# CyberLMS Course Catalog

Table of Contents

CompTIA -IT Fundamentals....4
CompTIA - Network+....6
CompTIA - Security+....8
CompTIA – CASP....10
ISACA – CISM....11
ISACA – CISA....13
ISC2 – CAP....15
ISC2 – CISSP....19
ISC2 – CISSP –ISSEP....21
EC|Council - CEH....23
MTA - Windows Server....25
Cisco - CCNA....26
Kali Linux....28
Red Hat....29
Game & App Design....30
Security Awareness....31
Intro to Cybersecurity....32
Advanced Cybersecurity....33
Threats, Attacks and Vulnerabilities....34
Technologies and Tools....36
Architecture and Design....37
Identity and Access Management....38
Risk Management Framework (RMF) ....39
Intro to Cryptography....40
Public Key Infrastructure....41
EMASS....42
Windows PowerShell....43
Linux Shell Scripting....44
Mobile Apps Development....45

Mobile Forensics.....46
Python.....47
Hacking Web Servers.....48
Database Hacking.....49
Red Team / Blue Team.....50
Vulnerability Assessments.....51
Penetration Testing.....52
Azure Fundamentals.....53

# CompTIA – IT Fundamentals

**Description:**
CompTIA IT Fundamentals helps professionals to decide if a career in IT is right for them or to develop a broader understanding of IT.

**Prerequisites:**
This exam is intended for candidates who are advanced end users and/or are considering a career in IT. The exam is also a good fit for individuals interested in pursuing professional-level certifications, such as A+.

**Learning Objectives:**
The CompTIA IT Fundamentals exam focuses on the essential IT skills and knowledge needed to perform tasks commonly performed by advanced end-users and entry-level IT professionals alike, including:

- Using features and functions of common operating systems and establishing network connectivity
- Identifying common software applications and their purpose
- Using security and web browsing best practices

**NICE Framework Connections:**

- Securely Provision
- Operate and maintain
- Protect and Defend

**Knowledge Skills and Abilities (KSAs) Mapping:**
The materials within this course focus on the Knowledge Skills and Abilities (KSAs) identified within the Specialty Areas listed below. Specialty Area details within the interactive National Cybersecurity Workforce Framework.

- Risk Management
- Systems Administration
- Vulnerability Assessment and Management

**Course Outline**:

- Operating systems
- Common File Extensions
- Hardware Accessories
- Common Connector Types
- Internal Hardware Components
- Threats attacks and Vulnerabilities
- Basic Computer Hardening
- Safe Web Browsing
- How to setup a SOHO
- Data Connections
- Methods of Sharing and Storage
- Setting up a workstation
- OS Navigation
- Basic Troubleshooting
- Intro to Databases
- Data Backups
- Exam info

# CompTIA – Network+

**Description:**
CompTIA Network+ helps develop a career in IT infrastructure covering troubleshooting, configuring, and managing networks.

**Prerequisites:**
Network+ ensures an IT professional has the knowledge and skills to:

- Design and implement functional networks
- Configure, manage, and maintain essential network devices
- Use devices such as switches and routers to segment network traffic and create resilient networks
- Identify benefits and drawbacks of existing network configurations
- Implement network security, standards, and protocols
- Troubleshoot network problems
- Support the creation of virtualized networks

**Learning Outcomes:**

- **Networking Concepts**
  Explain the purpose of a variety of networking concepts and implement them appropriately
- **Infrastructure**
  Determine & explain the appropriate cabling, device and storage technologies
- **Network Operations**
  Use best practices to manage the network, determine policies & ensure business continuity
- **Network Security**
  Summarize physical security & common attacks while securing the wired and wireless network
- **Network Troubleshooting & Tools**
  Explain the network troubleshooting methodology & appropriate tools to support connectivity & performance

**NICE Framework Connections:**

- Securely Provision
- Operate and maintain
- Protect and Defend

**Knowledge Skills and Abilities (KSAs) Mapping:**
The materials within this course focus on the Knowledge Skills and Abilities (KSAs) identified within the Specialty Areas listed below. Specialty Area details within the interactive National Cybersecurity Workforce Framework.

- Risk Management
- Systems Administration
- Vulnerability Assessment and Management

**Course Outline**:

- Network Concepts
- Network Operations
- Network Security
- Troubleshooting
- Infrastructure
- TCP IP and OSI Model
- Common Ports
- Switches
- Routers
- Router Definitions
- Routing Details
- Firewalls
- Stateful Packet Inspection
- VPN

# CompTIA – Security+

**Description:**
CompTIA Security+ is a global certification that validates the baseline skills you need to perform core security functions and pursue an IT security career.

**Prerequisites:**
Network+, IT Fundamentals

**Learning Outcomes:**

- No other certification that assesses baseline cybersecurity skills has performance-based questions on the exam. Security+ emphasizes hands-on practical skills, ensuring the security professional is better prepared to problem solve a wider variety of issues.
- More choose Security+ for DoD 8570 compliance than any other certification.
- Security+ focuses on the latest trends and techniques in risk management, risk mitigation, threat management and intrusion detection.
- The new Security+ certification covers the Junior IT Auditor/Penetration Tester job role, in addition to the previous job roles for Systems Administrator, Network Administrator, and Security Administrator.

**NICE Framework Connections:**

- Securely Provision
- Operate and maintain
- Protect and Defend

**Knowledge Skills and Abilities (KSAs) Mapping:**
The materials within this course focus on the Knowledge Skills and Abilities (KSAs) identified within the Specialty Areas listed below. Specialty Area details within the interactive National Cybersecurity Workforce Framework.

- Risk Management
- Systems Administration
- Vulnerability Assessment and Management

**Course Outline**:

- Threats, Attacks, and Vulnerabilities
- Tech and Tools
- Architecture and Design
- Identity and Access Management
- Risk Management
- TCP IP and OSI Model
- Crypto and PKI

# CompTIA – CASP

**Description:**
CompTIA Advanced Security Practitioner (CASP+) is the ideal certification for technical professionals who wish to remain immersed in technology, as opposed to strictly managing.

