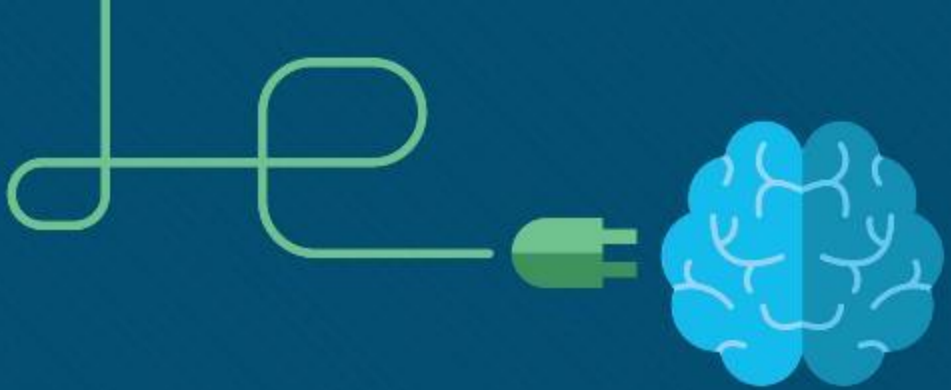
Networking Academy



CCNA Cybersecurity Operations

Course Deep Dive

Eugene Morozov

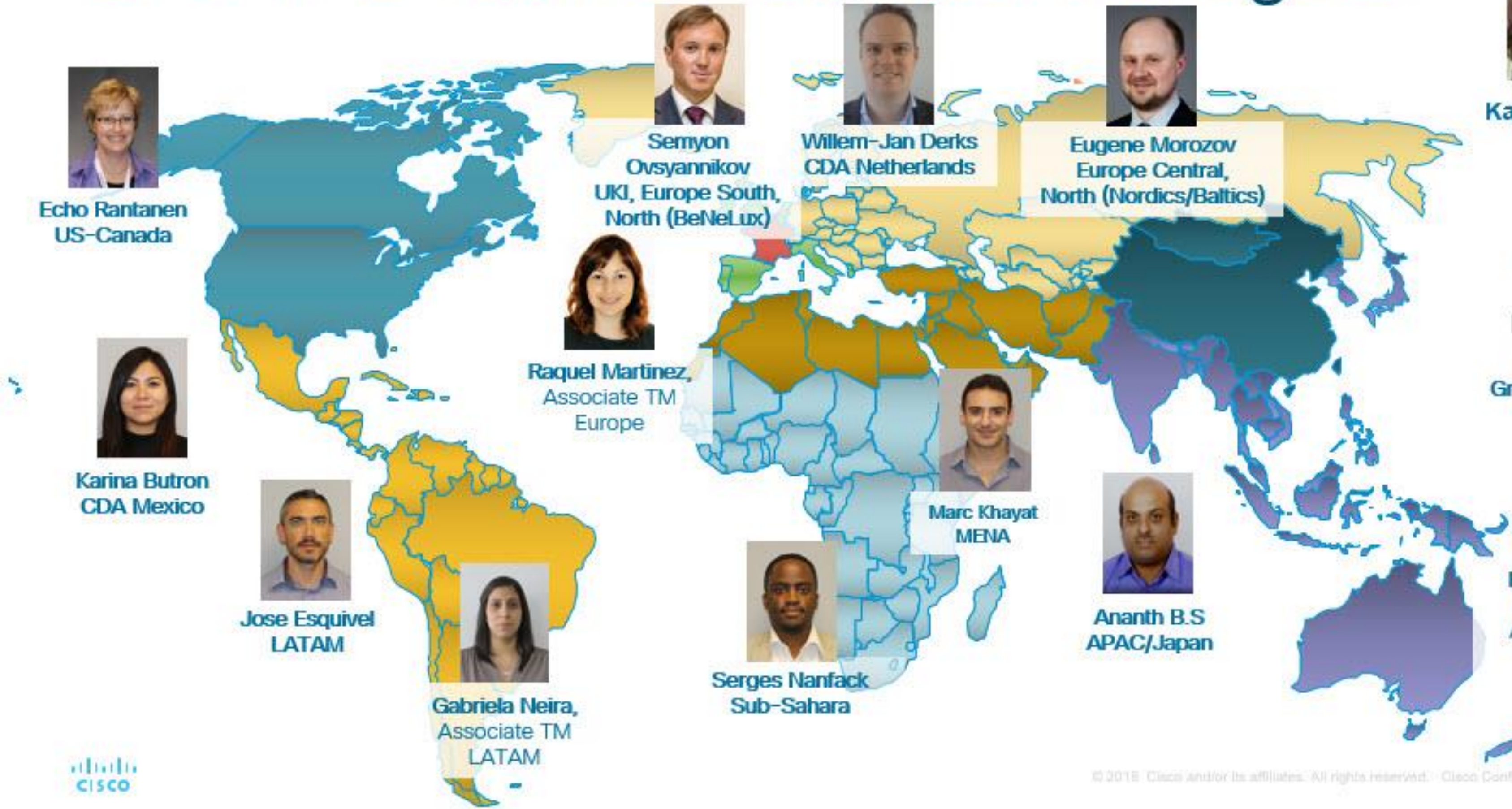
Heiko Knospe

23 November 2018
Essen

#NetAcadIPD

GFO TFE Team of Technical Managers

Karen Alderson



Echo Rantanen
US-Canada

Semyon Ovsyannikov
UKI, Europe South, North (BeNeLux)

Willem-Jan Derks
CDA Netherlands

Eugene Morozov
Europe Central, North (Nordics/Baltics)

Raquel Martinez,
