CISCO Cisco Networking Academy
Mind Wide Open
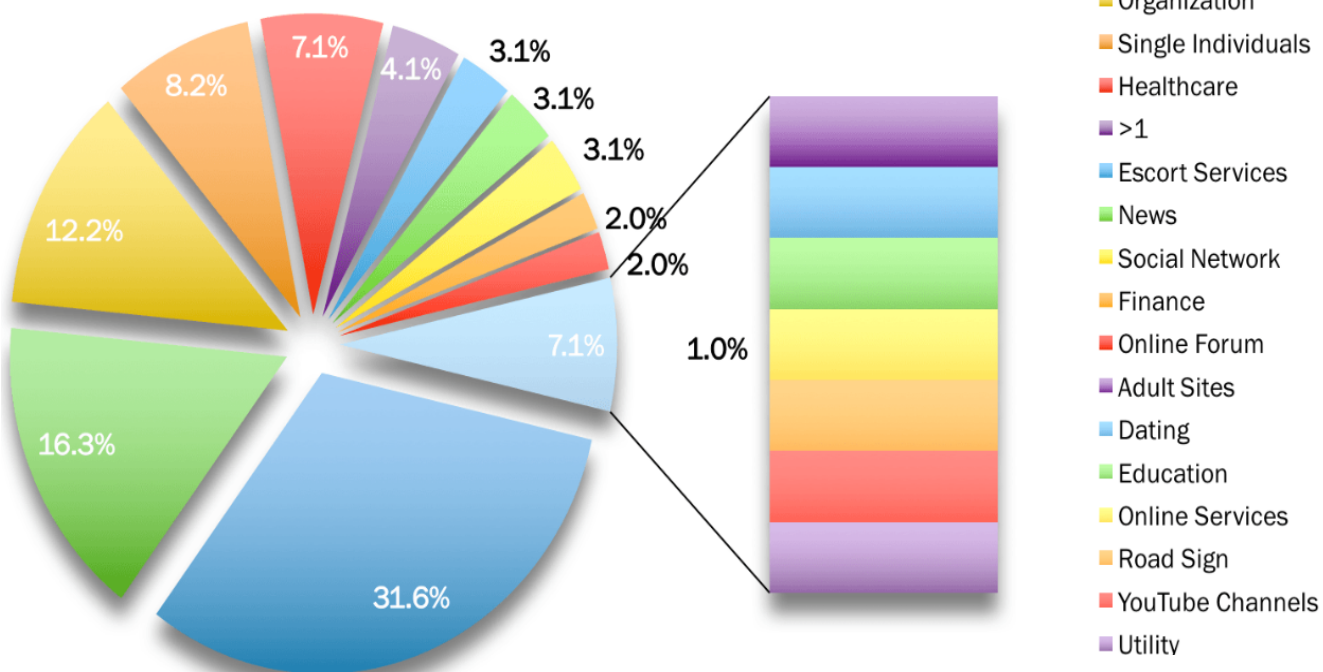
# Cybersecurity Essentials 1.0 Overview

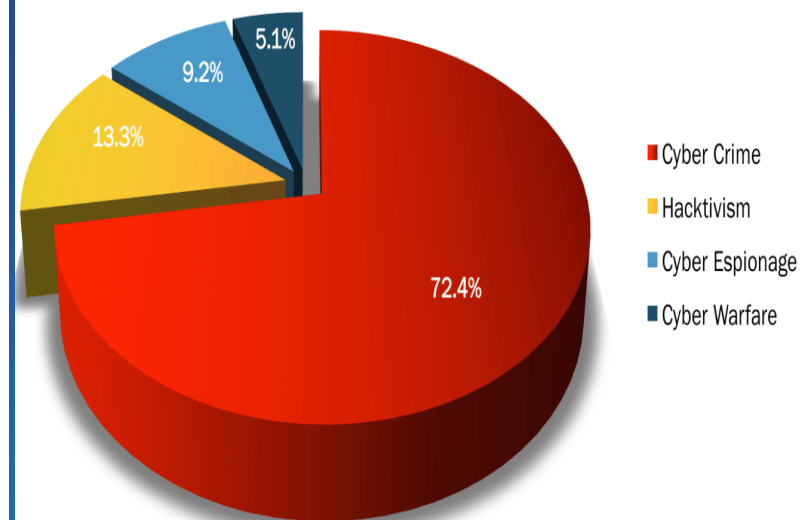October 2016

# Growth of Cyber Threats and Crimes

## Distribution of Targets
### July 2016

- Industry
- Government
- Organization
- Single Individuals
- Healthcare
- >1
- Escort Services
- News
- Social Network
- Finance
- Online Forum
- Adult Sites
- Dating
- Education
- Online Services
- Road Sign
- YouTube Channels
- Utility