**Prerequisites:**
A minimum of ten years of experience in IT administration, including at least five years of hands-on technical security experience.

**Learning Outcomes:**

CASP+ covers the technical knowledge and skills required to conceptualize, engineer, integrate and implement secure solutions across complex environments to support a resilient enterprise.

**NICE Framework Connections:**

- Securely Provision
- Operate and maintain
- Protect and Defend

**Knowledge Skills and Abilities (KSAs) Mapping:**
The materials within this course focus on the Knowledge Skills and Abilities (KSAs) identified within the Specialty Areas listed below. Specialty Area details within the interactive National Cybersecurity Workforce Framework.

- Risk Management
- Systems Administration
- Vulnerability Assessment and Management

**Course Outline**:

- Risk Management
- Enterprise Security Architecture
- Enterprise Security Operations – Deter & Delay
- Technical Integration of Enterprise Security - IAAA
- Research, Development and System Maintenance

# ISACA – CISM

**Description:**
ISACA - CISM certification indicates expertise in information security governance, program development and management, incident management and risk management. Take your career out of the technical realm to management.

**Prerequisites:**
CEH
ISSEP

**Learning Outcomes:**
This course is designed to provide management and other professionals with a basic understanding of the domains associated with the CISM certification

- Information Security Governance
- Information Risk Management
- Information Security Program development & management
- Information Security Incident Management

**NICE Framework Connections:**

- Securely Provision
- Operate and maintain
- Protect and Defend
- Oversee and Govern

**Knowledge Skills and Abilities (KSAs) Mapping:**
The materials within this course focus on the Knowledge Skills and Abilities (KSAs) identified within the Specialty Areas listed below. Specialty Area details within the interactive National Cybersecurity Workforce Framework.

- Risk Management
- Software Development
- Systems Administration
- Vulnerability Assessment and Management
- Systems Analysis
- Cybersecurity Management
- Program/Project Management and Acquisition

**Course Outline**:

- Information Security Governance
- Information Risk Management
- Information Security Program Development
- Incident Management and Response

# ISACA – CISA

**Description:**
ISACA's Certified Information Systems Auditor (CISA) certification is world-renowned as the standard of achievement for those who audit, control, monitor and assess an organization's information technology and business systems.

**Prerequisites:**
CEH
ISSEP

**Learning Outcomes:**
This course is designed to provide management and other professionals with a basic understanding of the domains associated with the CISA certification

- Information Systems Auditing Process
- Governance and Management of IT
- Information Systems Acquisition, Development, and Implementation
- Information Systems Operations and Business Resilience
- Protection of Information Assets

**NICE Framework Connections:**

- Securely Provision
- Operate and maintain
- Protect and Defend
- Oversee and Govern

**Knowledge Skills and Abilities (KSAs) Mapping:**
The materials within this course focus on the Knowledge Skills and Abilities (KSAs) identified within the Specialty Areas listed below. Specialty Area details within the interactive National Cybersecurity Workforce Framework.

- Risk Management
- Software Development
- Systems Administration
- Vulnerability Assessment and Management
- Systems Analysis
- Cybersecurity Management
- Program/Project Management and Acquisition

**Course Outline**:

- Information Systems Auditing Process
- Governance and Management of IT
- Information Systems Acquisition, Development, and Implementation
- Information Systems Operations and Business Resilience

# ISC² – CAP

**Description:**

ISC2 - CAP is the only certification under the DoD8570 mandate that aligns with each RMF step. It shows employers you have the advanced technical skills and knowledge to authorize and maintain information systems within the RMF using best practices, policies and procedures.

**Prerequisites:**

Earning the CAP certification is a proven way to build your career and demonstrate your expertise within the risk management framework (RMF). The CAP is the only certification under the DoD8570 mandate that aligns with each RMF step. It shows employers you have the advanced technical skills and knowledge to authorize and maintain information systems within the RMF using best practices, policies and procedures established by the cybersecurity experts at (ISC)².

**Learning Outcomes:**

The CAP is ideal for IT, information security, and information assurance practitioners and contractors who use the RMF in: The U.S. federal government, such as the U.S. Department of State or Department of Defense The military Civilian roles, such as federal contractors Local governments Private sector organizations

**NICE Framework Connections:**

- Securely Provision
- Operate and maintain
- Protect and Defend
- Oversee and Govern

**Knowledge Skills and Abilities (KSAs) Mapping:**

The materials within this course focus on the Knowledge Skills and Abilities (KSAs) identified within the Specialty Areas listed below. Specialty Area details within the interactive National Cybersecurity Workforce Framework.

- Risk Management
- Software Development
- Systems Administration
- Vulnerability Assessment and Management
- Systems Analysis
- Cybersecurity Management
- Program/Project Management and Acquisition

**Course Outline**:

- Risk Management Framework Lifecycle
- RMF Process
- Selection of Security Controls with eMASS
- Implementation of Security Controls – Tools
- Assessing with the Utility Belt
- Authorization of Information Systems
- Continuous Monitoring

# ISC$^2$ – CISSP

**Description:**

ISC2 - CISSP - Earning the CISSP proves you have what it takes to effectively design, implement and manage a best-in-class cybersecurity program. With a CISSP, you validate your expertise, unlocking a broad array of exclusive resources, educational tools, and peer-to-peer networking opportunities.

**Prerequisites:**

The CISSP is ideal for experienced security practitioners, managers and executives interested in proving their knowledge across a wide array of security practices and principles, including those in the following positions: Chief Information Security Officer Chief Information Officer Director of Security IT Director/Manager Security Systems Engineer Security Analyst Security Manager Security Auditor Security Architect Security Consultant Network Architect

**Learning Outcomes:**

Accelerate your cybersecurity career with the CISSP certification. Earning the CISSP proves you have what it takes to effectively design, implement and manage a best-in-class cybersecurity program. With a CISSP, you validate your expertise and become an (ISC)$^2$ member, unlocking a broad array of exclusive resources, educational tools, and peer-to-peer networking opportunities. Prove your skills, advance your career, and gain the support of a community of cybersecurity leaders here to support you throughout your career

**NICE Framework Connections:**

- Securely Provision
- Operate and maintain
- Protect and Defend
- Oversee and Govern

**Knowledge Skills and Abilities (KSAs) Mapping:**

The materials within this course focus on the Knowledge Skills and Abilities (KSAs) identified within the Specialty Areas listed below. Specialty Area details within the interactive National Cybersecurity Workforce Framework.