Associate TM
Europe

Karina Butron
CDA Mexico

Jose Esquivel
LATAM

Gabriela Neira,
Associate TM
LATAM

Serges Nanfack
Sub-Sahara

Marc Khayat
MENA

Ananth B.S
APAC/Japan

Difei Li
Greater China

Herfiedhantya Bhagaskara,
Associate TM
APJC

Lab 12.4.1.2

Lab 12.4.1.2

WiFi
SSID: WLANHNBK1
Password: wlanhnbk22112012
Username: HNBK-Gast
Password: HnbkWorkshop2018!

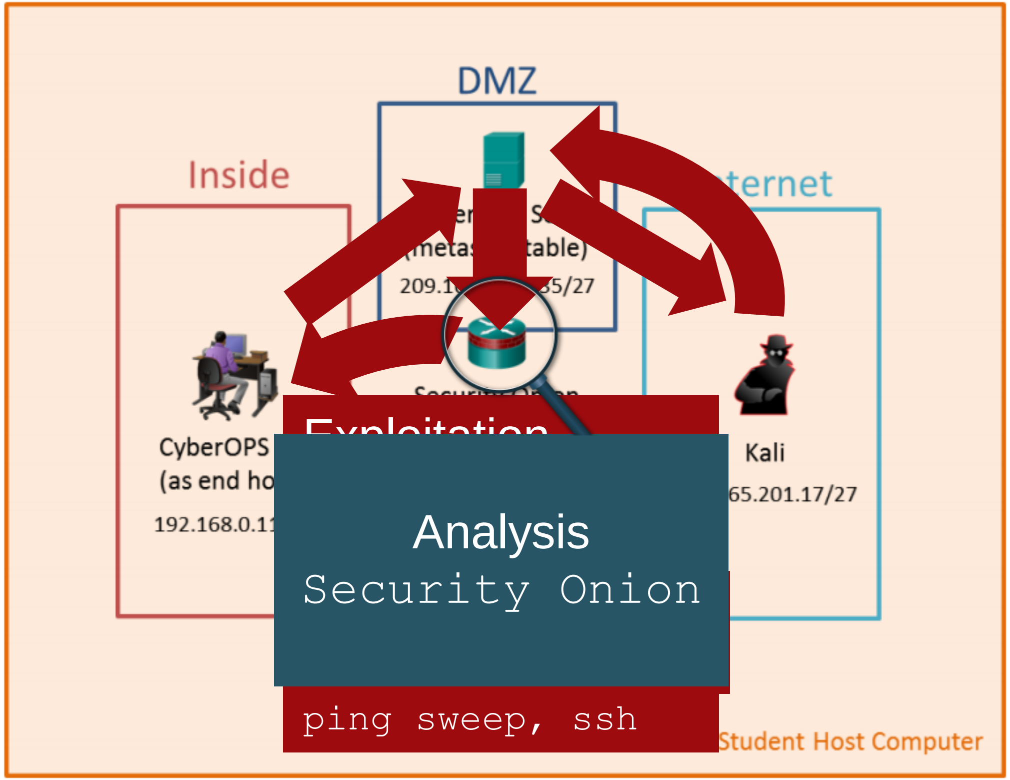
PC User: .\Workshop18
PC Password: cisco120

