INCIDENT
HANDLING / RESPONSE / MANAGEMENT
(penanganan insiden)

Budi Rahardjo
2025

ISO 27001 Domains

1. Security policy - management direction
2. Organization of information security - governance of information security
3. Asset management - inventory and classification of information assets
4. Human resources security - security aspects for employees joining, moving and leaving an organization
5. Physical and environmental security - protection of the computer facilities
6. Communications and operations management - management of technical security controls in systems and networks
7. Access control - restriction of access rights to networks, systems, applications, functions and data
8. Information systems acquisition, development and maintenance - building security into applications
9. **Information security incident management** - anticipating and responding appropriately to information security breaches
10. Business continuity management - protecting, maintaining and recovering business-critical processes and systems
11. Compliance - ensuring conformance with information security policies, standards, laws and regulations

ISO 27001:2022 Domains (Annex)

Annex A.5 – Information Security Policies
Annex A.6 – Organisation of Information Security
Annex A.7 – Human Resource Security
Annex A.8 – Asset Management
Annex A.9 – Access Control
Annex A.10 – Cryptography
Annex A.11 – Physical & Environmental Security
Annex A.12 – Operations Security
Annex A.13 – Communications Security
Annex A.14 – System Acquisition, Development & Maintenance
Annex A.15 – Supplier Relationships
Annex A.16 – Information Security Incident Management
Annex A.17 – Information Security Aspects of Business Continuity Management
Annex A.18 – Compliance

Insiden

- Insiden merupakan bagian dari kehidupan elektronik
  - Tidak sengaja vs disengaja
  - Sering terjadi pada waktu yang kurang “pas” (misal: admin sedang tidak ada, sedang ada deadline)

Contoh Insiden

- Contoh insiden
  - Wabah virus
  - Spam mail, mailbomb
  - Previlage attack, rootkit, intrusion
  - DoS attack
  - Unauthorized access
  - Penyadapan data
  - ...
  - Harus dipikirkan skenario lain yang mungkin terjadi

Definisi dari "incident"

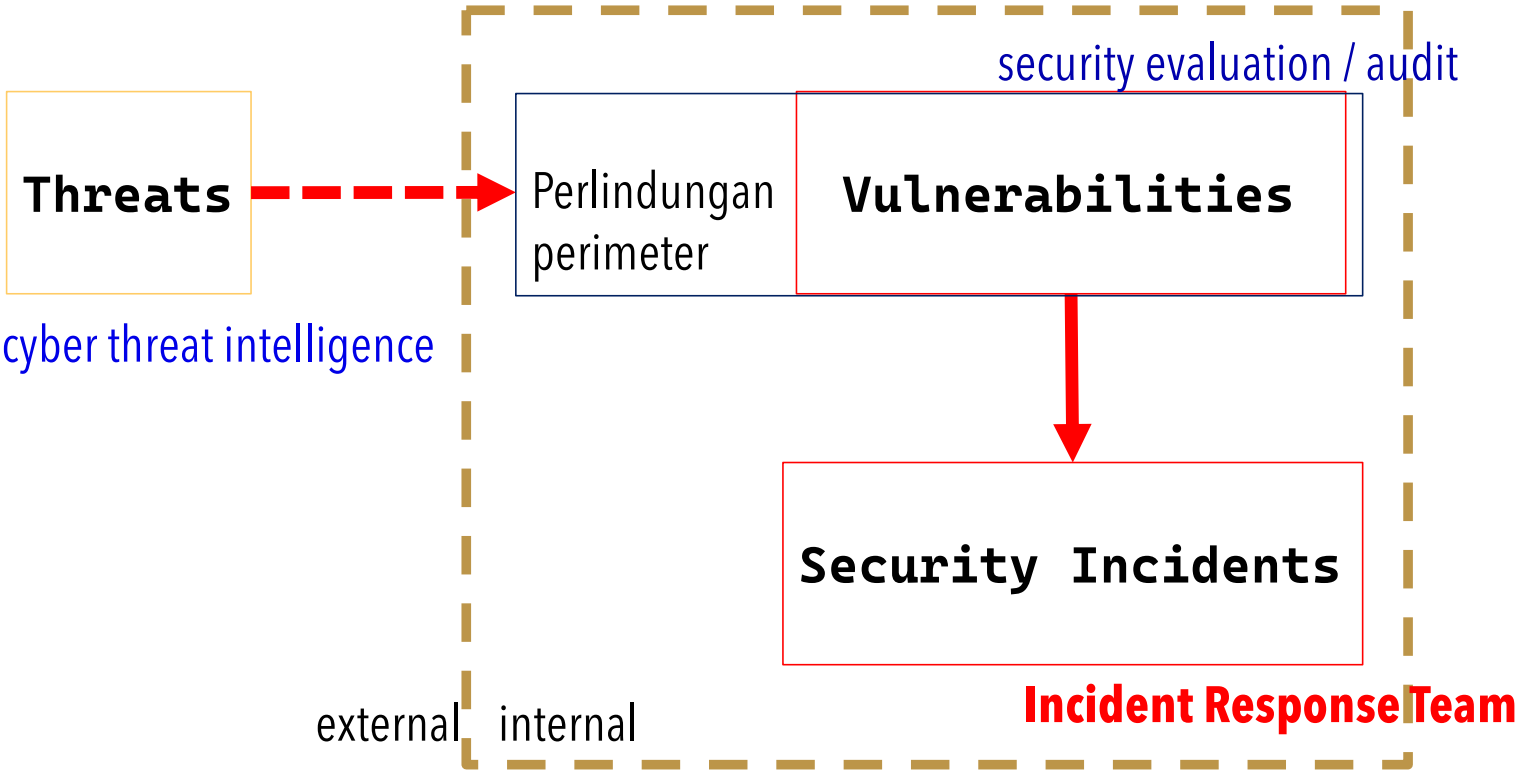
- David Theunissen, "Corporate Incident Handling Guidelines":

