# D7 - Security Operations

## Security Operations

## Understand and support investigations, Evidence collection, and handling

This is pretty generic. Make sure you confirm something is a problem before taking any actions. If something needs to be acted upon, contain it first(unplug ethernet or put up crime scene tape), and use procedures (write blocks or gloves to keep integrity of the object you are assessing). Forensics focuses on the legality of conducting an investigation.

- Reporting and documentation
- Investigative techniques
- Digital forensics tools, tactics, and procedures

## Understand requirements for investigation types

I've never seen these questions asked in practice tests so I wouldn't worry about them. They are also not covered in the 2 different CISSP books I have...

- Administrative
- Criminal
- Civil
- Regulatory
- Industry standards

## Conduct logging and monitoring activities

- Intrusion detection and prevention - detections looks for actions and reports, while prevention takes action. There are network based and host based.
- Security Information and Event Management (SIEM) - Security Information and Event Management. Most should provide traffic analysis, analyze logs, scan the network with a vulnerability scanner, and report actions/info via email, phone, etc.
- Continuous monitoring - this is a strategy. NIST 800-137 provides a plan for implimenting continuous monitoring that provides visibility of assets, awarness of threats/vulns, and security controls deployed.
- Egress monitoring - monitoring traffic leaving your network

## Securely provisioning resources

- Asset inventory - tracking: hardware, software, programs installed
- Asset management - updating software, replacing hardware, adding functionality, removing functionality, tracking their location
- Configuration management - process of establishing and maintaining consistent baselines of all of the systems. get baselines of everything

## Understand and apply foundational security operations concepts

- Need-to-know/least privileges - A user should have a need to know to access particular resources, and least privilege should be implemented to ensure she only accesses the resources she has a need to know.
- Separation of duties and responsibilities - Separation of duties is put into place to ensure that one entity cannot carry out a critical task alone.
- Privileged account management - privilege kreep tends to happen over time. need to ensure there is great justification always to have administrative privileges. administrative actions are logged.
- Job rotation - Rotation of duties enables a company to have more than one person trained in a position and can uncover fraudulent activities
- Information lifecycle - flow of information. overtime information becomes less useful and less sensitive. if someone stole your credit card info for your current one it would be bad, but one you had 15 years ago wouldn't really matter that much.
- Service Level Agreements (SLA) - helps decide what type of availability technology is appropriate.

# Apply resource protection techniques

Apply deterrents, monitoring, and protectin to keep assets undamaged and unstolen. Put in GPS tracking, bag inspections, and scanners

- Media management
- Hardware and software asset management

## Conduct incident management

- Detection - most important step is to realize that there is a problem. Must have a machine analyzing network, as well as a person to filter false positives.
- Response - need to determine an appropriate response. analyize all of the material before making a decision
- Mitigation - contain the incident. act on the situation to reduce damage and to keep the situation in a manageable state
- Reporting - summary of incident, indicators, related incidents, actions taken, chain of custody, impact assessment, identity, and next steps to be taken
- Recovery - trying to get the asset to a known good state
- Remediation - need to make sure attack or failure is not successful again. patch the issue, and figure out if this could happen again in future
- Lessons learned - what happened, what did we learn, any mistakes, what was good, can we do better next time, is there a good plan in place to deal with this in the future?

## Operate and maintain detective and preventative measures

- Firewalls - makes sure the right type of traffic is allowd in and out
    - Packet filtering - don't route, just accept or drop based on IP, packet type, port, etc
    - Circuit-level gateways - don't inspect packets, monitor TCP handhshake to see if session is legimate
    - Stateful - examine each packet and different sessions
    - application-level - like a proxy, affect performance, inspect packet and see if clients are trusted
    - Next-gen - packet inspection, stateful inspect, and deep packet inspection

- Intrusion detection and prevention systems - need to make sure they are configured to detect real events, and that IPS actions done don't hurt business because of too many false positives
- Whitelisting/blacklisting - white: allow certain applications. black: don't allow certain applications.
- Third-party provided security services - pentest, monitoring, storage, physical, contracting to impliment security controls, etc
- Sandboxing - run things in safe place so that if it is compromised it can't elevate privileges or effect systems around it
- Honeypots/honeynets - attractive targets that alter the network admin someone is attacking things on network
- Anti-malware - anti virus? local antivirus or network monitoring SIEMs can block traffic that is considered malicious

## Implement and support patch and vulnerability management

- Everything should be patched regularly(daily or weekly) and there should be a plan for immediate patching if zero day comes out.
- Look at the most concerning vulnerabilities first. look at what patches/solutions fix the most problems
- have good network segmentation. if finance department is compromised, it should be hard for the attacker to pivot to software department

## Understand and participate in change management processes

**Process**

1. Identifying a change
2. Proposing a change
3. Assessing the risk associated with the change
4. Testing the change
5. Scheduling the change
6. Notifying impacted parties of the change
7. Implementing the change
8. Reporting results of the change implementation

   **Person**

9. have closeout interview. sign NDA and other documents
10. security escort out of building
11. disable account
12. change passwords

## Implement recovery strategies

- Backup storage strategies - how often do you do full packups? incremental packups? how long do you keep these? how long does it take to restore?
- Recovery site strategies - hot, warm, cold sites. figure out what is absolutely needed when making a decision. obviously its nice to have a hot site, but is that the best for your $$$
- Multiple processing sites -
- System resilience, high availability, Quality of Service (QoS), and fault tolerance -

## Implement Disaster Recovery (DR) processes

- Response - have a fast way to analyze the issue
- Personnel - make sure trained personel are in charge and correct personel are alerted
- Communications - super hard to always update necessary personel in status of whats going on
- Assessment - assess if the current plan covers most all scenarios
- Restoration - procedure for how to recover/restore from different failures? like if HD failes?
- Training and awareness - peronsel should be properly trained and aware of what can happen

## Test Disaster Recovery Plans (DRP)

- Read-through/tabletop
- Walkthrough
- Simulation
- Parallel - test recovery of critical processing components at an alternate computing facility and recovery of system
- Full interruption - what to do if businesses is completely interrupted

## Participate in Business Continuity (BC) planning and exercises

Identitfy and prioritize critical IT systems and components. there are templates for this

## Implement and manage physical security

- Perimeter security controls - fences, cameras, guards, lights, detectors
- Internal security controls - man traps, RFID badge readers, RFID asset alarms, training, cameras, locks, and cameras

## Address personnel safety and security concerns

- Travel - what material can they cary with them? how can they safely work? safe means of travel/escape?
- Security training and awareness
- Emergency management - what to do if asset is lost? stolen? in danager?
- Duress - threats against someone to get them to do something against their better judgement

Home Page
To next domain! - D8 - Software Development Security