7.1%  4.1%  3.1%  3.1%  3.1%  2.0%  2.0%  1.0%
8.2%  12.2%  16.3%  31.6%  7.1%

## Motivations Behind Attacks
### July 2016

- Cyber Crime
- Hacktivism
- Cyber Espionage
- Cyber Warfare

72.4%  13.3%  9.2%  5.1%

Source: hackmageddon.com

## Computer and Network Intrusions

The collective impact is staggering. Billions of dollars are lost every year repairing systems hit by such attacks. Some take down vital systems, disrupting and sometimes disabling the work of hospitals, banks, and 9-1-1 services around the country.

# Cybersecurity Market and Opportunities

**Cybersecurity spending outlook: $1 trillion from 2017 to 2021**

Source: Cybersecurity Market Report by Cybersecurity Ventures

**4 SECURITY/CYBERSECURITY PROFESSIONALS**

**Ten Hot IT Job Skills for 2016**

More than 209,000 cybersecurity jobs in the U.S. are unfilled, and postings are up 74% over the past five years, according to a 2015 analysis of numbers from the Bureau of Labor Statistics by Peninsula Press, a project of the Stanford University Journalism Program.

A report from Cisco puts the global figure at one million cybersecurity job openings. Demand is expected to rise to 6 million globally by 2019,

**The Most Critical Skills Gap: Cybersecurity**

Data breaches are both costly and damaging to a company's reputation. But there aren't enough people to fill open cybersecurity positions.

**SECURITY**

**37%** **Growth** forecast for Security Analyst jobs by 2022

Information Security Administrator
High: $111,133
Avg: $77,015
Low: $52,235

Systems/Application Security Analyst
High: $114,135
Avg: $87,319
Low: $63,841

Information Security Manager
High: $143,474
Avg: $115,829
Low: $90,808

# Cybersecurity Essentials 1.0

## Course Overview

Cybersecurity Essentials covers foundation knowledge and essentials skills in all security domains in the cyber world – information security, systems security, network security, mobile security, physical security, ethics and laws, related technologies, defense and mitigation techniques use in protecting businesses

**Prerequisites:** Introduction to Cybersecurity

**Languages:** English

**Course Delivery:** Instructor-led or Self-paced

**Estimated Time to Complete**: 30 hours

**Next Course:** CCNA R&S or CCNA Security

## Learning Progression

High school and higher education students interested in learning about foundational knowledge and build essential skills in cyber security, and career opportunities in the cyber security field.



Cybersecurity Essentials

| | |
|---|---|
| **Chapter 0** Course Introduction | **Section 1.0** Introduction |
| **Chapter 1** Cybersecurity – A World of Wizards, Heroes, and Criminals | **Section 1.1** The Cybersecurity World |
| **Chapter 2** The Cybersecurity Sorcery Cube | **Section 1.2** Cyber Criminals versus Cyber Heroes |
| **Chapter 3** Cybersecurity Threats, Vulnerabilities, and Attacks | **Section 1.3** Threats to the Kingdom |
| **Chapter 4** The Art of Protecting Secrets | **Section 1.4** The Dark Forces of Cybersecurity |
| **Chapter 5** The Art of Ensuring Integrity | **Section 1.5** Creating More Heroes |

**Topic 1.0.1** Welcome

**Page 1.0.1.1** Chapter 1: Cybersecurity - A World of Wizards, Heroes, and Criminals

## Learning Components

- 8 chapters
- Interactive Multimedia Content
- 34 Activities, 10 Packet Tracer Activities, 12 Labs that reinforce learning
- 8 end-of-chapters quiz, and 1 final exam
- Links to related resources

# Cybersecuity Essentials Goals

Cybersecurity Essentials helps students:

- Understand the players in the cyber security world and motivation of cyber criminals and cybersecurity professionals.
- Learn to identify security attacks, symptoms, processes, and countermeasures.
- Learn foundational and essential knowledge in various security domains – cybersecurity, information security, application security, host and system security, network security, mobile security, security laws, ethics, and security policies.
- Build skills in security management, controls, protection and mitigation technologies.
- Explore the roles of different cybersecurity professionals and career options.
- Consider or advance a career in cybersecurity

# Cybersecurity Essentials Key Competencies

Upon completion of this course, students will be able to:

- Describe the characteristics of criminals and specialists in the cybersecurity realm.
- Describe how the principles of confidentiality, integrity, and availability as they relate to data states and cybersecurity countermeasures.
- Describe the tactics, techniques and procedures used by cyber criminals.
- Describe technologies, products and procedures used to protect confidentiality, ensure integrity and provide high availability.
- Explain how cybersecurity professionals use technologies, processes and procedures to defend all components of the network.
- Explain the purpose of laws related to cybersecurity.

# Course Design

- Easy-to-navigate graphical user interface

- 8 chapters with **modifiable** chapter quiz

- 34 interactive activities

- 10 Cisco Packet Tracer activities, require PT 6.3.x or above

- 12 hands-on labs, only PC required for lab

- 1 dynamic final exam

- 8 chapters containing accessible text and media text videos with closed captioning

- Available in English

- Certificate of Completion

# Course Outline

| Module | Learning Objectives |
|---|---|
| 1 Cybersecurity – A World of Wizards, Heros and Criminals | • Describe the cybersecurity world, criminals and professionals .<br>• Compare how cybersecurity threats affect individuals, business and organization.<br>• Explain the structure and efforts committed to expanding the security workforce. |
| 2 The Cybersecurity Sorcery Cube | • Explain the three dimensions of the McCumber Cube.<br>• Detail the ISO cybersecurity model.<br>• Explain the principles of confidentiality, integrity, and availability as they relate to data states and cybersecurity countermeasures. |
| 3 Cybersecurity Threats, Vulnerabilities, and Attacks | • Describe tactics, techniques and procedures used by cyber criminals.<br>• Explain the types of malware, malicious code and social engineering<br>• Cpmpare different types of cyber attacks. |
| 4 The Art of Protecting Secrets | • Outline technologies, products and procedures used to protect confidentiality.<br>• Explain encryption techniques and access control  techniques.<br>• Present concepts of obscuring data. |

# Course Outline

| Module | | Learning Objectives |
|---|---|---|
| 5 | The Art of Ensuring Integrity | • Explain technologies, products and procedures used to ensure integrity<br>• Detail the purpose of digital signature and certificates<br>• Explain the need for database integrity enforcement |
| 6 | The Realm of Five Nines | • Explain the concepts of high availability.<br>• Describe technologies, products, and procedures used to provide high availability.<br>• Represent how incident response plan and disaster recovering planning improves high availability and business continuity. |
| 7 | Fortifying the Kingdom | • Explain system, servers and data protection<br>• Explain network infrastructure and end device protection<br>• Explain physical security measures used to protect network equipment |
| 8 | Joining the Order of Cybersecurity Specialists | • Discuss cybersecurity domains and controls within the CIA triad.<br>• Explain ethics and cybersecurity laws.<br>• Name the cybersecurity tools.<br>• Explain how to become a cyber security professional. |

# Module 1: Cybersecurity – A World of Wizards, Heros and Criminals

*Learn the characteristics of criminals and specialists in the cyber security realm.*

Module 1 presents:

- The structure of the cybersecurity world and the reason it continues to grow with data and information as the prized currency.

- The role of cyber criminals and what motivates them.

- The factors that lead to the spread and growth of cybercrime.

