



Pearson

Courses Built On SIIA CODIE AWARD Winning Platform  
19 CODiE awards in 4 years

SIIA CODiE AWARDS

# Pearson IT Cybersecurity Curriculum (ITCC)

*Complete and flexible turn-key solution for today's classroom*



[pearson.com/ITCC](https://pearson.com/ITCC)

Cisco Press



PEARSON IT CERTIFICATION



# Inside you'll find

Pearson IT Cybersecurity Curriculum (ITCC) Features .....	3	Course 4: Linux Fundamentals for Cybersecurity.....	21
Courseware Components .....	4	<b>Standard Track</b> Linux Essentials for Cybersecurity.....	21
Complete Course Pathway At a Glance.....	5	<b>Certification Track</b> CompTIA Linux+ LPIC- 1	
Certificate Options		Cert Guide .....	22
Pathway 1 – Cybersecurity Fundamentals Certificate .....	6	Course 5: Ethical Hacking and Penetration Testing .....	23
Pathway 2 – Ethical Hacking and Penetration Testing Certificate.....	7	<b>Standard Track</b> Penetration Testing Fundamentals .....	23
Pathway 3 – Incident Response and Digital Forensics Certificate.....	8	<b>Certification Track</b> Certified Ethical Hacker (CEH) Version 9 Cert Guide .....	24
Track I – Standard Textbook Focus – ISBNs.....	9	Course 6: Networking Defense and Countermeasures .....	26
Track II – Certification Guide Focus – ISBNs .....	10	<b>Standard Track</b> Network Defense and Countermeasures.....	26
Job Roles and Average Salaries .....	11	<b>Certification Track</b> – <i>N/A There is no parallel track in an industry certification for this course.</i>	
<b>COURSE DESCRIPTIONS</b>		Course 7: Cybersecurity Operations (Incident Response and Digital Forensics).....	27
Course 1: IT Fundamentals.....	13	<b>Standard Track</b> A Practical Guide to Computer Forensics Investigations .....	27
<b>Standard Track</b> Complete CompTIA A+ Guide to IT Hardware and Software .....	13	<b>Certification Track One</b> CompTIA Cybersecurity Analyst (CSA+) Cert Guide .....	28
<b>Certification Track</b> CompTIA A+ Cert Guide.....	14	<b>Certification Track Two</b> CCNA Cyber Ops SECOPS #210– 255 Official Cert Guide.....	29
Course 2: Networking Fundamentals.....	15	Course 8: Developing Cybersecurity Programs and Policies... 31	
<b>Standard Track</b> Networking Essential.....	15	<b>Standard Track</b> Developing Cybersecurity Programs and Policies / Santos & Greene.....	31
<b>Certification Track</b> CompTIA Network+ N10– 007 Cert Guide .....	16	<b>Certification Track</b> – <i>N/A There is no parallel track in an industry certification for this course.</i>	
Course 3: Cybersecurity Fundamentals.....	17	Request a Review Copy .....	33
<b>Standard Track</b> Computer Security Fundamentals.....	17	Request Access to uCertify .....	33
<b>Certification Track</b> One CompTIA Security+ SYO– 501 Cert Guide.....	18	Ordering Information.....	33
<b>Certification Track</b> Two CCNA Cyber Ops SECFND #210– 250 Official Cert Guide.....	20		

# Pearson IT Cybersecurity Curriculum (ITCC)

*Focused on employability*

## Preparing students for a career in Cybersecurity

Pearson's IT Cybersecurity Curriculum (ITCC) series is a turn-key curriculum solution for two- or four-year degree or certificate programs. Designed to support the critical need for workforce development in cybersecurity, Pearson ITCC provides **multi-modal, real-world focused, hands-on courseware** that can be used as a **complete program** or **individual courses** that can be chosen ad hoc to fill in your program to fit your student profile, workforce needs, school requirements, and articulation agreements.

The Pearson ITCC series emphasis is on applied, hands-on learning and validation through certifications set by industry organizations like EC Council, CompTIA, and Cisco. Certifications augment the merit of an academic degree by providing students with practical, industry-valued, stackable credentials proving a baseline of knowledge acquisition and competency for future employment and workforce development.

*there will be* **3.5 million**

unfilled cybersecurity jobs by 2021

## Key features of the Pearson ITCC series:

- **Two parallel options for each course:** Teach as a standard course or as a certification course. Follow one track or pick and choose courses between tracks that fit your student profile or workforce goals for your program.
- **Flexible offerings:** Create certificate programs or fill in a degree program.
- **Low-priced, multi-modal delivery:** Book, online courseware, and virtual labs, plus valuable video subscription. Books are also available through Pearson's Direct Digital Access (DDA) program, making the curriculum even more affordable to students.
- **24x7 Tech Support:** Online courseware and virtual labs delivered through our award-winning partner, uCertify.
- **Mapped to leading certifications and industry standards:** Be assured of compliance with industry standards and topic coverage — mapping to NSA DHS CAE Knowledge Units, and aligned to NIST/NICE framework, and ACM CSEC2017 curricular guidance. Also, where applicable, the Pearson ITCC courses are confirmed and certified as CompTIA Approved Quality Content (CAQC) and are the only official Cisco authorized content.

*\*Planned release dates: Many Courses available now, full program release in Fall 2018.*

**Learn more, request a demo and access**

Contact Your Pearson Sales Rep at  
[pearson.com/us/contact-us/find-your-rep.html](https://pearson.com/us/contact-us/find-your-rep.html)

Series Editor: [marybeth.ray@pearson.com](mailto:marybeth.ray@pearson.com)  
Marketing Manager: [james.manly@pearson.com](mailto:james.manly@pearson.com)

Visit [pearson.com/ITCC](https://pearson.com/ITCC) for more information.

# Flexible and comprehensive delivery options and learning tools

## Powerful online courses and labs through our partner uCertify:

- Many in-line and end-of-chapter formative exercises to help increase knowledge retention including flashcards, quizzes, exercises, and more.
- Pre-/Post course assessment tests plus additional complete practice tests included with certification courses.
- ADA compliant meeting all accessibility standards.
- Mobile App allows for anywhere learning, any time, on mobile devices
- LMS integration for single sign on (SSO) and gradebook integration. *(A one time fee could apply based on level of integration)*
- Robust instructor resources including section creation, course sharing, student enrollment, course customization, summative assessment creation, and student progress tracking and reporting.
- **Includes 24x7 customer and onboarding support.**
- Certificate of completion badging for each course.
- Pre- and post- course and lab surveys track student expectations and performance.

ITCC courses powered by Pearson partner, uCertify, winner of **19 CODiE awards in 4 years.** See more at [pearson.ucertify.com](https://pearson.ucertify.com)



### Online Labs:

Cloud-based, hands-on virtual labs integrated into each course. Many will include both robust simulation environments as well as virtual labs.



### Print/eBook:

All of the ITCC courses are developed as standard Pearson print / eBooks with TWO OPTIONS where a correlating certification is available:

1. Standard textbook
2. Certification Guide

eBooks can be adopted through Pearson's Direct Digital Access (DDA) program making the curriculum even more affordable to students



### Instructor Supplements:

Each course will come complete with a full set of instructor supplements:

- Instructor's guide
- PowerPoint slides (Figure & Lecture versions)
- Test bank
- Instructors interested in applying for CAE designation can use our documentation to confirm coverage of applicable Knowledge Units



### Student Supplements:

**Video Subscription**—A low-cost, optional subscription to a selection of Pearson's professional Live Lessons or Complete Video Course video products. The streaming video is purchased and delivered through uCertify platform within the courses. These video products equal 15–25 hours of high-quality instructional video produced by many of the security industry's leading technologists. This valuable supplement can be used to flip the classroom and allow for independent study, or alternative delivery of lab/classroom instruction to showcase demonstrations of key technology topics. The video product also allows for student remediation outside of the classroom.



