DIGITAL FORENSICS AND INCIDENT ANALYSIS AND RESPONSE

Digital forensics dan incident response fokus pada bagaimana organisasi mengumpulkan, menganalisis, dan menangani bukti digital setelah terjadi insiden keamanan

EVIDENCE HANDLING AND ATTACK ATTRIBUTION

1. Menemukan dan memelihara bukti digital (IoC).
2. Mengikuti panduan NIST SP 800-86.
3. Tahapan forensik: collection, examination, analysis, reporting.
4. RFC 3227 → urutan pengambilan bukti berdasar volatilitas.
5. Chain of custody menjaga bukti tetap valid.
6. Threat attribution memakai TTP + threat intelligence + MITRE ATT&CK.

THE CYBER KILL CHAIN

Model 7 tahap untuk memahami alur serangan:

1. Reconnaissance
2. Weaponization
3. Delivery
4. Exploitation
5. Installation
6. Command & Control
7. Actions on Objectives

DIAMOND MODEL OF INTRUSION ANALYSIS

Satu event intrusion digambarkan melalui empat elemen utama:

a. Adversary
b. Capability
c. Infrastructure
d. Victim

- Meta-features: timestamp, phase, direction, methodology, result.
- Event berurutan membentuk rangkaian serangan yang dapat dipetakan ke Kill Chain.

DISASTER RECOVERY

Mencakup proses memperbaiki, memulihkan, dan mengembalikan aset setelah bencana, yang dilakukan melalui preventive, detective, dan corrective controls.
Business Continuity membutuhkan BIA untuk mengukur: RTO, RPO, MTTR, MTBF
Jenis latihan DRP: tabletop exercise, functional test, full operational simulation.

INCIDENT RESPONSE (NIST SP 800-61)

Tujuannya adalah membatasi dampak serangan, menganalisis kerusakan, dan melakukan pemulihan dengan membentuk CSIRC serta menyiapkan kebijakan dan prosedur, melibatkan stakeholders seperti IT, legal, HR, management, media/public affairs, dan security.
Empat fase IR lifecycle:

- Preparation
- Detection & Analysis
- Containment, Eradication, Recovery
- Post-Incident Activities

CINDY PERMATASARI LUBIS – 434231016