CISSP Domain 7 — Security Operations

Domain 7 — Security Operations

Know the "data lifecycle" phases, really a sequence and not a cycle:
Create
Store
Use
Share
Archive
Destroy

Legal

See the lists in Domain 1.

SIEM or Security Information and Event Management

- Aggregation
- Normalization
- Correlation
- Secure storage
- Analysis
- Reporting

Backups

- **Full:** All data, most expensive to collect.
- **Differential:** All data changed since the last Full. Fastest and easiest to restore: last full and last differential.
- **Incremental:** All data changed since the last Full or Incremental. Fastest to make backups. Slowest to restore: last full and all subsequent incrementals in order.

BC / DR Concepts

- Goal is usually "five nines", 99.999%, under six minutes per year
- **MAD = Maximum Allowable Downtime** — *Cannot be down longer than this. (or company fails, perhaps)*
- **RTO = Recovery Time Objective** — *We want to be back up this soon.* (significantly faster than MAD)
- **MTTR = Mean Time To Recovery** — *On average, recovery takes this long.*
- **RPO = Recovery Point Objective** — *We can afford to lose this much.*
- **MTBF = Mean Time Between Failures** — *On average, it fails this often.*
- **RSL = Recovery Service Level** — *During disaster and following recovery, we need at least this much.*

"About twice a year we have a major storage failure. We make backups nightly starting at 1 AM. Our goal is to get data restored within 1 hour. If we went 8 hours without data, our company would financially suffer. Over the past year, our data recovery process has averaged 41 minutes. While recovering one file system, we need at least 80% normal performance on the other unaffected file systems." For that story:

- MTBF = 6 months
- RPO = Within the past 24 hours
- RTO = 1 hour
- MAD = 8 hours
- MTTR = 41 minutes
- RSL = 80% or 0.8

RAID, SAN, and NAS

There's far more to RAID in reality, all you need to know is:

- **RAID 0:** Zero redundancy, striping only for performance
- **RAID 1:** One complete extra copy, mirroring.
- **RAID 5** and **RAID 6:** Combine striping and parity (redundancy) for performance and resilience. 6 has more redundancy, so it's more resilient.
- **RAID 10:** Combines RAID 0 and RAID 1 for performance and resilience.

Storage Area Network or SAN: Typically use Fibre Channel and iSCSI.

Network-Attached Storage or NAS: Typically an NFS server.

BC/DR Testing

In order of increased complexity, cost, intrusiveness, and risk:

1. Read-Through / Tabletop
2. Walk-Through
3. Simulation
4. Parallel
5. Full Interruption