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

Cisco Press PEARSON IT CERTIFICATION NICE NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Inside you'll find

COURSE DESCRIPTIONS

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 certi ications 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.

**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**

Email **rosa.wan@person.com** to request access or schedule a demo.

Visit **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.

uCertify

ITCC courses powered by Pearson partner, uCertify, winner of **19 CODiE awards in 4 years**. See more at **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

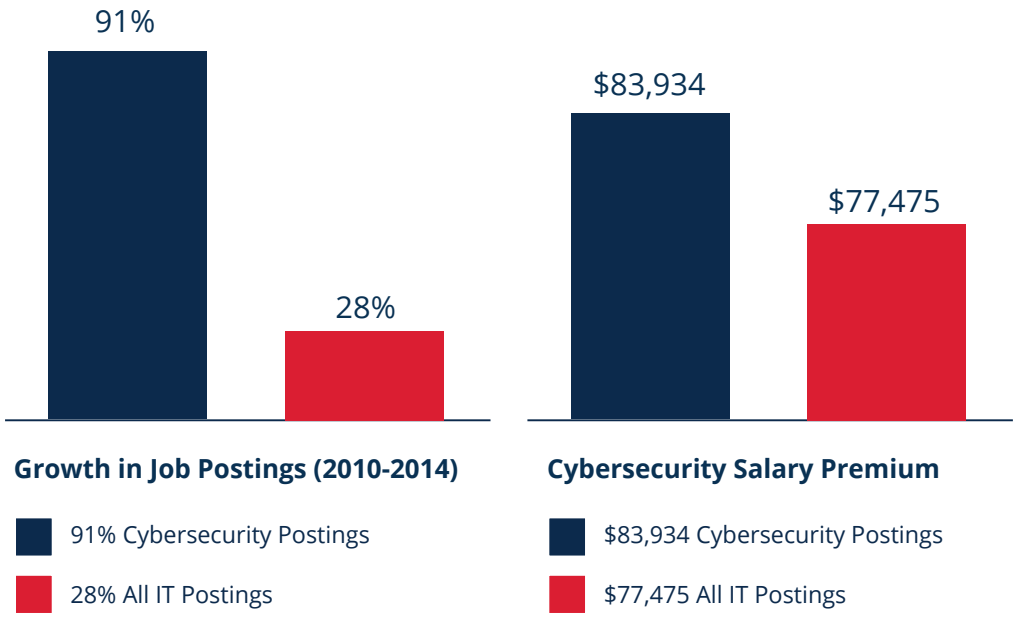
#	Course	Track I – Standard Textbook Focus	Track II – Certification Guide Focus
2	Networking Fundamentals	Networking Essentials	CompTIA Network+
3	Cybersecurity Fundamentals	Computer Security Fundamentals	CompTIA Security+
4	Linux Fundamentals for Cybersecurity	Linux Essentials for Cybersecurity	CompTIA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

Track II – Certification Guide Focus

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

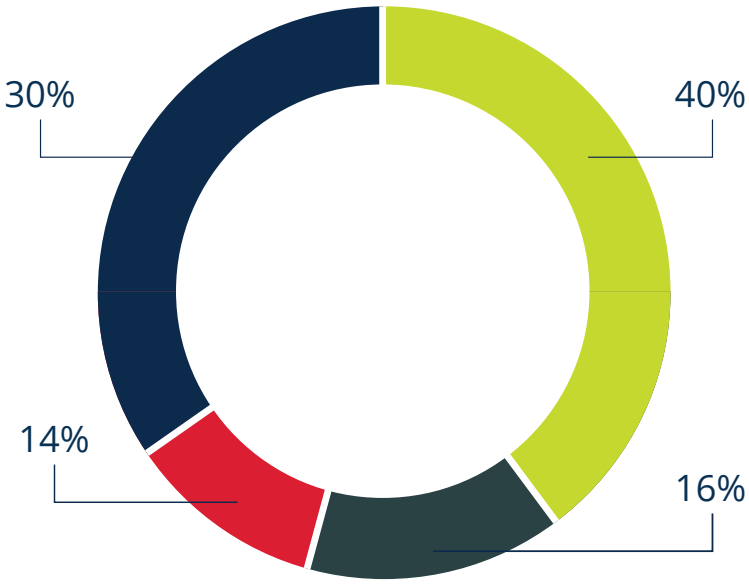
** No parallel certification, use Track I*

