CCNA Cybersecurity Operations

1. Cybersecurity and NetAcad
2. CCNA Cyber Ops 1.0 Learning Pathways
3. Getting Ready for CCNA Cyber Ops 1.0
4. CCNA Cyber Ops 1.0 Details
(more details in the Course Deep Dive session!)

Cybersecurity and the Networking Academy

Digital Disruption

Cybersecurity Opportunities

Cybercrime Costs

Cybersecurity Ventures: Cybersecurity Market Research- Top 15 statistics for 2017

Security Spending

Cybersecurity Ventures: Cybersecurity Market Research- Top 15 statistics for 2017

Unprecedented Opportunity

Cybersecurity Ventures: Cybersecurity Market Research- Top 15 statistics for 2017

The Networking Academy Learning Portfolio

Current & Planned

Aligns to Certification

Instructor Training required

Self-paced

* Available within 12 months

Collaborate for Impact

Introduction to Packet Tracer | Packet Tracer | Hackathons | Prototyping Lab | NetRiders | Internships

	Exploratory	Foundational	Career-Ready
Networking		Networking Essentials Mobility Fundamentals	**CCNA R&S:** Introduction to Networks, R&S Essentials, Scaling Networks, Connecting Networks **CCNP R&S:** Switch, Route, TShoot
Security	Introduction to Cybersecurity	Cybersecurity Essentials	CCNA Security CCNA Cyber Ops
IoT	Introduction to IoT	**IoT Fundamentals:** Connecting Things, Big Data & Analytics, Hackathon Playbook	
OS & IT	NDG Linux Unhatched	NDG Linux Essentials IT Essentials	NDG Linux I NDG Linux II
Programming		CLA: Programming Essentials in C CPA: Programming Essentials in C++ PCA: Programming Essentials in Python	CLP: Advanced Programming in C* CPP: Advanced Programming in C++*
Business	Be Your Own Boss	Entrepreneurship	
Digital Literacy	Get Connected		

August 2017

CCNA Cybersecurity Operations Curriculum

Overview

CCNA Cyber Ops introduces the core security concepts and skills needed to monitor, detect, analyze and respond to cybercrime, cyberespionage, insider threats, advanced persistent threats, regulatory requirements, and other cybersecurity issues facing organizations. It emphasizes the practical application of the skills needed to maintain and ensure security operational readiness of secure networked systems.

Career Prep

The skills developed in the curriculum prepares students for a career in the rapidly growing area of cybersecurity operations working in or with a security operations center (SOC) in entry-level job roles such as:

- Security SOC Analyst
- Incident Responder

Learning Components

- 13 chapters of interactive content, quizzes, and chapter exams
- Labs, and hands-on labs using virtual machine environment (PC required, no other equipment required)
- Cisco® Packet Tracer activities (PT 7.0)
- Certification practice exams, practice final, final exam and skills-based assessment

Features

Target Audience: Students enrolled in technology degree programs at institutions of higher education and IT professionals who wants to pursue a career in Security Operations.

