Security Operations | Ivan Notes 2022

- **Investigations**
  - 1. Secure the scene
  - 2. Collect & control evidence
    - Locard's principle
    - MOM
    - Sources
      - Oral / Writeen
      - Documents
      - digital forensics
        - Live evidence (volatile)
        - secondary (storage (HD)
        - VM instance / virtual disk
      - E discovery
    - Chain of custody
  - Types of evidence
    - Real
    - direct
    - best evidence rule
  - rules of evidence
    - authentic
    - accurate
    - complate
    - convincing / reliable
    - adminissible / believable
  - investigation techniques
    - media analysis

- software analysis
- network analysis

- types of investigations
  - criminal
  - civil
  - regulatory
  - administrative
- 3. Document & report

IR

- 1. Prep
- 2. Triage
  - detection
    - sources: SIEM, IDS/IPS, DLP, etc.
    - Event
    - Incident
  - Response - IR team deployed
- 3. Action / Investigation
  - mitigation - containment
  - reporting - relevant stakeholder
- 4. Recovery
  - recovery - return to normal
  - remediation - prevention
  - lessons learned - improve process

Malware

- Types
  - virus
  - worms
  - companion
  - macro
  - multipartite

- trojan
- botnets
- boot sector
- logic bomb
- stealth
- ransomware
- rootkit
- spyware / adware

- Zero Day

- Anti-malware
  - policy
    - training & awareness
  - prevention
    - whitelist
    - network segmentation
  - detection
    - signature based scanners
    - heuristic scanners
    - activity monitors
    - change detection
  - continuous updates

- **Patching**
  - 1. Determine if patches are available
    - threat intelligence
    - vendor notification
    - pro-active checking
      - agent
      - agentless
      - passive
  - 2. Implement through change mgmt

- timing
- deploy
  - automated
  - manual

Change mgmt

- 1. change request
- 2. assess impact
  - emergency change vs standard process
- 3. approval
  - based on impact, severity, etc
  - CCB, CAB, ECAB
- 4. built & test
- 5. notification
- 6. implement
- 7. validation
  - test new functionality
  - regression testing
- 8. version & baseline

Recovery Strategies

- backup storage
  - archive bit
  - types
    - mirror
    - full
    - incremental
    - differential
  - validation
    - checksum/CRC
  - data storage
    - offsite

- tape rotation
- spare parts
  - cold
  - warm
  - hot
- RAID
  - RAID 0 = striping
  - RAID 1 = mirroring
  - RAID 5 = parity
- HA system
  - clutering
  - redundancy
- recovery sites
  - types
    - cold
    - warm
    - hot
    - mobile
    - redundant
  - geographically remote

BCM

- focuses on critical and essential functions of business
- Goals
  - 1. safety of people
  - 2. minimize damage
  - 3. survival of business
- BIA
  - identify critical processes & systems
  - measurements of time
    - RPO, RTO, WRT, MTD

- owner approval of #'s and associated costs

- types of plans
  - BCP
  - DRP
- testing plans
  - read-through / checklist
  - walkthrough
  - simulation
  - parallel
  - full-interruption / full-scale
- restoration order
  - most critical first
  - dependency charts