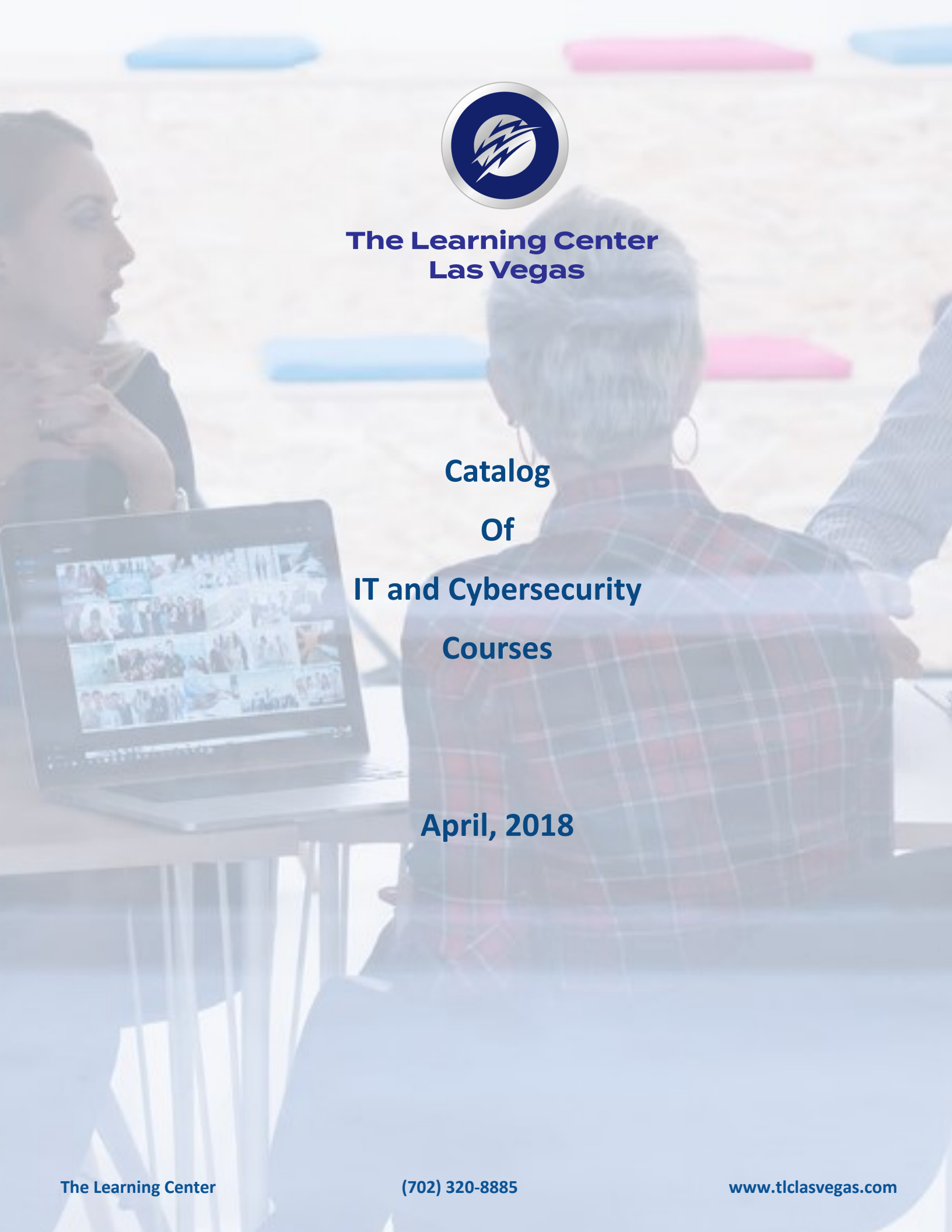


The Learning Center
Las Vegas

Catalog

Of

IT and Cybersecurity

Courses

April, 2018

TABLE OF CONTENTS

TABLE OF CONTENTS

e-Learning Courses

Cybersecurity:

Security+
CASP
CSA
CISA
CISM
CISSP
CEH
CIH
CHFI
LPT
Adv LPT
Certified Security Sentinel (CSS)
Certified Info Security Officer

IT Networking:

A+
Network+
MCSA Server 2012/16
MCSE Server 2012/16
Windows 7
Windows 10

Wireless:

CWNA Certified Wireless Network Admin
CWNP Certified Wireless Security Professional

Cisco

CCNA Routing & Switching
CCNP Routing & Switching

VMWare:

VMware vSphere 6.0 Ultimate Bootcamp
Certified Virtualization Security Expert

OFFICIAL CYBERSECURITY TRAINING

YOUR LEARNING PARTNER FOR THE LONG TERM

IT and Cybersecurity Training

Delivering the highest quality training for any size organization, meeting the most specific needs.

Recognized *Flexible* *Official* *Dependable* *Authorized*

The Learning Center has been a leading provider of IT and Cybersecurity training in the Las Vegas valley since May of 1985. TLC has grown with the industry and continues to provide superior IT training programs with expert instruction that will allow your IT staff to effectively deploy, manage, expand and maintain successful IT infrastructures.

Partnered With Global Leaders . . .

TLC provides training, certification, and team skills development in all areas of IT and Cybersecurity. A credentialed learning partner delivering the latest curriculum within a wide range of competencies to include:

- CompTIA
- Microsoft
- Cisco
- $(ISC)^2$
- ISACA
- EC-Council

Cyber Collaboration Center . . .

Home to advance training courses and cyber warfare exercises that will provide your team with the latest training and education resources to identify, assess, and respond to **simulated cyber attacks** in the safety of a virtual sandbox environment.

As an authorized and accredited Cybersecurity training provider by both $(ISC)^2$ and EC-Council, our Cybersecurity instructors are highly skilled in the delivery of high level instruction.

TLC is located in the heart of the Las Vegas Technology Center Business Park II. Classrooms are well-appointed with all new equipment, and can accommodate large groups to individual learning solutions. We offer many options to customize your company's IT training objectives.

- Cyber Collaboration Range On-Site
- Content Support Lab Exercises - Develop Skills & Abilities
- Corporate IT Training & Certification
- Enterprise, Small/Medium Business & Individual Solutions
- Traditional Instructor-Led At Our Location
- Custom On-Site At Your Location
- eLearning & Remote Live Classrooms
- State-Of-The-Art Testing Center; Pearson Vue/ Kryterion

Our Staff . . .

Our most important asset is our instructor team, as they are among the highest rated, authorized, credentialed individuals with real-world experience.

TLC sales staff prides themselves on the greatest customer service, and will work with your IT teams to customize solutions that will accommodate your training objectives.

Affiliations . . .

- NICE - National Initiative for Cybersecurity Education
- State pf Nevada Governor's Apprenticeship Council
- UNLV/Lee Business School Advisory Board— IT/Cybersecurity Programs

For more information contact Education Coach at (702) 320-8885 or tlc@tlclasvegas.com

Microsoft Partner | CompTIA Authorized Partner | EC-Council | (ISC)² Official Training Provider | Cisco

OFFICIAL CYBERSECURITY TRAINING

TRAINING DELIVERY OPTIONS

Training Delivery Methods That Are. . .

Convenient & Versatile

Recognized *Flexible* *Official* *Dependable* *Authorized*

Live Classroom . . .

The Learning Center offers specialized technical training in various levels of computer software and hardware competencies. Our in-depth courses provide students with Knowledge, Skills and Abilities (KSAs) needed for today's latest IT certifications. Our public schedule includes courses for CompTIA, Microsoft, Cisco, ISC², EC-Council, and more. Classes are scheduled as Bootcamps for experienced IT professionals, and individual Certification courses from novice to intermediate.

- Instructor-Led Curriculum
- Schedules Available @ www.tlclasvegas.com
- Supplemental eLearning Solution

Customized Team Training . . .

TLC prides itself on providing technical customized training for project driven initiatives. We will provide your organization with a solution that is cost effective, yet meets the needs of your objectives.

Virtual Instructor-Led / Distance Learning . . .

Students connect to the virtual course from their own computer and Internet connection, joined by a certified instructor that will administer the live session. You can attend from anywhere, as the classroom is delivered via Internet.

eLearning . . .

TLC can provide your organization with an eLearning solution to accommodate the learn at your own pace workforce, anytime, anywhere. Whether they're at the office, out of town or at home, they can log on wherever there's a WiFi connection.

Cybersecurity Range Training . . .

TLC is strategically positioned to provide your organization with authorized and accredited training in the Cybersecurity realm. These global organizations, ISC² EC-Council and CompTIA have developed official curriculum which is geared to intensive lab environments to solidify skill sets and ensure individuals can "perform" on the job.

- Performance-Based Learning & Assessment
- Simulated Environment For Teams To Work Together
- Labs Hosted In Secure Sandbox Area
- Real-Time Feedback
- Simulate On-The-Job Experience
- Environment For New Idea Testing
- Team Complex Cyber Problem Solving
- Professionals, Students, Educators & Organizations
- Personal Assessment & Certification

Assessments . . .

Assessments "validate competencies" and provide us with identifiable skills gaps intended to assist in developing customized training programs for teams or individuals. From top level department heads, to end-users, we can administer a training needs assessment to identify training programs that would best suit your department and/or the entire company. This approach provides a cost-effective method of skills delivery and reduces your investment in training programs.

Vendor Training Voucher. . .

Use your Microsoft Software Assurance Vouchers for Microsoft courses. Qualified organizations receive learning vouchers within purchase of Microsoft licensed software products. One voucher equals one training day used for technical classroom training.

For more information contact an Education Coach at (702) 320-8885 or tlc@TLCLasVegas.com.

Microsoft Partner | CompTIA Authorized Partner | EC-Council | (ISC)² Official Training Provider | Cisco

OFFICIAL CYBERSECURITY TRAINING

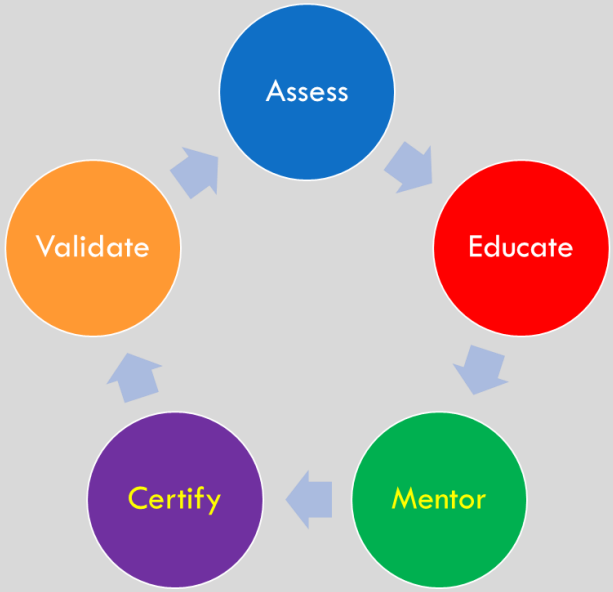
The Learning Center
Las Vegas

CompTIA A+

Course Description:

IT success stories start with CompTIA A+ certification. It validates understanding of the most common hardware and software technologies in business and certifies the skills necessary to support complex IT infrastructures. CompTIA A+ is a powerful credential that helps IT professionals worldwide ignite their IT career. Held by over 1 million IT professionals worldwide, CompTIA A+ is the most essential IT certification for establishing an IT career. If you're new to the IT industry, this will help you put your best foot forward. And if you're already an IT professional, the CompTIA A+ certification validates your skills and can boost your career.

The Learning Center Model:



Our unique model follows a streamlined approach to workforce development and skills attainment:

Assess

Assess each individual and teams to determine existing skill sets

Educate

Deliver goal specific training utilizing all delivery modalities

Mentor

Expose students to instructor/ mentors with front-line cyber/IT experience

Certify

Certify students with the requisite hands-on skills to perform the tasks related to their functional roles

Validate

Validate students "abilities" through performance analytics and real-world exercises hosted on a cyber range

OFFICIAL CYBERSECURITY TRAINING

Exam Objectives: 800-901

1.0 Hardware	34%
2.0 Networking	21%
3.0 Mobile Devices	17%
4.0 Hardware & Network Troubleshooting	28%
Total	**100%**

Exam Objectives: 800-902

1.0 Windows Operating Systems	29%
2.0 Other Operating Systems & Technologies	12%
3.0 Security	22%
4.0 Software Troubleshooting	24%
5.0 Operational Procedures	13%
Total	**100%**

The Learning Center
Las Vegas

WHY CHOOSE TLC?

