By the end of this course, a student should be able to:

— Construct a Defense-in-Depth strategy
— Explain firewall principles and practices
— Summarize intrusion detection and prevention principles and practices
— Create bastion hosts
— Outline access control lists, authorization and authentication
— Explain the malware ecosystem

Course Outline

1. Network Defense
   1.1 Firewalls
   1.2 Proxies
   1.3 Intrusion Detection and Prevention
   1.4 Segmentation
   1.5 Demilitarized Zones
   1.6 Malware Detection and Prevention
   1.7 Content Filtering
   1.8 Event Logging
   1.9 System Auditing
2. Host Defense
   2.1 Firewalls
   2.2 Intrusion Detection and Prevention
   2.3 Malware Detection and Prevention
   2.4 Event Logging
   2.5 System Auditing
   2.6 System Service Management
   2.7 Bastion Host
3. Access Controls
   3.1 Digital Identities in Enterprise
   3.2 Authorization
   3.3 Authentication
   3.4 Rights
   3.5 Permissions
   3.6 Least Permission Principle
   3.7 Business Roles
   3.8 Separation of Duties