- Risk Management
- Systems Analysis
- Vulnerability Assessment and Management

- Cybersecurity Management
- Program/Project Management and Acquisition

**Course Outline**:

- Security and Risk Management
- Asset Security
- Asset Security - Intellectual Property
- Security Architecture and Engineering
- Security Architecture and Engineering - Models
- Network Security - Architecture and Design
- Network Security - EAP PEAP LEAP
- Identity and Access Management (IAM) - Active Directory
- Identity and Access Management (IAM) - IAAA
- Identity and Access Management (IAM) - Principle of Least Privilege
- Identity and Access Management (IAM) - Provisioning Accounts
- Identity and Access Management (IAM) - RBAC
- Identity and Access Management (IAM) - Federation
- Security Assessment and Testing
- Security Assessment and Testing - Types
- Security Operations - Defense in Depth
- Security Operations - HIDS vs. NIDS
- Software Development Security
- Software Development Security - Methods

# ISC² - CISSP – ISSEP

**Description:**

ISC2 - CISSP - ISSEP is the security engineering certification that recognizes your keen ability to practically apply systems engineering principles and processes to develop secure systems. You have the knowledge and skills to incorporate security into projects, applications, business processes and all information systems.

**Prerequisites:**

This security engineering certification is an excellent way to hone your craft. But is it right for you? You're a great fit for the CISSP-ISSEP if you: Are a life-long learner who craves a new challenge. Want to go beyond the CISSP. You have a competitive spirit and want to stand out from your peers. Want to be seen as a subject matter expert and prove your knowledge in a more focused area. Are looking ahead in your career. The CISSP-ISSEP will help you achieve an even higher level of success. Need this concentration to move into a specific job. The CISSP-ISSEP is ideal for those working in roles such as: Senior systems engineer Information assurance systems engineer Information assurance officer Information assurance analyst Senior security analyst

**Learning Outcomes:**

You're on the leading edge of your craft. Here are just a few reasons to challenge yourself with this security certification: A demonstration of excellence. You want to stand out from your fellow CISSPs. This concentration proves you have an elite level of knowledge and expertise. New opportunities. The CISSP-ISSEP opens doors: from new career paths and jobs, to more exciting work. Growth and learning. This is an opportunity to dive deep and hone your craft. You'll find new ways to grow and stay on the forefront of information security. And earning your concentration is a big challenge. Ease of continuing education and dues. As a CISSP, you already have a relationship with (ISC)². If you earn the CISSP-ISSEP, you only have to share your Continuing Professional Education (CPE) credits with one organization. You may apply your CISSP-ISSEP CPE credits toward your CISSP requirement (as long as these credits are specific to security engineering). And your dues are a lot less than if you pursue an advanced certification with a separate organization. You'll make great use of your time, energy and money.

**NICE Framework Connections:**

- Securely Provision
- Operate and maintain
- Protect and Defend
- Oversee and Govern

**Knowledge Skills and Abilities (KSAs) Mapping:**
The materials within this course focus on the Knowledge Skills and Abilities (KSAs) identified within the Specialty Areas listed below. Specialty Area details within the interactive National Cybersecurity Workforce Framework.

- Risk Management
- Systems Analysis
- Vulnerability Assessment and Management
- Cybersecurity Management
- Program/Project Management and Acquisition

**Course Outline**:

- Security Engineering Principles
- Risk Management
- Security Planning, Design, and Implementation
- Secure Planning, Design, and Implementation
- Security Architecture and Engineering - Models
- Network Security - Architecture and Design

# EC|Council – CEH

**Description:**

EC|Council - CEH is the most comprehensive ethical hacking course on the globe to help information security professionals grasp the fundamentals of ethical hacking.

**Prerequisites:**

The course outcome helps you become a professional who systematically attempts to inspect network infrastructures with the consent of its owner to find security vulnerabilities which a malicious hacker could potentially exploit. The course helps you assess the security posture of an organization by identifying vulnerabilities in the network and system infrastructure to determine if unauthorized access is possible. The CEH is the first of a series of 3 comprehensive courses (CEH, ECSA and the APT course) to help a cyber security professional master penetration testing.

**Learning Outcomes:**

The Purpose of the CEH credential is to: Establish and govern minimum standards for credentialing professional information security specialists in ethical hacking measures. Inform the public that credentialed individuals meet or exceed the minimum standards. Reinforce ethical hacking as a unique and self-regulating profession.

**NICE Framework Connections:**

- Securely Provision
- Operate and maintain
- Protect and Defend
- Oversee and Govern

**Knowledge Skills and Abilities (KSAs) Mapping:**

The materials within this course focus on the Knowledge Skills and Abilities (KSAs) identified within the Specialty Areas listed below. Specialty Area details within the interactive National Cybersecurity Workforce Framework.

- Risk Management
- Systems Analysis
- Vulnerability Assessment and Management
- Cybersecurity Management
- Program/Project Management and Acquisition

**NICE Framework Connections:**

- Securely Provision
- Operate and maintain
- Protect and Defend
- Oversee and Govern

**Knowledge Skills and Abilities (KSAs) Mapping:**

The materials within this course focus on the Knowledge Skills and Abilities (KSAs) identified within the Specialty Areas listed below. Specialty Area details within the interactive National Cybersecurity Workforce Framework.

- Risk Management
- Systems Analysis
- Vulnerability Assessment and Management
- Cybersecurity Management
- Program/Project Management and Acquisition

# MTA - Windows Server

**Description:**
MTA - Windows Server is a great place to start if you would like to get into the technology field. MTA certifications address a wide spectrum of fundamental technical concepts, assess and validate core technical knowledge, and enhance technical credibility.

