JASON DION

TRAINING THE CYBER SECURITY WORKFORCE

Detecting Identity Attacks

Security Architecture & Tool Sets

Detecting Identity Attacks

- Identity and Access Management systems should be fed into the SIEM

- Configure your SIEM to detect:
  - Privileged account usage
  - Privilege changes and grants
  - Account creation or modifications
  - Terminated user account usage
  - Lifecycle management events
  - Separation of duty violations

Active Monitoring

- Knowledgeable technicians should actively monitor identity systems
- Humans should analyze reports to identify issues
- Remember, you must know what normal looks like in order to detect the abnormal