**Ancillary Texts**—Where applicable, Pearson produces key supplementary books and web editions that could be bundled with the main course books:

- 31 Days Before Your Certification Exam — Digital Study Guide
- Portable Command Guide
- Lab manuals

## Complete Course Pathway At-A-Glance — Stackable Credentials & Multiple Pathways

Credit Hours	#	Course	Track I - Standard Textbook focus	Track II - Certification Guide Focus
4-6	1	IT Fundamentals	Complete CompTIA A+ Guide to IT Hardware and Software	CompTIA A+
3	2	Networking Fundamentals	Networking Essentials	CompTIA Network+
3	3	Cybersecurity Fundamentals	Computer Security Fundamentals	CompTIA Security+ or CCNA Cyber Ops - SECFND
3	4	Linux Fundamentals for Cybersecurity	Linux Essentials for Cybersecurity	CompTIA Linux+/LPIC-1
3	5	Ethical Hacking and Penetration Testing	Penetration Testing Fundamentals	Certified Ethical Hacker (CEH)
3	6	Network Defense & Countermeasures	Network Defense and Countermeasures	**
3	7	Cybersecurity Operations – Incident Response & Digital Forensics	A Practical Guide to Computer Forensics Investigations	CompTIA CSA+ or CCNA Cyber Ops - SECOPS
3	8	Developing Cybersecurity Programs and Policies	Developing Cybersecurity Programs and Policies	**

\*\* No parallel certification, use Track I



## Other Certificate options — focused on employability

The Pearson ITCC series can be offered as a part of a full degree program when integrated with general education course requirements. Schools also have the option of offering these courses as part of a cybersecurity certificate program or pathway. The entire 8-course curriculum could be used as a Cybersecurity Certificate.

This would qualify students for the following job roles:

- Cybersecurity Specialist
- Cybersecurity Technician
- Incident Analyst/Responder

In addition to this 8-course certificate, the following are examples of some other certificate program options.



### Pathway 1: Cybersecurity Fundamentals Certificate

#	Course	Track I – Standard Textbook Focus	Track II – Certification Guide Focus
1	IT Fundamentals	Complete CompTIA A+ Guide to IT Hardware and Software	CompTIA A+
2	Networking Fundamentals	Networking Essentials	CompTIA Network+
3	Cybersecurity Fundamentals	Computer Security Fundamentals	CompTIA Security+

This 3-course option provides foundational knowledge of computer hardware and operating systems, networking, and cybersecurity. There are three industry certifications that can be obtained after completion of these courses (CompTIA A+, CompTIA Network+, and CompTIA Security+) Completion of this program qualifies students for the following cybersecurity job roles:

- Security Specialist
- Security Consultant
- Security Engineer
- Security Administrator

In 2017, the U.S employed

**780,000** *people in cybersecurity positions,*

..... WITH APPROXIMATELY **350,000**  
**current cybersecurity openings**

Source: CyberSeek



## Pathway 2: Ethical Hacking and Penetration Testing Cybersecurity Certificate

#	Course	Track I – Standard Textbook Focus	Track II – Certification Guide Focus
2	Networking Fundamentals	Networking Essentials	CompTIA Network+
3	Cybersecurity Fundamentals	Computer Security Fundamentals	CompTIA Security+
4	Linux Fundamentals for Cybersecurity	Linux Essentials for Cybersecurity	CompTIA Linux+/LPIC-1
5	Ethical Hacking and Penetration Testing	Penetration Testing Fundamentals	Certified Ethical Hacker (CEH)
6	Network Defense & Countermeasures	Network Defense and Countermeasures	**

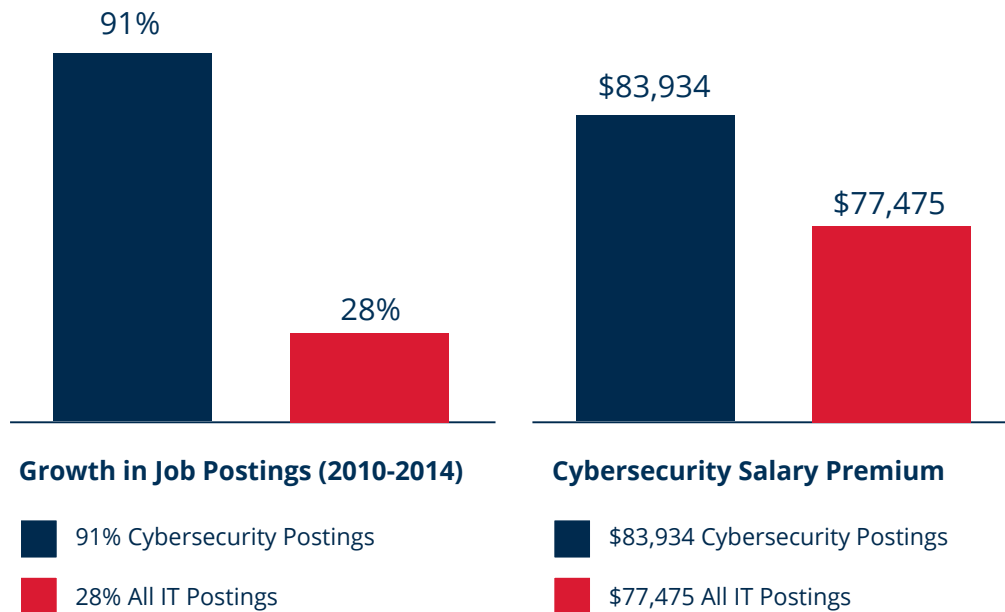
\*\* No parallel certification, use Track I

This 5-course certificate assumes basic knowledge of computer hardware/operating systems and starts with networking and cybersecurity fundamentals. It then builds upon this foundation with a focus on ethical hacking and penetration testing. A course on Linux is offered as most hacking tools run on Linux. The program wraps up with course on network defense and countermeasures, teaching students how to plug the holes they found in the hacking course. Four industry certifications can be obtained after completion of

the courses (CompTIA Network+, CompTIA Security+, CompTIA Linux+, and EC-Council's Certified Ethical Hacker). Completion of the program qualifies students for the following cybersecurity job roles:

- Ethical Hacker
- Penetration Tester
- Homeland Security Specialist
- IT Security Consultant
- IT Security Specialist

“Every IT position is also a cybersecurity position now” according to the *CyberSecurity Jobs Report, 2017*



•According to the International Information System Security Certification Consortium, Inc., (ISC)<sup>2</sup>® membership counts as of July 14,2015



### Pathway 3: Incident Response and Digital Forensics Cybersecurity Certificate

#	Course	Track I – Standard Textbook Focus	Track II – Certification Guide Focus
2	Networking Fundamentals	Networking Essentials	CompTIA Network+
3	Cybersecurity Fundamentals	Computer Security Fundamentals	CompTIA Security+ or CCNA Cyber Ops -SECFND
6	Linux Fundamentals for Cybersecurity	Network Defense and Countermeasures	**
7	Ethical Hacking and Penetration Testing	A Practical Guide to Computer Forensics Investigations	CompTIA CSA+ or CCNA Cyber Ops-SECOPS
8	Network Defense & Countermeasures	Developing Cybersecurity Program and Policies	**

\*\* No parallel certification, use Track I

This 5-course certificate also assumes basic knowledge of computer hardware/operating systems and starts with the networking and cybersecurity fundamentals. From there, it builds towards the forensics focus by covering networking security, incident response/ computer forensics, and cybersecurity programs and policies. There are 2-3 industry certifications that can be earned in this option, depending on whether schools focus on the CompTIA cybersecurity certifications or the Cisco CCNA CyberOps certification. Completion of the program qualifies students for the following cybersecurity job roles:

- Security Analyst
- Security Engineer
- Vulnerability Analyst
- Security Operations Center Analyst
- Cybersecurity Specialist
- Computer Forensics Technician
- Cybersecurity Analyst