**Prerequisites:**
MTA certifications are a great place to start if you would like to get into the technology field. MTA certifications address a wide spectrum of fundamental technical concepts, assess and validate core technical knowledge, and enhance technical credibility. Note: MTA exams do not qualify for MCP certification, nor are they a prerequisite for MCSA or MCSD certification.

**Learning Outcomes:**
Get hired, demonstrate clear business impact, and advance your skills. Microsoft offers a wide range of online certification programs designed to take your career to the next level.

**NICE Framework Connections:**

- Securely Provision
- Operate and maintain
- Protect and Defend

**Knowledge Skills and Abilities (KSAs) Mapping:**
The materials within this course focus on the Knowledge Skills and Abilities (KSAs) identified within the Specialty Areas listed below. Specialty Area details within the interactive National Cybersecurity Workforce Framework.

- Risk Management
- Systems Analysis
- Vulnerability Assessment and Management

**Course Outline**:

- Understanding Server Installation
- Understanding Active Directory
- Understanding Server Roles
- Understanding Storage
- Understanding Server Performance and Management
- Understanding Server Maintenance

# Cisco – CCNA

**Description:**

Cisco - CCNA certification will not only prepare you with the knowledge of foundational technologies, but ensure you stay relevant with skill sets needed for the adoption of next generation technologies.

**Prerequisites:**

As Enterprises migrate toward controller based architectures, the role and skills required of a core network engineer are evolving and more vital than ever. To prepare for this network transition, the CCNA Routing and Switching certification will not only prepare you with the knowledge of foundational technologies, but ensure you stay relevant with skill sets needed for the adoption of next generation technologies.

**Learning Outcomes:**

This exam tests a candidate's knowledge and skills related to: Network fundamentals LAN switching technologies IPv4 and IPv6 routing technologies WAN technologies Infrastructure services Infrastructure security Infrastructure management.

**NICE Framework Connections:**

- Securely Provision
- Operate and maintain
- Protect and Defend

**Knowledge Skills and Abilities (KSAs) Mapping:**

The materials within this course focus on the Knowledge Skills and Abilities (KSAs) identified within the Specialty Areas listed below. Specialty Area details within the interactive National Cybersecurity Workforce Framework.

- Risk Management
- Systems Analysis
- Vulnerability Assessment and Management

# Kali Linux – Basics

**Description:**
Kali Linux - Basics introduces the Kali Linux penetration testing platform. After taking this course you can demonstrate a thorough understanding of the Kali Linux operating system.

**Prerequisites:**
Understanding of Linux and command line interface (CLI) would be very helpful

**Learning Outcomes:**
Intro to Kali Linux is an online, self-paced course designed for penetration testers and security professionals who want to advance in the world of professional pentesting. This course is designed to provide professionals the knowledge and skills that hackers use to target systems so that they can work legally and ethically to improve security systems.

**NICE Framework Connections:**

- Securely Provision
- Operate and maintain
- Protect and Defend

**Knowledge Skills and Abilities (KSAs) Mapping:**
The materials within this course focus on the Knowledge Skills and Abilities (KSAs) identified within the Specialty Areas listed below. Specialty Area details within the interactive National Cybersecurity Workforce Framework.

- Risk Management
- Systems Analysis
- Vulnerability Assessment and Management

**Course Outline**:

- History
- Downloading Kali
- Firing it Up
- Main uses of Kali
- Linux Basics
- Basic Commands
- Help! I need someone
- Users and Groups
- Managing File Permissions
- Account Management
- So you want to be a hacker huh?

# Introduction to Red Hat

**Description:**

Introduction to Red Hat takes a peek at one of the leading enterprise Linux platform. We will teach the foundation from which you can scale existing apps and roll out emerging technologies across bare-metal, virtual, container, and all types of cloud environments.

**Prerequisites:**

basic Linux experience and command line interface (CLI) experience would be helpful.

**Learning Outcomes:**

As IT systems and workloads get more complex, the underlying architecture and operating system must be reliable, scalable, and performance driven. Linux is the stable foundation for all IT workloads and deployments—whether traditional or innovative—from bare metal to virtual, cloud, and containers.

**NICE Framework Connections:**

- Securely Provision
- Operate and maintain
- Protect and Defend

**Knowledge Skills and Abilities (KSAs) Mapping:**

The materials within this course focus on the Knowledge Skills and Abilities (KSAs) identified within the Specialty Areas listed below. Specialty Area details within the interactive National Cybersecurity Workforce Framework.

- Risk Management
- Systems Analysis
- Vulnerability Assessment and Management

**Course Outline**:

# Game Development

**Description:**
Game Design course offers an introduction to the primary concepts of gaming, and an exploration of how these basic concepts affect the way gamers interact with games.

**Prerequisites:**

- Basic computing skills.
- Ability to follow directions.

**Learning Outcomes:**
You will learn an introduction to the primary concepts of how to create games

**NICE Framework Connections:**

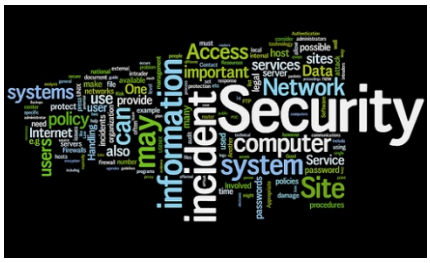
- Securely Provision
- Operate and maintain
- Protect and Defend

**Knowledge Skills and Abilities (KSAs) Mapping:**
The materials within this course focus on the Knowledge Skills and Abilities (KSAs) identified within the Specialty Areas listed below. Specialty Area details within the interactive National Cybersecurity Workforce Framework.

- Risk Management
- Systems Analysis
- Vulnerability Assessment and Management

**Course Outline**:

- Setup
- Creating a Character




# Security Awareness Fundamentals

**Description:**

Security Awareness Fundamentals is a mix of end user training content that addresses relevant threats and teaches security concepts that are critical to your workplace.

**Prerequisites:**

- None

**Learning Outcomes:**

Our security awareness training for employees will help you build a powerful cyber security program that focuses on your organization's needs and learning levels.