The Learning Center, a division of The Learning Center, has operated for 31 years in IT training and certification field. TLC is an is an Official Training Partner of $(ISC)^2$, EC-Council Accredited Training Center, ISACA Approved Training Center and CompTIA Alliance member. One of two training organizations certified/approved by 4 out of the 5 global credentialing bodies, a unique distinction. ,

Additionally, TLC has partnered with Merit.edu to deliver “world-class” training and education supported by use of the Michigan Cyber Range. The Michigan Cyber Range is the most mature and robust deliverable training platform in the world today. This partnership enables TLC to uniquely deliver skills-based training, assessment, and certifications in alignment with the National Initiative for Cybersecurity Education (NICE) Framework. Our lab content and assessment services are a one-of-a-kind model for developing performance defined cybersecurity professionals capable of meeting current and future employer demand.

OFFICIAL CYBERSECURITY TRAINING

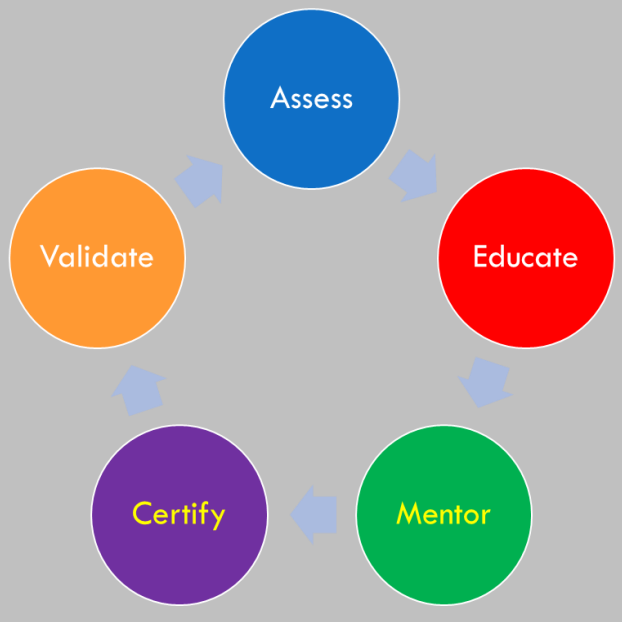
The Learning Center
Las Vegas

CompTIA Network+

Course Description:

CompTIA Network+ is a vendor neutral networking certification that is trusted around the world. It validates the essential knowledge and skills needed to confidently design, configure, manage and troubleshoot any wired and wireless networks. CompTIA Network+ certified individuals are in-demand worldwide. The stakes are high. Data networks are more crucial for businesses than ever before. They are the lifeline to the critical financial, healthcare and information services that need to function at the highest, most secure level. With a CompTIA Network+ certification, you will possess the key skills to troubleshoot, configure and manage these systems and keep your company productive.

The Learning Center Model:



Our unique model follows a streamlined approach to workforce development and skills attainment:

Assess

Assess each individual and teams to determine existing skill sets

Educate

Deliver goal specific training utilizing all delivery modalities

Mentor

Expose students to instructor/mentors with front-line cyber/IT experience

Certify

Certify students with the requisite hands-on skills to perform the tasks related to their functional roles

Validate

Validate students “abilities” through performance analytics and real-world exercises hosted on a cyber range

OFFICIAL CYBERSECURITY TRAINING

The Learning Center
Las Vegas

Course Outline

1. Network Media and Devices
Topologies and the OSI Model
Cabling and Connectors
Ethernet
Bridge and Switches

2. Addressing and Routing
Internet Protocol
Addressing Schemes
DHCP and APIPA
IPv6
Routing

3. Network Applications
Transport Protocols
Name Resolution
Web Services
Communication Services
WAN Technologies
Remote Access

4. Network Security
Security Fundamentals
Security Appliances
Authentication
Installing Wireless Networks

5. Management, Monitoring, Troubleshooting
Configuration Management
Installing Wired Networks

WHY CHOOSE TLC?

The Learning Center, a division of The Learning Center, has operated for 31 years in IT training and certification field. TLC is an is an Official Training Partner of $(ISC)^2$, EC-Council Accredited Training Center, ISACA Approved Training Center and CompTIA Alliance member. One of two training organizations certified/approved by 4 out of the 5 global credentialing bodies, a unique distinction. ,

Additionally, TLC has partnered with Merit.edu to deliver "world-class" training and education supported by use of the Michigan Cyber Range. The Michigan Cyber Range is the most mature and robust deliverable training platform in the world today. This partnership enables TLC to uniquely deliver skills-based training, assessment, and certifications in alignment with the National Initiative for Cybersecurity Education (NICE) Framework. Our lab content and assessment services are a one-of-a-kind model for developing performance defined cybersecurity professionals capable of meeting current and future employer demand.

Exam Objectives:

1.0 Network Architecture	22%
2.0 Network Operations	20%
3.0 Network Security	18%
4.0 Troubleshooting	24%
5.0 Industrial Standards, Practices and Network Theory	16%
Total	**100%**

OFFICIAL CYBERSECURITY TRAINING

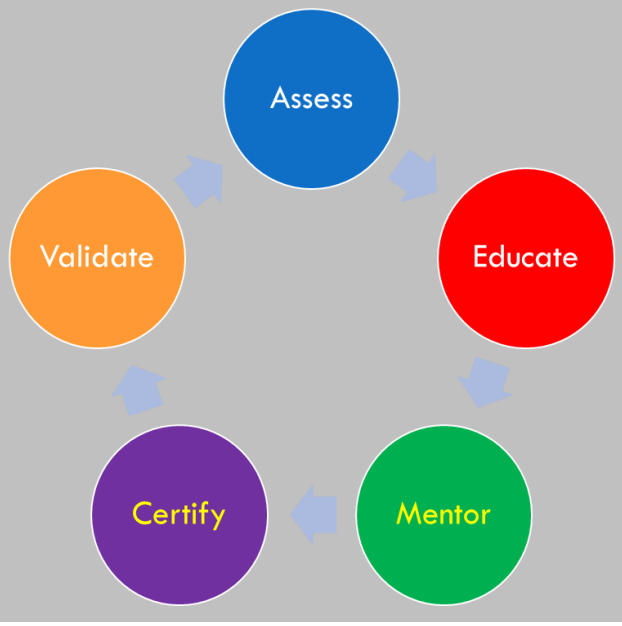
The Learning Center
Las Vegas

CompTIA Security+

Course Description:

CompTIA Security+ is the certification globally trusted to validate foundational, vendor-neutral IT security knowledge and skills. As a benchmark for best practices in IT security, this certification covers the essential principles for network security and risk management – making it an important stepping stone of an IT security career. IT security is paramount to organizations as cloud computing and mobile devices have changed the way we do business. With the massive amounts of data transmitted and stored on networks throughout the world, it's essential to have effective security practices in place. That's where CompTIA Security+ comes in. Get this certification and employers are sure you're ready for the hackers.

The Learning Center Model:



Our unique model follows a streamlined approach to work-force development and skills attainment:

Assess

Assess each individual and teams to determine existing skill sets

Educate

Deliver goal specific training utilizing all delivery modalities

Mentor

Expose students to instructor/mentors with front-line cyber/IT experience

Certify

Certify students with the requisite hands-on skills to perform the tasks related to their functional roles

Validate

Validate students "abilities" through performance analytics and real-world exercises hosted on a cyber range

OFFICIAL CYBERSECURITY TRAINING

The Learning Center
Las Vegas

Course Topics:

1. Security Threats and Controls

- Security Controls
- Threats and Attacks
- Network Attacks
- Assessment Tools and Techniques

2. Cryptography and Access Control

- Ciphers, Hashes, and Steganography
- Public Key Infrastructure
- Password Authentication
- Authorization and Account Management

3. Network Security

- Secure Network Design
- Security Appliances and Applications
- Wireless Network Security
- VPN and Remote Access Security
- Network Application Security

4. Host, Data, and Application Security

- Host Security
- Data Security
- Web Services Security
- Web Application Security
- Virtualization and Cloud Security

5. Operational Security

- Site Security
- Mobile and Embedded Device Security
- Risk Management
- Disaster Recovery
- Incident Response and Forensics
- Security Policies and Training

WHY CHOOSE TLC?

The Learning Center, a division of The Learning Center, has operated for 31 years in IT training and certification field. TLC is an is an Official Training Partner of $(ISC)^2$, EC-Council Accredited Training Center, ISACA Approved Training Center and CompTIA Alliance member. One of two training organizations certified/approved by 4 out of the 5 global credentialing bodies, a unique distinction. ,

Additionally, TLC has partnered with Merit.edu to deliver "world-class" training and education supported by use of the Michigan Cyber Range. The Michigan Cyber Range is the most mature and robust deliverable training platform in the world today. This partnership enables TLC to uniquely deliver skills-based training, assessment, and certifications in alignment with the National Initiative for Cybersecurity Education (NICE) Framework. Our lab content and assessment services are a one-of-a-kind model for developing performance defined cybersecurity professionals capable of meeting current and future employer demand.

OFFICIAL CYBERSECURITY TRAINING

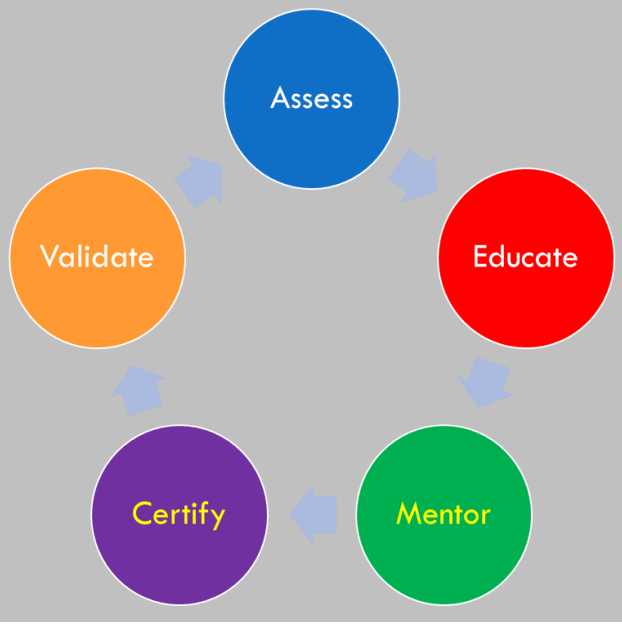
The Learning Center
Las Vegas

CompTIA CASP

Course Description:

CompTIA Advanced Security Practitioner (CASP) meets the growing demand for advanced IT security in the enterprise. Recommended for IT professionals with at least 5 years of experience, CASP certifies critical thinking and judgment across a broad spectrum of security disciplines and requires candidates to implement clear solutions in complex environments. The current landscape of cybersecurity requires specialized skills to troubleshoot via customized hacks and build solid solutions. Each hack is unique and must be combated with master-level security skills and experience.

The Learning Center Model:



Our unique model follows a streamlined approach to workforce development and skills attainment:

Assess

Assess each individual and teams to determine existing skill sets

Educate

Deliver goal specific training utilizing all delivery modalities

Mentor

Expose students to instructor/mentors with front-line cyber/IT experience

Certify

Certify students with the requisite hands-on skills to perform the tasks related to their functional roles

Validate

Validate students “abilities” through performance analytics and real-world exercises hosted on a cyber range

OFFICIAL CYBERSECURITY TRAINING

The Learning Center
Las Vegas

Exam Objectives:

Exam Codes	CAS-002
Launch Date	January 20, 2015
Exam Description	CASP covers enterprise security, risk management and incident response, research and analysis, integration of computing, communications and business disciplines as well as technical integration of enterprise components.
Number of Questions	Maximum of 90 questions
Type of Questions	Multiple choice and performance-based
Length of Test	165 Minutes
Passing Score	Pass/Fail only. No scaled score.
Recommended Experience	10 years experience in IT administration, including at least 5 years of hands-on technical security experience
Languages	English

WHY CHOOSE TLC?