Lab instructions

- http://cs.co/IPD19/ and self-enroll
- Deutsch
- Download

Lab – Isolated Compromised Host Using 5-Tuple

Topology



Analysis

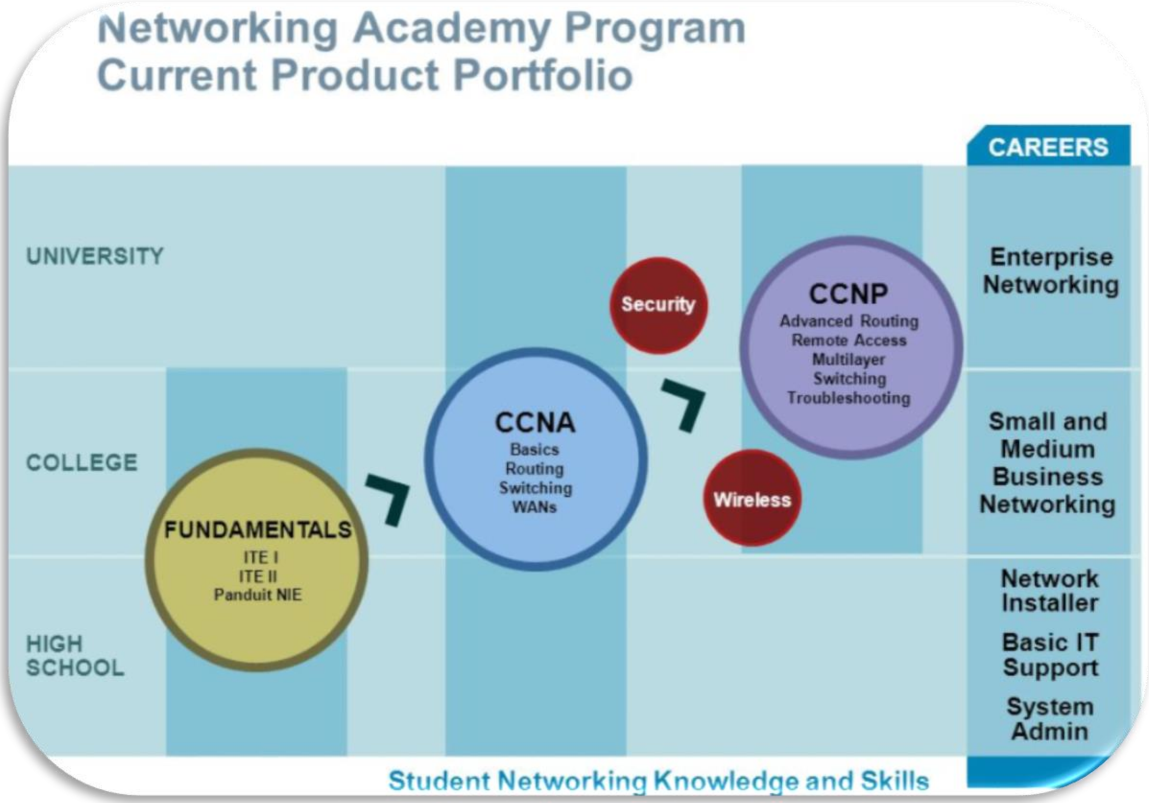
Security Onion

ping sweep, ssh

Agenda

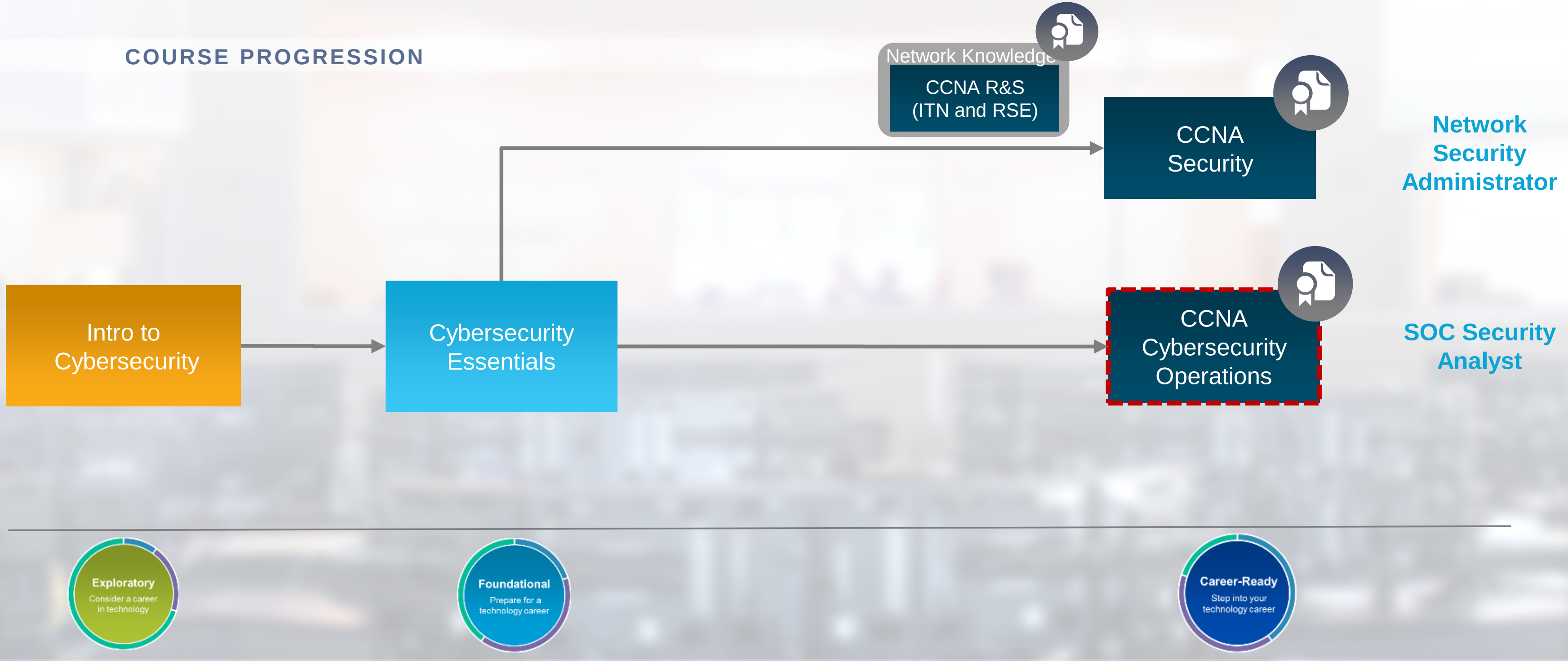
- Cybersecurity Learning Pathway
- What Cyber Ops teaches and what does not
- Certification and Vouchers
- Course Structure
- Equipment Requirements
- Instructor Training and Fast Track
- Instructor Resources
- Demo

Flashback from 2007



Security Learning Pathways

COURSE PROGRESSION



Network Knowledge

CCNA R&S (ITN and RSE)

Intro to Cybersecurity

Cybersecurity Essentials

CCNA Security

CCNA Cybersecurity Operations

Network Security Administrator

SOC Security Analyst

Exploratory
Consider a career in technology

Foundational
Prepare for a technology career

Career-Ready
Step into your technology career

Certification

CCNA Cyber Ops Certification

Exam code	Full name	Price, USD	Topics
210-250 SECFND	Understanding Cisco Cybersecurity Fundamentals	Base price: $300	• Network Concepts • Security Concepts • Cryptography • Host-Based Analysis • Security Monitoring • Attack Methods
210-255 SECOPS	Implementing Cisco Cybersecurity Operations	Base price: $300	• Endpoint Threat Analysis and Computer Forensics • Network Intrusion Analysis • Incident Response • Data and Event Analysis • Incident Handling

CCNA Cyber Ops Certification (cont.)

- 2 exams only option. No “composite” option with just 1 exam
- No prerequisites to take exams
- Recertification: Pass any current Associate-level exam except for the ICND1 (CCENT), or higher level exam
- Discount Vouchers: available!

- As per exams blueprint, no device configuration or simulation questions: only have to “describe”, “define”, “compare”, “interpret” etc.

CCNA Cyber Ops

Learning Outcomes

Explain role of Cybersecurity Operations Analyst

Learn Operating Systems features needed to support cybersecurity analyses

Explain operation of network infrastructure and classify the various network attacks

Analyze the operation of network protocols and services; and use monitoring tools to identify attacks.

Use various methods to prevent malicious access to computer hosts and data

Explain the impacts of cryptography on network security monitoring

Explain how to investigate and evaluate endpoint vulnerabilities and network security alerts

Use virtual machines to implement, evaluate, and analyze cybersecurity threat events

Analyze network intrusion data to identify compromised hosts and vulnerabilities

Apply incident response model (CSIRSTs and NIST) to manage security incidents.

