

SmartStep CCNA Cyber Security Operations

Fachkursleitung:
Peter Infanger
Dozent Informatik

Mail: peter.infanger@hslu.ch

Agenda

1. Cybersecurity and NetAcad

2. Learning Pathways

3. Curriculum & Details

4. Schedule

Cybersecurity Opportunities

Cybercrime Costs

Security Spending

Unprecedented Opportunity

CYBERCRIME COSTS



Cybercrime damages will cost the world **\$6 trillion annually by 2021**, up from \$3 trillion in 2015. Costs include destruction of data, stolen money, and other.

SECURITY SPENDING



The world will spend **\$1 trillion cumulatively from 2017-2021** on cybersecurity products and services - to combat cybercrime.

CYBERSECURITY JOBS



There are **1 million cybersecurity job openings in 2016**, with a projected shortfall of 1.5 million by 2019. Unemployment stays at 0%.

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

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

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







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

	Exploratory	Foundational	Career-Ready
Networking		<ul style="list-style-type: none">  Networking Essentials  Mobility Fundamentals 	<ul style="list-style-type: none">   CCNA R&S: Introduction to Networks, R&S Essentials, Scaling Networks, Connecting Networks   CCNP R&S: Switch, Route, TShoot
Security	<ul style="list-style-type: none">  Introduction to Cybersecurity 	<ul style="list-style-type: none">  Cybersecurity Essentials 	<ul style="list-style-type: none">   CCNA Security   CCNA Cyber Ops
IoT	<ul style="list-style-type: none">  Introduction to IoT 	<ul style="list-style-type: none">  IoT Fundamentals: Connecting Things, Big Data & Analytics, Hackathon Playbook 	
OS & IT	<ul style="list-style-type: none">  NDG Linux Unhatched 	<ul style="list-style-type: none">   NDG Linux Essentials  IT Essentials 	<ul style="list-style-type: none">  NDG Linux I  NDG Linux II
Programming		<ul style="list-style-type: none">  CLA: Programming Essentials in C  CPA: Programming Essentials in C++  PCA: Programming Essentials in Python 	<ul style="list-style-type: none">  CLP: Advanced Programming in C*  CPP: Advanced Programming in C++*
Business	<ul style="list-style-type: none">  Be Your Own Boss 	<ul style="list-style-type: none">  Entrepreneurship 	
Digital Literacy	<ul style="list-style-type: none">  Get Connected 		

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 want to pursue a career in Security Operations.

