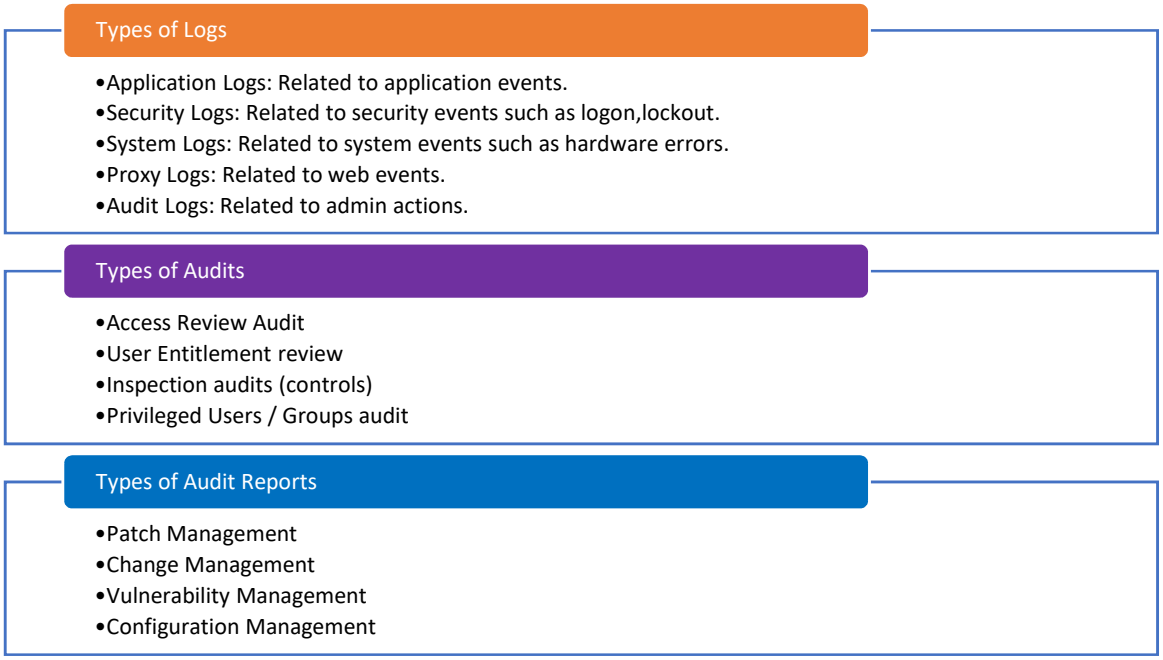
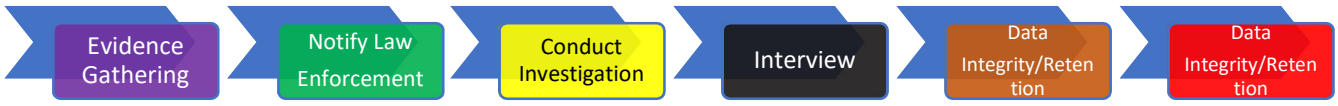
Unit 9: System Logging and Forensics

In this unit, we studied and covered the type of Logs.



We also covered the investigation process as part of Forensic Investigation techniques.



Chain of Evidence Custody

- Persons Involved (Who): All people who handled evidence.
- Description of Evidence (What)
- Location of Evidence (Where)
- Date/Time (When)
- Methods Used (How): How was it handled?

Evidence Lifecycle

- Collection & Identification
- Marked and Identified:
- Analysis
- Storage, Preservation,
- Transportation
- Presentation in Court
- Return to Victim/Owner.