## Pearson ITCC Program Tracks



### Track 1 – Standard Textbook Focus

Course		Track I – Standard Textbook Focus
1	IT Fundamentals	<i>Complete CompTIA A+ Guide to IT Hardware and Software</i> 7th Ed Schmidt <b>Book:</b> 9780789756459 <b>Course + Lab:</b> 9780789757548 <b>Book+Course+Lab:</b> 9780789757562
2	Networking Fundamentals	<i>Networking Essentials: A CompTIA Network+ N10-007 Textbook</i> , 7th Ed Beasley & Nilkaew <b>Book:</b> 9780789758743 <b>Book+Course+Lab:</b> 9780789759870 <b>Course + Lab:</b> 9780789758729
3	Cybersecurity Fundamentals	<i>Computer Security Fundamentals</i> , 3rd Ed Easttom <b>Book:</b> 9780789757463 <b>Book+Course+Lab:</b> 9780789759566 <b>Course + Lab:</b> 9780789759559
4	Linux Fundamentals for Cybersecurity	<i>Linux Essentials for Cybersecurity</i> Rothwell & Pheils <b>Book:</b> 9780789759351 <b>Book+Course+Lab:</b> 9780789759368 <b>Course + Lab:</b> 9780789759344
5	Ethical Hacking and Penetration Testing	<i>Penetration Testing Fundamentals</i> Easttom <b>Book:</b> 9780789759375 <b>Book+Course+Lab:</b> 9780789759610 <b>Course + Lab:</b> 9780789759627
6	Network Defense & Countermeasures	<i>Network Defense and Countermeasures</i> , 3rd Ed Easttom <b>Book:</b> 9780789759962 <b>Book+Course+Lab:</b> 9780789759993 <b>Course + Lab:</b> 9780789759986
7	Cybersecurity Operations – Incident Response & Digital Forensics	<i>A Practical Guide to Computer Forensics Investigations</i> Hayes <b>Book:</b> 9780789741158 <b>Book+Course+Lab:</b> 9780789759719 <b>Course + Lab:</b> 9780134998688 <b>NEW EDITION coming:</b> Spring 2019
8	Developing Cybersecurity Programs and Polices	<i>Developing Cybersecurity Programs and Policies</i> Santos <b>Book:</b> 9780789759405 <b>Book+Course:</b> 9780789759436 <b>Course:</b> 9780134858685



## Track II – Certification Guide Focus

Course		Track II - Certification Guide Focus
1	IT Fundamentals	<i>CompTIA A+ Cert Guide Academic Edition</i> Soper <b>Book:</b> 9780789756534 <b>Book+Course+Lab:</b> 9780789757609 <b>Course + Lab:</b> 9780789757593
2	Networking Fundamentals	<i>CompTIA A+ Cert Guide Academic Edition</i> Soper <b>Book:</b> 9780789756534 <b>Book+Course+Lab:</b> 9780789757609 <b>Course + Lab:</b> 9780789757593
3	Cybersecurity Fundamentals	<i>CompTIA Security+ SYO-501 Cert Guide, Academic Edition, 2nd Ed</i> Prowse <b>Book:</b> 9780789759122 <b>Book+Course+Lab:</b> 9780789759153 <b>Course + Lab:</b> 9780789759139 – OR – <i>CCNA Cyber Ops SECFND #210-250 Official Cert Guide</i> Santos, Muniz, & De Crescenzo <b>Book:</b> 9781587147029 <b>Book+Course+Lab:</b> 9780789760050 <b>Course + Lab:</b> 9780789760043
4	Linux Fundamentals for Cybersecurity	<i>CompTIA Linux+ LPIC-1 Cert Guide</i> Brunson & Walberg <b>Book:</b> 9780789754554 <b>Book+Course+Lab:</b> 9780789757975 <b>Course + Lab:</b> 9780789758453
5	Ethical Hacking and Penetration Testing	<i>Certified Ethical Hacker (CEH) Version 9 Cert Guide, 2nd Ed</i> Gregg <b>Book:</b> 9780789756916 <b>Book+Course+Lab:</b> 9780789756930 <b>Course + Lab:</b> 9780789756923
6	Network Defense & Countermeasures	N/A*
7	Cybersecurity Operations – Incident Response & Digital Forensics	<i>CompTIA Cybersecurity Analyst (CSA+) Cert Guide</i> MacMillan <b>Book:</b> 9780789756954 <b>Book+Course+Lab:</b> 9780789760029 <b>Course + Lab:</b> 9780789760012 –OR– <i>CCNA Cyber Ops SECOPS #210-255 Official Cert Guide</i> Santos & Muniz <b>Book:</b> 9781587147036 <b>Book+Course+Lab:</b> 9781587147104 <b>Course + Lab:</b> 9781587147098
8	Developing Cybersecurity Programs and Policies	N/A*

\* No parallel certification, use Track I



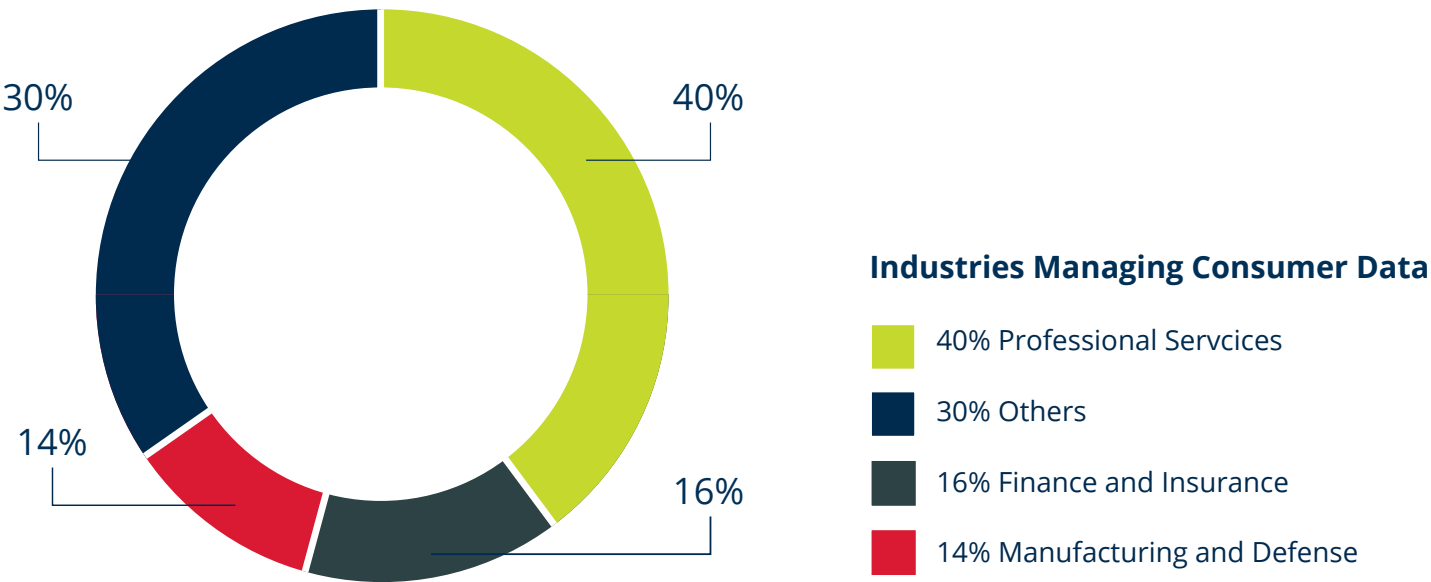
## Job Role/Salaries

	Course	Course Entry-level Job Roles	Average Salaries	Program Entry-Level Job Role <sup>1</sup>	Average Salary <sup>3</sup>
1	IT Fundamentals	<ul style="list-style-type: none"> <li>·Technical Support Specialist</li> <li>·Field Service Technician</li> <li>·IT Support Technician</li> <li>·IT Administrator</li> </ul>	~ \$77,053 <sup>2</sup>	<ul style="list-style-type: none"> <li>·Cybersecurity Specialist - Technician</li> <li>·Incident Analyst / Responder</li> </ul>	~ \$96,500
2	Networking Fundamentals	<ul style="list-style-type: none"> <li>·Network Field Technician</li> <li>·Network Administrator</li> <li>·IS Consultant</li> <li>·Network Field Engineer</li> </ul>	~ \$79,459 <sup>2</sup>		
3	Cybersecurity Fundamentals	<ul style="list-style-type: none"> <li>·Security Specialist</li> <li>·Security Consultant</li> <li>·Security Engineer</li> <li>·Security Administrator</li> </ul>	~ \$87,673 <sup>2</sup>		
4	Linux Fundamentals for Cybersecurity	<ul style="list-style-type: none"> <li>·Linux Database Administrator</li> <li>·Junior Linux Administrator</li> <li>·Junior Network Administrator</li> </ul>	~ \$78,593 <sup>2</sup>		
5	Ethical Hacking and Penetration Testing	<ul style="list-style-type: none"> <li>·Ethical Hacker</li> <li>·Penetration Tester</li> <li>·Homeland Security Specialist</li> <li>·IT Security Consultant</li> <li>·IT Security Specialist</li> </ul>	~\$120,220 <sup>4</sup>		
6	Network Defense & Countermeasures	<ul style="list-style-type: none"> <li>·Network Security Administrator</li> <li>·Network Security Specialist</li> <li>·Security Technician</li> <li>·Network Security Support Engineer</li> </ul>	~ \$84,652 <sup>2</sup>		
7	Cybersecurity Operations – Incident Response & Digital Forensics	<ul style="list-style-type: none"> <li>·Security Analyst</li> <li>·Vulnerability Analyst</li> <li>·Cybersecurity Specialist</li> <li>·Cybersecurity Analyst</li> <li>·Security Engineer</li> <li>·Security Operations Center Analyst</li> <li>·Computer Forensics Technician</li> </ul>	~ \$92,000 <sup>5</sup>		
8	Developing Cybersecurity Programs and Policies	<ul style="list-style-type: none"> <li>·Security Operations Center Analyst</li> </ul>	n/a		