Prerequisites: None

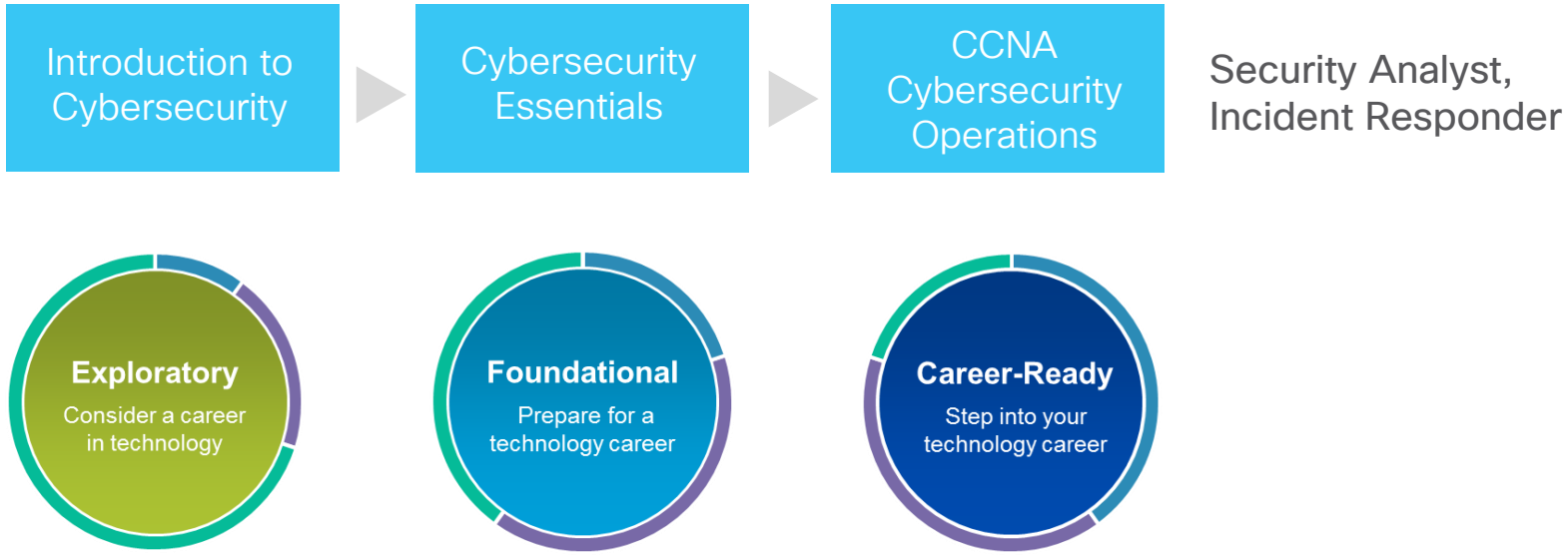
Languages: English

Course Delivery: Instructor-led

Estimated Time to Complete: 70 hours

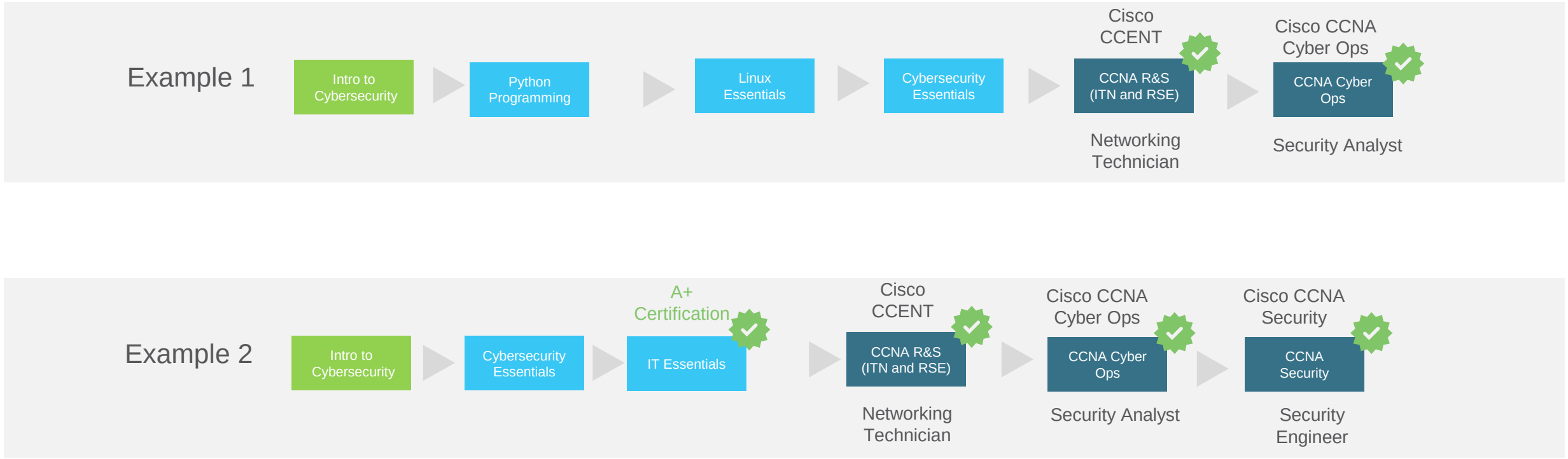
CCNA Cybersecurity Operations Learning Pathways

CCNA Cyber Ops
Recommended Pathways



Examples of Career-Ready Pathways

Cybersecurity Program at 4-year Vocational College/University



Certification

Getting Ready for CCNA Cybersecurity Operations 1.0

Recommended Entry Knowledge

Recommended pre-requisite knowledge :

- PC and Internet navigation skills
- Basic Windows and Linux system concepts
- Basic Networking concepts
- Binary and Hexadecimal understanding
- Awareness of basic programming concepts
- Awareness of basic SQL queries
- Familiarity with Cisco Packet Tracer, a network simulation application.