The Learning Center, a division of The Learning Center, has operated for 31 years in IT training and certification field. TLC is an is an Official Training Partner of $(ISC)^2$, EC-Council Accredited Training Center, ISACA Approved Training Center and CompTIA Alliance member. One of two training organizations certified/approved by 4 out of the 5 global credentialing bodies, a unique distinction. ,

Additionally, TLC has partnered with Merit.edu to deliver “world-class” training and education supported by use of the Michigan Cyber Range. The Michigan Cyber Range is the most mature and robust deliverable training platform in the world today. This partnership enables TLC to uniquely deliver skills-based training, assessment, and certifications in alignment with the National Initiative for Cybersecurity Education (NICE) Framework. Our lab content and assessment services are a one-of-a-kind model for developing performance defined cybersecurity professionals capable of meeting current and future employer demand.

OFFICIAL CYBERSECURITY TRAINING

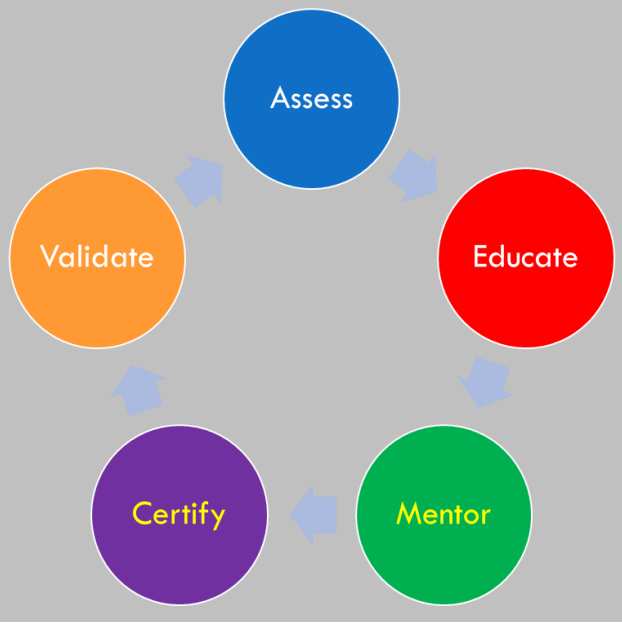
The Learning Center
Las Vegas

CompTIA Linux+ POWERED BY LPI

Course Description:

Linux has grown into an industry-leading software and service delivery platform that is used for everything from super computers and Web servers to virtualized systems and your Android phone. This growth creates a high demand for qualified Linux professionals. With CompTIA's Linux+ Powered by LPI certification, you'll acquire the fundamental skills and knowledge you need to successfully configure, manage and troubleshoot Linux systems. The Linux footprint continues to grow. In addition to its significant presence in the server room, all the major public cloud providers offer Linux images as a way of speeding up virtual instance creation. Add on that Linux-based Android accounts for approximately 80% of the smartphone market and you'll find many IT careers are founded on Linux skills.

The Learning Center Model:



Our unique model follows a streamlined approach to workforce development and skills attainment:

Assess

Assess each individual and teams to determine existing skill sets

Educate

Deliver goal specific training utilizing all delivery modalities

Mentor

Expose students to instructor/mentors with front-line cyber/IT experience

Certify

Certify students with the requisite hands-on skills to perform the tasks related to their functional roles

Validate

Validate students "abilities" through performance analytics and real-world exercises hosted on a cyber range

OFFICIAL CYBERSECURITY TRAINING

WHY CHOOSE TLC?

The Learning Center, a division of The Learning Center, has operated for 31 years in IT training and certification field. TLC is an is an Official Training Partner of $(ISC)^2$, EC-Council Accredited Training Center, ISACA Approved Training Center and CompTIA Alliance member. One of two training organizations certified/approved by 4 out of the 5 global credentialing bodies, a unique distinction. ,

Additionally, TLC has partnered with Merit.edu to deliver "world-class" training and education supported by use of the Michigan Cyber Range. The Michigan Cyber Range is the most mature and robust deliverable training platform in the world today. This partnership enables TLC to uniquely deliver skills-based training, assessment, and certifications in alignment with the National Initiative for Cybersecurity Education (NICE) Framework. Our lab content and assessment services are a one-of-a-kind model for developing performance defined cybersecurity professionals capable of meeting current and future employer demand.

Exam Objectives:

Exam Codes	LX0-103	LX0-104
Exam Description	CompTIA Linux+ covers common tasks in major distributions of Linux, including the Linux command line, basic maintenance, installing and configuring workstations, and networking. Linux+ is comprised of two exams – LX0-103 and LX0-104. Candidates must pass LX0-103 before taking LX0-104.	
Number of Questions	60 questions	60 questions
Type of Questions	Multiple Choice (Single Response), Multiple Response and Fill-in-the-Blank	Multiple Choice (Single Response), Multiple Response and Fill-in-the-Blank
Length of Test	90 Minutes	90 Minutes
Passing Score	500 (on a scale of 200 to 800)	500 (on a scale of 200 to 800)
Recommended Experience	CompTIA A+, CompTIA Network+ and 12 months of Linux admin experience	CompTIA A+, CompTIA Network+ and 12 months of Linux admin experience
Languages	English, German, Portuguese, Spanish	English, German, Portuguese, Spanish

OFFICIAL CYBERSECURITY TRAINING

The Learning Center Las Vegas

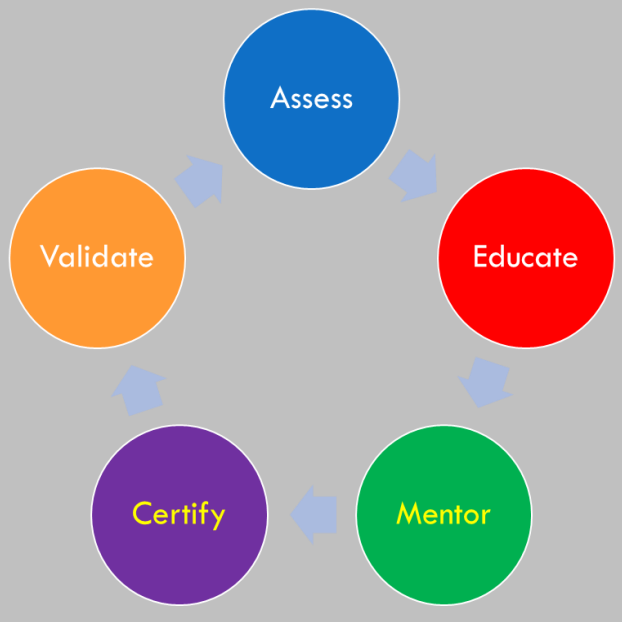
CompTIA Cloud+

Course Description:

The CompTIA Cloud+ certification validates the skills and expertise of IT practitioners in implementing and maintaining cloud technologies. Cloud+ accredits IT professionals with the constantly changing and advancing knowledge they need to be successful in today's cloud environment.

As more and more businesses shift their IT operations to cloud platforms, skills in cloud computing and virtualization have become a frequently required qualification for IT professionals. Cloud+ is globally recognized and accredited. CompTIA Cloud+ is compliant with ISO 17024 standards. Adding CompTIA Cloud+ to your resume demonstrates your ability to implement and maintain cloud technologies and enables you to jump into a rapidly growing market.

The Learning Center Model:



Our unique model follows a streamlined approach to workforce development and skills attainment:

Assess

Assess each individual and teams to determine existing skill sets

Educate

Deliver goal specific training utilizing all delivery modalities

Mentor

Expose students to instructor/mentors with front-line cyber/IT experience

Certify

Certify students with the requisite hands-on skills to perform the tasks related to their functional roles

Validate

Validate students "abilities" through performance analytics and real-world exercises hosted on a cyber range

OFFICIAL CYBERSECURITY TRAINING

The Learning Center
Las Vegas

Exam Objectives:

Exam Codes	**CV0-001**
Exam Description	CompTIA Cloud+ covers competency in cloud models, virtualization, infrastructure, security, resource management and business continuity.
Number of Questions	100 questions
Type of Questions	Multiple choice
Length of Test	90 Minutes
Passing Score	750 (on a scale of 100-900)
Recommended Experience	24 to 36 months of work experience in networking, storage or IT data center administration. Familiarity with any major hypervisor technologies for server virtualization.
Languages	English

WHY CHOOSE TLC?

The Learning Center, a division of The Learning Center, has operated for 31 years in IT training and certification field. TLC is an is an Official Training Partner of $(ISC)^2$, EC-Council Accredited Training Center, ISACA Approved Training Center and CompTIA Alliance member. One of two training organizations certified/approved by 4 out of the 5 global credentialing bodies, a unique distinction. ,

Additionally, TLC has partnered with Merit.edu to deliver "world-class" training and education supported by use of the Michigan Cyber Range. The Michigan Cyber Range is the most mature and robust deliverable training platform in the world today. This partnership enables TLC to uniquely deliver skills-based training, assessment, and certifications in alignment with the National Initiative for Cybersecurity Education (NICE) Framework. Our lab content and assessment services are a one-of-a-kind model for developing performance defined cybersecurity professionals capable of meeting current and future employer demand.

OFFICIAL CYBERSECURITY TRAINING

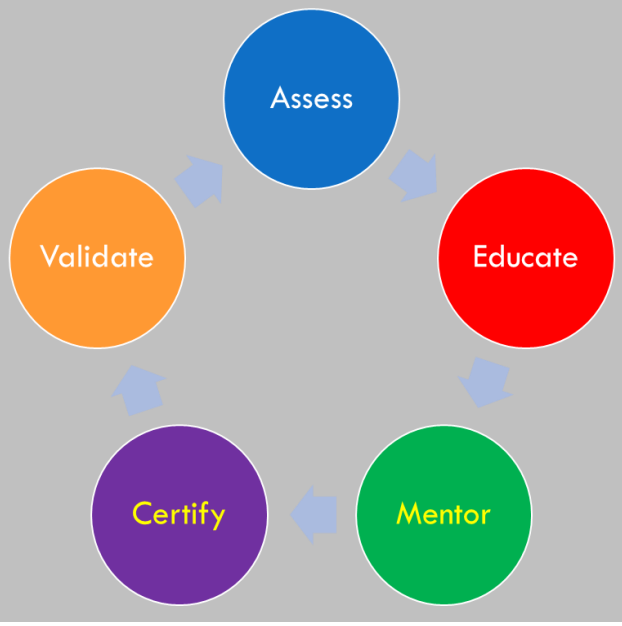
The Learning Center
Las Vegas

CompTIA CTT+

Course Description:

CompTIA Certified Technical Trainer (CTT+) certification is for instructors who want to verify they have attained a standard of excellence in the training field. CTT+ validates the knowledge and use of tools and techniques necessary for successfully teaching in today's learning environments. Earning the CTT+ certification designates you as an exceptional trainer in your field. As an instructor, you not only have to plan engaging classroom lectures, practice tasks and exams, but you must also be a knowledgeable and effective communicator. CTT+ certification provides comprehensive training standards to validate your skills in a traditional or virtual classroom environment, and ensures that you can teach effectively and step up to the front of the class with confidence.

The Learning Center Model:



Our unique model follows a streamlined approach to workforce development and skills attainment:

Assess

Assess each individual and teams to determine existing skill sets

Educate

Deliver goal specific training utilizing all delivery modalities

Mentor

Expose students to instructor/mentors with front-line cyber/IT experience

Certify

Certify students with the requisite hands-on skills to perform the tasks related to their functional roles

Validate

Validate students "abilities" through performance analytics and real-world exercises hosted on a cyber range

OFFICIAL CYBERSECURITY TRAINING

Exam Details

Exam Codes	CTT+ Essentials – TK0-201	CTT+ Classroom Performance Based Exam – TK0-202 CTT+ Virtual Classroom Performance Based Exam - TK0 -203
Exam Description	The CTT+ certification exam tests in and out of class teaching expertise, including preparation, facilitation and physical or virtual classroom evaluation. To earn the certification, two exams must be passed. In addition to TK0-201, you'll have to pass either TK0-202, or TK0-203.	
Number of Questions	95 questions	N/A
Type of Questions	Multiple choice questions (single and multiple response), and drag and drops	N/A
Length of Test	90 Minutes	Length of instruction recording must be between 17 minutes and 22 minutes
Passing Score	655 (on a scale of 100-900)	36 (on a scale of 48)
Recommended Experience	6 to 12 months of trainer/instructor experience	6 to 12 months of trainer/instructor experience
Languages	English, German, Japanese, Portuguese, Spanish	Recordings can be submitted in English, German, Dutch, Japanese, Spanish, Brazilian, Portuguese or Korean

WHY CHOOSE TLC?

