORENSICS

Digital forensics adalah disiplin yang menangani identifikasi, pengumpulan, pelestarian, dan analisis bukti digital dalam sebuah insiden. Tujuannya memastikan bukti valid secara teknis maupun hukum, dengan menekankan akurasi, objektivitas, serta keterlacakan proses investigasi.

01 PROSES DIGITAL FORENSICS

Proses forensik berlangsung melalui tahapan identifikasi, pelestarian, pengumpulan, pemeriksaan, analisis, dan pelaporan. Setiap langkah harus dilakukan secara berurutan dan terdokumentasi agar integritas bukti tetap terjaga.

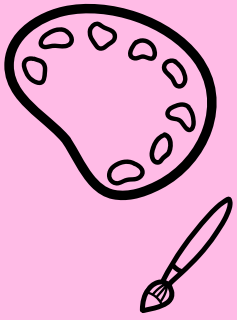
02 EVIDENCE HANDLING



Penanganan bukti mencakup pemahaman jenis bukti, prioritas pengumpulan (terutama bukti volatile), serta penerapan chain of custody. Hashing digunakan untuk memastikan bukti tidak berubah selama pemeriksaan.

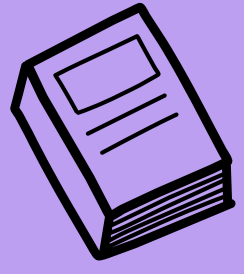
03 CYBER ATTACK ANALYSIS FRAMEWORKS

Framework seperti Cyber Kill Chain dan Diamond Model membantu memetakan tahapan dan pola serangan. Kill Chain menggambarkan alur serangan, sementara Diamond Model menyoroti hubungan antara penyerang, kemampuan, infrastruktur, dan korban.



04 INCIDENT RESPONSE PROCESS

Kerangka kerja NIST mencakup persiapan, deteksi, containment, eradication, pemulihan, dan kegiatan pasca-insiden. Tujuannya memastikan respon insiden berlangsung cepat, efektif, dan mampu mencegah kejadian berulang.



05 INCIDENT ANALYSIS

Analisis insiden mencakup identifikasi indikator kompromi, penelusuran alur serangan, pembuatan timeline, serta penilaian dampak. Aktivitas ini memerlukan korelasi berbagai sumber data untuk memahami ruang lingkup insiden.

06 POST-INCIDENT & IMPROVEMENT

Tahap pasca-insiden menekankan evaluasi proses, penyusunan laporan, serta pembaruan kebijakan dan kontrol keamanan. Hasil evaluasi digunakan untuk meningkatkan kesiapan organisasi menghadapi insiden berikutnya.