Note:

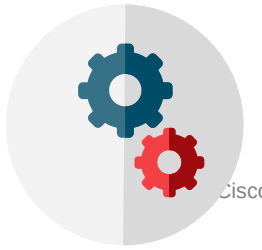
While not mandatory, taking one or more of the following Networking Academy courses enhances and maximizes student learning:

IT & OS (one or more of the following
- IT Essentials
- NDG Linux Essentials

Networking (one or more of the following)
- Networking Essentials
- CCNA R&S: Introduction to Networks

Security
- Introduction to Cybersecurity
- Cybersecurity Essentials

Packet Tracer
- Introduction to Packet Tracer



CCNA Cyber Ops contains optional refresher material for the above skills within the instructional flow

CCNA Cyber Ops
Instructor Training Requirements

Instructor Training & Support:

1. Academies must align with an ASC.

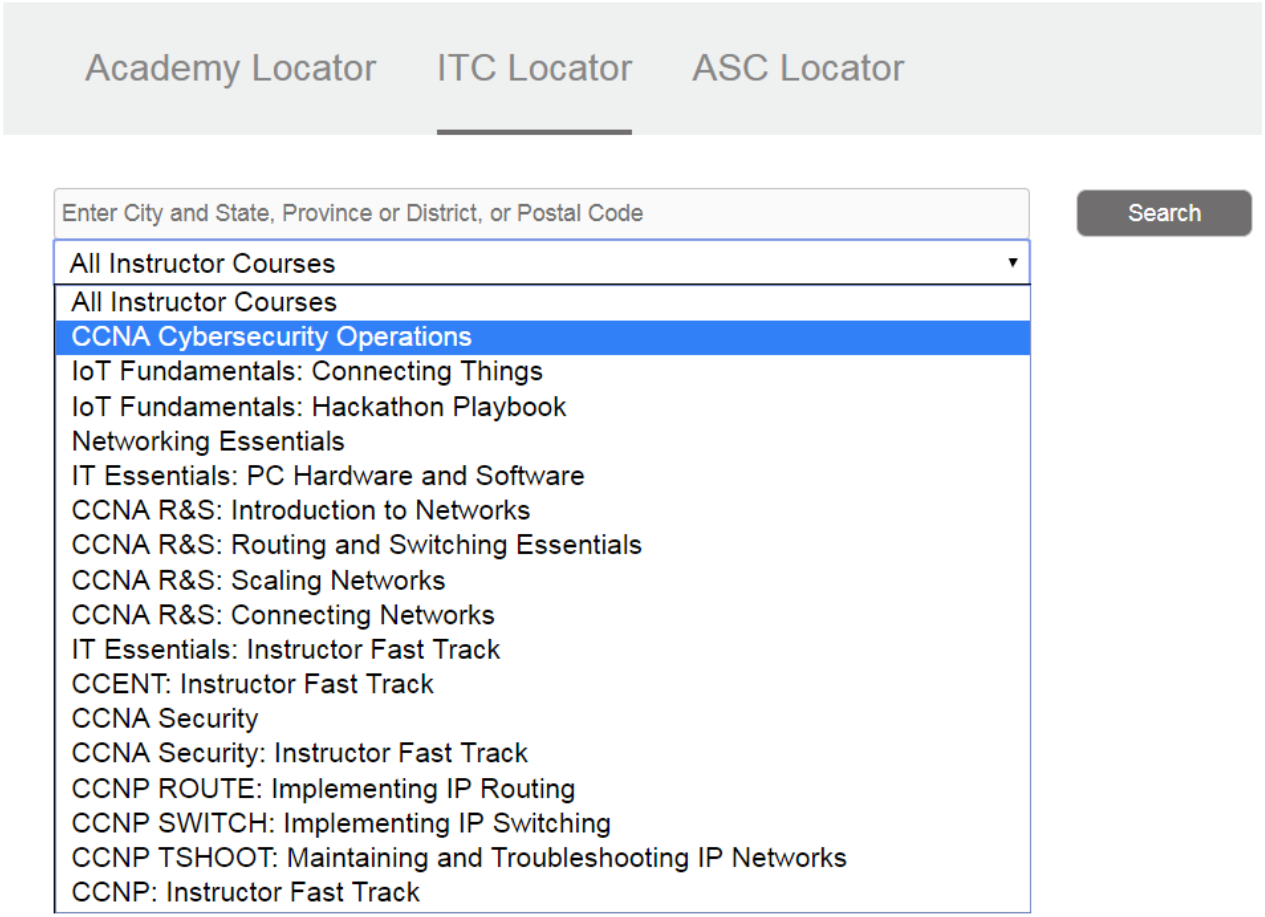
2. Instructor Training is required.
    - Instructor accredited during Limited Availability can continue to teach with no additional instructor training
    - New instructors will require training and accreditation by ITC
    - Instructor candidates with current, valid CCNA Cybersecurity Operations certification are eligible for Instructor Fast Track option. Contact your ITC Academy