Prerequisites: None

Languages: English

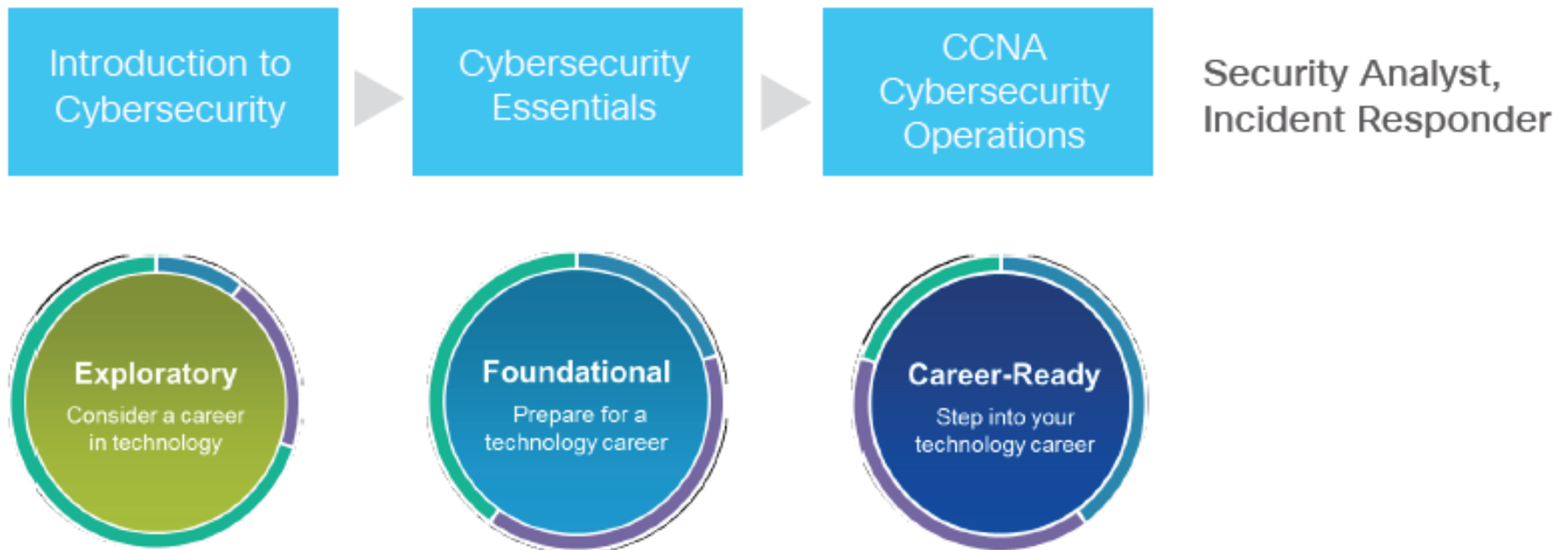
Course Delivery: Instructor-led

Estimated Time to Complete: 70 hours

CCNA Cyber Sec Ops Value Proposition

- Gain understanding and hands-on experience on how to detect and respond to security incidents
- Understand how organizations deal with cybercrime, cyberespionage, insider threats, advanced persistent threats, regulatory requirements, and related issues
- Gain job-ready practical skills for in-demand job roles in cybersecurity operations
- Prepare for industry recognize CCNA Cybersecurity Operations certification

CCNA Cyber Ops Recommended Pathways



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

Course Structure

Chapter	Title	Theme
1	Cybersecurity and the Security Operations Center	Introduction
2	Windows Operating System	OS Fundamentals
3	Linux Operating System	
4	Network Protocols and Services	Networking Fundamentals
5	Network Infrastructure	
6	Principles of Network Security	Cybersecurity Fundamentals
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	

CCNA Cyber Sec Ops Equipment

Equipment Requirements

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

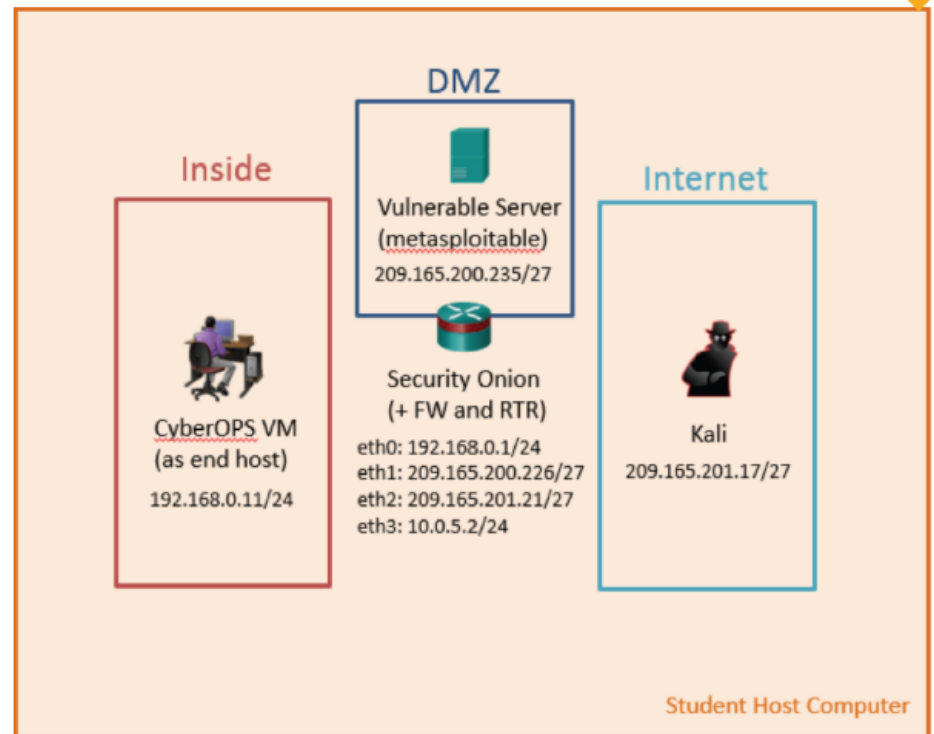
Platform	Description
Desktop PC	<ul style="list-style-type: none">• OS: Windows 7, 8, or 10, MAC OSX• Processor: 64-bit processor with Virtualization Support , see https://www.computerhope.com/issues/ch001121.htm to determine if computer has a 64-bit processor• Memory: 8 gigabyte (GB) RAM (standard) 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. http://www.oracle.com/technetwork/server-storage/virtualbox/downloads/index.html
Windows Experience Index (WEI)	6.5 (recommended)
Packet Tracer	Minimum version 7.0 or later