CCNA Cyber Ops

Course Overview

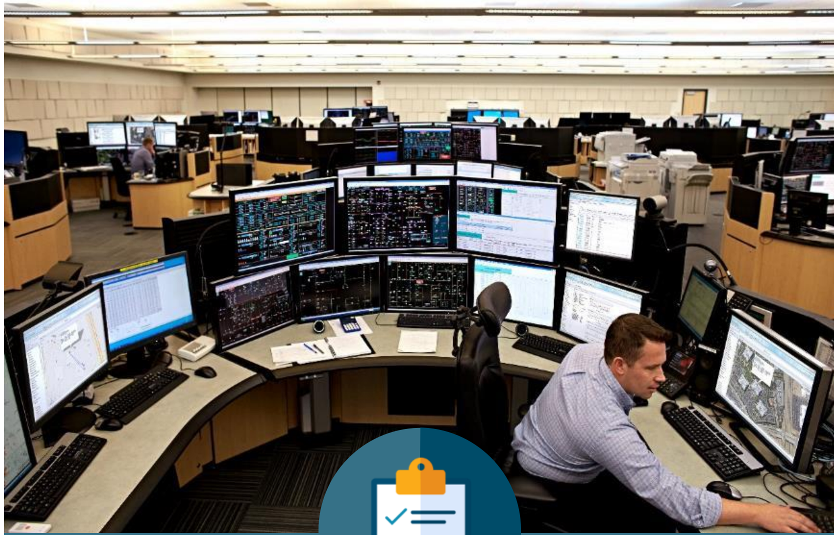
CCNA Cyber Ops introduces the core security concepts and skills needed to monitor, detect, analyze and respond to cybercrime, cyberespionage, insider threats, advanced persistent threats, regulatory requirements, and other cybersecurity issues facing organizations. It emphasizes the practical application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

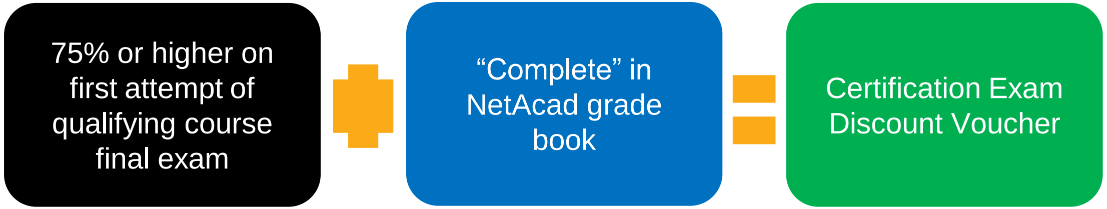
Estimated Time to Complete: 70 hours

Recommended Next Course: CCNA Security

Instructor Training: Required

CCNA Cyber Ops Certification Vouchers

Available from 17 April 2018



75% or higher on first attempt of qualifying course final exam + "Complete" in NetAcad grade book = Certification Exam Discount Voucher

Understanding Cisco Cybersecurity Fundamentals (SECFND) certification exam (210-250)	Voucher Validity – 3 months
Implementing Cisco Cybersecurity Operations (SECOPS) certification exam (210-255)	Voucher Validity – 6 months