3. Instructors can register for training with an ITC.

Finding Instructor Trainings

1. Use ITC Locator
2. Filter by CCNA CyberOps

https://www.netacad.com/get-started/instructor-training-locator/



Instructor Training Options by ITC

New instructor or prefer in-person training

Experienced instructors with one or more qualifying skills

Instructor candidates with CCNA Cyber Ops certification

Option 1

Instructor Trainer-led In-person

Best in class training by a Cisco Qualified Instructor Trainer

- Instructor Trainer will deliver instructor-led training in an in-person format
- Recommended minimum duration is seven working days

Option 2

Instructor Trainer-led Remote

Most flexible solution for experienced instructors

- Instructor Trainer will deliver instructor-led training in a remote format
- ITC Academy opens online class and administers exam/assessment online

Option 3

Instructor Trainer-led Remote + In-person

Experienced instructors that require some in-person support in some elements of the training

- Instructor Trainer will deliver instructor-led training in remote format and an in-person format
- Recommended minimum duration for in-person portion is three working days and includes review of chapters 1 to 11, instruction on chapters 12 & 13, and final multiple-choice assessment and skills-based assessment

Option 4

Instructor Fast track

CCNA Cyber Ops certified instructor candidates demonstrate hands-on skills knowledge

- Candidate provides proof of certification and demonstrates they have the skills needed to teach the course.
- Instructor Trainer administers skills-based assessment.

Instructor Resources

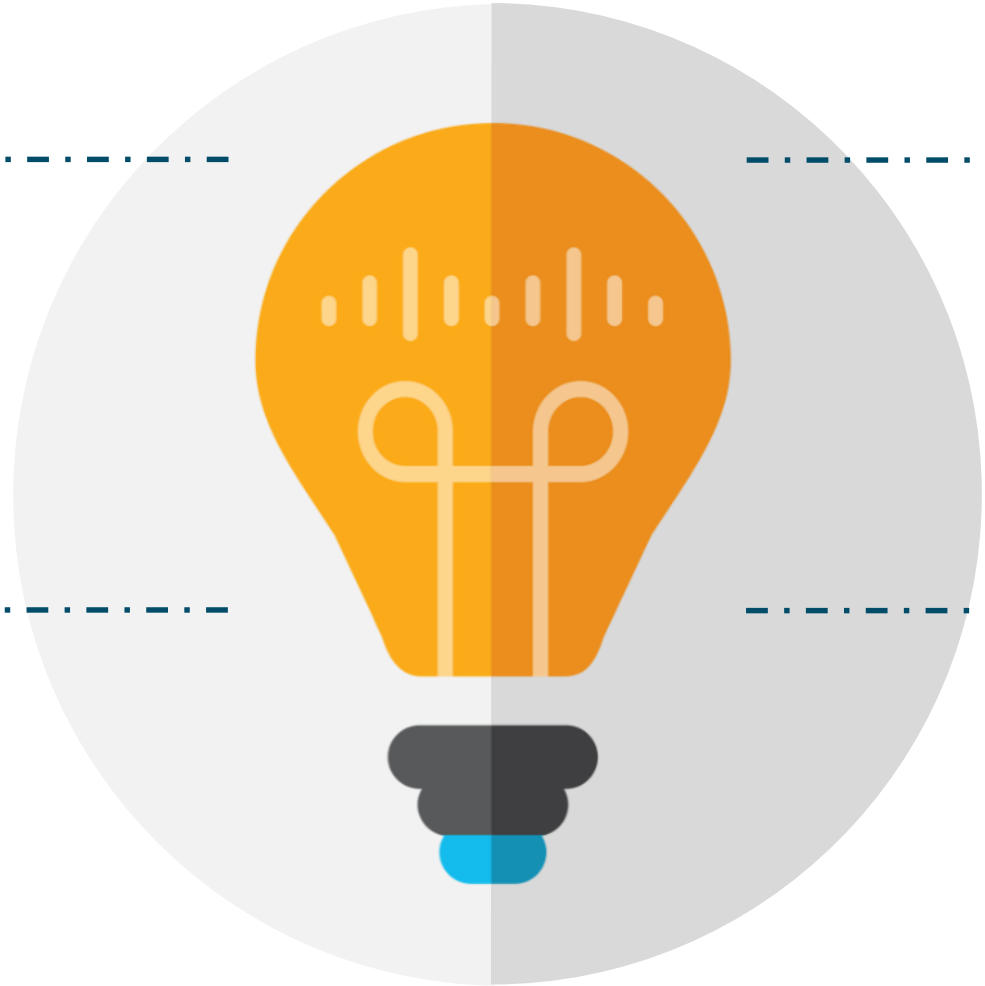
https://www.netacad.com/group/resources/ccna-cyberops/1.0