**References:** **1.** Salaries will vary based on experience and location. This is just a general benchmark. **2.** Source: 2017 IT Skills & Salary Report by Global Knowledge | Base: 14,000+ IT Professionals **3.** Based on junior-level cybersecurity job postings in Talent Neuron for last 12 months. Median salary **4.** Source: Certification Magazine 2016 salary survey **5.** Estimate, as these are new certifications: between Sec+ and CASP (\$97K)



# Fastest cybersecurity demand sectors are in industries managing consumer data



Source: Job Market Intelligence: Cybersecurity Jobs, 2015-2016 Burning Glass Technologies

# Course 1: IT Fundamentals

This course establishes the foundation for understanding information technology for a cybersecurity career. The course demonstrates how to build, connect, manage, and troubleshoot multiple

devices in authentic scenarios. The material builds on the CompTIA A+ exam objectives including coverage of Windows, Linux, Mac, mobile, cloud, and expanded troubleshooting and security.

## Standard Track

### Schmidt

Complete CompTIA A+ Guide to IT Hardware and Software, 7th Edition

Book: 9780789756459

Book+Course+Lab: 9780789757562

Course + Lab: 9780789757548

This unique all-in-one textbook and lab manual teaches the fundamentals of IT device installation, configuration, maintenance, and networking with thorough instruction built on the CompTIA A+ 220-901 and 220-902 exam objectives. Students will learn all the skills they need to become certified professionals and customer-friendly technicians using today's tools and technologies.

- Written by Network Engineering Technology professor with industry experience, Cheryl Schmidt
- The modern IT Tech Support learning guide that also helps prepare students for the latest A+ certification exam
- Includes over 100 hands-on labs PLUS hundreds more online with optional uCertify bundle
- Includes review questions, soft skills sections, tech tips, key terms, glossary, hundreds of learning exercises, critical thinking activities, and other learning tools that establish a solid foundation for understanding
- Realistic coverage includes common legacy technologies along with non-certification topics like Windows 10

### About the author

**Cheryl Schmidt** is a professor of Network Engineering Technology at Florida State College at Jacksonville. Prior to joining the faculty ranks, she oversaw the LAN and PC support for the college and other organizations.



### Table of Contents

#### Introduction

#### Features of This Book

#### Part I CompTIA 200-901 Exam Focus

- Chapter 1: Intro to the World of IT
- Chapter 2: Connectivity
- Chapter 3: On the Motherboard
- Chapter 4: Intro to Configuration
- Chapter 5: Disassembly and Power
- Chapter 6: Memory
- Chapter 7: Storage Devices
- Chapter 8: Multimedia Devices
- Chapter 9: Video Technologies
- Chapter 10: Printers
- Chapter 11: Mobile Devices
- Chapter 12: Computer Design and Troubleshooting Review
- Chapter 13: Internet Connectivity
- Chapter 14: Introduction to Networking

#### Part II CompTIA 220-902 Exam Focus

- Chapter 15: Basic Windows
- Chapter 16: Windows Vista, 7, 8, and 10
- Chapter 17: OS X and Linux Operating Systems
- Chapter 18: Computer and Network Security
- Chapter 19: Operational Procedures
- Appendix A: Subnetting
- Appendix B: Certification Exam Objectives (Online)
- Glossary

## Certification Track

### Soper

CompTIA A+ Cert Guide, Academic Edition

Book: 9780789756534

Book+Course+Lab: 9780789757609

Course + Lab: 9780789757593

In this best-of-breed full-color study guide, a leading expert helps students master all the topics they need to know to succeed on the CompTIA 220-901 and 902 exams and move into a successful career as an IT technician. The Academic Edition is ideal for the classroom and includes bonus content such as exam objectives table for easy navigation by chapter, a full objectives index for each exam, and a master list of key topics, each of which give the student the page number where the objective/topic can be found. Every feature of this book is designed to support both efficient exam preparation and long-term mastery.

#### *About the author*

**Mark Edward Soper** has been working with PCs since the days of the IBM PC/XT and AT as a salesperson, technology advisor, consultant, experimenter, technology writer, and content creator. Since 1992, he has taught thousands of students across the country how to repair, manage, and troubleshoot the hardware, software, operating systems, and firmware inside their PCs.

#### *Table of Contents:*

##### **Introduction**

Chapter 1: Technician Essentials and Computer/Device Anatomy

Chapter 2: Configure and Use BIOS/UEFI Tools

Chapter 3: Motherboard Components

Chapter 4: RAM Types and Features

Chapter 5: PC Expansion Cards

Chapter 6: Storage Devices

Chapter 7: CPUs



Chapter 8: Ports and Interfaces

Chapter 9: Designing and Building Custom PC Configurations

Chapter 10: Using, Maintaining, and Installing Printers and Multifunction Devices

Chapter 11: Networking

Chapter 12: Mobile Devices

Chapter 13: Hardware and Network Troubleshooting

#### **Supplemental Texts**

31 Days Before your CompTIA A+ Exam  
9780789758163

31 Days Before your CompTIA A+ Exam  
Digital Study Guide  
9780134540030

CompTIA A+ 220-901 and 220-902  
Practice Questions Exam Cram  
9780789756305

CompTIA A+ 220-901 and 220-902 Exam Cram  
9780789756312

# Course 2: Networking Fundamentals

Learning how a network works is essential to understanding how vulnerabilities are assessed, corrected, and issues are mitigated. This course provides

a comprehensive foundation in networking concepts and technologies. Students will learn how to use, install, and configure basic networking technologies.

## Standard Track

### Beasley & Nilkaew

Networking Essentials: A CompTIA Network+ N10-007 Textbook, 7th Edition

Book: 9780789758743

Book+Course+Lab: 9780789759870

Course + Lab: 9780789758729

*Networking Essentials*, 7th Edition guides students from an entry-level knowledge in computer networks to advanced concepts in Ethernet and TCP/IP networks; routing protocols and router configuration; local, campus, and wide area network configuration; network security; wireless networking; optical networks; Voice over IP; the network server; and Linux networking. This new edition includes expanded coverage of mobile and cellular communications; configuring static routing with RIPv2, OSPF, EIGRP, and IS-IS; physical security, access control, and biometric access control; cloud computing and virtualization; and codes and standards.

Clear goals are outlined for each chapter, and every concept is introduced in easy to understand language that explains how and why networking technologies are used. Each chapter is packed with real-world examples and practical exercises that reinforce all concepts and guide you through using them to configure, analyze, and fix networks.

### About the authors

**Jeffrey S. Beasley** is with the Department of Engineering Technology and Surveying Engineering at New Mexico State University. He has been teaching with the department since 1988.

**Piyasat Nilkaew** is a network engineer with 15 years of experience in network management and consulting, and has extensive expertise in deploying and integrating multiprotocol and multi vendor data, voice, and video network solutions on limited budgets.