CCNA Cyber Sec Ops Equipment

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
Security Onion VM*	10 GB	3 GB

* Chapter 12 labs provide an option of using only one Alternative Security Onion VM



Lab Setup

Security Onion: a Network Security Manager

Security Onion_SA [wird ausgeführt] - Oracle VM VirtualBox

File Maschine Anzeige Eingabe Geräte Hilfe

SGUIL-0.9.0 - Connecte... ELSA - Chromium Terminal - analyst@Sec...

SGUIL-0.9.0 - Connected To localhost

File Query Reports Sound: Off ServerName: localhost UserName: analyst UserID: 2 2019-02-27 16:48:04 GMT

RealTime Events Escalated Events Event Query Cat VII

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	27	seconion-eth1-1	5.5714	2017-07-31 19:22:00	209.165.200.235		192.168.0.11		1	GPL ICMP_INFO PING *NIX
RT	67	seconion-eth1-1	5.5767	2017-07-31 19:23:09	209.165.201.17		209.165.200.235		1	GPL ICMP_INFO PING *NIX
RT	67	seconion-eth2-1	7.5723	2017-07-31 19:23:09	209.165.201.17		209.165.200.235		1	GPL ICMP_INFO PING *NIX
RT	67	seconion-eth2-1	7.5725	2017-07-31 19:25:01	192.168.0.11		209.165.201.17		1	GPL ICMP_INFO PING BSDtype
RT	67	seconion-eth2-1	7.5726	2017-07-31 19:25:01	192.168.0.11		209.165.201.17		1	GPL ICMP_INFO PING *NIX
RT	7	seconion-ossec	1.4162	2017-07-31 19:33:07	0.0.0.0		0.0.0.0		0	[OSSEC] Integrity checksum changed.
RT	1	seconion-eth0-1	3.722	2017-09-07 15:31:12	192.168.0.12	50450	93.114.64.118	80	6	ET POLICY Outdated Flash Version M1
RT	1	seconion-eth0-1	3.723	2017-09-07 15:31:13	192.168.0.12	50457	173.201.198.128	80	6	ET CURRENT_EVENTS 32-byte by 32-byte PHP EK Gate with HTTP P...
RT	28	seconion-eth0-1	3.724	2017-09-07 15:31:15	192.99.198.158	80	192.168.0.12	50467	6	ET CURRENT_EVENTS DRIVEBY Angler EK Apr 01 2014
RT	28	seconion-eth0-1	3.728	2017-09-07 15:31:15	192.99.198.158	80	192.168.0.12	50467	6	ET CURRENT_EVENTS Angler EK Oct 22 2014
RT	28	seconion-eth0-1	3.732	2017-09-07 15:31:15	192.99.198.158	80	192.168.0.12	50467	6	ET CURRENT_EVENTS Angler EK Feb 04 2015 M2
RT	12	seconion-eth0-1	3.772	2017-09-07 15:31:20	192.99.198.158	80	192.168.0.12	50473	6	ET CURRENT_EVENTS Angler EK Encoded Shellcode IE
RT	1	seconion-eth0-1	3.784	2017-09-07 15:31:23	192.168.0.12	50474	208.113.226.171	80	6	ET POLICY External Timezone Check (earthtools.org)
RT	1	seconion-eth0-1	3.785	2017-09-07 15:31:23	192.168.0.12	50474	208.113.226.171	80	6	ET TROJAN Possible Bedep Connectivity Check (2)
RT	1	seconion-eth0-1	3.786	2017-09-07 15:31:27	192.168.0.1	53	192.168.0.12	59968	17	ET TROJAN Zeus GameOver Possible DGA NXDOMAIN Responses
RT	2	seconion-eth0-1	3.787	2017-09-07 15:31:29	209.126.97.209	443	192.168.0.12	50476	6	ET TROJAN Bedep SSL Cert
RT	1	seconion-eth0-1	3.788	2017-09-07 15:31:34	192.168.0.12	50468	192.99.198.158	80	6	ET CURRENT_EVENTS Angler EK Flash Exploit URI Struct