Job Role/Salaries

	Course	Course Entry-level Job Roles	Average Salaries	Program Entry-Level Job Role[1]	Aveage Salary[3]
1	IT Fundamentals	·Technical Support Specialist ·Field Service Technician ·IT Support Technician ·IT Administrator	~ $77,053[2]	·Cybersecurity Specialist - Technician ·Incident Analyst / Responder	~ $96,500
2	Networking Fundamentals	·Network Field Technician ·Network Administrator ·IS Consultant ·Network Field Engineer	~ $79,459[2]		
3	Cybersecurity Fundamentals	·Security Specialist ·Security Consultant ·Security Engineer ·Security Administrator	~ $87,673[2]		
4	Linux Fundamentals for Cybersecurity	·Linux Database Administrator ·Junior Linux Administrator ·Junior Network Administrator	~ $78,593[2]		
5	Ethical Hacking and Penetration Testing	·Ethical Hacker ·Penetration Tester ·Homeland Security Specialist ·IT Security Consultant ·IT Security Specialist	~$120,220[4]		
6	Network Defense & Countermeasures	·Network Security Administrator ·Network Security Specialist ·Security Technician ·Network Security Support Engineer	~ $84,652[2]		
7	Cybersecurity Operations – Incident Response & Digital Forensics	·Security Analyst ·Vulnerability Analyst ·Cybersecurity Specialist ·Cybersecurity Analyst ·Security Engineer ·Security Operations Center Analyst ·Computer Forensics Technician	~ $92,000[5]		
8	Developing Cybersecurity Programs and Polices	·Security Operations Center Analyst	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



Industries Managing Consumer Data

- 40% Professional Servcices
- 30% Others
- 16% Finance and Insurance
- 14% Manufacturing and Defense

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

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:

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:

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:

ONLINE ELEMENTS:

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:

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+ SY0-501 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+ SY0-501 Exam Cram 9780789759009

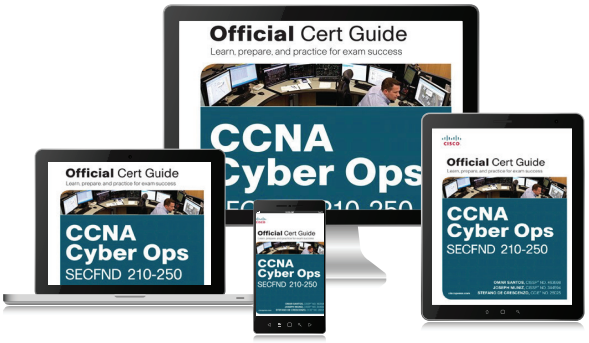
A new report out from **Cybersecurity Ventures** estimates

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:

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

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:

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:

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:

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

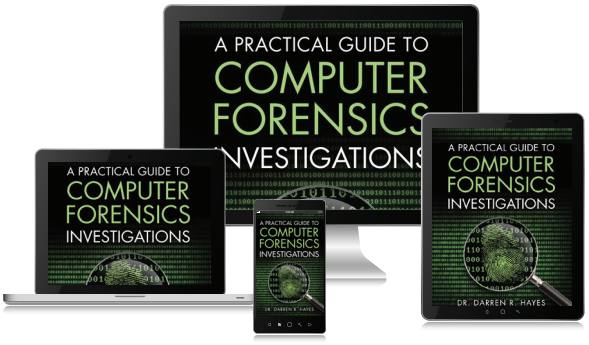
Chuck Easttom currently teaches computer/network security courses at two colleges, and does additional computer security consulting work.

Table of Contents:

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:

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:

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:

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

Too Many Threats

7 1/2 MONTHS

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

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

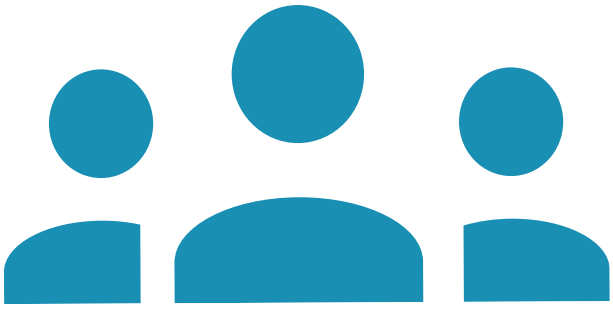
Developing Cybersecurity Programs and Policies is a complete guide to establishing a cybersecurity program and governance in an organization. In this book, students will learn how to create cybersecurity policies, standards, procedures, guidelines, and plans — and the differences among them. This book 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:



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 **rosa.wan@pearson.com**
- To learn more about the Pearson IT Cybersecurity Curriculum (ITCC), contact the series editor **james.manly@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

Pearson