### Table of Contents:

- Chapter 1: Introduction to Computer Networks
- Chapter 2: Physical Layer Cabling: Twisted Pair
- Chapter 3: Physical Layer Cabling: Fiber Optics
- Chapter 4: Wireless Networking
- Chapter 5: Interconnecting the LANs
- Chapter 6: TCP/IP
- Chapter 7: Introduction to Router Configuration
- Chapter 8: Introduction to Switch Configuration
- Chapter 9: Routing Protocols
- Chapter 10: Internet Technologies: Out to the Internet
- Chapter 11: Troubleshooting
- Chapter 12: Network Security
- Chapter 13: Cloud Computing and Virtualization
- Chapter 14: Codes and Standar

## Certification Track

### Sequeira & Taylor

CompTIA Network+ N10-007 Cert Guide,  
Deluxe Edition

Book: 9780789759825

Book+Course+Lab: 9780789759856

Course + Lab: 9780789759849

*CompTIA Network+ N10-007 Cert Guide, Deluxe Edition* contains proven study features that enable students to succeed on the exam the first time. Best-selling author and expert instructors Anthony Sequeira and Keith Barker share preparation hints and test-taking tips, helping students identify areas of weakness and improve both their conceptual knowledge and hands-on skills.

#### About the author

**Anthony Sequeira**, CCIE No. 15626, is a seasoned trainer and author regarding all levels and tracks of Cisco certification. When not writing for Cisco Press and Pearson IT Certification, Anthony is a full-time instructor at CBT Nuggets.

Network+ Certified since 2003, **Michael Taylor** currently serves as Computer Sciences Department Head for a career college in the eastern United States where he has taught for the past ten years.

#### Table of Contents:

##### Introduction

Chapter 1: Computer Network Fundamentals

Chapter 2: The OSI Reference Model

Chapter 3: Network Components

Chapter 4: Ethernet Technology

Chapter 5: IPv4 and IPv6 Addresses

Chapter 6: Routing IP Packets

Chapter 7: Wide Area Networks (WANs)

Chapter 8: Wireless Technologies



Chapter 9: Network Optimization

Chapter 10: Command-Line Tools

Chapter 11: Network Management

Chapter 12: Network Security

Chapter 13: Network Policies and Best Practices

Chapter 14: Network Troubleshooting

Chapter 15: Final Preparation Appendix A Answers to Review Questions Appendix B CompTIA Network+ N10-07 Cert Guide Exam Updates Glossary

#### ONLINE ELEMENTS:

Appendix C: Memory Tables

Appendix D: Memory Tables Answer Key

Appendix E: Study Planner

Exam Essentials Interactive Study Guide

Key Terms Flash Cards Application

Instructional Videos

Performance-Based Exercises

CompTIA Network+ N10-007 Hands-on Lab

Simulator Lite Software

#### Supplemental Text

CompTIA Network+ N10-007 Exam Cram 9  
780789758750



# Course 3: Cybersecurity Fundamentals

This course introduces students to the knowledge necessary to improve security by identifying and prioritize potential threats and vulnerabilities of a network including raising cybersecurity awareness; halting malware including viruses, spyware, worms, and Trojans; resist modern social engineering and phishing attacks; defend against denial of service (DoS) attacks;

implement a layered approach to security; learning the motivations of hackers; identification and selection of appropriate security technologies and policies for a given scenario. Advanced topics of encryption selection, cyberterrorism and information warfare, and basic computer forensics are discussed. Introduces the legal aspects of policies and issues with compliance.

## Standard Track

### Easttom

Computer Security Fundamentals, 3rd Edition

Book: 9780789757463

Book+Course+Lab: 9780789759566

Course + Lab: 9780789759559

*The Computer Security Fundamentals*, 3rd Edition covers web attacks, hacking, spyware, network defense, security appliances, VPNs, password use, and much more. Its many tips and examples reflect new industry trends and the state-of-the-art in both attacks and defense. Exercises, projects, and review questions in every chapter help students deepen their understanding and apply all they've learned.

- The most up-to-date computer security concepts text on the market
- Strong coverage and comprehensive analysis of key attacks, including denial of service, malware, and viruses
- Covers oft-neglected subject areas such as cyberterrorism, computer fraud, and industrial espionage
- Contains end-of-chapter exercises, projects, review questions, and plenty of real-world tips

### About the author

**Chuck Easttom** spent many years in the IT industry, followed by three years teaching computer science and security at a technical college. He has since returned to industry as an IT manager with system security responsibilities. He has also served as a subject matter expert for CompTIA in developing or revising four certification exams, including Security+.



### Table of Contents:

#### Introduction

Chapter 1: Introduction to Computer Security

Chapter 2: Networks and the Internet

Chapter 3: Cyber Stalking, Fraud, and Abuse

Chapter 4: Denial of Service Attacks

Chapter 6: Techniques Used by Hackers

Chapter 7: Industrial Espionage in Cyberspace

Chapter 8: Encryption

Chapter 9: Computer Security Technology

Chapter 10: Security Policies

Chapter 11: Network Scanning and Vulnerability Scanning

Chapter 12: Cyber Terrorism and Information Warfare

Chapter 13: Cyber Detective

Chapter 14: Introduction to Forensics

Appendix A: Glossary

Appendix B: Resources

## Certification Track I

### Prowse

CompTIA Security+ SYO-501 Cert Guide,  
Academic Edition, 2nd Edition

Book: 9780789759122

Book+Course+Lab: 9780789759153

Course + Lab: 9780789759139

*The CompTIA Security+ SYO-501 Cert Guide, Academic Edition, 2nd Edition*, helps students learn, prepare, and practice for CompTIA Security+ SYO-501 exam success with this full-color CompTIA Authorized Cert Guide. This book includes access to four complete practice tests, chapter summaries, and case studies including simulations and hands-on video exercises to reinforce the learning.

#### About the author

**David L. Prowse** is an author, a computer specialist, and a technical trainer. He loves computer technology, and enjoys sharing with others what he has learned.

#### Table of Contents:

##### Introduction

Chapter 1: Introduction to Security  
Chapter 2: Computer Systems Security Part I  
Chapter 3: Computer Systems Security Part II  
Chapter 4: OS Hardening and Virtualization  
Chapter 5: Application Security  
Chapter 6: Network Design Elements  
Chapter 7: Networking Protocols and Threats  
Chapter 8: Network Perimeter Security  
Chapter 9: Securing Network Media and Devices  
Chapter 10: Physical Security and Authentication Models  
Chapter 11: Access Control Methods and Models  
Chapter 12: Vulnerability and Risk Assessment  
Chapter 13: Monitoring and Auditing  
Chapter 14: Encryption and Hashing Concepts



Chapter 15: PKI and Encryption Protocols  
Chapter 16: Redundancy and Disaster Recovery  
Chapter 17: Social Engineering, User Education, and Facilities Security  
Chapter 18: Policies and Procedures  
Chapter 19: Taking the Real Exam  
Glossary 458  
Elements Available Online  
Appendix A: Answers to the Review Questions  
Answers to Practice Exam 1  
View Recommended Resources  
Real-World Scenarios  
Flash Cards

### SUPPLEMENTAL TEXT

CompTIA Security+ SYO-501 Exam Cram 9780789759009



A new report out from  
**Cybersecurity Ventures** estimates

*there will be*

**3.5** MILLION

***unfilled cybersecurity jobs by 2021***

up from 1 million openings last year.

## Certification Track II

### Santos, Muniz, & De Crescenzo

CCNA Cyber Ops SECFND #210-250

Official Cert Guide

Book: 9781587147029

Book+Course+Lab: 9780789760050

Course + Lab: 9780789760043

*CCNA Cyber Ops SECFND 210-250 Official Cert Guide* from Cisco Press allows students to succeed on the exam the first time. Cisco enterprise security experts Omar Santos, Joseph Muniz, and Stefano De Crescenzo share preparation hints and test-taking tips, helping students identify areas of weakness, and improve both their conceptual knowledge and hands-on skills.