IP Resolution Agent Status Snort Statistics System Msgs User Msgs

```
[2018-11-10 11:45:53] seconion-eth2: Error: No pcap files in /nsm/sensor_data/seconion-eth2/dailylogs/2018-11-10.
[2018-11-10 11:50:31] seconion-eth0: Error: No pcap files in /nsm/sensor_data/seconion-eth0/dailylogs/2018-11-10.
[2018-11-10 11:50:42] seconion-eth1: Error: No pcap files in /nsm/sensor_data/seconion-eth1/dailylogs/2018-11-10.
[2018-11-10 11:50:53] seconion-eth2: Error: No pcap files in /nsm/sensor_data/seconion-eth2/dailylogs/2018-11-10.
[2018-11-10 11:55:33] seconion-eth0: Error: No pcap files in /nsm/sensor_data/seconion-eth0/dailylogs/2018-11-10.
[2018-11-10 11:55:44] seconion-eth1: Error: No pcap files in /nsm/sensor_data/seconion-eth1/dailylogs/2018-11-10.
[2018-11-10 11:55:55] seconion-eth2: Error: No pcap files in /nsm/sensor_data/seconion-eth2/dailylogs/2018-11-10.
[2018-11-10 12:00:33] seconion-eth0: Error: No pcap files in /nsm/sensor_data/seconion-eth0/dailylogs/2018-11-10.
[2018-11-10 12:00:44] seconion-eth1: Error: No pcap files in /nsm/sensor_data/seconion-eth1/dailylogs/2018-11-10.
[2018-11-10 12:00:55] seconion-eth2: Error: No pcap files in /nsm/sensor_data/seconion-eth2/dailylogs/2018-11-10.
```

Show Packet Data Show Rule

```
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"GPL ICMP_INFO PING *NIX"; itype:8; content:"| 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F|"; depth:32; classtype:misc-activity; sid:2100366; rev:8;)
/nsm/server_data/securityonion/rules/seconion-eth1-1/downloaded.rules: Line 7767
```

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum
IP	209.165.200.235	192.168.0.11	4	5	0	84	0	2	0	64	57188

ICMP	Type	Code	ChkSum	ID	Seq #
ICMP	8	0	9756	24851	1

DATA	Hex	Text
DATA	71 D1 75 59 9D A1 01 00 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37	q.uY..... !"#%&'()*+,-./ 01234567