PPT

Instructor Powerpoints, CCNA Cybersecurity Operations Overview and Video

FAQ

Frequently Asked Questions



S&S

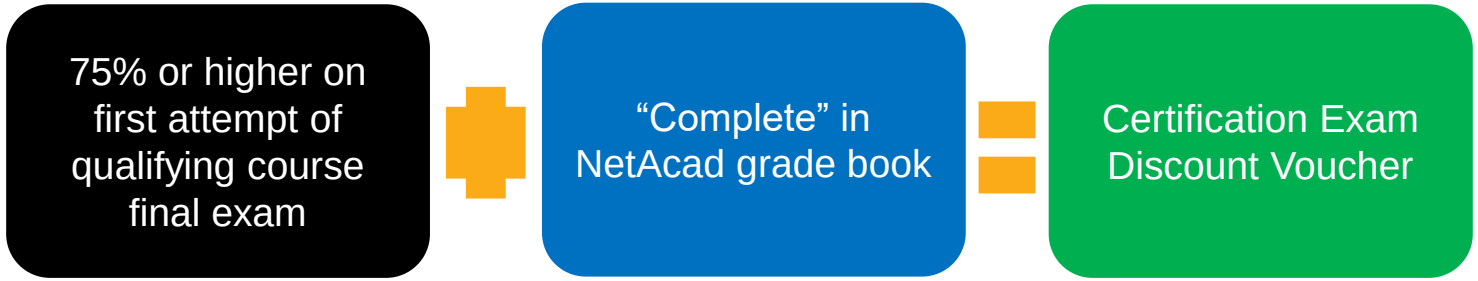
Scope & Sequence Document

Plus

Additional information & resources

Certification Vouchers

Availability starts in June 2018



- Understanding Cisco Cybersecurity Fundamentals (SECFND) certification exam (210-250)
- Implementing Cisco Cybersecurity Operations (SECOPS) certification exam (210-255).