#### About the authors

**Omar Santos** is an a principal engineer of the Cisco Product Security Incident Response Team (PSIRT).

**Joseph Muniz** is an architect at Cisco Systems and a security researcher.

**Stefano De Crescenzo** is a senior incident manager with the Cisco Product Security Incident Response Team (PSIRT).

#### Table of Contents:

##### Introduction

##### Part I Network Concepts

Chapter 1: Fundamentals of Networking Protocols and Networking Devices

Chapter 2: Network Security Devices and Cloud Services

##### Part II Security Concepts

Chapter 3: Security Principles

Chapter 4: Introduction to Access Controls

Chapter 5: Introduction to Security Operations Management



##### Part III Cryptography

Chapter 6: Fundamentals of Cryptography and Public Key Infrastructure (PKI)

Chapter 7: Introduction to Virtual Private Networks (VPNs)

##### Part IV Host-Based Analysis

Chapter 8: Windows-Based Analysis

Chapter 9: Linux- and Mac OS X—Based Analysis

Chapter 10: Endpoint Security Technologies

##### Part V Security Monitoring and Attack Methods

Chapter 11: Network and Host Telemetry

Chapter 12: Security Monitoring Operational Challenges

Chapter 13: Types of Attacks and Vulnerabilities

Chapter 14: Security Evasion Techniques

##### Part VI Final Preparation

Chapter 15: Final Preparation

##### Part VII Appendixes

Appendix A: Answers to the “Do I Know This Already?” Quizzes and Q&A

Questions

Glossary

Elements Available on the Book Website

Appendix B: Memory Tables

Appendix C: Memory Tables Answer Key

Appendix D: Study Planner

# Course 4: Linux Fundamentals for Cybersecurity

This course supplies critical knowledge for securing this common OS, and also for using cybersecurity tools in future classes. Linux is an alternative to more common platforms for security, cost, and scalability. This course introduces fundamental Linux concepts from proper set-up installation through administration of accounts

devices, services, processes, and functions — with a unique primary focus on security. This course also covers basic scripting taught to understand tools used later for Penetration Testing and cybersecurity threat detection.

## Standard Track

### Rothwell & Pheils

Linux Essentials for Cybersecurity

Book: 9780789759351

Book+Course+Lab: 9780789759368

Course + Lab: 9780789759344

*Linux Fundamentals for Cybersecurity* introduces fundamental Linux concepts from proper set-up installation through administration of accounts, devices, services, processes, and functions. This course also covers basic scripting taught to understand tools for Penetration Testing and cybersecurity threat detection.

The focus of this book will be to provide a very practical and hands-on description of Linux Operating System components with an emphasis on how to deploy and use each securely. Each chapter will include hands-on practice exercises, providing the learner with the ability to practice what they learn.

### About the authors

**William “Bo” Rothwell** is the founder and president of One Course Source, an IT training organization.

**Denise Pheils**, PhD, is a Professor of Cybersecurity and Networking, Owens Community College.

### Table of Contents

#### Part I: Introducing Linux

Chapter 1: Distributions and key components

Chapter 2: Working on the command line

Chapter 3: Getting help

Chapter 4: Editing files

Chapter 5: When things go wrong

#### Part II: User and group accounts

Chapter 6: Managing group accounts

Chapter 7: Managing user account

Chapter 8: Develop an account security policy

#### Part III: File and data storage

Chapter 9: File permissions

Chapter 10: Manage local storage: Concepts

Chapter 11: Manage local storage: Practical application

Chapter 12: Manage network storage

Chapter 13: Develop a storage security policy

#### Part IV: Automation

Chapter 14: Crontab and at

Chapter 15: Scripting

Chapter 16: Common automation tasks

Chapter 17: Develop an automation security policy

#### Part V: Networking

Chapter 18: Networking basics

Chapter 19: Network configuration

Chapter 20: Network service configuration: Essential services

Chapter 21: Network service configuration: Web services

Chapter 22: Connecting to remote systems

Chapter 23: Develop a network security policy

#### Part VI: Process and log administration

Chapter 24: Process control

Chapter 25: System logging

Chapter 26: Develop a process and log security policy

#### Part VII: Software management

Chapter 27: Red Hat-based software management

Chapter 28: Debian-based software management

Chapter 29: Addition management tools

Chapter 30: System booting

Chapter 31: Develop a software management security policy

#### Part VIII: Security tasks

Chapter 32: Footprinting

Chapter 33: Firewalls

Chapter 34: Intrusion Detection Systems

Chapter 35: Additional security tasks



## CertificationTrack

### Brunson & Walberg

CompTIA Linux+ LPIC-1 Cert Guide

Book: 9780789754554

Book+Course+Lab: 9780789757975

Course + Lab: 9780789758453

*The Linux+ / LPIC-1 Authorized Cert Guide* has a single goal: to help students pass the new version of the Linux Professional Institute LPIC-1 exams. Authored by long-time Linux trainers, it presents focused, straight-to-the-point coverage of all LPIC-1 exam topics that power the CompTIA Linux+ exams.

#### *About the authors*

**Ross Brunson** is a contract instructor and consultant with Beacon Technologies.

**Sean Walberg** is currently a network engineer for a large Canadian financial services company.

#### *Table of Contents:*

Chapter 1: Installing Linux  
Chapter 2: Boot Process and Runlevels  
Chapter 3: Package Install and Management  
Chapter 4: Basic Command Line Usage  
Chapter 5: File Management  
Chapter 6: Text Processing/Advanced Command Line  
Chapter 7: Process Management  
Chapter 8: Editing Text  
Chapter 9: Partitions and Filesystems  
Chapter 10: Permissions and Ownership  
Chapter 11: Customizing Shell Environments  
Chapter 12: Shell Scripting  
Chapter 13: Basic SQL Management  
Chapter 14: Configuring User Interfaces and Desktops  
Chapter 15: Managing Users and Groups  
Chapter 16: Schedule and Automate Tasks



Chapter 17: Configuring Print and Email Services

Chapter 18: Logging and Time Services

Chapter 19: Networking Fundamentals

Chapter 20: System Security

Chapter 21: Final Preparation

Appendix A: Answers to the "Do I Know This Already?"  
Quizzes and Review Questions

Glossary

#### **SUPPLEMENTAL TEXT**

CompTIA Linux+ Portable Command Guide  
9780789757111

# Course 5: Ethical Hacking and Penetration Testing

Sometimes finding the holes in a network first is the best way to learn how to secure a network better. This course introduces the concepts and practices to provide reliable security audits. Penetration testing or Ethical Hacking is the process of applying a variety of tools and hacking techniques in order to test the security of a

network. Coverage in this course includes the concepts, terminology, and issues, along with essential practical skills to conduct reliable security audits. Learn theory and standards with a great deal of hands-on techniques. Understanding of basic security policies is also covered.

## Standard Track

### Easttom

Penetration Testing Fundamentals

Book: 9780789759375

Book+Course+Lab: 9780789759610

Course + Lab: 9780789759627

Leading security expert, researcher, instructor, and author Chuck Easttom has brought together all the essential knowledge in a single comprehensive guide that covers the entire penetration testing lifecycle. Easttom integrates concepts, terminology, challenges, and theory, and walks you through every step, from planning to effective post-test reporting. He presents a start-to-finish sample project relying on free open source tools, as well as quizzes, labs, and review sections throughout. *Penetration Testing Fundamentals* is also the only book to cover pen testing standards from NSA, PCI, and NIST.

### About the author

**Chuck Easttom** spent many years in the IT industry. Easttom currently teaches computer/network security courses at two colleges, and does additional computer security consulting work.

### Table of Contents:

Chapter 1: Introduction to Penetration Testing  
Chapter 2: Standards  
Chapter 3: Cryptography  
Chapter 4: Reconnaissance  
Chapter 5: Malware  
Chapter 6: Hacking Windows  
Chapter 7: Web Hacking  
Chapter 8: Vulnerability Scanning  
Chapter 9: Introduction To Linux  
Chapter 10: Linux Hacking



Chapter 11. Introduction to Kali Linux  
Chapter 12. General Techniques  
Chapter 13. Introduction to Metasploit  
Chapter 14. More with Metasploit  
Chapter 15. Introduction to Scripting with Ruby  
Chapter 16. Write Your Own Metasploit Exploits with Ruby  
Chapter 17. General Hacking Knowledge  
Chapter 18. Additional Pen Testing Topics  
Chapter 19. A Sample Pen Test Project

## Certification Track

### Gregg

Certified Ethical Hacker (CEH)  
Version 9 Cert Guide, 2nd Edition

Book: 9780789756916  
Book+Course+Lab: 9780789756930  
Course + Lab: 9780789756923

In *Certified Ethical Hacker (CEH) Version 9 Cert Guide*, 2nd Edition, leading expert Michael Gregg helps students master all the topics they need to know to succeed on their Certified Ethical Hacker Version 9 exam and advance their career in IT security. Michael's concise, focused approach explains every exam objective from a real-world perspective, helping students quickly identify weaknesses and retain everything they need to know.