Search Packet Payload Hex Text NoCase

STRG-RECHTS

Packet Tracer Simulator

Cisco Packet Tracer - D:\Cisco\Academy\CCNA CyberOps\Labs\7.1.2.7 Packet Tracer - Logging Network Activity.pka

File Edit Options View Tools Extensions Help

Logical Back [Root] New Cluster Move Object Set Tiled Background Viewport Environment: 10:30:00

PT Activity: 00:01:59

Packet Tracer - Logging Network Activity

Addressing Table

Device	Private IP Address	Public IP Address
FTP_Server	192.168.30.253	209.165.200.227
SYSLOG_SERVER	192.168.11.254	209.165.200.229
Router2	N/A	209.165.200.226

Time Elapsed: 00:01:59

Top Check Results Reset Activity < 1/1 >

Time: 00:01:57 Power Cycle Devices Fast Forward Time Realtime

1941 2901 2911 8191OX 819HGW 829 1240 Generic Generic 1841 2620XM 2621XM 2811

2621XM

Timeline

Fachkurs / SmartStep

CCNA Cyber Security Operations (CySecOp)

<https://www.hslu.ch/de-ch/informatik/weiterbildung/networking-and-innovative-technologies/fk-ccna-cysecop/>

Start:

Donnerstag. 9. Mai – 27. Juni 2019 jeweils 16:00 – 20:50
7 Kontaktstudienblöcke + 1 praktischer Abschlusstest (4h)

Kosten: Fr. 3950.-

Einbettung

Teil eines Grösseren:

CAS Cyber Security Defence & Response

Ausschreibung startet anfangs März

(<https://www.hslu.ch/de-ch/informatik/weiterbildung/>)

mit Start im Herbst 2019 (Sept./Okt.)

Fragen und Kommentare



Backup Slides

CCNA Cyber Sec Ops Course Outline

Chapter	Chapter Titles	Summary Description
1	Cybersecurity and the Security Operations Center	Understand the who, what, and why of cyberattacks. Different people commit cybercrime for different reasons. Security Operations Centers work to combat cybercrime.
2	Windows Operating System	Understand basic concepts of Windows, including how the operating system works and the tools used to secure Windows endpoints.
3	Linux Operating System	Perform basic Linux operations, administrative and security-related tasks.
4	Network Protocols and Services	Explain how networks normally behave using the TCP/IP suite of protocols, and associated services that enable tasks on computer networks.

CCNA Cyber Sec Ops Course Outline

Chapter	Chapter Titles	Summary Description
5	Network Infrastructure	Explain the basic operation of network infrastructures, including wired and wireless networks, network security, and network designs.
6	Principles of Network Security	Use the variety of tools and methods that threat actors use to launch network attacks.
7	Network Attacks: A Deeper Look	Understand the importance of traffic monitoring and how it is conducted. Classify vulnerabilities of network protocols and services including IP, TCP, UDP, ARP, DNS, DHCP, HTTP, and email.
8	Protecting the Network	Explain the approaches to network security defense, access control methods, and the various sources cybersecurity analysts rely on for threat intelligence.

CCNA Cyber Sec Ops Course Outline

Chapter	Chapter Titles	Summary Description
9	Cryptography and the Public Key Infrastructure	Explain the impact of cryptography on network security monitoring.
10	Endpoint Security and Analysis	Explain how to investigate endpoint vulnerabilities and attacks.
11	Security Monitoring	Explain security technologies and log files used in security monitoring.
12	Intrusion Data Analysis	Understand how network security alerts are reported, evaluated, analyzed, escalated, and preserved as evidence.
13	Incident Response and Handling	Apply incident response and handling models and procedures including the Cyber Kill Chain, the Diamond Model, the VERIS schema and National Institute of Standards and Technologies (NIST) guidelines for the structure of Computer Security Incident Response Teams (CSIRTs) and processes for handling an incident.