The Learning Center, a division of The Learning Center, has operated for 31 years in IT training and certification field. TLC is an is an Official Training Partner of $(ISC)^2$, EC-Council Accredited Training Center, ISACA Approved Training Center and CompTIA Alliance member. One of two training organizations certified/approved by 4 out of the 5 global credentialing bodies, a unique distinction. ,

Additionally, TLC has partnered with Merit.edu to deliver "world-class" training and education supported by use of the Michigan Cyber Range. The Michigan Cyber Range is the most mature and robust deliverable training platform in the world today. This partnership enables TLC to uniquely deliver skills-based training, assessment, and certifications in alignment with the National Initiative for Cybersecurity Education (NICE) Framework. Our lab content and assessment services are a one-of-a-kind model for developing performance defined cybersecurity professionals capable of meeting current and future employer demand.

OFFICIAL CYBERSECURITY TRAINING

The Learning Center
Las Vegas

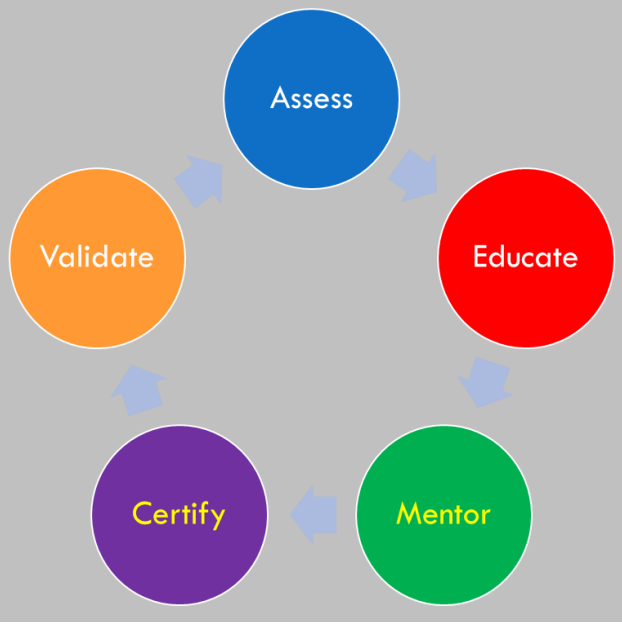
CompTIA
CSA+

Course Description:

CompTIA Cybersecurity Analyst (CSA+) is an international, vendor-neutral IT professional certification that applies behavioral analytics to improve the overall state of IT security.

It validates the knowledge and skills required to configure and use threat detection tools, perform data analysis and interpret the results to identify vulnerabilities, threats and risks to an organization, with the end goal of securing and protecting applications and systems within an organization.

The Learning Center Model:



Our unique model follows a streamlined approach to work-force development and skills attainment:

Assess

Assess each individual and teams to determine existing skill sets

Educate

Deliver goal specific training utilizing all delivery modalities

Mentor

Expose students to instructor/mentors with front-line cyber/IT experience

Certify

Certify students with the requisite hands-on skills to perform the tasks related to their functional roles

Validate

Validate students “abilities” through performance analytics and real-world exercises hosted on a cyber range

OFFICIAL CYBERSECURITY TRAINING

The Learning Center
Las Vegas

CompTIA Cybersecurity Certification Path

CompTIA CSA+ bridges the skills gap between CompTIA Security+ and the CompTIA Advanced Security Practitioner (CASP) exam and creates a vendor-neutral certification path, as shown in Figure 1 below.

CompTIA CSA+ follows CompTIA Security+ in the career pathway because the skills needed to pass the exam reflect 3 to 4 years of security experience, versus the 2 years of experience reflected by Security+. After CSA+, IT pros can pursue CASP to prove their mastery of the hands-on cybersecurity skills required at the 5- to 10-year experience level.

Performance-Based Assessment

The CSA+ exam is performance based and includes hands-on simulations. These simulations require test takers to perform security analyst job tasks during the exam. To prepare for these performance-based questions, trainers, educators and publishers should emphasize open-source analytics tools, teamwork and cyberwarfare exercises with red teams as pen testers and blue teams as security analysts/incident responders.

OFFICIAL CYBERSECURITY TRAINING

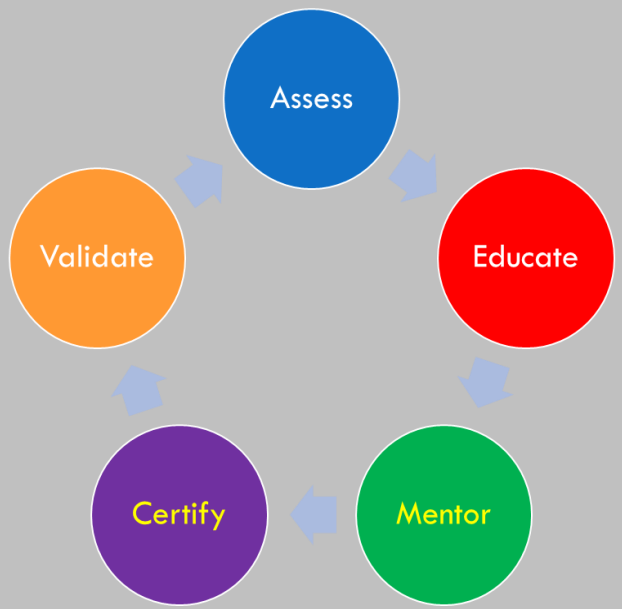
The Learning Center
Las Vegas

CISSP®

Course Description:

The CISSP certification is the ideal credential for those with proven deep technical and managerial competence, skills, experience, and credibility to-build and maintain security programs to protecting organizations from growing sophisticated attacks. The CISSP draws from a comprehensive, up-to-date, global common body of knowledge that ensures security leaders have a deep knowledge and understanding of new threats, technologies, regulations, standards, and practices. Backed by (ISC)2®, the globally recognized, not-for-profit organization dedicated to advancing the information security field, the CISSP was the first credential in the field of information security to meet the stringent requirements of ISO/ IEC Standard 17024. Not only is the CISSP an objective measure of excellence, but also a globally recognized standard of achievement.

The Learning Center Model:



Our unique model follows a streamlined approach to work-force development and skills attainment:

Assess

Assess each individual and teams to determine existing skill sets

Educate

Deliver goal specific training utilizing all delivery modalities

Mentor

Expose students to instructor/mentors with front-line cyber/IT experience

Certify

Certify students with the requisite hands-on skills to perform the tasks related to their functional roles

Validate

Validate students “abilities” through performance analytics and real-world exercises hosted on a cyber range

OFFICIAL CYBERSECURITY TRAINING

Globally Recognized Standard in Information Security

The CISSP covers critical areas with up-to-date, global Common Body of Knowledge training that ensures security leaders have a deep knowledge and understanding of new threats, technologies, regulations, standards, and practices. The CISSP exam tests competence in following 8 domains of the CISSP CBK:

- Security and Risk Management
- Asset Security
- Security Engineering
- Communications and Network Security
- Identity and Access Management
- Security Assessment and Testing
- Security Operations
- Software Development Security

The Learning Center Las Vegas

WHY CHOOSE TLC?

The Learning Center, a division of The Learning Center, has operated for 31 years in IT training and certification field. TLC is an is an Official Training Partner of $(ISC)^2$, EC-Council Accredited Training Center, ISACA Approved Training Center and CompTIA Alliance member. One of two training organizations certified/approved by 4 out of the 5 global credentialing bodies, a unique distinction. ,

Additionally, TLC has partnered with Merit.edu to deliver "world-class" training and education supported by use of the Michigan Cyber Range. The Michigan Cyber Range is the most mature and robust deliverable training platform in the world today. This partnership enables TLC to uniquely deliver skills-based training, assessment, and certifications in alignment with the National Initiative for Cybersecurity Education (NICE) Framework. Our lab content and assessment services are a one-of-a-kind model for developing performance defined cybersecurity professionals capable of meeting current and future employer demand.

OFFICIAL CYBERSECURITY TRAINING

The Learning Center Las Vegas

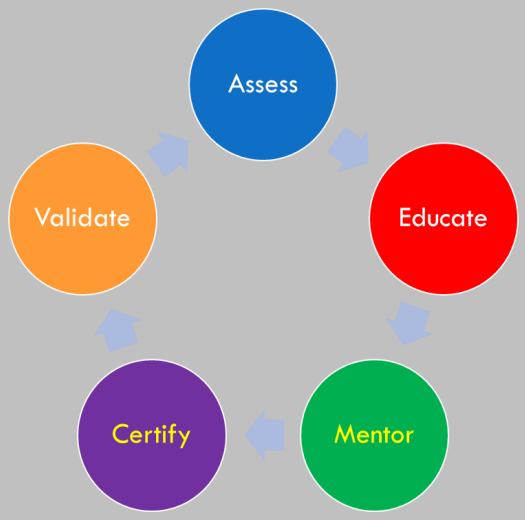
CSSLP®

Course Description:

Enabling the Next Generation to Build Secure Software

Attackers and researchers continue to expose new application vulnerabilities, and it's no wonder that application vulnerabilities are ranked the #1 threat to cybersecurity professionals (according to the 2015 (ISC)² Global Information Security Workforce Study). Web application security must be a priority for organizations to protect their business and reputation. For this reason, it is crucial that anyone involved in the software development lifecycle (SDLC) be knowledgeable and experienced in understanding how to build secure software. The CSSLP certification validates software professionals have the expertise to incorporate security practices – authentication, authorization and auditing – into each phase of the SDLC, from software design and implementation to testing and deployment. CSSLPs have proven proficiency.

The Learning Center Model:



Our unique model follows a streamlined approach to workforce development and skills attainment:

Assess

Assess each individual and teams to determine existing skill sets

Educate

Deliver goal specific training utilizing all delivery modalities

Mentor

Expose students to instructor/mentors with front-line cyber/IT experience

Certify

Certify students with the requisite hands-on skills to perform the tasks related to their functional roles

Validate

Validate students “abilities” through performance analytics and real-world exercises hosted on a cyber range

OFFICIAL CYBERSECURITY TRAINING

The Learning Center
Las Vegas

Who should obtain the CSSLP certification?

The Certified Secure Software Lifecycle Professional (CSSLP) is for everyone involved in the SDLC with at least 4 years of cumulative paid full-time work experience in 1 or more of the 8 domains of the CSSLP CBK. CSSLPs often hold positions such as the following:

- Software Architect
- Software Engineer
- Software Developer
- Application Security Specialist
- Software Program Manager
- Quality Assurance Tester
- Penetration Tester
- Software Procurement Analyst
- Project Manager
- Security Manager
- IT Director/Manager

Globally Recognized Proficiency in Application Security

The CSSLP draws from a comprehensive, up-to-date, global common body of knowledge that ensures software professionals have deep knowledge and understanding of how to build secure software. CSSLP tests one competence in the following 8 domains:

Secure Software Concepts

Secure Software Requirements

Secure Software Design

Secure Software Implementation/Coding

Secure Software Testing

Software Acceptance

Software Deployment, Operations, Maintenance and Disposal

Supply Chain and Software Acquisition

WHY CHOOSE TLC?

The Learning Center, a division of The Learning Center, has operated for 31 years in IT training and certification field. TLC is an is an Official Training Partner of $(ISC)^2$, EC-Council Accredited Training Center, ISACA Approved Training Center and CompTIA Alliance member. One of two training organizations certified/approved by 4 out of the 5 global credentialing bodies, a unique distinction. ,

Additionally, TLC has partnered with Merit.edu to deliver "world-class" training and education supported by use of the Michigan Cyber Range. The Michigan Cyber Range is the most mature and robust deliverable training platform in the world today. This partnership enables TLC to uniquely deliver skills-based training, assessment, and certifications in alignment with the National Initiative for Cybersecurity Education (NICE) Framework. Our lab content and assessment services are a one-of-a-kind model for developing performance defined cybersecurity professionals capable of meeting current and future employer demand.