#### *About the author*

**Michael Gregg**, CISSP is the president of Superior Solutions, Inc., a Houston based training and consulting firm.

#### *Table of Contents:*

##### **Introduction**

Chapter 1: An Introduction to Ethical Hacking  
Chapter 2: The Technical Foundations of Hacking  
Chapter 3: Footprinting and Scanning  
Chapter 4: Enumeration and System Hacking  
Chapter 5: Malware Threats  
Chapter 6: Sniffers, Session Hijacking, and Denial of Service  
Chapter 7: Web Server Hacking, Web Applications, and Database Attacks  
Chapter 8: Wireless Technologies, Mobile Security, and Attacks  
Chapter 9: IDS, Firewalls, and Honeypots  
Chapter 10: Physical Security and Social Engineering  
Chapter 11: Cryptographic Attacks and Defenses



Chapter 12: Cloud Computing and Botnets

Chapter 13: Final Preparation

Glossary

##### **ONLINE CONTENT**

Glossary

Appendix A: Answers to the "Do I Know This Already?"  
Quizzes and Review Questions

Appendix B: Memory Tables

Appendix C: Memory Tables Answer Key





# Course 6: Networking Defense and Countermeasures

After learning where the penetration can happen in a network, now learn how to shore up the vulnerabilities. This course covers essential network security concepts, challenges, and careers; learn how modern attacks work; discover how firewalls, intrusion detection systems (IDS), and virtual private networks (VPNs) combine to protect modern networks; select the right security technologies for any network environment; use encryption to protect information; harden Windows and Linux systems and keep them patched; securely configure web browsers to resist attacks; defend against

malware; define practical, enforceable security policies; use the “6 Ps” to assess technical and human aspects of system security; detect and fix system vulnerability; apply proven security standards and models, including Orange Book, Common Criteria, and Bell-LaPadula; ensure physical security and prepare for disaster recovery; know your enemy: learn basic hacking, and see how to counter it; understand standard forensic techniques and prepare for investigations of digital crime.

**Industry Certification Preparation:** There is no parallel track in an industry certification for this course.

## Standard Track

### Easttom

Network Defense and Countermeasures, 3rd Edition

Book: 9780789759962

Book+Course+Lab: 9780789759993

Course + Lab: 9780789759986

*Network Defense and Countermeasures: Principles and Practices, 3rd Edition* is designed to be the ideal one-volume gateway into the field of network defense. It brings together thoroughly updated coverage of all basic concepts, terminology, and issues, along with the practical skills essential to network defense. Drawing on his extensive experience as both an IT professional and instructor, Chuck Easttom covers core topics such as practical applications of firewalls, intrusion detection systems, encryption fundamentals, operating system hardening, defending against virus attacks, Trojan horses and spyware, Ransomware, malware, security policies, and security standards. Unlike many other authors, however, he also fully addresses more specialized issues, including cryptography, industrial espionage and encryption — including public/private key systems, digital signatures, and certificates.

### About the author

**Chuck Easttom** currently teaches computer/network security courses at two colleges, and does additional computer security consulting work.



### Table of Contents:

- Chapter 1: Introduction to Network Security
- Chapter 2: Types of Attacks
- Chapter 3: Fundamentals of Firewalls
- Chapter 4: Firewall Practical Applications
- Chapter 5: Intrusion Detection Systems
- Chapter 6: Encryption Fundamentals
- Chapter 7: Virtual Private Networks
- Chapter 8: Operating System Hardening
- Chapter 9: Defending Against Virus Attacks
- Chapter 10: Defending against Trojan Horses, Spyware, and Adware
- Chapter 11: Security Policies
- Chapter 12: Assessing System Security
- Chapter 13: Security Standards
- Chapter 14: Physical Security and Disaster Recovery
- Chapter 15: Techniques Used by Attackers
- Chapter 16: Introduction to Forensics
- Chapter 17: Cyber Terrorism
- Appendix A: Answers
- Appendix A: References
- Glossary

# Course 7: Cybersecurity Operations (Incident Response and Digital Forensics)

If your network has been breached, now what? This course covers the entire lifecycle of incident response, including preparation, data collection, data analysis, and remediation. Provides a thorough hands-on understanding of Security Operations, Cyber defense

analysis, Cyber defense infrastructure support, how to respond to and manage incidents of breach and effectively assess and manage current and future vulnerabilities.

## Standard Track

### Hayes

A Practical Guide to Computer Forensics Investigations

Book: 9780789741158

Book+Course+Lab: 9780134998688

Course + Lab: 9780789759719

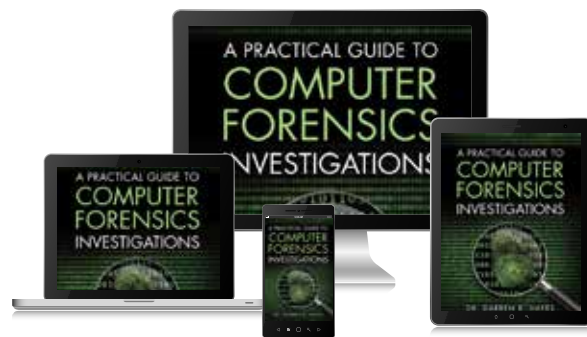
2nd EDITION coming: Spring 2019

*In A Practical Guide to Computer Forensics Investigations*, Dr. Darren Hayes presents complete best practices for capturing and analyzing evidence, protecting the chain of custody, documenting investigations, and scrupulously adhering to the law, so evidence can always be used.

Hayes introduces today's latest technologies and technical challenges, offering detailed coverage of crucial topics such as mobile forensics, Mac forensics, cyberbullying, and child endangerment. This guide's practical activities and case studies give students hands-on mastery of modern digital forensics tools and techniques. Its many realistic examples reflect the author's extensive and pioneering work as a forensics examiner in both criminal and civil investigations.

### About the author

**Darren R. Hayes** is CIS Program Chair and Lecturer at Pace University. He is also a consultant for the Department of Education in New York City, where he provides high school teachers with training in computer forensics. He is passionate about computer forensics, works closely with law enforcement, and believes that the field of study is a great way to get students interested in computing.



### Table of Contents:

#### Introduction

- Chapter 1: The Scope of Computer Forensics
- Chapter 2: Windows Operating and File Systems
- Chapter 3: Handling Computer Hardware
- Chapter 4: Acquiring Evidence in a Computer Forensics Lab
- Chapter 5: Online Investigations
- Chapter 6: Documenting the Investigation
- Chapter 7: Admissibility of Digital Evidence
- Chapter 8: Network Forensics
- Chapter 9: Mobile Forensics
- Chapter 10: Photograph Forensics
- Chapter 11: Mac Forensics
- Chapter 12: Case Studies

## Certification Track One

### MacMillan

#### CompTIA Cybersecurity Analyst (CySA+) Cert Guide

Book: 9780789756954

Book+Course+Lab: 9780789760029

Course + Lab: 9780789760012

*CompTIA Cybersecurity Analyst (CSA+) Cert Guide*, presents students with an organized test-preparation routine through the use of proven series elements and techniques. Exam topic lists make referencing easy. Chapter-ending exam preparation tasks help students drill on key concepts they must know thoroughly. Review questions help them assess their knowledge, and a final preparation chapter guides them through the tools and resources to help them craft their final study plan.

#### About the author

**Troy McMillan** is a Product Developer and Technical Editor for Kaplan Cert Prep as well as a full time trainer and writer.

