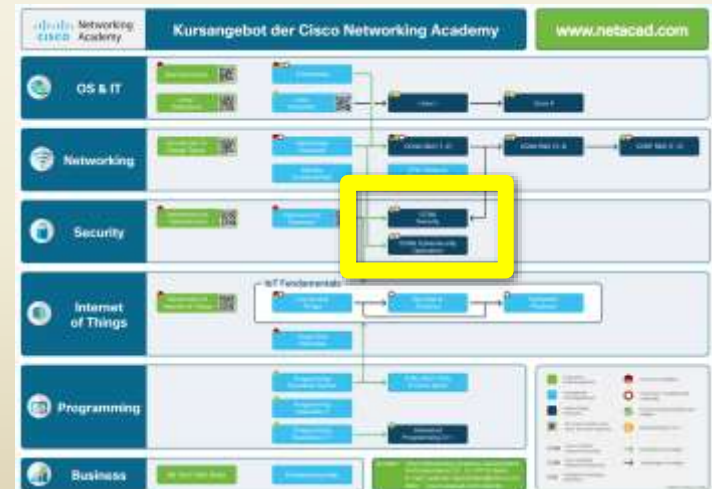




CCNA Security versus CCNA Cybersecurity Operations

Almut Leykauff-Bothe, MMBbS Hannover
 Andreas Ruhland, Bürgernetz Dillingen
 Christoph Seifert, Hochschule Fulda,





CCNA SECURITY Ziel

Mit einer CCNA Security Zertifizierung werden Fähigkeiten erworben, die für die Entwicklung einer Sicherheitsinfrastruktur erforderlich sind. Bedrohungen und Sicherheitsanfälligkeiten in Netzwerken werden erkannt sowie behoben.

Cisco CCNA Security Certification: [210-260 IINS \(Implementing Cisco Network Security\)](#)

1.0 Security Concepts	12%
2.0 Secure Access	14%
3.0 VPN	17%
4.0 Secure Routing and Switching	18%
5.0 Cisco Firewall Technologies	18%
6.0 IPS	9%
7.0 Content and Endpoint Security	12%





CCNA CYBER OPS Ziel

Die CCNA Cyber Ops-Zertifizierung bereitet Kandidaten darauf vor, eine Karriere in Zusammenarbeit mit Cybersecurity-Analysten auf Unternehmensebene in Sicherheitszentralen zu beginnen.

Cisco CCNA Cyber Ops Certification:

210-250 SECFND (Cybersecurity Fundamentals)

1.0 Network Concepts	12%
2.0 Security Concepts	17%
3.0 Cryptography	12%
4.0 Host-Based Analysis	19%
5.0 Security Monitoring	19%
6.0 Attack Methods	21%

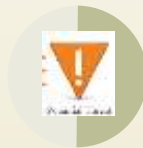
210-255 SECOPS (Cybersecurity Operations)

1.0 Endpoint Threat Analysis and Computer Forensics	15%
2.0 Network Intrusion Analysis	22%
3.0 Incident Response	18%
4.0 Data and Event Analysis	23%
5.0 Incident Handling	22%



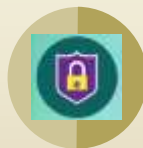
CCNA Security

Learning how to harden the network perimeter.



Cyber Ops

Learning how to identify and investigate cyberattacks.



Ethical Hacking

Learning how to assess vulnerabilities in a computer system using penetration testing techniques in a legal manner.





CCNA SECURITY Curriculum

Chapter	Title	Labs
1	Modern Network Security Threats	
2	Securing Network Devices	- Securing the Router for Administrative Access
3	Authentication, Authorization, and Accounting	- Securing Administrative Access Using AAA and RADIUS
4	Implementing Firewall Technologies	- Configuring Configuring Zone-Based Policy Firewalls
5	Implementing Intrusion Prevention	- Configuring an Intrusion Prevention System (IPS)
6	Securing the Local-Area Network	- Securing Layer 2 Switches
7	Cryptographic Systems	