  Incidents is "*the act of violating or threatening to violate an explicit or implied security policy*"

- Kevin Mandia & Chris Prosise, "Incident Response":

  "*Incidents are events that interrupt normal operating procedure and precipitate some level of crisis*"

Threats, Vulnerabilities and Incidents



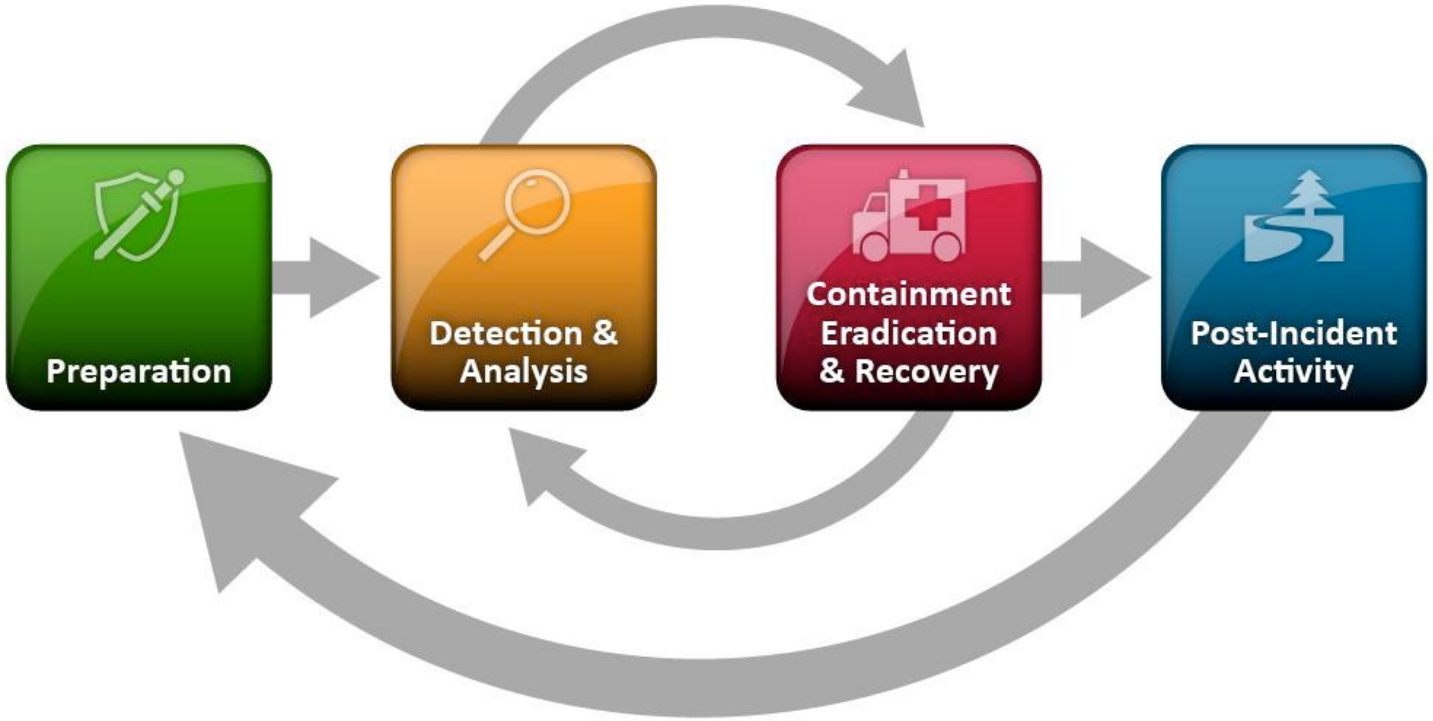
Tujuan dari "Incident Handling"