Students	Instructors	Instructor Trainers
60% Discount	70% Discount	80% Discount

CCNA Cybersecurity Operations 1.0 Curriculum Details

CCNA Cyber Ops

Course Overview

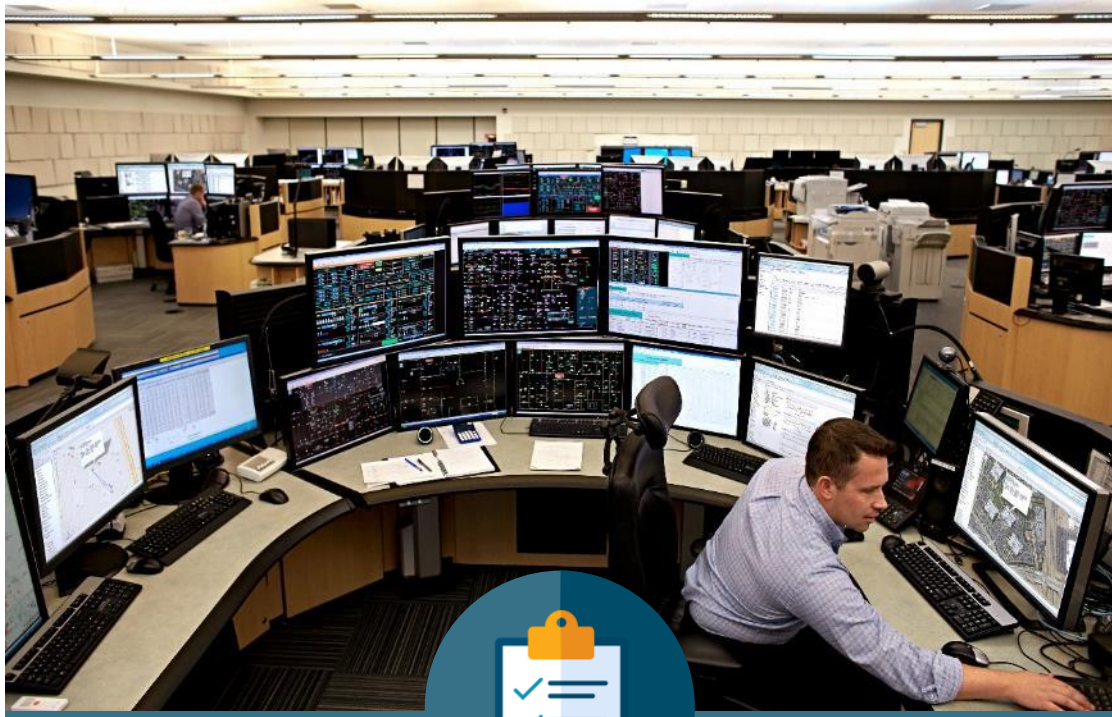
CCNA Cyber Ops introduces the core security concepts and skills needed to monitor, detect, analyze and respond to cybercrime, cyberespionage, insider threats, advanced persistent threats, regulatory requirements, and other cybersecurity issues facing organizations. It emphasizes the practical application of the skills needed to maintain and ensure security operational readiness of secure networked systems.

Benefits

Students acquire and applied skills in the rapidly growing area of cybersecurity operations at the associate level, with alignment to the Cisco CCNA Cybersecurity Operations certification.

Learning Components

- 13 Chapters, modifiable chapter quizzes and chapter exams
- 13 terms & concepts practice quizzlets
- 54 interactive activities
- 45 hands-on labs (27 uses VM)
- 5 Packet Tracer activities
- One each: Skill-based assessment, practice final exam, final exam
- 2 certification practice exams
  - 1x 210-250 SECFND
  - 1x 210-255 SECOPS



Certification Aligned

Features

Target Audience: Students enrolled in technology degree programs at institutions of higher education and IT professionals who wants to pursue a career in Security Operations.

Entry Knowledge: Basic operating system and networking knowledge

Languages: English

Course Delivery: Instructor-led

Estimated Time to Complete: 70 hours

Recommended Next Course: CCNA Security

Instructor Training: Required

CCNA Cyber Ops

Equipment Requirements

Curriculum requirements: 1 student Personal Computer (Desktop/Notebook) per student (recommended), at most 2 students per PC

