Correlation & Triaging

Duration: 1 day

- **Fundamentals of Event Correlation**
  - Purpose and benefits of correlation
  - Role in security operations
- **Correlation Techniques in SIEM**
  - Rule-based correlation
  - Behavioral correlation
  - AI-driven techniques
- **Alert Accuracy and Quality**
  - Identifying false positives and true positives
  - Strategies to reduce noise in alerts
- **Alert Prioritization**
  - Assessing severity levels
  - Evaluating business impact
  - Building effective prioritization criteria
- **Triage Techniques**
  - Manual triage process
  - Automated triage methods
  - Documentation and escalation practices