CCNA SECURITY Curriculum

Chapter	Title	Labs
8	Implementing Virtual Private Networks	<ul style="list-style-type: none">- Configuring a Site-to-Site VPN Using Cisco IOS
9	Implementing the Cisco Adaptive Security Appliance	<ul style="list-style-type: none">- Configuring ASA Basic Settings and Firewall Using CLI- Configure ASA Basic Settings and Firewall using ASDM
10	Advanced Cisco Adaptive Security Appliance	<ul style="list-style-type: none">- Configure ASA Basic Settings and Firewall using ASDM- Configure a Site-to-Site IPsec VPN between an ISR and an ASA- Configure Clientless Remote Access SSL VPNs Using ASDM- Configure AnyConnect Remote Access SSL VPN Using ASDM





CCNA CYBER OPS Curriculum

Chapter	Title	Labs
1	Cybersecurity and the Security Operations Center	<ul style="list-style-type: none">- Installing the CyberOPS Workstation Virtual Machine- Cybersecurity Case Studies- Learning the Details of Attacks- Visualizing the Black Hats- Becoming a Defender
2	Windows Operating System	<ul style="list-style-type: none">- Exploring Processes, Threads, Handles, and Windows Registry- Create User Accounts- Using Windows PowerShell- Windows Task Manager- Monitor and Manage System Resources in Windows
3	Linux Operation System	<ul style="list-style-type: none">- Working with Text Files in the CLI- Getting Familiar with the Linux Shell- Linux Servers- Locating Log Files- Navigating the Linux Filesystem and Permission Settings





CCNA CYBER OPS Curriculum

Chapter	Title	Labs
4	Network Protocols and Services	<ul style="list-style-type: none">- Tracing a Route- Introduction to Wireshark- Using Wireshark to:<ul style="list-style-type: none">- Examine Ethernet Frames- Observe the TCP 3-Way Handshake- Examine a UDP DNS Capture- Examine TCP and UDP Capture- Examine HTTP and HTTPS Traffic- Exploring Nmap
5	Network Infrastructure	
6	Principles of Network Security	<ul style="list-style-type: none">- Anatomy of Malware- Social Engineering
7	Network Attacks: A Deep Look	<ul style="list-style-type: none">- Exploring DNS Traffic- Attacking a MySQL Database- Reading Server Logs
8	Protection the Network	





CCNA CYBER OPS Curriculum

Chapter	Title	Labs
9	Cryptography and the Public Key Infrastructure	<ul style="list-style-type: none">- Encrypting and Decrypting Data Using OpenSSL- Encrypting and Decrypting Using a Hacker Tool- Examining Telnet and SSH in Wireshark- Hashing Things Out- Certificate Authority Stores
10	Endpoint Security and Analysis	
11	Security Monitoring	<ul style="list-style-type: none">- Setup a Multi-VM Environment
12	Intrusion Data Analysis	<ul style="list-style-type: none">- Snort and Firewall Rules- Convert Data into a Universal Format- Regular Expression Tutorial- Extract an Executable from a PCAP- Interpret HTTP and DNS Data to Isolate Threat Actor- Isolate Compromised Host using 5-Tuple
13	Incident Response and Handling	<ul style="list-style-type: none">- Incident Handling





CCNA SECURITY Voraussetzungen

Gibt es Voraussetzungen für die Teilnahme von Studierenden am CCNA Security-Kurs?

Für einen optimalen Lernerfolg wird dringend empfohlen, dass Sie vor der Einschreibung in den CCNA Security Course über CCNA-Kenntnisse (mindestens CCNA 1+2 [CCENT Level]) verfügen





CCNA SECURITY Kurseinsatz

Organisations- und Planungsbeispiele

Fachinformatikern der Fachrichtung Systemintegration an der MMBbS

- Wahlfreikurs im 3. Ausbildungsjahr
- 8 Termine à 6 Stunden
- Laborarbeit

Technikerschulen in Deutschland

leider KEIN Angebot in ganz Deutschland

- als Wahlfach im 2. Ausbildungsjahr
- 50 UE ergänzend (blended und in-persona)
- Laborarbeit (nur in-persona)





CCNA CYBER OPS Voraussetzungen

Gibt es Voraussetzungen für die Teilnahme von Studierenden am CCNA Cyber OPS-Kurs?

