Foundations of Cybersecurity

Provider: Google (Coursera, part of the Google Cybersecurity Certificate)
Completion Date: May 21, 2025

Overview

This course introduced the field of cybersecurity, the responsibilities of security professionals, and the core concepts for entry-level roles. It emphasized how security protects operations, ensures compliance, and maintains trust, while covering frameworks, controls, common attack types, and CISSP domains.

Key Topics Covered

- CIA Triad: confidentiality, integrity, availability
- Security roles: analyst, SOC analyst, information security specialist
- Benefits of security: compliance, continuity, trust
- Threats: internal, external, and insider risks
- Common attacks: malware, phishing, ransomware, social engineering
- Frameworks and controls: NIST, CISSP domains
- Analyst skills: communication, collaboration, problem-solving, SIEM tools
- Ethics and regulatory compliance
- Career preparation: Security+ pathway

Practical Applications

- Monitoring networks for threats and vulnerabilities
- Supporting compliance and audits
- Conducting security audits and incident response
- Using SIEM tools and forensics to investigate alerts
- Applying frameworks and controls to improve posture

Personal Reflection

This course gave me a strong foundation in cybersecurity concepts and analyst responsibilities. I learned how technical practices connect to compliance and business needs, preparing me for advanced study and certification in GRC, forensics, and secure operations.