**NICE Framework Connections:**

- Securely Provision
- Operate and maintain
- Protect and Defend

**Knowledge Skills and Abilities (KSAs) Mapping:**

The materials within this course focus on the Knowledge Skills and Abilities (KSAs) identified within the Specialty Areas listed below. Specialty Area details within the interactive National Cybersecurity Workforce Framework.

- Risk Management
- Systems Administration
- Vulnerability Assessment and Management

**Course Outline**:

- Security is a Big Responsibility
- Who are the Hackers?
- Social Engineering
- Types of Malware
- Beware of Phishing Emails
- What's the Worst that could Happen?
- Detecting Attacks

# Introduction to Cybersecurity

**Description:**
Introduction to Cybersecurity provides a broad overview of key cybersecurity concepts and practices and broadly characterizes the organizational security landscape.

**Prerequisites:**

- None

**Learning Outcomes:**
Key cybersecurity concepts and practices and broadly characterizes the organizational security landscape.

**NICE Framework Connections:**

- Securely Provision
- Operate and maintain
- Protect and Defend

**Knowledge Skills and Abilities (KSAs) Mapping:**
The materials within this course focus on the Knowledge Skills and Abilities (KSAs) identified within the Specialty Areas listed below. Specialty Area details within the interactive National Cybersecurity Workforce Framework.

- Risk Management
- Systems Administration
- Vulnerability Assessment and Management

**Course Outline**:

- Cybersecurity Basics
- CIA Trad
- Cybersecurity Framework
- Roles and Responsibilities
- Intro to Social Engineering
- Attack Vectors
- Network Defense

# Advanced Cybersecurity

**Description:**
Advanced Cybersecurity course includes security architecture, cryptographic systems, security protocols, and security management tools.

**Prerequisites:**
- Introduction to Cybersecurity

**Learning Outcomes:**
Subjects in this course include virus and worm propagation, malicious software scanning, cryptographic tools, intrusion detection, DoS, firewalls, best practices, and policy management.

**NICE Framework Connections:**
- Securely Provision
- Operate and maintain
- Protect and Defend
- Oversee and Govern

**Knowledge Skills and Abilities (KSAs) Mapping:**
The materials within this course focus on the Knowledge Skills and Abilities (KSAs) identified within the Specialty Areas listed below. Specialty Area details within the interactive National Cybersecurity Workforce Framework.

- Risk Management
- Systems Administration
- Vulnerability Assessment and Management
- Program/Project Management and Acquisition

**Course Outline**:
- Roles and Responsibilities
- Risk Assessments
- Business Impact Analysis
- Asset Security
- IAAA(Identification, Authentication, Authorization and Accountability)
- Why is Active Directory so Important?
- Account Management
- Practice the Principle of Least Privilege
- Role Based Access Control
- Hot, Warm, Cold Sites
- Cloud as A Service
- HIDS vs. NIDS
- Digital Forensics and Incident Response
- Advanced Persistent Threats
- Intro to SQL and Webservers
- Secure Remote Connections – IPSEC

## Threats, Attacks and Vulnerabilities

**Description:**
Threats, Attacks and Vulnerabilities course provides an overview of networks, and then move to network attacks, such as Denial-of-service attacks.
**Prerequisites:**
Introduction to Cybersecurity

**Learning Outcomes:**
This course is designed to provide management and other professionals an understanding of the vulnerabilities in information systems, to better prepare them to mitigate attacks.

- Basics of Threats, Vulnerabilities, and Attacks
- Network security Concerns
- Network Reconnaissance Attacks
- Network Access Attacks
- DoS and DDoS
- Malware Attacks
- Viruses

**NICE Framework Connections:**

- Securely Provision
- Operate and maintain
- Protect and Defend

**Knowledge Skills and Abilities (KSAs) Mapping:**
The materials within this course focus on the Knowledge Skills and Abilities (KSAs) identified within the Specialty Areas listed below. Specialty Area details within the interactive National Cybersecurity Workforce Framework.

- Risk Management
- Systems Analysis
- Vulnerability Assessment and Management

**Course Outline**:

- Vulnerabilities, Threats, & Attacks oh my!
- Threats and Vulnerabilities
- Threat Agents of Today
- Attack Vectors
- Types of Malware
- Trojans and Backdoors
- Adware, Ransomware, and Logic Bombs
- Application Attacks
- Botnets, Ransomware, and Rootkits
- Zombies and Botnets
- Service Request Flood
- SYN Flood Attack
- MITM Attacks
- Social Engineering
- Mitigation

# Technologies and Tools

**Description:**
Technologies and Tools course will help you to understand what the tools and tech security engineers typically know to perform their job.

**Prerequisites:**
Introduction to Cybersecurity

**Learning Outcomes:**
Students will learn various tools that are common in the cybersecurity workforce

**NICE Framework Connections:**

- Securely Provision
- Operate and maintain
- Protect and Defend

**Knowledge Skills and Abilities (KSAs) Mapping:**
The materials within this course focus on the Knowledge Skills and Abilities (KSAs) identified within the Specialty Areas listed below. Specialty Area details within the interactive National Cybersecurity Workforce Framework.

- Risk Management
- Systems Analysis
- Vulnerability Assessment and Management

**Course Outline**:

- Hubs
- Switches get stiches..
- Router Basics
- Router Definition
- Firewalls
- Stateful Packet Inspection and NAT
- Virtual Private Network
- Detecting Malware with Netstat
- Detecting Virus TCPView
- Netcat

# Architecture and Design

**Description:**
Architecture and Design course will help you to understand what the fundamentals of enterprise architecture and design that security engineers typically know to perform their job.

**Prerequisites:**
Introduction to Cybersecurity

**Learning Outcomes:**
Fundamentals concepts of enterprise architecture

**NICE Framework Connections:**

- Securely Provision
- Operate and maintain
- Protect and Defend

**Knowledge Skills and Abilities (KSAs) Mapping:**
The materials within this course focus on the Knowledge Skills and Abilities (KSAs) identified within the Specialty Areas listed below. Specialty Area details within the interactive National Cybersecurity Workforce Framework.