- The structure and efforts committed to expanding the cybersecurity workforce.
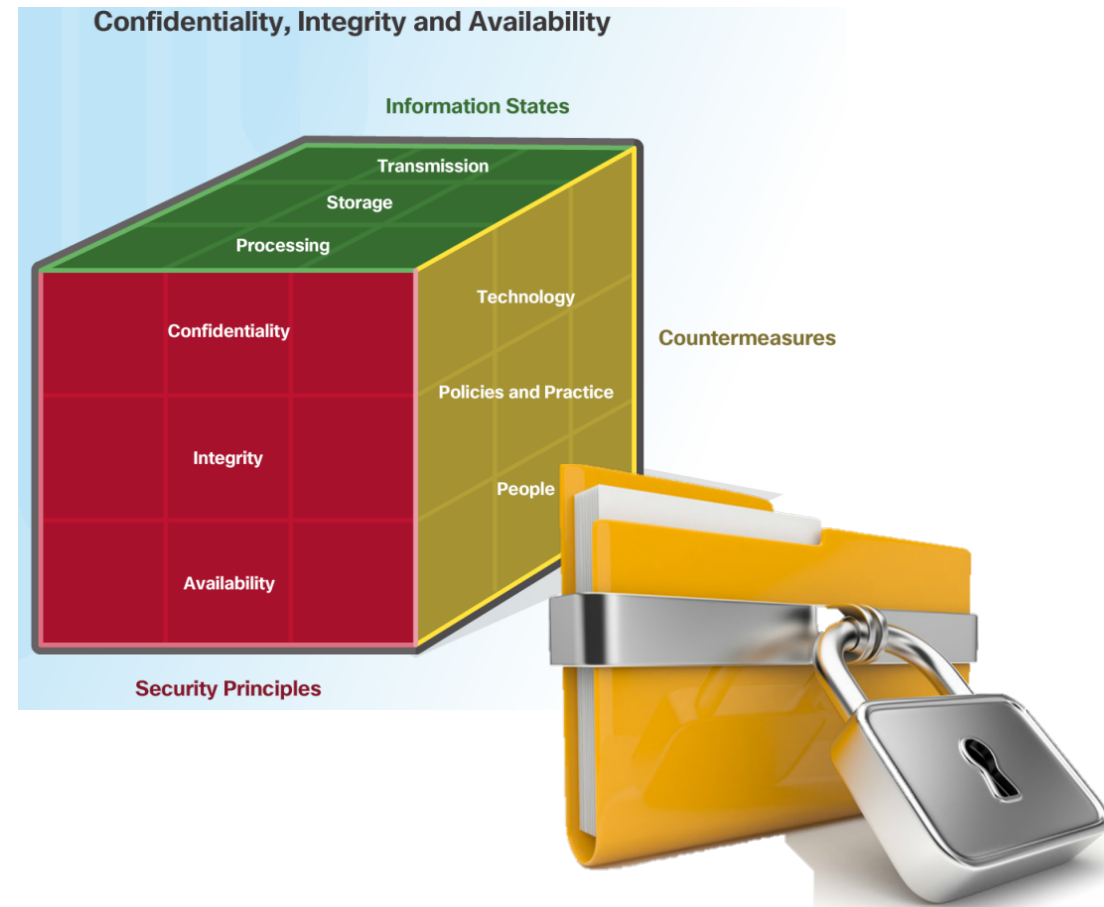
# Module 2: The Cybersecurity Sorcery Cube

*Learn the principles of confidentiality, integrity, and availability as they relate to data states and cybersecurity countermeasures.*

Module 2 details:

- The three dimensions of the McCumber Cube – the CIA Triad; the three states of data; the three categories of cybersecurity safeguards.

- The ISO cybersecurity model, an international framework standard for the management of information systems.

.



Confidentiality, Integrity and Availability

Information States

Transmission
Storage
Processing

Technology

Confidentiality

Countermeasures

Policies and Practice

Integrity

People

Availability

Security Principles

# Module 3: Cybersecurity Threats, Vulnerabilities, and Attacks

*Threats, vulnerabilities, and attacks are the central focus of the cyber criminals. Learn tactics, techniques and procedures used by cyber criminals.*

Module 3 covers:

- The types of malware and malicious code.

- The different methods used in social engineering.

- The different types of cyber attacks.

# Module 4: The Art of Protecting Secrets

*Learn the technologies, products and procedures used to protect confidentiality.*

Module 4 presents

- The principles of cryptology used to secure communications. It explains and compares symmetric and asymmetric encryption algorithms and used examples.

- The access control models and techniques used to protect confidentiality.