OFFICIAL CYBERSECURITY TRAINING

The Learning Center
Las Vegas

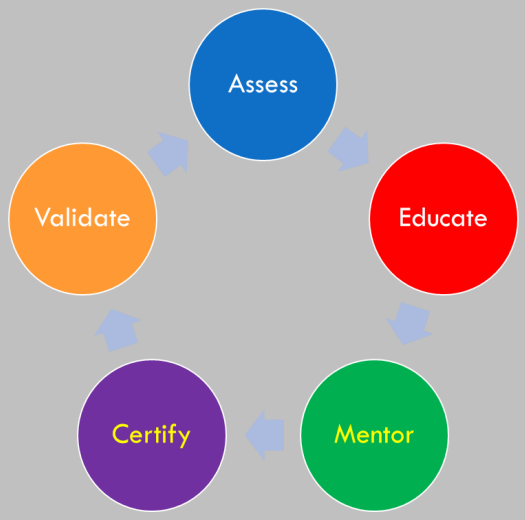
SSCP®

Course Description:

The SSCP certification is the ideal credential for those with proven technical skills and practical security knowledge in hands-on operational IT roles. It provides industry-leading confirmation of a practitioner's ability to implement, monitor and administer IT infrastructure in accordance with information security policies and procedures that ensure data confidentiality, integrity and availability.

The SSCP indicates a practitioner's technical ability to tackle the operational demands and responsibilities of security practitioners, including authentication, security testing, intrusion detection/prevention, incident response and recovery, attacks and countermeasures, cryptography, malicious code countermeasures, and more.

The Learning Center Model:



Our unique model follows a streamlined approach to workforce development and skills attainment:

Assess

Assess each individual and teams to determine existing skill sets

Educate

Deliver goal specific training utilizing all delivery modalities

Mentor

Expose students to instructor/mentors with front-line cyber/IT experience

Certify

Certify students with the requisite hands-on skills to perform the tasks related to their functional roles

Validate

Validate students "abilities" through performance analytics and real-world exercises hosted on a cyber range

OFFICIAL CYBERSECURITY TRAINING

The Learning Center Las Vegas

Globally Recognized Proficiency in Information Security

Offered by (ISC)², the world leader in educating and certifying security professionals worldwide, SSCPs benefit from a global network of certified members and valuable resources and support to help them to continually develop and advance in their careers.

The SSCP credential draws from a comprehensive, up-to-date global body of knowledge that ensures candidates have the right information security knowledge and skills to be successful in IT operational roles. It demonstrates competency in the following CBK Domains:

- Access Controls
- Security Operations and Administration
- Risk Identification, Monitoring, and Analysis
- Incident Response and Recovery
- Cryptography
- Network and Communications Security
- Systems and Application Security

SSCP Exam Information

Length of exam	3 hours
Number of questions	125
Question format	Multiple choice questions
Passing grade	700 out of 1000 points
Exam languages	English, Japanese, and Brazilian Portuguese
Testing center	Pearson Vue Testing Center
Study tools	*Official (ISC)² Guide to the SSCP CBK Textbook* *Official (ISC)² SSCP Study Guide* Official Study App Official (ISC)² Training Exam Outline Interactive Flashcards

(ISC)² OFFICIAL TRAINING PROVIDER

WHY CHOOSE TLC?

The Learning Center, a division of The Learning Center, has operated for 31 years in IT training and certification field. TLC is an is an Official Training Partner of (ISC)², EC-Council Accredited Training Center, ISACA Approved Training Center and CompTIA Alliance member. One of two training organizations certified/approved by 4 out of the 5 global credentialing bodies, a unique distinction. ,

Additionally, TLC has partnered with Merit.edu to deliver "world-class" training and education supported by use of the Michigan Cyber Range. The Michigan Cyber Range is the most mature and robust deliverable training platform in the world today. This partnership enables TLC to uniquely deliver skills-based training, assessment, and certifications in alignment with the National Initiative for Cybersecurity Education (NICE) Framework. Our lab content and assessment services are a one-of-a-kind model for developing performance defined cybersecurity professionals capable of meeting current and future employer demand.

OFFICIAL CYBERSECURITY TRAINING

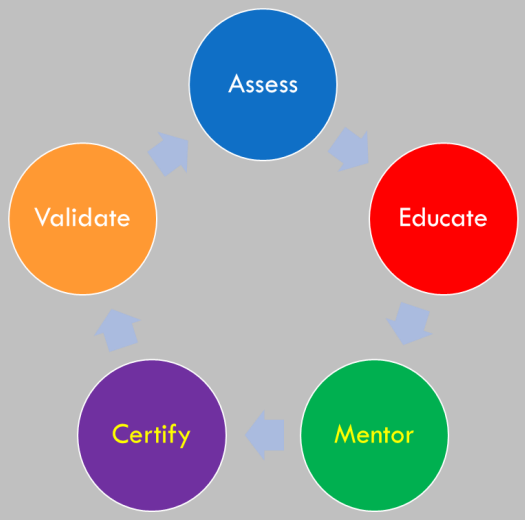
The Learning Center Las Vegas

CCFP®

Course Description: Leadership for the Field of Cyber Forensics

The evolving field of cyber forensics requires professionals who understand far more than just hard drive or intrusion analysis. The field requires CCFP professionals who demonstrate competence across a globally recognized common body of knowledge that includes established forensics disciplines as well as newer challenges, such as mobile forensics, cloud forensics, anti-forensics, and more. The CCFP credential indicates expertise in forensics techniques and procedures, standards of practice, and legal and ethical principles to assure accurate, complete, and reliable digital evidence admissible in a court of law. It also indicates the ability to apply forensics to other information security disciplines, such as e-discovery, malware analysis, or incident response. In other words, the CCFP is an objective measure of excellence valued by courts and employers alike.

The Learning Center Model:



Our unique model follows a streamlined approach to work-force development and skills attainment:

Assess

Assess each individual and teams to determine existing skill sets

Educate

Deliver goal specific training utilizing all delivery modalities

Mentor

Expose students to instructor/mentors with front-line cyber/IT experience

Certify

Certify students with the requisite hands-on skills to perform the tasks related to their functional roles

Validate

Validate students “abilities” through performance analytics and real-world exercises hosted on a cyber range

OFFICIAL CYBERSECURITY TRAINING

The Learning Center Las Vegas

Who should obtain the CCFP credential?

CCFP addresses more experienced cyber forensics professionals who already have the proficiency and perspective to effectively apply their cyber forensics expertise to a variety of challenges. In fact, many new CCFP professionals likely hold one or more other digital forensics certifications.

Given the varied applications of cyber forensics, CCFP professionals can come from an array of corporate, legal, law enforcement, and government occupations, including:

- Digital forensic examiners in law enforcement to support criminal investigations
- Cybercrime and cybersecurity professionals working in the public or private sectors
- Computer forensic engineers & managers working in corporate information security
- Digital forensic and e-discovery consultants focused on litigation support
- Cyber intelligence analysts working for defense/intelligence agencies
- Computer forensic consultants working for management or specialty consulting firms.

Who should obtain the CCFP credential?

CCFP addresses more experienced cyber forensics professionals who already have the proficiency and perspective to effectively apply their cyber forensics expertise to a variety of challenges. In fact, many new CCFP professionals likely hold one or more other digital forensics certifications.

Given the varied applications of cyber forensics, CCFP professionals can come from an array of corporate, legal, law enforcement, and government occupations, including:

- Digital forensic examiners in law enforcement to support criminal investigations
- Cybercrime and cybersecurity professionals working in the public or private sectors
- Computer forensic engineers & managers working in corporate information security
- Digital forensic and e-discovery consultants focused on litigation support
- Cyber intelligence analysts working for defense/intelligence agencies
- Computer forensic consultants working for management or specialty consulting firms.

(ISC)² OFFICIAL TRAINING PROVIDER

WHY CHOOSE TLC?

The Learning Center, a division of The Learning Center, has operated for 31 years in IT training and certification field. TLC is an is an Official Training Partner of (ISC)², EC-Council Accredited Training Center, ISACA Approved Training Center and CompTIA Alliance member. One of two training organizations certified/approved by 4 out of the 5 global credentialing bodies, a unique distinction. ,

Additionally, TLC has partnered with Merit.edu to deliver “world-class” training and education supported by use of the Michigan Cyber Range. The Michigan Cyber Range is the most mature and robust deliverable training platform in the world today. This partnership enables TLC to uniquely deliver skills-based training, assessment, and certifications in alignment with the National Initiative for Cybersecurity Education (NICE) Framework. Our lab content and assessment services are a one-of-a-kind model for developing performance defined cybersecurity professionals capable of meeting current and future employer demand.

OFFICIAL CYBERSECURITY TRAINING

The Learning Center
Las Vegas

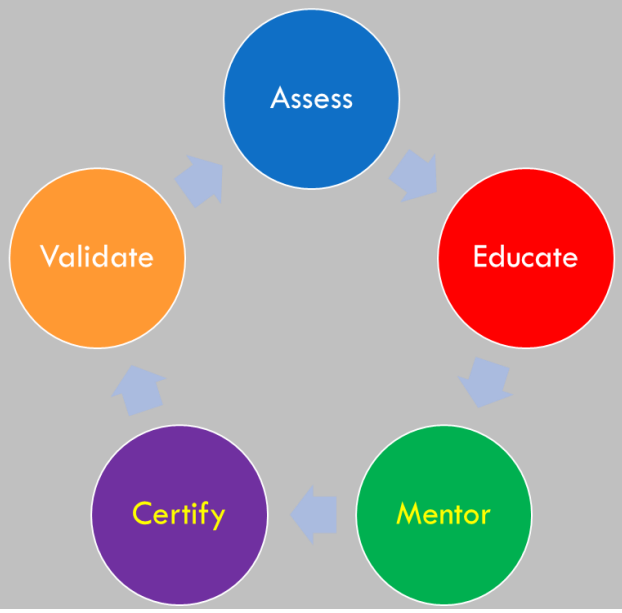
CCSP℠

Course Description:

Emerging cloud computing demands individuals who understand its information security risks and mitigation strategies. Legacy approaches are inadequate, and organizations need competent, experienced professionals equipped with the right cloud security knowledge and skills to be successful.

Globally recognized and backed by the two leading non-profits focused on cloud and information security, the Cloud Security Alliance (CSA) and (ISC)², the CCSP credential denotes professionals with deep-seated knowledge and competency derived from hands-on experience with cyber, information, software and cloud computing infrastructure security. CCSPs help you achieve the highest standard for cloud security expertise and enable your organization to benefit from the power of cloud computing while keeping sensitive data secure.

The Learning Center Model:



Our unique model follows a streamlined approach to workforce development and skills attainment:

Assess

Assess each individual and teams to determine existing skill sets

Educate

Deliver goal specific training utilizing all delivery modalities

Mentor

Expose students to instructor/mentors with front-line cyber/IT experience

Certify

Certify students with the requisite hands-on skills to perform the tasks related to their functional roles

Validate

Validate students “abilities” through performance analytics and real-world exercises hosted on a cyber range

OFFICIAL CYBERSECURITY TRAINING

The Learning Center
Las Vegas

Who should obtain the CCSP credential?

The Certified Cloud Security Professional certification is most appropriate for those well versed in IT and information security, with some experience in cloud computing. The ideal candidate will have experience in applying security concepts and controls to cloud environments. To attain CCSP, applicants must have a minimum of five years of cumulative, paid, full-time working experience in information technology, of which three years must be in information security and one year in one of the six CBK domains. Earning the Cloud Security Alliance's Certificate of Cloud Security Knowledge (CCSKTM) can be substituted for one year of experience in one of the six domains of the CCSP CBK. Earning the (ISC)² Certified Information Systems Security Professional (CISSP) credential can be substituted for the entire CCSP experience requirement.

WHY CHOOSE TLC?

The Learning Center, a division of The Learning Center, has operated for 31 years in IT training and certification field. TLC is an is an Official Training Partner of (ISC)², EC-Council Accredited Training Center, ISACA Approved Training Center and CompTIA Alliance member. One of two training organizations certified/approved by 4 out of the 5 global credentialing bodies, a unique distinction. ,

Additionally, TLC has partnered with Merit.edu to deliver “world-class” training and education supported by use of the Michigan Cyber Range. The Michigan Cyber Range is the most mature and robust deliverable training platform in the world today. This partnership enables TLC to uniquely deliver skills-based training, assessment, and certifications in alignment with the National Initiative for Cybersecurity Education (NICE) Framework. Our lab content and assessment services are a one-of-a-kind model for developing performance defined cybersecurity professionals capable of meeting current and future employer demand.