Für einen optimalen Lernerfolg wird dringend empfohlen, dass Sie vor der Einschreibung in den CCNA Security Course über CCNA-Kenntnisse (mindestens CCNA 1+2 [CCENT Level]) verfügen

- Linux Grundlagen
- Windows Grundlagen
- und Cybersecurity Essentials sind hier von Vorteil





CCNA CYBER OPS Kurseinsatz

Organisations- und Planungsbeispiele

- Fachinformatikern der Fachrichtung Systemintegration an der MMBbS
 - Teilnahme am Wahlpflichtfach der FH
 - 8 CP
 - Blended learning
 - Laborarbeit
- Technikerschulen in Deutschland (Vorschlag, da leider KEIN Angebot in Deutschland)
 - als Wahlfach im 2. Ausbildungsjahr
 - 50 UE ergänzend (blended und in-persona)
 - Laborarbeit (nur in-persona)
- Studiengang Wirtschaftsinformatik Leibniz FH Hannover
 - Wahlpflichtfach im 5. und 6. Semester
 - 8 CP
 - Blended learning
 - Laborarbeit






CCNA SECURITY Equipment




Back

Search

maintenance

 **NetAcad Maintenance - Image & Hardware Support.xls**
Folder: Home » Programs » Equipment Information » NetAcad Maintenance

 **NetAcad Maintenance FAQs.pdf**
Folder: Home » Programs » Equipment Information » NetAcad Maintenance

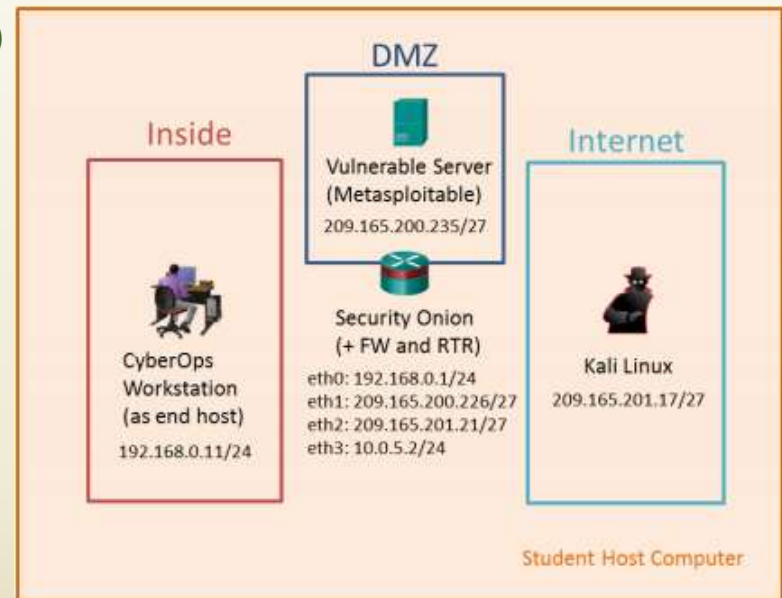




CCNA CYBER OPS Equipment

Equipment Requirements

- 1x PC / Laptop (8 GB RAM / 45 GB HDD)
je Teilnehmer





CCNA SECURITY Instructor Training

- Für neue CCNA Security Instruktoren ist eine Schulung für Instruktoren erforderlich
 - Fast Track Option verfügbar mit dem Nachweis einer CCNA Security Zertifizierung und Erfahrungen aus der Industrie
- Instruktoren Schulungen werden von Instructor Trainings Centern (ITCs) angeboten
- 40 Stunden Schulung: in-person, blended oder remote





CCNA CYBER OPS Instructor Training

- Für neue CCNA Cyber OPS Instruktoren ist eine Schulung für Instruktoren erforderlich
 - Fast Track Option verfügbar mit dem Nachweis einer CCNA CyOPS Zertifizierung und Erfahrungen aus der Industrie
- Instruktoren Schulungen werden von Instructor Trainings Centern (ITCs) angeboten
- 40 Stunden Schulung: in-person, blended oder remote





Kursangebot 2018 (CCNA CyOPS für ITQs und Instruktoren):

Bürgernetz Dillingen in Zusammenarbeit mit der Akademie für Lehrerfortbildung und Personalführung (ALP)