- The concept of obscuring data, and how data obfuscation and steganography accomplishes data masking.
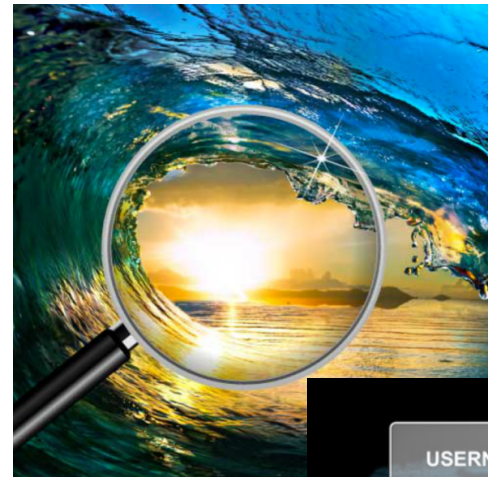
# Module 5: The Art of Ensuring Integrity

*Learn the technologies, products and procedures used to ensure data integrity.*

Module 5 covers

- The types of data integrity controls.

- The purpose of digital signatures and certificates as tools for verifying authenticity of messages and documents.

- The need for database integrity enforcement to ensure stability, performance and maintainability of the database system.

# Module 6: The Realm of Five Nines

*Learn the technologies, products, and procedures used to provide high availability.*

Module 6 details

- The concepts of five nines, a high availability industry standard.

- The technologies, procedures and design used by organizations to provide high system availability, redundancy, and resiliency to ensure quick recovery and continual operation.

- Incident response plan and disaster recovery planning to improves high availability and business continuity.





INCIDENT RESPONSE

# Module 7: Fortifying the Kingdom

*Learn the technologies, processes and procedures used to defend all components of the network.*

Module 7 presents

- Host-hardening includes securing the operating system, implementing an anti-virus solution, and using host-based solutions such as firewalls and intrusion detection systems.

- Server hardening includes managing remote access, securing privileged accounts, and monitoring services.

- Data protection includes file access control and implementing security measure to ensure the confidentiality, integrity, and availability of data.

- Device hardening also involves implementing proven methods of physically securing network devices.

# Module 8: Joining the Order of Cybersecurity Specialists

*Understand the cybersecurity domains and controls; laws and ethics, various roles in the cybersecurity profession.*

Module 8 covers

- The security domains and proper controls in each domain.

- The laws governing security, and ethical behavior

- The available cybersecurity tools

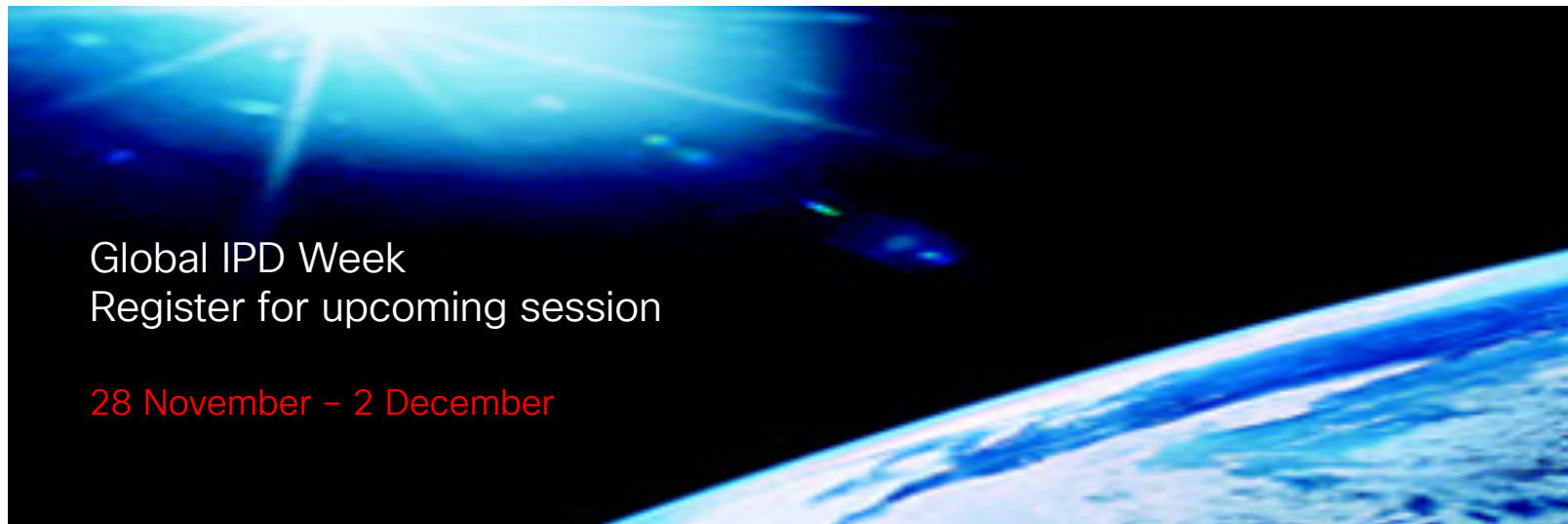- The opportunities and roles in the cybersecurity profession.