- Memastikan bahwa insiden terjadi atau tidak terjadi
- Melakukan pengumpulan informasi yang akurat
- Melakukan pengambilan dan penanganan bukti-bukti (menjaga chain of custody)
- Menjaga agar kegiatan berada dalam kerangka hukum (misalnya masalah privacy, legal action)
- Meminimalkan gangguan terhadap operasi bisnis dan jaringan
- Membuat laporan yang akurat berserta rekomendasinya

Metodologi

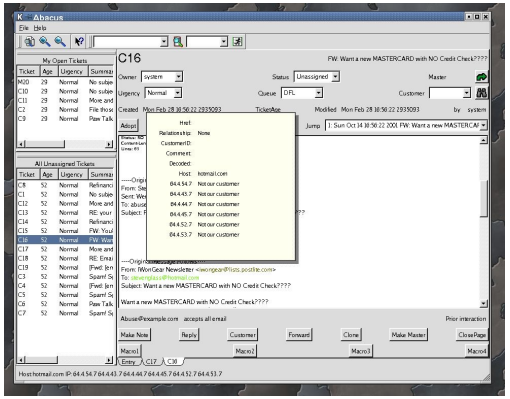
- From Kevin Mandia & Chris Prosise - “Incident Response”
  - Pre-incident preparation
  - Detection of incidents
  - Initial response
  - Response strategy formulation
  - Duplication (forensic backups)
  - Investigation
  - Security measure implementation
  - Network monitoring
  - Recovery
  - Follow-up

Metodologi (2)



NIST SP 800-61 Computer Security Incident Handling Guide

Permasalahan *Incident Handling*



- Teknis
  - Apa saja yang harus dilaporkan?
    - Apakah ada informasi yang *confidential*? (nomor IP, userid, password, data, files)
    - Perlunya packet scrubbing?
    - Terlalu sedikit/banyak data yang dilaporkan
  - Ketersediaan trouble ticketing system, help desk (24 jam?)
  - Data-data log sering tidak tersedia sehingga menyulitkan incident handling
  - Penggunaan perangkat yang sudah disertifikasi sebagai perangkat penanganan insiden (misal disk copier)
  - Ketersediaan tools (in general)

Permasalahan Incident Handling (2)

- Ada banyak topik yang spesifik terhadap jenis insidennya
  - Malware
  - Ransomware
  - Software
  - Industrial systems

Permasalahan Incident Handling (3)

- Non-teknis
  - Organisasi:
    - Kemana (kepada siapa) harus melapor jika terjadi insiden? Perlunya "Incident Response Team" (IRT)
    - Melapor ke organisasi yang lebih tinggi di luar institusi lokal? (misal ke ID-CERT, APSIRC, CERT)
      Untuk keperluan statistik (ada wabah regional?)
    - Melapor kepada perusahaan pengembang?
  - Hubungan dengan *policy & procedures*, SOP yang seringkali tidak dimiliki oleh institusi
  - Ketersediaan SDM
    - Kualifikasi apa yang dibutuhkan?

ID-CERT

- Organisasi informal berbasis voluntir dibentuk tahun 1997/1998
- Menggunakan internet untuk melakukan koordinasi dan memberikan layanan
  - Mailing list
  - Abuse handling
  - *Advisory*
  - *Outreach education*
- Berbasis RFC 2350: *Expectations for Computer Security Incident Response*
- Salah satu founder APCERT (Asia Pacific CERT)

Mengenal IRT lain

- Negara lain:
  - SingCERT
  - MyCERT
  - AusCERT
  - …
- Regional
  - APSIRC / APCERTF
  - Eropa, Amerika
- Lain-lain
  - FIRST: http://www.first.org
  - CERT: http://www.cert.org

Topik Terkait

- Cyber Threat Intelligence (CTI)
- Protocol to exchange information

Bahan Bacaan

- SANS Reading Room
  - http://rr.sans.org/incident/incident_list.php
- ID-CERT
  - http://www.cert.or.id
- Lain-lain
  - http://www.incidentresponsebook.com
  - ISO 27001 (Annex A)