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

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		

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

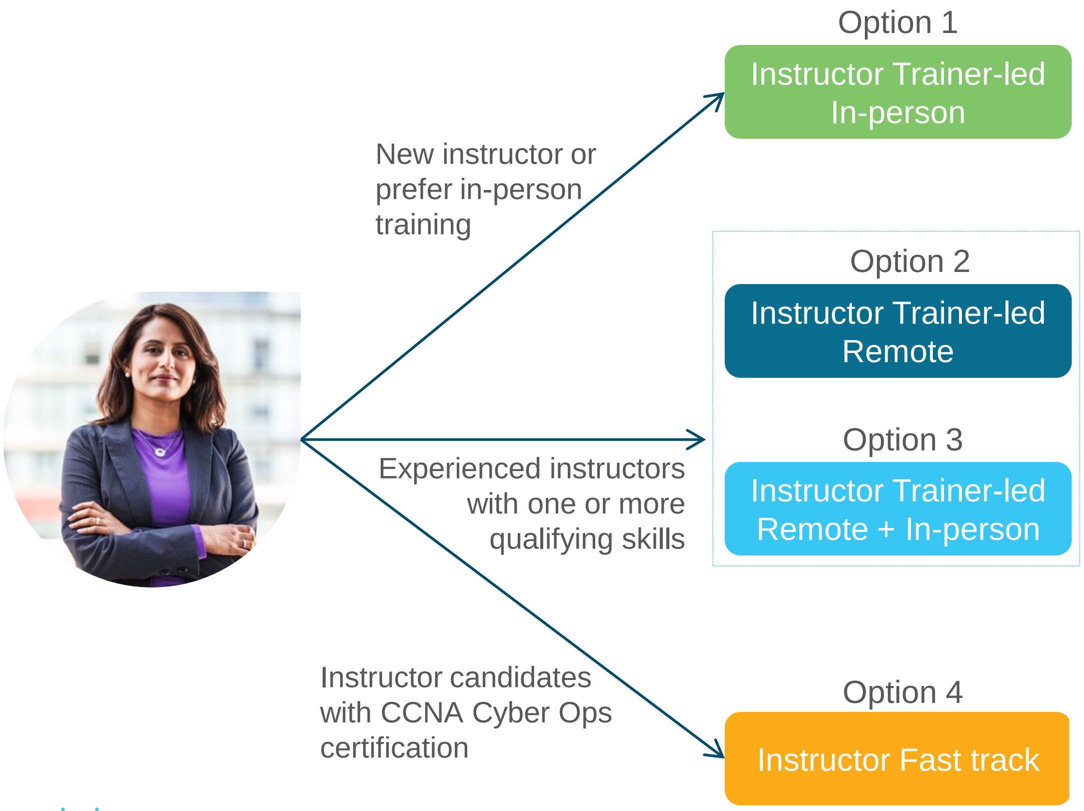
CCNA Cyber Ops

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.

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 Completion Requirements

1 Instructor Trainer is responsible for the quality of the newly accredited instructors.

2 Instructor candidate must complete the course, lab activities, chapter exams, quizzes, final skills-based assessment and score a 75% on the multiple-choice final before the Instructor Trainer will accredit them as an instructor.

Instructor Fast Track Completion Requirements

1 Instructor Trainer is responsible for the quality of the newly accredited instructors.

2 Instructor candidate must review the course, lab activities, chapter exams, quizzes and multiple-choice final.

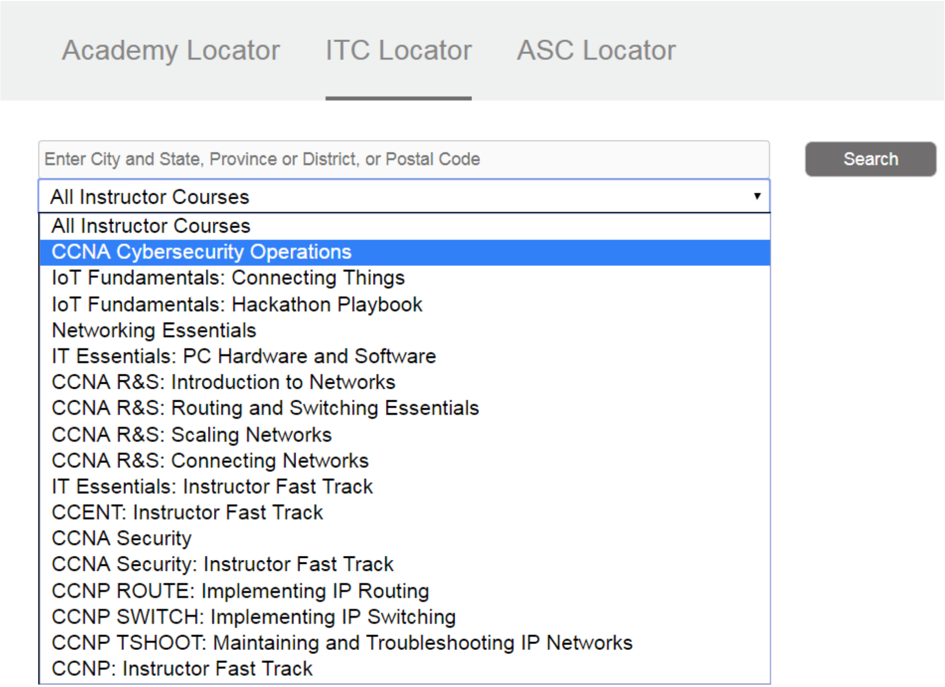
3 Instructor candidate must score 80% or more on the skills-based assessment.

Finding Instructor Trainings

1 Use ITC Locator

2 Filter by CCNA CyberOps

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



All Instructor Courses

- All Instructor Courses
- CCNA Cybersecurity Operations
- IoT Fundamentals: Connecting Things
- IoT Fundamentals: Hackathon Playbook
- Networking Essentials
- IT Essentials: PC Hardware and Software
- CCNA R&S: Introduction to Networks
- CCNA R&S: Routing and Switching Essentials
- CCNA R&S: Scaling Networks
- CCNA R&S: Connecting Networks
- IT Essentials: Instructor Fast Track
- CCENT: Instructor Fast Track
- CCNA Security
- CCNA Security: Instructor Fast Track
- CCNP ROUTE: Implementing IP Routing
- CCNP SWITCH: Implementing IP Switching
- CCNP TSHOOT: Maintaining and Troubleshooting IP Networks
- CCNP: Instructor Fast Track