- Risk Management
- Systems Analysis
- Vulnerability Assessment and Management

**Course Outline**:

- Defense in Depth Approach
- Physical Security Control
- Cyber Frameworks to Live By
- Law, Directives and Regulations
- Due Care vs. Due Diligence
- Privacy
- Hardening the Enterprise
- Web Applications
- Cloud Computing
- Applying Controls

# Identity and Access Management

**Description:**
Identity and Access Management course will help you to understand what identity and access management vernacular security engineers typically know to perform their job.

**Prerequisites:**
Introduction to Cybersecurity

**Learning Outcomes:**
Topics like Active Directory, X.500, Federation and other will be covered in this course.

**NICE Framework Connections:**

- Securely Provision
- Operate and maintain
- Protect and Defend

**Knowledge Skills and Abilities (KSAs) Mapping:**
The materials within this course focus on the Knowledge Skills and Abilities (KSAs) identified within the Specialty Areas listed below. Specialty Area details within the interactive National Cybersecurity Workforce Framework.

- Risk Management
- Systems Analysis
- Vulnerability Assessment and Management

**Course Outline**:

- What is Identity Management
- Multifactor Authentication
- Principle of Least Privilege
- Single Sign-On (SSO)
- Federations
- Directory Servers
- Authentication Protocols
- Account Management

Risk Management Framework

# Risk Management Framework (RMF)

**Description:**
Risk Management Framework (RMF) training program is suitable for DoD employees and contractors.

**Prerequisites:**
None

**Learning Outcomes:**
his program includes comprehensive coverage on policy background, roles and responsibilities, lifecycle process, security controls/assessment and documentation.

**NICE Framework Connections:**

- Securely Provision
- Operate and maintain
- Oversee and Govern

**Knowledge Skills and Abilities (KSAs) Mapping:**
The materials within this course focus on the Knowledge Skills and Abilities (KSAs) identified within the Specialty Areas listed below. Specialty Area details within the interactive National Cybersecurity Workforce Framework.

- Risk Management
- Systems Analysis
- Program/Project Management and Acquisition

**Course Outline**:

- RMF and eMASS Overview
- Building your Utility Belt
- Practical Exercise
- RMF Lifecycle
- RMF Process
- eMASS Intro
- Tools and Techniques
- POAM

# Introduction to Cryptography

**Description:**
Introduction to Cryptography course introduces the concepts of modern cryptography.

**Prerequisites:**
None

**Learning Outcomes:**
We cover planning and managing system security within a TCP/IP network environment. Key topics include security architecture, cryptographic systems, security protocols, and security management tools.

**NICE Framework Connections:**

- Securely Provision
- Protect and Defend

**Knowledge Skills and Abilities (KSAs) Mapping:**
The materials within this course focus on the Knowledge Skills and Abilities (KSAs) identified within the Specialty Areas listed below. Specialty Area details within the interactive National Cybersecurity Workforce Framework.

- Risk Management
- Systems Development
- Systems Requirements Planning
- Systems Architecture
- Vulnerability Assessment and Management

**Course Outline**:

- Cryptography Overview
- Symmetric Cryptography
- Asymmetric Cryptography
- Hash Functions
- Perfect Forward Secrecy
- Stream and Block Ciphers
- Substitution vs Transposition
- Steganography

# Public Key Infrastructure

**Description:**
Public Key Infrastructure course focuses on providing students with the knowledge and skills to understand public key infrastructure (PKI) on windows servers to support applications that require certificate based security.

**Prerequisites:**
Windows Server, Identity Management, X.500, X.509

**Learning Outcomes:**
Understanding of PKI concepts and ability to communicate effectively about PKI.

**NICE Framework Connections:**

- Securely Provision
- Protect and Defend

**Knowledge Skills and Abilities (KSAs) Mapping:**
The materials within this course focus on the Knowledge Skills and Abilities (KSAs) identified within the Specialty Areas listed below. Specialty Area details within the interactive National Cybersecurity Workforce Framework.

- Risk Management
- Systems Development
- Systems Requirements Planning
- Systems Architecture
- Vulnerability Assessment and Management

**Course Outline**:

- Certificates
- Trust Models
- Revocation and Expiration
- X.500 vs. X.509
- How PKI ties it all together

# eMASS

**Description:**
eMASS course is a top-rated course and is open to all students (government and contractors) with interest in eMASS.

**Prerequisites:**
Our eMASS course includes simulations of eMASS, and learners are not required to have an eMASS account, or even a DoD Common Access Card (CAC), to attend.

**Learning Outcomes:**
Students will learn how to use eMASS

**NICE Framework Connections:**

- Securely Provision
- Operate and maintain
- Oversee and Govern

**Knowledge Skills and Abilities (KSAs) Mapping:**
The materials within this course focus on the Knowledge Skills and Abilities (KSAs) identified within the Specialty Areas listed below. Specialty Area details within the interactive National Cybersecurity Workforce Framework.

- Risk Management
- Systems Administration
- Program/Project Management and Acquisition

**Course Outline**:

- eMASS overview
- System Registration and Categorization
- Implementing Security Controls
- RMF and FEDRAMP
- Continuous Monitoring
- Important Controls for Azure

# Introduction to PowerShell

**Description:**
Introduction to PowerShell course is aimed at complete beginners who have never programmed before, as well as existing programmers who want to increase their career options by learning PowerShell.

**Prerequisites:**
None

**Learning Outcomes:**
Students will learn PowerShell basics and understand capabilities in PowerShell

**NICE Framework Connections:**

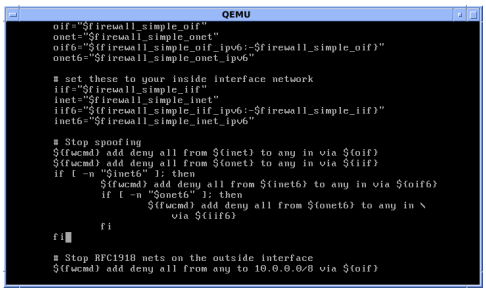
- Securely Provision
- Operate and Maintain
- Protect and Defend

**Knowledge Skills and Abilities (KSAs) Mapping:**
The materials within this course focus on the Knowledge Skills and Abilities (KSAs) identified within the Specialty Areas listed below. Specialty Area details within the interactive National Cybersecurity Workforce Framework.