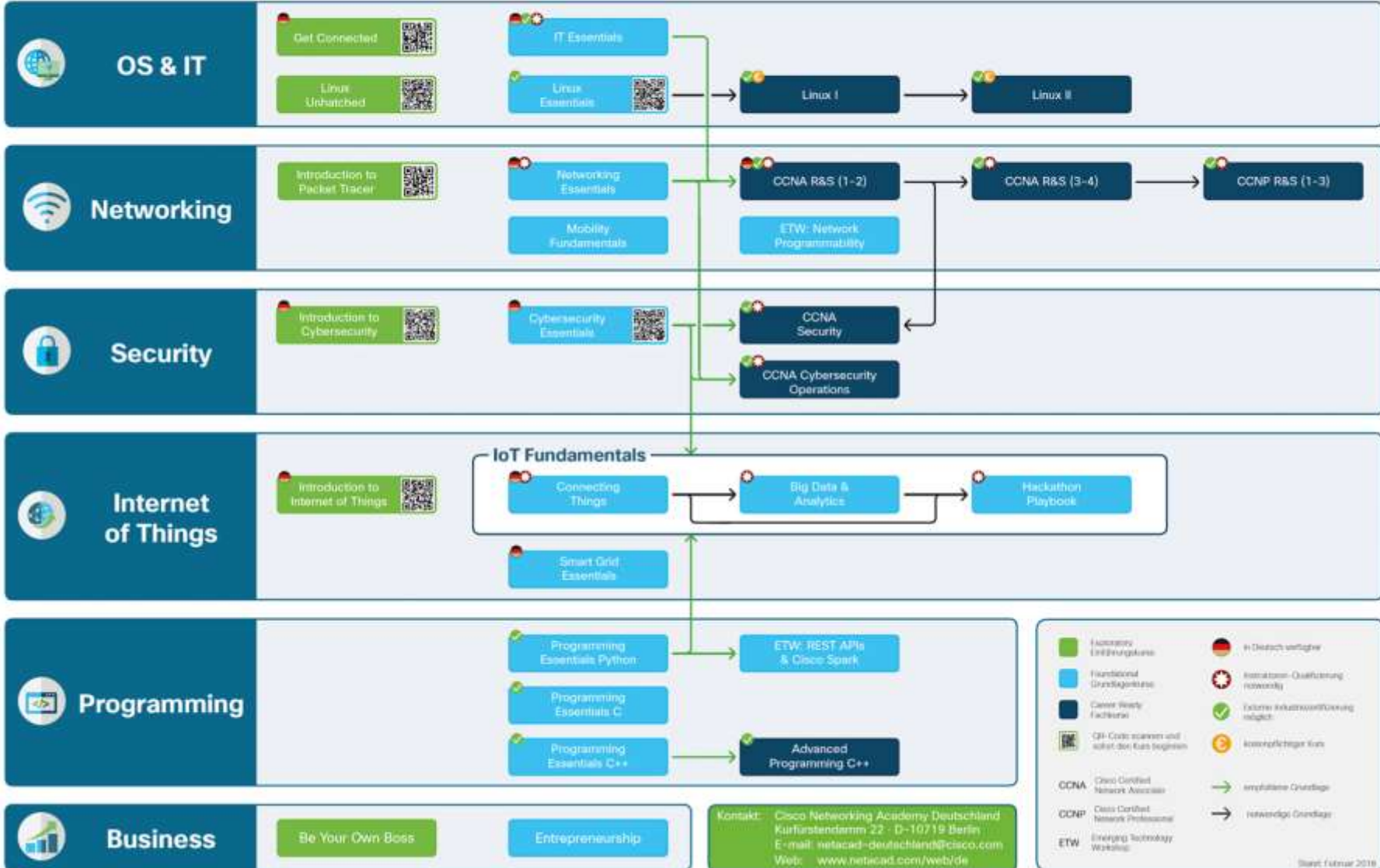
ab 01.07.18 blended learning für Kapitel 1 bis 5

27.08. bis 31.08.2018 (4 Tage Vollzeit - Präsenzphase ab Kapitel 6)

CCNA Cybersecurity Operations (CCNACyberOps) - Instruktorenqualifizierung

- Termin: 01. Juni bis 31. August 2018
- Kursort: Blended Learning; MM-BbS in Hannover
- Anmeldung: jederzeit möglich
- Instruktoren: Almut Leykauff
- Kosten: 100,00 €
- [Informationen zum Kurs](#)
- [Formular zur Kursanmeldung](#)
- Anmeldung über [Almut Leykauff-Bothe](#)







www.it-bildungsnetz.de