# Instructor Requirements

- All Instructors are recommended to have CCNA-level networking (CCNA R&S), or security (CCNA Security, CISSP, Security+ ) knowledge and skills

- Instructor training is optional, but recommended for new instructors. Training options:

  - Take Introduction to Cybersecurity 2.0 and Cybersecurity Essentials self-paced courses

  - Take an instructor training delivered by Instructor Training Centers (ITCs)

- 15-hour training: in-person, blended, or remote delivery formats
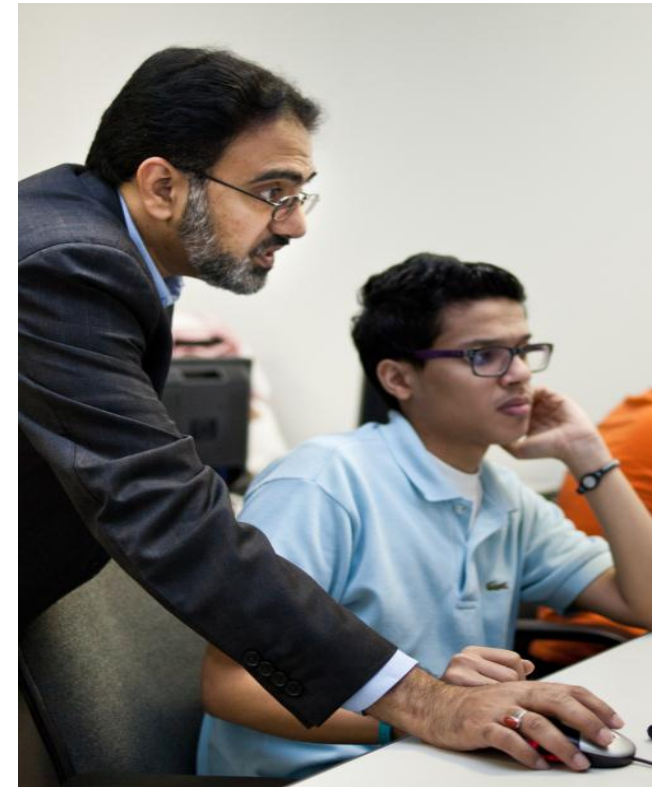
# Instructor IPD Event

- IPD for instructors during Global IPD Week by TFE team (November 2016)

- Resulting recordings will be used for instructor resources/reference

Global IPD Week
Register for upcoming session

28 November – 2 December

# Instructor Resources

https://www.netacad.com/group/resources/cybersecurity-essentials/1.0

■ ■ ■  Beginning    Duration: 30 Hours    Self-paced / Instructor-led

Select your course language

📝 Edit ⚙ Select Web Content 📄 Add

## Cybersecurity Essentials

Version 1.0 | Released October 2016 Release Notes & Versions

WEB CONTENT DISPLAY

### Quick Links

Scope and Sequence

Packet Tracer Resource

### Course Overview

The **Cybersecurity Essentials** course develops foundational understanding of cybersecurity and how it relates to information and network security. The 30-hour course introduces students to characteristics of cyber crime, security principles, technologies, and procedures to defend networks. Through interactive, multimedia content, lab activities, and multi-industry case studies, students build technical and professional skills to pursue careers in cybersecurity.

- Learn procedures to implement data confidentiality, integrity, availability and security controls on networks, servers and applications.