- Risk Management
- Systems Development
- Systems Administration
- Vulnerability Assessment and Management

**Course Outline**:

- PowerShell Introductions
- Variables
- Padding and Decimal Precision
- Manipulating Dates and Times
- Loops and Logic/ For Each and If Then
- Gathering Computer Info
- Get Process and Apps
- Power Ping and Pop Up Scripts




# Shell Scripting

**Description:**
This course introduces the student to shell scripting in the Linux environment. Shell Scripting is a computer program designed to be run by the Linux shell. A shell is a command-line interpreter and typical operations performed by shell scripts include file manipulation, program execution, and printing text.

**Prerequisites:**
None

**Learning Outcomes:**

- Shell Scripting Basics
- Scripting Troubleshooting Techniques

**NICE Framework Connections:**

- Operate and maintain

**Knowledge Skills and Abilities (KSAs) Mapping:**
The materials within this course focus on the Knowledge Skills and Abilities (KSAs) identified within the Specialty Areas listed below. Specialty Area details within the interactive National Cybersecurity Workforce Framework.

- Systems Administration

**Course Outline**:

- Shell Scripting Overview
- Putty and SSH
- Intro to Linux
- Setting up WinSCP

# Mobile Forensics

**Description:**
Digital Forensics course teaches the basics for collecting digital evidence.

**Prerequisites:**
None

**Learning Outcomes:**
Students will learn how to develop a sterile virtual lab environment, collect of digital evidence, provide digital evidence analytics, analyze log data, touches on analysis and reversing of malware, ; recover damaged digital evidence, write technical reports on malware and incidents and lastly look at the legal and ethical components of digital forensic science.

**NICE Framework Connections:**

- Securely Provision
- Operate and Maintain
- Protect and Defend

**Knowledge Skills and Abilities (KSAs) Mapping:**
The materials within this course focus on the Knowledge Skills and Abilities (KSAs) identified within the Specialty Areas listed below. Specialty Area details within the interactive National Cybersecurity Workforce Framework.

- Risk Management
- Systems Development
- Systems Administration
- Vulnerability Assessment and Management

**Course Outline**:

- Mobile Forensics Overview
- Basic Steps
- Introduction to Digital Evidence
- Introduction to Documentation
- Introduction to Investigations
- Legal Aspects

# Python

**Description:**
Python course is aimed at complete beginners who have never programmed before, as well as existing programmers who want to increase their career options by learning Python.

**Prerequisites:**
None

**Learning Outcomes:**
Students will learn basic Python programming.

**NICE Framework Connections:**

- Securely Provision
- Operate and Maintain
- Protect and Defend

**Knowledge Skills and Abilities (KSAs) Mapping:**
The materials within this course focus on the Knowledge Skills and Abilities (KSAs) identified within the Specialty Areas listed below. Specialty Area details within the interactive National Cybersecurity Workforce Framework.

- Risk Management
- Systems Development
- Systems Administration
- Vulnerability Assessment and Management

**Course Outline**:

- Intro to Python
- Python for Cyber
- If Then Statements
- Using Lists

# Hacking Web Servers

**Description:**
Hacking Web Servers course covers all important hacking techniques used by hackers and system administrators for hacking web servers.

**Prerequisites:**
Experience with Web Servers and Databases would be helpful

**Learning Outcomes:**
This course is designed to provide professionals the knowledge and skills that hackers use to target systems so that they can work legally and ethically to improve security systems. Students will also learn the basics of SQL Injection, XSS, CSRF

**NICE Framework Connections:**

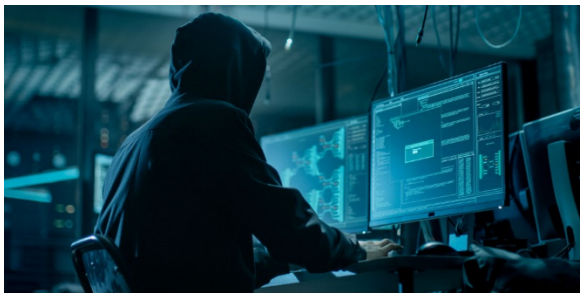
- Securely Provision
- Operate and Maintain
- Protect and Defend
- Oversee and Govern

**Knowledge Skills and Abilities (KSAs) Mapping:**
The materials within this course focus on the Knowledge Skills and Abilities (KSAs) identified within the Specialty Areas listed below. Specialty Area details within the interactive National Cybersecurity Workforce Framework.

- Risk Management
- Network Services
- Systems Analysis
- Vulnerability Assessment and Management
- Program/Project Management and Acquisition

**Course Outline**:

- Hacking Web Servers
- Cloud As A Service
- Into to SQL
- Footprinting and Recon
- Google Hacking Techniques
- Footprinting using Netcraft
- System Hacking Passwords
- Application Attacks
- Types of Password Attacks
- Why use SFTP and not TFTP
- Parameter Tampering
- Hacking Consequences



# Database Hacking

**Description:**
Database Hacking course covers all important hacking techniques used by hackers and system administrators for hacking databases servers.

**Prerequisites:**
Some experience with Web Servers and Databases would be helpful

**Learning Outcomes:**
This course is designed to provide professionals the knowledge and skills that hackers use to target systems so that they can work legally and ethically to improve security systems. Students will learn how common attacks are made on Databases.

**NICE Framework Connections:**

- Securely Provision
- Operate and Maintain
- Protect and Defend
- Oversee and Govern

**Knowledge Skills and Abilities (KSAs) Mapping:**
The materials within this course focus on the Knowledge Skills and Abilities (KSAs) identified within the Specialty Areas listed below. Specialty Area details within the interactive National Cybersecurity Workforce Framework.