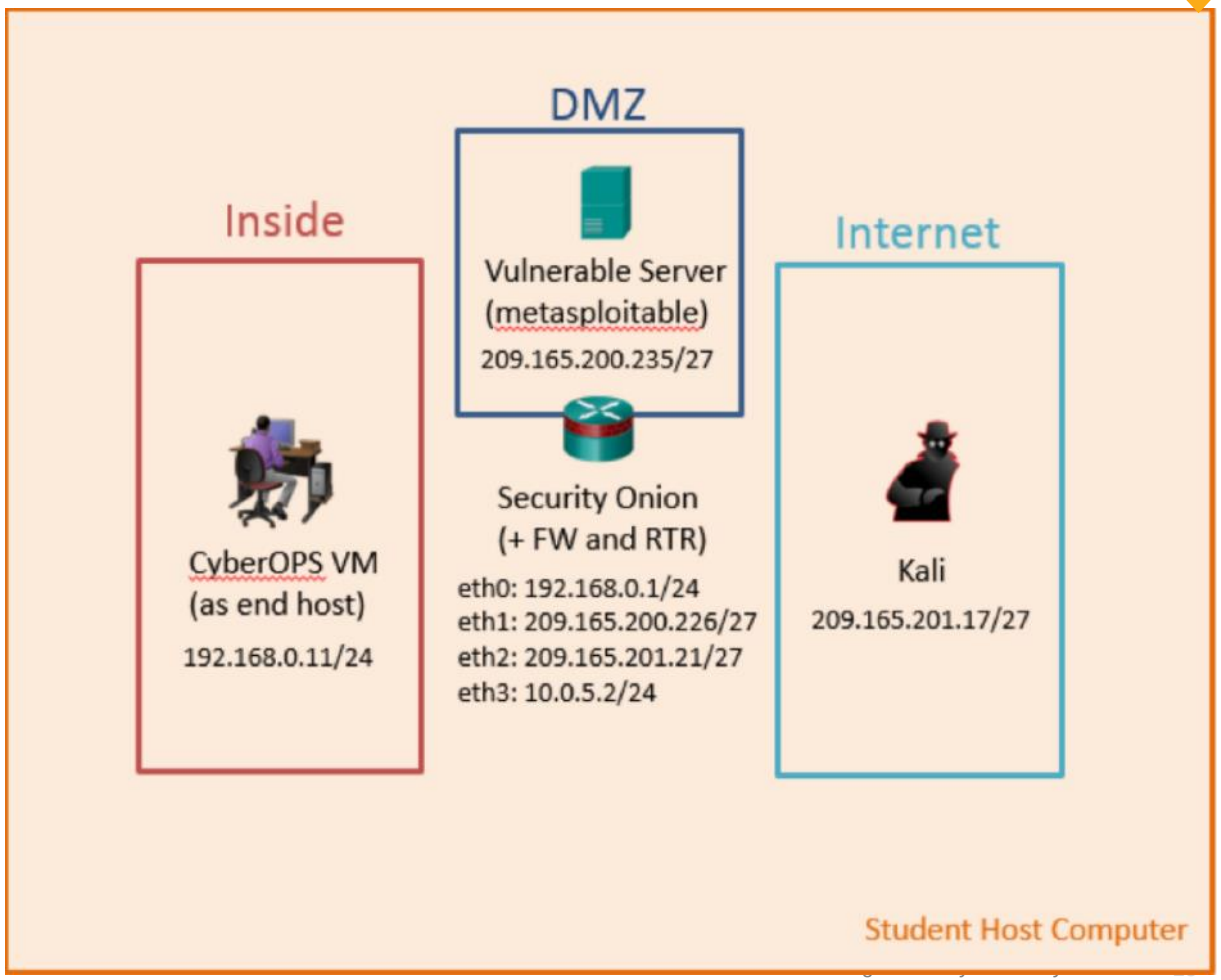
Platform	Description
Desktop PC	• OS: Windows 7, 8, or 10, MAC OSX • Processor: Intel Core i7 4600U 2.7GHz (with Virtualization Support) • Memory: 8 gigabyte (GB) RAM (standard) or 4 GB (alternate option) • Display Adapter: PCI, PCIe (recommended), or AGP video card (DirectX 9 graphics device with WDDM driver) • Disk: 45 GB hard drive. See table in the next slide for details. • Network: 1 Ethernet Card or 1 Wireless Ethernet Card
Web Browser	The most recent version of Microsoft Internet Explorer, Google Chrome, or Mozilla Firefox with the most recent versions of Java and Flash Player installed.
Oracle VirtualBox	The latest version. Currently 5.2.6
Windows Experience Index (WEI)	6.5 (recommended)
Packet Tracer	Version 7.0 Latest build

CCNA Cyber Ops

Equipment Requirements

Virtual Machine Name	Disk Space	RAM
CyberOps Workstation VM	7 GB	1 GB
Kali Linux VM	10 GB	*1 GB
MetaSploitable VM	8 GB	*512 MB
Security Onion VM	10 GB	4 GB (standard) 3 GB (alternate option)

* Not needed for alternate option



Lab Setup

Course Structure

Chapter	Title	Theme	Student Profile
1	Cybersecurity and the Security Operations Center	Introduction	
2	Windows Operating System	OS Fundamentals	Students with ITE, Linux Essentials knowledge
3	Linux Operating System		
4	Network Protocols and Services	Networking Fundamentals	Students with CCNA R&S (ITN) knowledge
5	Network Infrastructure		
6	Principles of Network Security	Cybersecurity Fundamentals	Students with Cybersecurity Essentials and CCNA Security knowledge
7	Network Attacks: A Deeper Look		
8	Protecting the Network		
9	Cryptography and the Public Key Infrastructure		
10	Endpoint Security and Analysis		
11	Security Monitoring	Cybersecurity Operations	
12	Intrusion Data Analysis		
13	Incident Response and Handling		

More details in the Course Deep Dive session!