📝 Edit ⚙ Select Web Content 📄 Add

Read More

### News

Translated Languages for CCNA R&S 6.0 Bridging Course Available
August 17, 2016

New Student Interface Images Available
July 20, 2016

Learning Portfolio Grows with New C++ Programming Course
July 27, 2016

Get the Latest Packet Tracer
June 23, 2016

Cybersecurity Scholarships for Linux and CCNA Students
June 28, 2016

### Classroom Resources

Instructor Powerpoints

### Lab Resources

Instructor Lab Manual (PDF)

Instructor Lab PDF Files (ZIP)

Instructor Lab Source Files (ZIP)

# Instructors
# Enrollment and Support

- Enroll students and teach Cybersecurity Essentials in their classrooms through the same process used for other Networking Academy courses

- If you need assistance, contact your Academy Support Center (ASC)

**Create a Course**

Select an Academy/Institution

TSI Instructor Training Center - ITC

Find out how to
Teach More Courses

Course Name | Course ID
Cybersecurity Essentials | CyberEss

Create a Course

Select a NetAcad Course
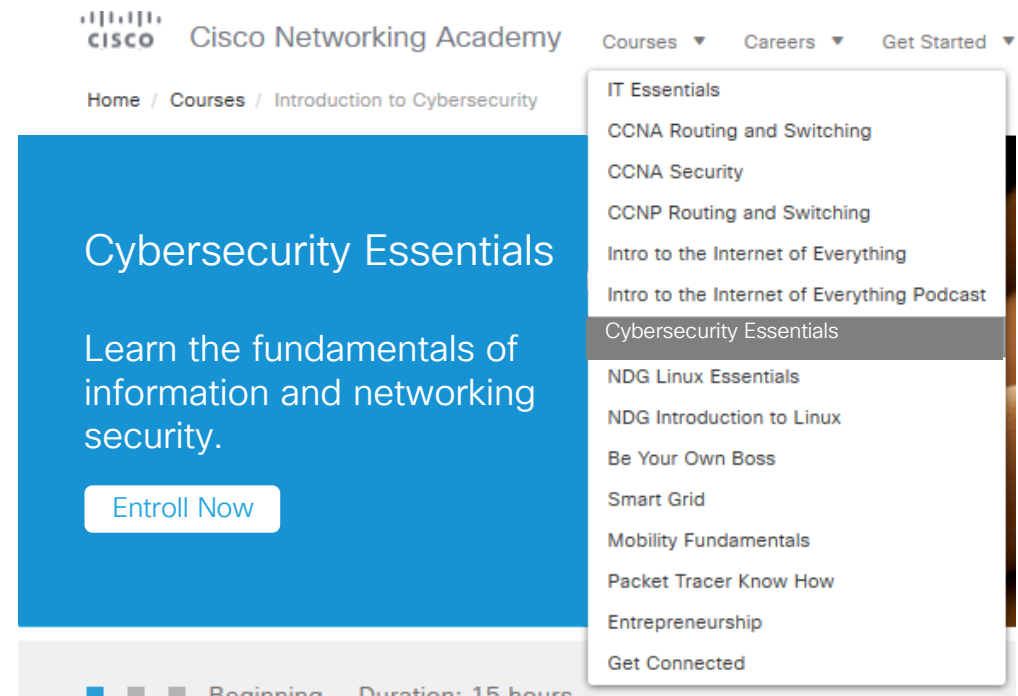
CCNA Discovery 3: Introducing Routing and Switching in the Enterprise
CCNA Discovery 4: Designing and Supporting Computer Networks
CCNA Exploration 1: Network Fundamentals
CCNA Exploration 2: Routing Protocols and Concepts
CCNA Exploration 3: LAN Switching and Wireless
CCNA Exploration 4: Accessing the WAN
CCENT: Instructor Fast Track
CCNA: Instructor Fast Track
CCNA Security
CCNA Security: Instructor Fast Track
CCNP ROUTE: Implementing IP Routing
CCNP SWITCH: Implementing IP Switching
CCNP TSHOOT: Maintaining and Troubleshooting IP Networks
Cybersecurity Essentials
ITC Instructor Support Offering - CCNA
ITC Instructor Support Offering - ITE
ITC Instructor Support Offering - CCNP
ITC Instructor Support Offering - CCNA Security
Partner: NDG Linux Essentials
Partner: NDG Linux Essentials - ITE Instructor Trainers

# Students
# Enrollment and Support

Students:

- Visit the [Course information page](#) on Cisco NetAcad.com to enroll in the self-paced course.

- If you need assistance, post questions on the [Cisco Networking Academy Facebook page](#)

Thank you.

‧i‧i‧i‧i‧
CISCO

Cisco Networking Academy
Mind Wide Open