OFFICIAL CYBERSECURITY TRAINING

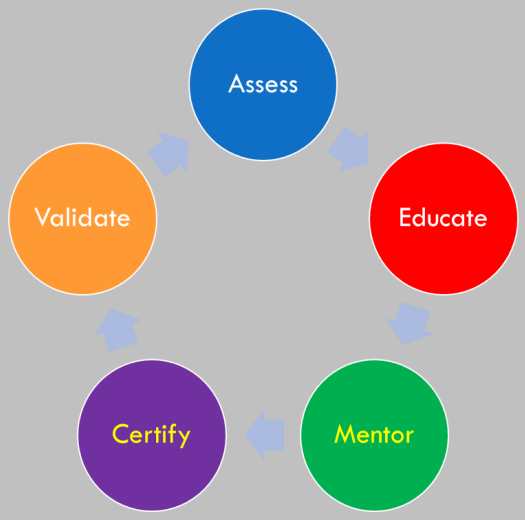
The Learning Center
Las Vegas

HCISPP®

Course Description:

As the rapidly evolving healthcare industry faces increasing challenges to keeping personal health information protected, there is a growing need to ensure knowledgeable and credentialed security and privacy practitioners are in place to protect this sensitive information. HCISPPs provide the front-line defense in protecting health information. Backed by (ISC)², a global not-for-profit organization that delivers the gold standard for information security certifications, the HCISPP credential confirms a practitioner's core knowledge and experience in security and privacy controls for personal health information.

The Learning Center Model:



Our unique model follows a streamlined approach to workforce development and skills attainment:

Assess

Assess each individual and teams to determine existing skill sets

Educate

Deliver goal specific training utilizing all delivery modalities

Mentor

Expose students to instructor/mentors with front-line cyber/IT experience

Certify

Certify students with the requisite hands-on skills to perform the tasks related to their functional roles

Validate

Validate students "abilities" through performance analytics and real-world exercises hosted on a cyber range

OFFICIAL CYBERSECURITY TRAINING

The Learning Center
Las Vegas

(ISC)² OFFICIAL TRAINING PROVIDER

The Front-Line Defense for Protecting Patient Data

As the rapidly evolving healthcare industry faces increasing challenges to keeping personal health information protected, there is a growing need to ensure knowledgeable and credentialed security and privacy practitioners are in place to protect this sensitive information.

HCISPPs provide the front-line defense in protecting health information. Backed by (ISC)², a global not-for-profit organization that delivers the gold standard for information security certifications, the HCISPP credential confirms a practitioner's core knowledge and experience in security and privacy controls for personal health information.

Who should obtain the HCISPP certification?

HCISPPs are at the forefront of protecting patient health information. These are the practitioners whose foundational knowledge and experience unite healthcare information security and privacy best practices and techniques under one credential to protect organizations and sensitive patient data against emerging threats and breaches. HCISPPs are instrumental to a variety of job functions, including:

- Compliance officer
- Information security manager
- Privacy officer
- Compliance auditor
- Risk analyst
- Medical records supervisor
- Information technology manager
- Privacy and security consultant
- Health information manager
- Practice manager

WHY CHOOSE TLC?

The Learning Center, a division of The Learning Center, has operated for 31 years in IT training and certification field. TLC is an is an Official Training Partner of (ISC)², EC-Council Accredited Training Center, ISACA Approved Training Center and CompTIA Alliance member. One of two training organizations certified/approved by 4 out of the 5 global credentialing bodies, a unique distinction. ,

Additionally, TLC has partnered with Merit.edu to deliver "world-class" training and education supported by use of the Michigan Cyber Range. The Michigan Cyber Range is the most mature and robust deliverable training platform in the world today. This partnership enables TLC to uniquely deliver skills-based training, assessment, and certifications in alignment with the National Initiative for Cybersecurity Education (NICE) Framework. Our lab content and assessment services are a one-of-a-kind model for developing performance defined cybersecurity professionals capable of meeting current and future employer demand.

OFFICIAL CYBERSECURITY TRAINING

The Learning Center
Las Vegas

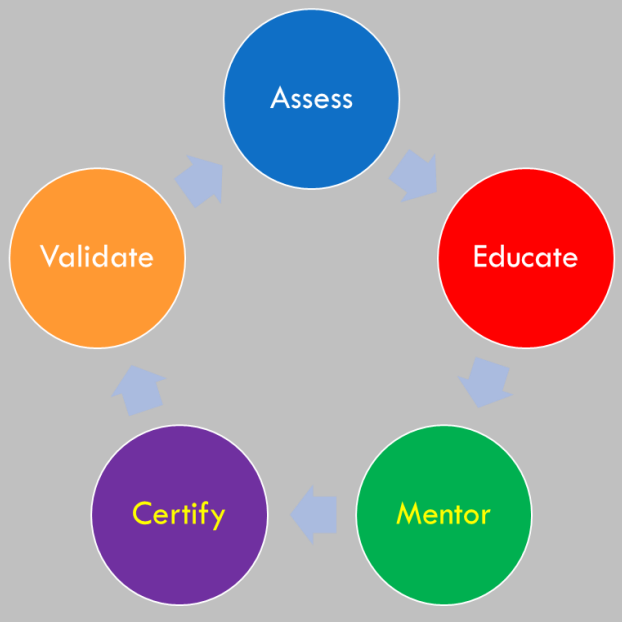
cisco

CCNA Routing and Switching

Course Description:

As Enterprises migrate toward controller based architectures, the role and skills required of a core network engineer are evolving and more vital than ever. To prepare for this network transition, the CCNA Routing and Switching certification will not only prepare you with the knowledge of foundational technologies, but ensure you stay relevant with skill sets needed for the adoption of next generation technologies.

The Learning Center Model:



Our unique model follows a streamlined approach to workforce development and skills attainment:

Assess

Assess each individual and teams to determine existing skill sets

Educate

Deliver goal specific training utilizing all delivery modalities

Mentor

Expose students to instructor/mentors with front-line cyber/IT experience

Certify

Certify students with the requisite hands-on skills to perform the tasks related to their functional roles

Validate

Validate students “abilities” through performance analytics and real-world exercises hosted on a cyber range

OFFICIAL CYBERSECURITY TRAINING

The Learning Center Las Vegas

Routing and Switching

As Enterprises migrate toward controller based architectures, the role and skills required of a core network engineer are evolving and more vital than ever. To prepare for this network transition, the CCNA Routing and Switching certification will not only prepare you with the knowledge of foundational technologies, but ensure you stay relevant with skill sets needed for the adoption of next generation technologies.

Demand for Trained and Experienced Routing and Switching Professionals

The digital transformation of business is driving adoption of programmable network architectures with a corresponding need for expanded skills and knowledge from network engineers. To meet these evolving job roles, Cisco continues to develop training and certification products that enable Enterprises to successfully innovate and migrate to a digital-ready network.

The program includes:

- **Skills Building:** Recommended tools to help you learn best practices and gain hands-on experience. From entry level to expert level, we offer instructor-led and self-paced training options with a hands-on focus for every learning style and budget.
- **Skills Validation:** Assess Cisco routing and switching knowledge and new skills proving to hiring managers that IT professionals are ready to design and deploy digital-ready network.
- **Skills Reinforcement:** Continually hone skills throughout your career as an Enterprise network engineer.

The certification prepares you for the following roles:

- Network Administrators
- Network Support Engineers
- Network Engineer Associate
- Network Specialist
- Network Analyst

WHY CHOOSE TLC?

The Learning Center, a division of The Learning Center, is an Official Training Partner of $(ISC)^2$., operating for 31 years in IT training and certification programs can offer you the best in education and training. TLC is an EC-Council Accredited Training Center. One of only 700 accredited training centers globally, TLC **is proud to be one of 15 global partners selected to deliver the C|CISO curriculum.**

Additionally, TLC in partnership with Merit.edu has partnered to deliver "world-class" training and education supported by use of the Michigan Cyber Range. This Cyber Range is the most state-of-the-art deliverable training method to ensure "skills set" learning by use of Alphaville, a virtual environment to practice and hone Cybersecurity skills. Students receive the official training, plus access to the Cyber Range. ***Click here for more***.

OFFICIAL CYBERSECURITY TRAINING

The Learning Center
Las Vegas

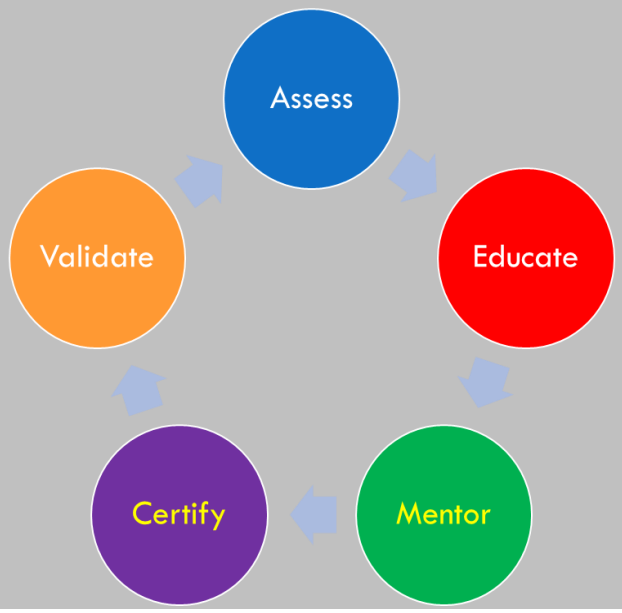
CAP®

Course Description:

The Certified Authorization Professional (CAP) certification is an objective measure of the knowledge, skills and abilities required for personnel involved in the process of authorizing and maintaining information systems. Specifically, this credential applies to those responsible for formalizing processes used to assess risk and establish security requirements and documentation. Their decisions will ensure that information systems possess security commensurate with the level of exposure to potential risk, as well as damage to assets or individuals.

The CAP credential is appropriate for commercial markets, civilian and local governments, and the U.S. Federal government including the State Department and the Department of Defense (DoD). **See CAP and DoD 8570.** Job functions such as authorization officials, system owners, information owners, information system security officers, and certifiers as well as all senior system managers apply.

The Learning Center Model:



Our unique model follows a streamlined approach to work-force development and skills attainment:

Assess

Assess each individual and teams to determine existing skill sets

Educate

Deliver goal specific training utilizing all delivery modalities

Mentor

Expose students to instructor/mentors with front-line cyber/IT experience

Certify

Certify students with the requisite hands-on skills to perform the tasks related to their functional roles

Validate

Validate students “abilities” through performance analytics and real-world exercises hosted on a cyber range

OFFICIAL CYBERSECURITY TRAINING

The Learning Center Las Vegas

The ideal candidate should have experience, skills or knowledge in:

- IT security
- Information assurance
- Information risk management
- Certification
- Systems administration
- 1-2 years of general technical experience
- 2 years of general systems experience
- 1-2 years of database/systems development/network experience
- Information security policy
- Technical or auditing experience within government, the U.S. Department of Defense, the financial or health care industries, and/or auditing firms
- Strong familiarity with NIST documentation

CAP Exam Information

Length of exam	3 hours
Number of questions	125
Question format	Multiple choice questions
Passing grade	700 out of 1000 points
Exam Language	English
Testing center	Pearson Vue Testing Center
Study tools	Official (ISC)² Guide to the CAP CBK Textbook Official (ISC)² training seminar Interactive Flashcards Exam outline

WHY CHOOSE TLC?

The Learning Center, a division of The Learning Center, is an Official Training Partner of (ISC)^2., operating for 31 years in IT training and certification programs can offer you the best in education and training. TLC is an EC-Council Accredited Training Center. One of only 700 accredited training centers globally, TLC **is proud to be one of 15 global partners selected to deliver the C|CISO curriculum.**

Additionally, TLC in partnership with Merit.edu has partnered to deliver "world-class" training and education supported by use of the Michigan Cyber Range. This Cyber Range is the most state-of-the-art deliverable training method to ensure "skills set" learning by use of Alphaville, a virtual environment to practice and hone Cybersecurity skills. Students receive the official training, plus access to the Cyber Range. ***Click here for more***.