- Risk Management
- Network Services
- Systems Analysis
- Vulnerability Assessment and Management
- Program/Project Management and Acquisition

**Course Outline**:

- Understanding Relational Databases
- Flaw Hypothesis Methodology
- Taxonomy and Genesis of Programming Flaws
- Malicious/Intentional/Unintentional Programming Flaws
- When Flaws Occur
- Where Flaws Occur
- Examples of Common Programming Flaws

# Red Team / Blue Team

**Description:**
Red Team / Blue Team course is a key focus for SOC managers, CISOs and any party involved in cybersecurity staff training.

**Prerequisites:**
Certified Ethical Hacker (CEH) course

**Learning Outcomes:**
Students will learn how to execute a Red Team / Blue Team exercise. This course is designed to provide professionals the knowledge and skills that hackers use to target systems so that they can work legally and ethically to improve security systems.

**NICE Framework Connections:**

- Securely Provision
- Operate and Maintain
- Protect and Defend
- Oversee and Govern

**Knowledge Skills and Abilities (KSAs) Mapping:**
The materials within this course focus on the Knowledge Skills and Abilities (KSAs) identified within the Specialty Areas listed below. Specialty Area details within the interactive National Cybersecurity Workforce Framework.

- Risk Management
- Network Services
- Systems Analysis
- Vulnerability Assessment and Management
- Program/Project Management and Acquisition

**Course Outline**:

- Offensive Security
- Defensive Security & Threat Hunting
- Ethical Hacker
- Penetration Test
- When Flaws Occur
- Where Flaws Occur
- Examples of Common Programming Flaws

# Vulnerability Assessments

**Description:**
Vulnerability Assessments introduces wired and wireless computer networks basics, devices, network-based vulnerabilities and protocols in a step-by-step pace.

**Prerequisites:**
None

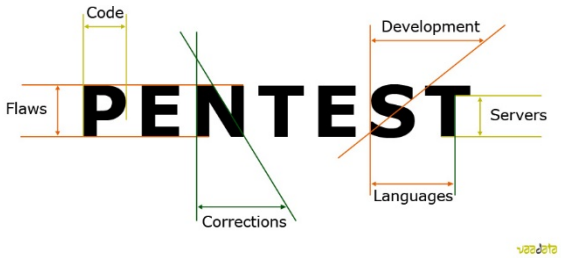
**Learning Outcomes:**
Students will learn how to perform vulnerability assessments. This course is designed to provide professionals the knowledge and skills that hackers use to target systems so that they can work legally and ethically to improve security systems.

**NICE Framework Connections:**

- Securely Provision
- Operate and Maintain
- Protect and Defend
- Oversee and Govern

**Knowledge Skills and Abilities (KSAs) Mapping:**
The materials within this course focus on the Knowledge Skills and Abilities (KSAs) identified within the Specialty Areas listed below. Specialty Area details within the interactive National Cybersecurity Workforce Framework.

- Risk Management
- Systems Administration
- Vulnerability Assessment and Management
- Program/Project Management and Acquisition




**Course Outline**:

- Vulnerability Overview
- Vulnerability Vs. Penetration Test
- Threats and Vulnerabilities
- Conducting Vulnerability Assessments
- Footprinting and Recon
- Network Topology
- Networks
- Network analysis using Wireshark
- Wireshark Filters
- Active Ports

## Penetration Test

**Description:**

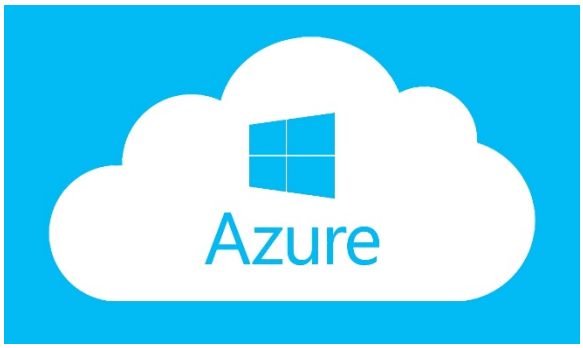
**Prerequisites:**

**Learning Outcomes:**

**NICE Framework Connections:**

**Knowledge Skills and Abilities (KSAs) Mapping:**
The materials within this course focus on the Knowledge Skills and Abilities (KSAs) identified within the Specialty Areas listed below. Specialty Area details within the interactive National Cybersecurity Workforce Framework.

**Course Outline**:




## Azure Fundamentals

**Description:**
Microsoft Azure is an ever-expanding set of cloud services to help your organization meet your business challenges.

**Prerequisites:**

**Learning Outcomes:**
This course is designed to provide management and other professionals with the fundamentals of Microsoft Azure:

- Cloud computing basics
- Cloud services
- Management
- Compute concepts
- Data storage
- Shape

**NICE Framework Connections:**

- Securely Provision
- Operate and Maintain
- Protect and Defend
- Oversee and Govern

**Knowledge Skills and Abilities (KSAs) Mapping:**
The materials within this course focus on the Knowledge Skills and Abilities (KSAs) identified within the Specialty Areas listed below. Specialty Area details within the interactive National Cybersecurity Workforce Framework.

- Cybersecurity Management
- Data Administration
- Network Services
- Software Development
- System Development

**Course Outline**:

- Types of Cloud Services
- Geography
- Management
- Computing Concepts
- Data Storage
- Networking

# Software Development

**Description:**

This course is designed to give the basics about Software Development Security

**Prerequisites:**

Introduction to Cybersecurity
Threats, Attacks and Vulnerabilities

**Learning Outcomes:**

This course is designed to provide management and other professionals an understanding of the vulnerabilities in information systems, to better prepare them to mitigate attacks.

- DEVOPS
- Lifecycle Security
- Software Development Methods
- Trends of Dealing with Security
- Capability Maturity Model

**NICE Framework Connections:**

- Securely Provision

**Knowledge Skills and Abilities (KSAs) Mapping:**

The materials within this course focus on the Knowledge Skills and Abilities (KSAs) identified within the Specialty Areas listed below. Specialty Area details within the interactive National Cybersecurity Workforce Framework.

- Systems Development

**Course Outline**:

- Overview
- Lifecycle Security
- DEVOPS

- Trends of Dealing with Security
- Lifecycle Security
- Capability Maturity Model