#### Table of Contents:

##### Introduction

Chapter 1: Applying Environmental Reconnaissance Techniques

Chapter 2: Analyzing the Results of Network Reconnaissance

Chapter 3: Recommending and Implementing the Appropriate Response and Countermeasure

Chapter 4: Practices Used to Secure a Corporate Environment

Chapter 5: Implementing an Information Security Vulnerability Management Process

Chapter 6: Analyzing Scan Output and Identifying Common Vulnerabilities

Chapter 7: Identifying Incident Impact and Assembling a Forensic Toolkit

Chapter 8: The Incident Response Process

Chapter 9: Incident Recovery and Post-Incident Response

Chapter 10: Frameworks, Policies, Controls, and Procedures

Chapter 11: Remediating Security Issues Related to Identity and Access Management

Chapter 12: Security Architecture and Implementing Compensating Controls

Chapter 13: Application Security Best Practices

Chapter 14: Using Cybersecurity Tools and Technologies

Chapter 15: Final Preparation

Appendix A: Answers to the "Do I Know This Already?" Quizzes and Review Questions

Glossary



## Certification Track Two

### Santos & Muniz

CCNA Cyber Ops SECOPS #210-255  
Official Cert Guide

Book: 9781587147036  
Book+Course+Lab: 9781587147104  
Course + Lab: 9781587147098

*CCNA Cyber Ops SECOPS 210-255 Official Cert Guide*, presents students with an organized test preparation routine through the use of proven series elements and techniques. The study guide helps students master all the topics on the SECOPS #210-255 exam, including:

- Threat analysis
- Forensics
- Intrusion analysis
- NetFlow for cybersecurity
- Incident response and the incident handling process
- Incident response teams
- Compliance frameworks
- Network and host profiling
- Data and event analysis
- Intrusion event categories

#### About the authors

**Omar Santos** is a principal engineer of the Cisco Product Security Incident Response Team (PSIRT).

**Joseph Muniz** is an architect at Cisco Systems and a security researcher.



#### Table of Contents:

##### Introduction xvii

##### Part I Threat Analysis and Computer Forensics

Chapter 1: Threat Analysis

Chapter 2: Forensics

##### Part II Network Intrusion Analysis

Chapter 3: Fundamentals of Intrusion Analysis

Chapter 4: NetFlow for Cybersecurity

##### Part III Incident Response

Chapter 5: Introduction to Incident Response and the Incident Handling Process

Chapter 6: Incident Response Teams

Chapter 7: Compliance Frameworks

Chapter 8: Network and Host Profiling

##### Part IV Data and Event Analysis

Chapter 9: The Art of Data and Event Analysis

##### Part V Incident Handling

Chapter 10: Intrusion Event Categories

##### Part VI Final Preparation

Chapter 11: Final Preparation

##### Part VII Appendix

Appendix A: Answers to the "Do I Know This Already?" Quizzes and Q&A

Glossary

Elements Available on the Book Website

Appendix B: Memory Tables and Lists

Appendix C: Memory Tables and Lists Answers

Appendix D: Study Planner



ON AVERAGE

**52%**

of IT professionals surveyed stated fewer than **25%** of all applicants were qualified

Source: State Cybersecurity: Implications for 2015: An ISACA and RSA Conference Survey



**7 1/2**  
MONTHS

is the average time an **advanced threat goes UNNOTICED** on victim's network

## Too Many Threats



**ONE IN FIVE**

organizations have *experienced an apt attack*



**62%**

increase in breaches in **IN 2013**

**2.5**  
**BILLION**



**EXPOSED RECORDS** as a result of data breach in the past 5 years

# Course 8: Developing Cybersecurity Programs and Policies

Now that you understand the full spectrum of threats and how to protect networks put it into practice by developing sound Cybersecurity programs and policies. This course prepares students to master modern information security regulations and frameworks, and learn specific best-practice policies for key industry sectors, including finance, healthcare, online commerce, and small business. Learn how to: establish program objectives, elements, domains, and governance; understand policies, standards, procedures, guidelines, and plans—and the differences among them; write policies in “plain language,” with the right level of detail; apply the Confidentiality, Integrity & Availability (CIA) security model; use the internationally recognized

NIST resources and ISO/IEC standards; align security with business strategy; define, inventory, and classify your information and systems; systematically identify, prioritize, and manage InfoSec risks; reduce “people-related” risks with role-based Security Education, Awareness, and Training (SETA); implement effective physical, environmental, communications, and operational security; effectively manage access control; secure the entire system development lifecycle; respond to incidents and ensure continuity of operations; comply with laws and regulations, including GLBA, HIPAA/HITECH, FISMA, state data security and notification rules, and PCI DSS.

**Industry Certification Preparation:** There is no parallel track in an industry certification for this course.

## Standard Track

### Santos

Developing Cybersecurity Programs and Policies

Book: 9780789759405  
Book+Course: 9780789759436  
Course: 9780134858685

*Developing Cybersecurity Programs and Policies* is a complete guide to establishing a cybersecurity program and governance in an organization. In this book, students will learn how to create cybersecurity policies, standards, procedures, guidelines, and plans — and the differences among them. This book covers the Confidentiality, Integrity & Availability (CIA) security model. Students will also learn how threat actors are launching attacks against their victims compromising confidentiality, integrity, and availability of systems and networks. This book covers the NIST Cybersecurity Framework and ISO/IEC 27000-series standards. Students will learn how to align security with business strategy, as well as define, inventory, and classify your information and systems.

This book teaches students how to systematically identify, prioritize, and manage cybersecurity risks and reduce social engineering (human) risks with role-based Security Education, Awareness, and Training (SETA). Students will also learn how to implement

effective physical, environmental, communications, and operational security; and effectively manage access control. In this book students will learn how to respond to incidents and ensure continuity of operations and how to comply with laws and regulations, including GLBA, HIPAA/HITECH, FISMA, state data security and notification rules, and PCI DSS.

### About the authors

**Omar Santos** is an active member of the cyber security community, where he leads several industry-wide initiatives and standards bodies. His active role helps businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to increasing the security of their critical infrastructures.





### Table of Contents:

- Chapter 1: Understanding Cybersecurity Policy and Governance
- Chapter 2: Cybersecurity Policy Organization, Format and Styles
- Chapter 3: Cybersecurity Framework
- Chapter 4: Governance and Risk Management
- Chapter 5: Asset Management and Data Loss Prevention
- Chapter 6: Human Resources Security
- Chapter 7: Physical and Environmental Security
- Chapter 8: Communications and Operations Security
- Chapter 9: Access Control Management
- Chapter 10: Information Systems Acquisition, Development, and Maintenance
- Chapter 11: Cybersecurity Incident Response
- Chapter 12: Business Continuity Management
- Chapter 13: Regulatory Compliance for Financial Institutions
- Chapter 14: Regulatory Compliance for the Healthcare Sector
- Chapter 15: PCI Compliance for Merchants
- Appendix A: Information Security Program Resources
- Appendix B: Sample Information Security Policy
- Appendix C: Information Systems Acceptable Use Agreement and Policy



Hardest to fill  
**SKILLS** in cybersecurity  
job postings

Software Architecture  
Network Attached Storage (NAS)  
Software Issue Resolution  
Internet Security  
Legal Compliance  
Data Communication  
Platform as a Service (PaaS)  
Computer Forensics  
Internal Auditing  
Apache Hadoop

Source: Job Market Intelligence Cybersecurity Jobs,  
2015-2016 Burning Glass Technologies





# Here's how you can get started with the IT Cybersecurity Curriculum (ITCC)

## *Next Steps*

- To Request a review copy of the Textbooks in the Pearson IT Cybersecurity Curriculum, contact your Pearson Rep. If you don't know who your Pearson Rep is, use the Pearson Rep Locator
- To learn more about the Pearson uCertify online course and labs, request a demo, and to request access, contact [rachel.langlois@pearson.com](mailto:rachel.langlois@pearson.com)
- To learn more about the Pearson IT Cybersecurity Curriculum (ITCC), contact the series editor [marybeth.ray@pearson.com](mailto:marybeth.ray@pearson.com)

## *Ordering Information*

- Order from Pearson to make sure you get exactly what you want, and receive the best pricing.
- Your bookstore can order through Pearson's OASIS ordering system.
- Your rep can help you handle DDA\* ordering options.
- Contact your Pearson rep if you need help ascertaining the correct ISBN for the exact material you wish to use.\*\*
- Your Students can buy directly from Pearson. All Pearson IT Cybersecurity Course materials (except DDA) can be purchased directly from My Pearson Store. All in stock orders will ship within 24-48 hours.

## 3 easy steps



Visit  
**MyPearsonstore.com**



Enter the ISBN in  
the **Search** Field



**Add to Cart** and  
Proceed to Checkout

\*uCertify Course and Labs are not available in the DDA Program, only the e-text version of the Pearson Textbooks  
\*\* find the Product Code/ISBN on pages 10-11 of this brochure