OFFICIAL CYBERSECURITY TRAINING

The Learning Center
Las Vegas

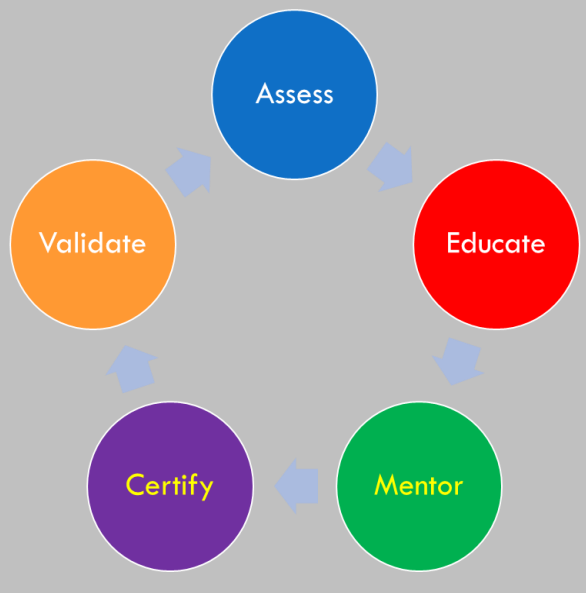
CISCO

CCNA Collaboration

Course Description:

For network video engineers, collaboration engineers, IP telephony and IP network engineers who want to develop and advance their collaboration and video skills in line with the convergence of voice, video, data and mobile applications, the Cisco CCNA Collaboration certification is a job-role focused training and certification program. It will allow you to maximize your investment in your education, and increase your professional value by giving you the skills to help your IT organization meet increased business demands resulting from these technology transitions.

The Learning Center Model:



Our unique model follows a streamlined approach to work-force development and skills attainment:

Assess

Assess each individual and teams to determine existing skill sets

Educate

Deliver goal specific training utilizing all delivery modalities

Mentor

Expose students to instructor/mentors with front-line cyber/IT experience

Certify

Certify students with the requisite hands-on skills to perform the tasks related to their functional roles

Validate

Validate students “abilities” through performance analytics and real-world exercises hosted on a cyber range

OFFICIAL CYBERSECURITY TRAINING

The Learning Center Las Vegas

The best way to prepare for this certification is to take the Cisco-approved training:

Implementing Cisco Collaboration Devices (CICD)

This course focuses on providing the skills and knowledge necessary to implement Cisco Unified Communications (UC) solutions. It covers administration of end-user interfaces, telephony and mobility features, and Cisco UC solutions maintenance.

» Learn More

Implementing Cisco Video Network Devices, Part 1 (CIVND1)

This is a 3-day ELT designed to provide students with the necessary knowledge to describe characteristics of video solutions and assess the requirements for a successful implementation of a video solution.
It covers the characteristics of a video solution and enables students to evaluate the general requirements for video deployments such as codec options, media formats, protocols, network impact, high-level architectural components, interactions, and requisites to the environment.

» Learn More

Implementing Cisco Video Network Devices, Part 2 (CVIND2)

This course is designed to provide students with the necessary knowledge and skills to implement various Cisco Collaboration endpoints in converged Cisco infrastructures.
It covers the describes Cisco Collaboration solutions and enables students to implement and troubleshoot Cisco Unified Communication and Collaboration, TelePresence, and Digital Media Player in different Cisco Collaboration solution architectures.

Exams & Recommended Training

Required Exam(s)	Recommended Training
210-060 CICD	Implementing Cisco Collaboration Devices (CICD)
210-065 CIVND	Implementing Cisco Video Network Devices, Part 1 (CIVND1) Implementing Cisco Video Network Devices, Part 2 (CIVND2)

WHY CHOOSE TLC?

The Learning Center, a division of The Learning Center, is an Official Training Partner of $(ISC)^2$., operating for 31 years in IT training and certification programs can offer you the best in education and training. TLC is an EC-Council Accredited Training Center. One of only 700 accredited training centers globally, TLC **is proud to be one of 15 global partners selected to deliver the C|CISO curriculum.**

Additionally, TLC in partnership with Merit.edu has partnered to deliver "world-class" training and education supported by use of the Michigan Cyber Range. This Cyber Range is the most state-of-the-art deliverable training method to ensure "skills set" learning by use of Alphaville, a virtual environment to practice and hone Cybersecurity skills. Students receive the official training, plus access to the Cyber Range. ***Click here for more***.

OFFICIAL CYBERSECURITY TRAINING

The Learning Center
Las Vegas

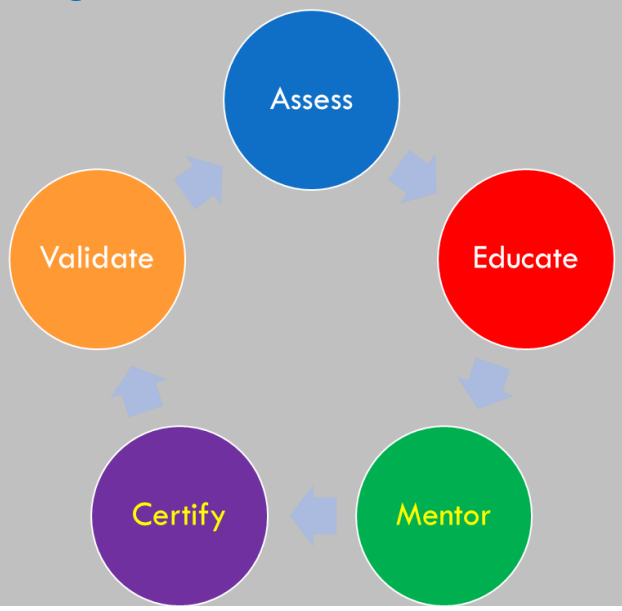
CISCO

CCNA Security

Course Description:

Cisco Certified Network Associate Security (CCNA Security) validates associate-level knowledge and skills required to secure Cisco networks. With a CCNA Security certification, a network professional demonstrates the skills required to develop a security infrastructure, recognize threats and vulnerabilities to networks, and mitigate security threats. The CCNA Security curriculum emphasizes core security technologies, the installation, troubleshooting and monitoring of network devices to maintain integrity, confidentiality and availability of data and devices, and competency in the technologies that Cisco uses in its security structure.

The Learning Center Model:



Our unique model follows a streamlined approach to workforce development and skills attainment:

Assess

Assess each individual and teams to determine existing skill sets

Educate

Deliver goal specific training utilizing all delivery modalities

Mentor

Expose students to instructor/mentors with front-line cyber/IT experience

Certify

Certify students with the requisite hands-on skills to perform the tasks related to their functional roles

Validate

Validate students “abilities” through performance analytics and real-world exercises hosted on a cyber range

OFFICIAL CYBERSECURITY TRAINING

The Learning Center Las Vegas

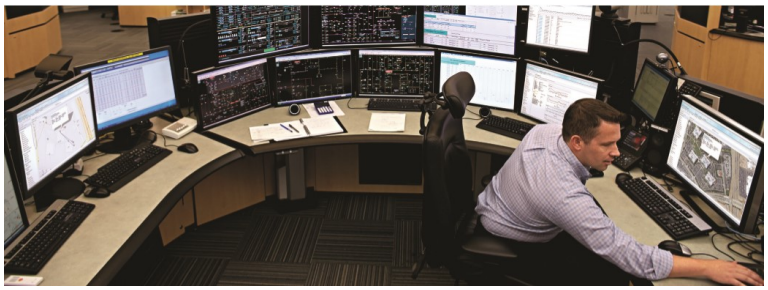
Increasing Demand for Practical Network Security Skills

Cisco has taken note of the evolution of the role of the network security professional and its relevance to the industry. The speed at which network security is evolving demands more practical, hands-on skills in network security engineering and has made network security performance more visible to the entire organization. Network security engineers in the marketplace today understand the products and the discipline of good network security, the practices and compliance mandates of industry and government, and the need to protect their organizations from increasingly sophisticated threats to their systems. Cisco network security engineers have real-world security implementation and troubleshooting skills.

Achieving CCNA Security Certification

CCNA Security certification offers professionals job-ready training and skills. The certification lays the foundation for job roles such as network security technician, administrator, and network security support engineer. Candidates gain knowhow in securing information and devices using the latest Cisco security hardware and software solutions.

Required Exam	Exam Name and Recommended Training
210-260	Implementing Cisco Network Security (IINS)



WHY CHOOSE TLC?

The Learning Center, a division of The Learning Center, has operated for 31 years in IT training and certification field. TLC is an is an Official Training Partner of $(ISC)^2$, EC-Council Accredited Training Center, ISACA Approved Training Center and CompTIA Alliance member. One of two training organizations certified/approved by 4 out of the 5 global credentialing bodies, a unique distinction. ,

Additionally, TLC has partnered with Merit.edu to deliver “world-class” training and education supported by use of the Michigan Cyber Range. The Michigan Cyber Range is the most mature and robust deliverable training platform in the world today. This partnership enables TLC to uniquely deliver skills-based training, assessment, and certifications in alignment with the National Initiative for Cybersecurity Education (NICE) Framework. Our lab content and assessment services are a one-of-a-kind model for developing performance defined cybersecurity professionals capable of meeting current and future employer demand.

OFFICIAL CYBERSECURITY TRAINING

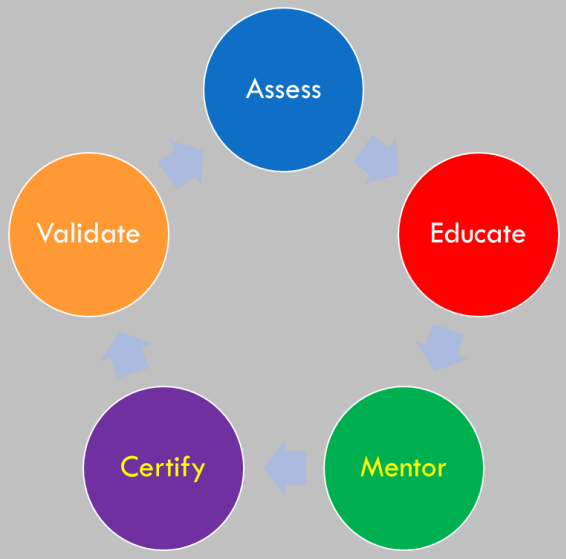
The Learning Center Las Vegas

CCNA Data Center

Course Description:

Agility is the hallmark of today's successful data center. Built for rapid application deployment and supported by a highly elastic infrastructure, the data center has become core to businesses competing in our digital era. CCNA Data Center certification provides the confidence and nimbleness you need to install, configure, and maintain data center technology. Gain grounding in data center infrastructure, data center networking concepts and technologies, storage networking, unified computing, network virtualization, data center automation and orchestration, and Cisco Application Centric Infrastructure (ACI).

The Learning Center Model:



Our unique model follows a streamlined approach to workforce development and skills attainment:

Assess

Assess each individual and teams to determine existing skill sets

Educate

Deliver goal specific training utilizing all delivery modalities

Mentor

Expose students to instructor/mentors with front-line cyber/IT experience

Certify

Certify students with the requisite hands-on skills to perform the tasks related to their functional roles

Validate

Validate students “abilities” through performance analytics and real-world exercises hosted on a cyber range

OFFICIAL CYBERSECURITY TRAINING

The Learning Center Las Vegas

Demand for IT Professionals with Expertise in Data Center Infrastructure

Core to supporting new business models involving the Internet of Things (IoT), big data, and cloud, or to modernizing existing business-critical applications, is an enterprise-class data center. Agile delivery of business transformation initiatives relies on modern data center infrastructure.

In-demand IT professionals focused on data center requirements continue to be presented with an ever-increasing and evolving set of responsibilities. Cisco's certification and training program enables key skills needed for world-class data center operations, rapid application deployment and delivery of successful business outcomes.

Exams & Recommended Training

Required Exam(s)	Recommended Training
640-911 DCICN Last day to test: April 11, 2017 OR	Introducing Cisco Data Center Networking (DCICN) v1.0
200-150 DCICN	Introducing Cisco Data Center Networking (DCICN) v6.0
640-916 DCICT Last day to test: April 11, 2017 OR	Introducing Cisco Data Center Networking Technologies (DCICT) v1.0
200-155 DCICT	Introducing Cisco Data Center Networking Technologies (DCICT) v6.0

The certification prepares you for the following roles:

- Network Administrators
- Network Support Engineers
- Network Engineer Associate
- Network Specialist
- Network Analyst

WHY CHOOSE TLC?