CCNA Cyber Ops

Equipment Requirements

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

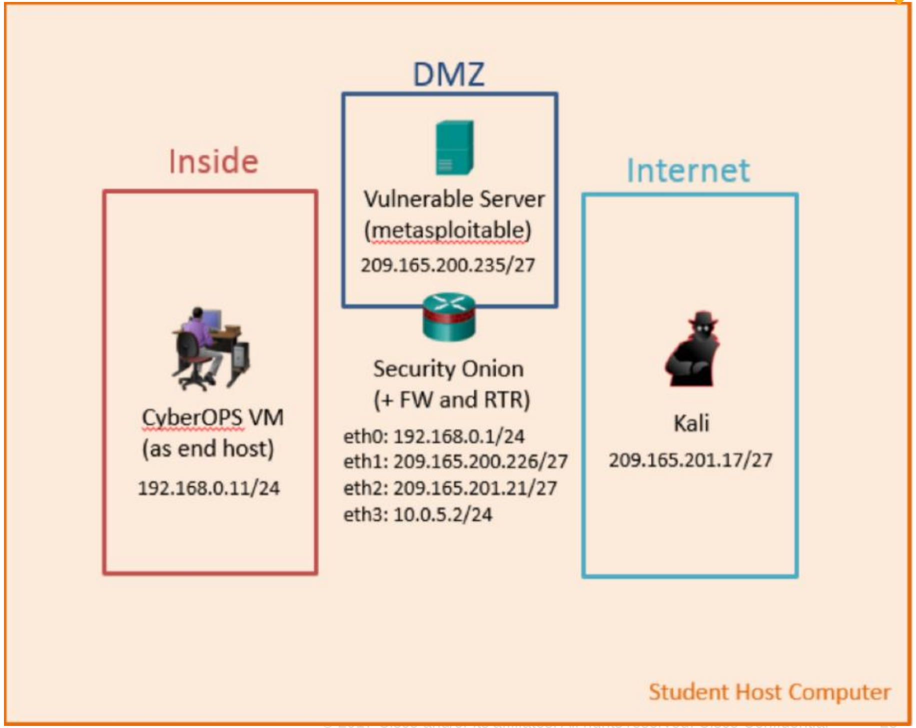
Platform	Description
Desktop PC	- OS: Windows 7, 8, or 10, MAC OSX - Processor: Intel Core i7 4600U 2.7GHz (with Virtualization Support) - Memory: 8 gigabyte (GB) RAM (standard) or 4 GB (alternate option) - Display Adapter: PCI, PCIe (recommended), or AGP video card (DirectX 9 graphics device with WDDM 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)

