Incident Response and Digital Forensics

Provider: Google (Coursera)
Completion Date: August 3, 2025

Overview:
This course explored the fundamentals of incident response and digital forensics from a SOC analyst's perspective. It focused on identifying, analyzing, and responding to security incidents through hands-on exercises, worksheets, and playbook development. Students developed a structured approach to managing incidents and investigated potential attacks using realistic data samples.

Key Topics:

- Security alert analysis and ticket documentation
- Incident handler's responsibilities and response journal logging
- Threat modeling and forensic steps
- USB baiting and data exfiltration scenarios
- Risk-based triage and response
- Evidence handling and investigation workflow

Practical Applications:

- Developed and documented incident response plans
- Investigated mock ransomware and USB-based incidents
- Practiced log analysis and forensics data handling
- Completed a detailed analysis of data breach and alert cases

Reflection:
This course sharpened technical and procedural knowledge necessary for working within a SOC environment. The exercises in alert analysis, journaling, and mock incident triage helped reinforce the importance of traceability and response discipline. It helped bridge theoretical knowledge with real-world investigation practices.