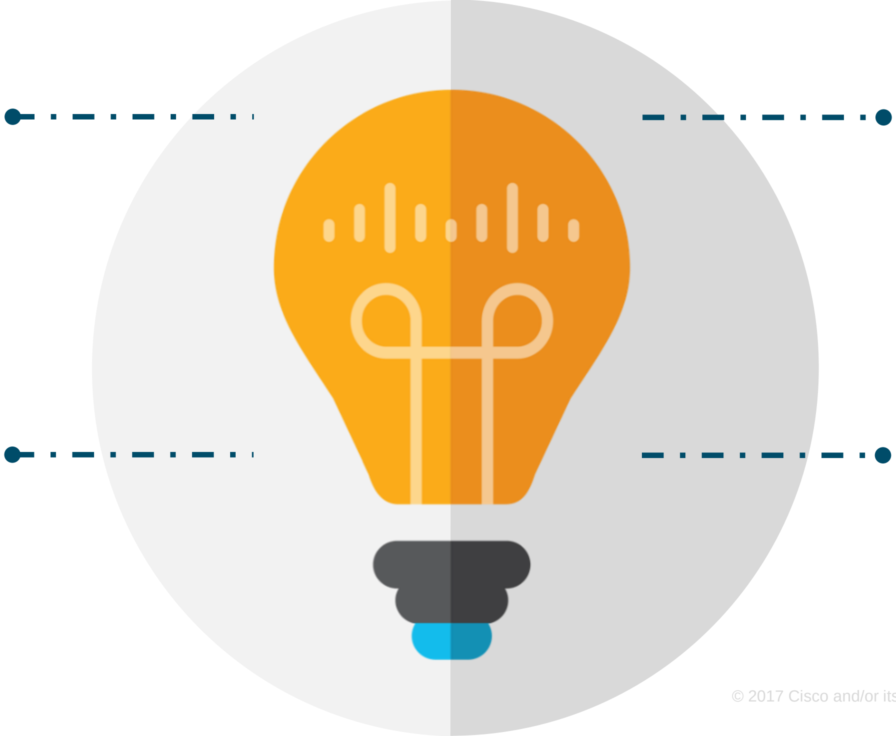
* Not needed for alternate option



Lab Setup

Instructor Resources

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



PPT

Instructor Powerpoints, CCNA Cybersecurity Operations Overview and Video

S&S

Scope & Sequence Document

FAQ

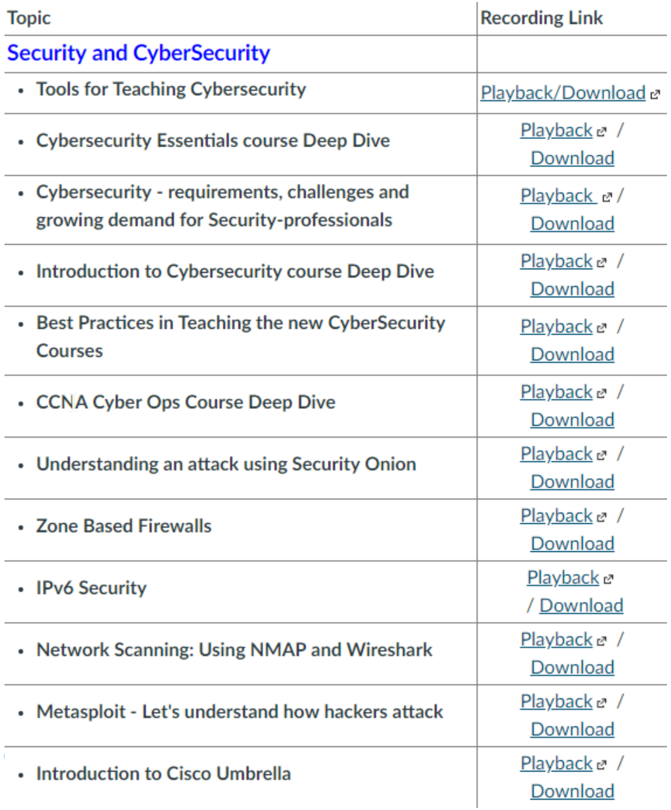
Frequently Asked Questions

Plus

Additional information & resources

IPD Week – http://cs.co/IPD19/

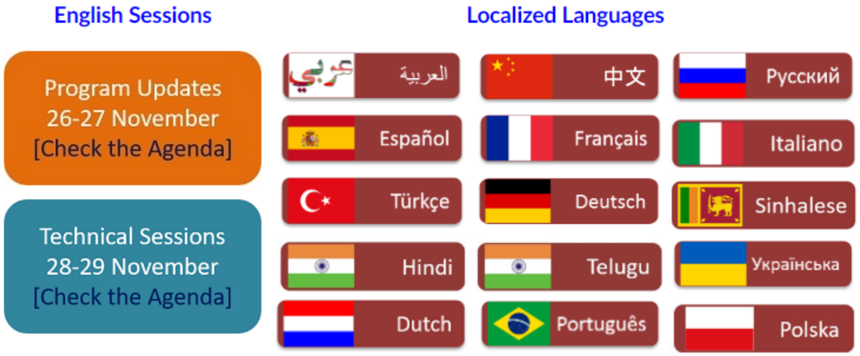
Archive:



Topic	Recording Link
Security and CyberSecurity	
• Tools for Teaching Cybersecurity	Playback/Download
• Cybersecurity Essentials course Deep Dive	Playback / Download
• Cybersecurity - requirements, challenges and growing demand for Security-professionals	Playback / Download
• Introduction to Cybersecurity course Deep Dive	Playback / Download
• Best Practices in Teaching the new CyberSecurity Courses	Playback / Download
• CCNA Cyber Ops Course Deep Dive	Playback / Download
• Understanding an attack using Security Onion	Playback / Download
• Zone Based Firewalls	Playback / Download
• IPv6 Security	Playback / Download
• Network Scanning: Using NMAP and Wireshark	Playback / Download
• Metasploit - Let's understand how hackers attack	Playback / Download
• Introduction to Cisco Umbrella	Playback / Download

November 2018

- **Wireshark Tips & Tricks Part 2**
- **Attacking Networks using Kali Linux**
- Hands-on for Model-driven Programmability
- SDN: an Open Source Demo
- NetAcad Equipment Deep Dive
- **CCNA Cyber Ops Game**



English Sessions

Localized Languages

Program Updates
26-27 November
[Check the Agenda]

Technical Sessions
28-29 November
[Check the Agenda]

cisco