The Learning Center, a division of The Learning Center, is an Official Training Partner of $(ISC)^2$., operating for 31 years in IT training and certification programs can offer you the best in education and training. TLC is an EC-Council Accredited Training Center. One of only 700 accredited training centers globally, TLC **is proud to be one of 15 global partners selected to deliver the C|CISO curriculum.**

Additionally, TLC in partnership with Merit.edu has partnered to deliver "world-class" training and education supported by use of the Michigan Cyber Range. This Cyber Range is the most state-of-the-art deliverable training method to ensure "skills set" learning by use of Alphaville, a virtual environment to practice and hone Cybersecurity skills. Students receive the official training, plus access to the Cyber Range. ***Click here for more***.

OFFICIAL CYBERSECURITY TRAINING

The Learning Center
Las Vegas

CISCO

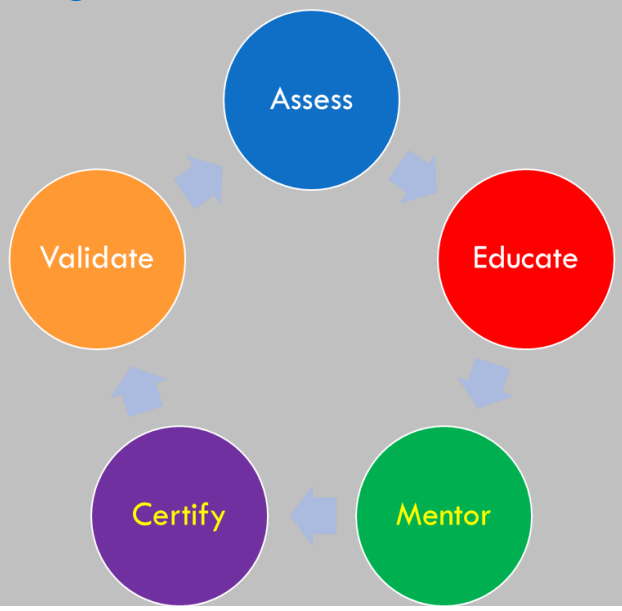
CCNA Cyber Ops

Course Description:

Today's organizations are challenged with rapidly detecting cybersecurity breaches and effectively responding to security incidents. Teams of people in Security Operations Centers (SOC's) keep a vigilant eye on security systems, protecting their organizations by detecting and responding to cybersecurity threats.

The CCNA Cyber Ops certification prepares candidates to begin a career working with associate-level cybersecurity analysts within security operations centers.

The Learning Center Model:



Our unique model follows a streamlined approach to workforce development and skills attainment:

Assess

Assess each individual and teams to determine existing skill sets

Educate

Deliver goal specific training utilizing all delivery modalities

Mentor

Expose students to instructor/mentors with front-line cyber/IT experience

Certify

Certify students with the requisite hands-on skills to perform the tasks related to their functional roles

Validate

Validate students "abilities" through performance analytics and real-world exercises hosted on a cyber range

OFFICIAL CYBERSECURITY TRAINING

The Learning Center
Las Vegas

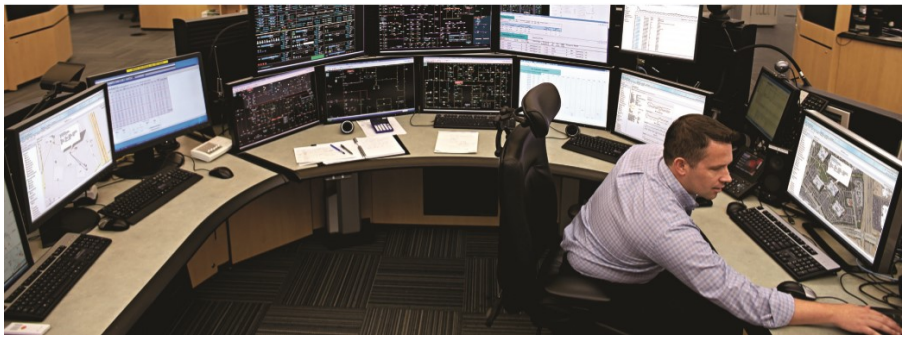
Increasing Demand for Practical Network Security Skills

Cisco has taken note of the evolution of the role of the network security professional and its relevance to the industry. The speed at which network security is evolving demands more practical, hands-on skills in network security engineering and has made network security performance more visible to the entire organization. Network security engineers in the marketplace today understand the products and the discipline of good network security, the practices and compliance mandates of industry and government, and the need to protect their organizations from increasingly sophisticated threats to their systems. Cisco network security engineers have real-world security implementation and troubleshooting skills.

Exams & Recommended Training

Required Exam(s)	Recommended Training
210-250 SECFND	Understanding Cisco Cybersecurity Fundamentals (SECFND)
210-255 SECOPS	Implementing Cisco Cybersecurity Operations (SECOPS)

NOTE: The training courses for the CCNA Cyber Ops Certification will be made available in March of 2017. Date is subject to change without notice.



WHY CHOOSE TLC?

The Learning Center, a division of The Learning Center, has operated for 31 years in IT training and certification field. TLC is an is an Official Training Partner of $(ISC)^2$, EC-Council Accredited Training Center, ISACA Approved Training Center and CompTIA Alliance member. One of two training organizations certified/approved by 4 out of the 5 global credentialing bodies, a unique distinction. ,

Additionally, TLC has partnered with Merit.edu to deliver "world-class" training and education supported by use of the Michigan Cyber Range. The Michigan Cyber Range is the most mature and robust deliverable training platform in the world today. This partnership enables TLC to uniquely deliver skills-based training, assessment, and certifications in alignment with the National Initiative for Cybersecurity Education (NICE) Framework. Our lab content and assessment services are a one-of-a-kind model for developing performance defined cybersecurity professionals capable of meeting current and future employer demand.

OFFICIAL CYBERSECURITY TRAINING

The Learning Center
Las Vegas

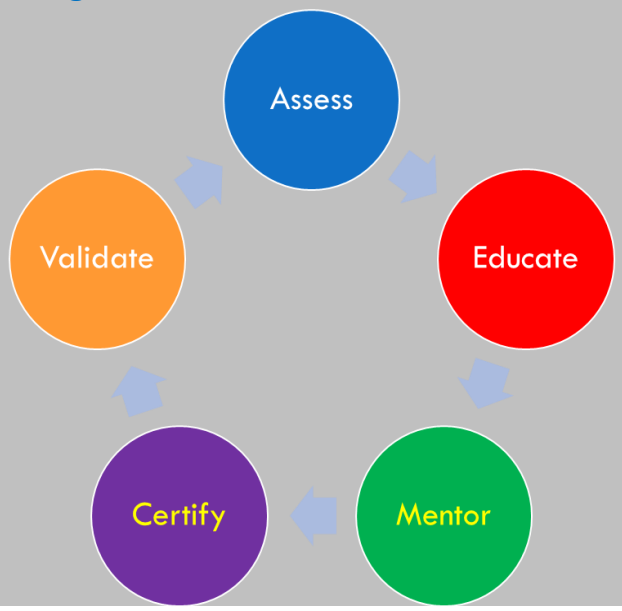
CISCO

CCNA CLOUD

Course Description:

Many companies are embracing the Cloud to help them to be more agile, flexible, and effective at delivering better business outcomes. Today, the majority of companies are already using XaaS offerings, and by 2018, it's estimated that 78% of workloads will be processed through the cloud. The CCNA Cloud certification is a job role focused certification and training program that helps Cloud engineers, Cloud Administrators, and Network Engineers to develop, advance, and validate their cloud skill set, and enables them to help their IT organization meet changing business demands. With a CCNA Cloud certification, you will obtain the skills to perform entry-level provisioning and support of Cisco cloud solutions. Learn from the only company that has an end-to-end Cloud and Intercloud story.

The Learning Center Model:



Our unique model follows a streamlined approach to workforce development and skills attainment:

Assess

Assess each individual and teams to determine existing skill sets

Educate

Deliver goal specific training utilizing all delivery modalities

Mentor

Expose students to instructor/mentors with front-line cyber/IT experience

Certify

Certify students with the requisite hands-on skills to perform the tasks related to their functional roles

Validate

Validate students "abilities" through performance analytics and real-world exercises hosted on a cyber range

OFFICIAL CYBERSECURITY TRAINING

The Learning Center
Las Vegas

The best way to prepare for this certification is to take the Cisco-approved training:

Understanding Cisco Cloud Fundamentals (CLDFND)

This course is designed to provide students with the necessary knowledge, skills and abilities to perform foundational tasks related to cloud computing. It will review cloud characteristics and deployment models and explore the cloud basic components which consist of compute, storage and networking.
» Learn More

Introducing Cisco Cloud Administration (CLDADM)

This course is designed to provide students with the necessary knowledge and skills to perform the essentials of cloud administration and operations.
» Learn More

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

- Identify the components of the Cisco Cloud management software solution
- Understand the fundamentals of Cloud infrastructure administration
- Describe reporting and charge-back
- Provision Clouds using pre-configured templates
- Perform Cloud management, monitoring and remediation

The certification prepares you for the following roles:

- Network Administrators
- Network Support Engineers
- Network Engineer Associate
- Network Specialist
- Network Analyst

WHY CHOOSE TLC?

The Learning Center, a division of The Learning Center, has operated for 31 years in IT training and certification field. TLC is an is an Official Training Partner of $(ISC)^2$, EC-Council Accredited Training Center, ISACA Approved Training Center and CompTIA Alliance member. One of two training organizations certified/approved by 4 out of the 5 global credentialing bodies, a unique distinction. ,

Additionally, TLC has partnered with Merit.edu to deliver “world-class” training and education supported by use of the Michigan Cyber Range. The Michigan Cyber Range is the most mature and robust deliverable training platform in the world today. This partnership enables TLC to uniquely deliver skills-based training, assessment, and certifications in alignment with the National Initiative for Cybersecurity Education (NICE) Framework. Our lab content and assessment services are a one-of-a-kind model for developing performance defined cybersecurity professionals capable of meeting current and future employer demand.

OFFICIAL CYBERSECURITY TRAINING

The Learning Center
Las Vegas

CISCO

CCNP Routing and Switching

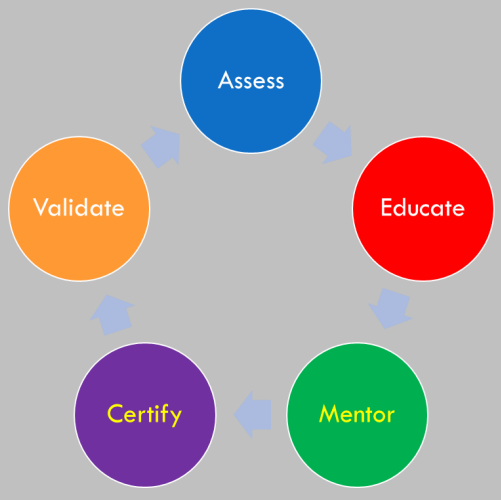
Course Description:

Routing and Switching

CCENT | CCNA | CCNP | CCIE

Cisco Certified Network Professional (CCNP) Routing and Switching certification validates the ability to plan, implement, verify and troubleshoot local and wide-area enterprise networks and work collaboratively with specialists on advanced security, voice, wireless and video solutions. The CCNP Routing and Switching certification is appropriate for those with at least one year of networking experience who are ready to advance their skills and work independently on complex network solutions. Those who achieve CCNP Routing and Switching have demonstrated the skills required in enterprise roles such as network engineer, support engineer, systems engineer or network technician. The routing and switching protocol knowledge from this certification will provide a lasting foundation as these skills are equally relevant in the physical networks of today and the virtualized network functions of tomorrow.

The Learning Center Model:



Our unique model follows a streamlined approach to work-force development and skills attainment:

Assess

Assess each individual and teams to determine existing skill sets

Educate

Deliver goal specific training utilizing all delivery modalities

Mentor

Expose students to instructor/mentors with front-line cyber/IT experience

Certify

Certify students with the requisite hands-on skills to perform the tasks related to their functional roles

Validate

Validate students “abilities” through performance analytics and real-world exercises hosted on a cyber range

OFFICIAL CYBERSECURITY TRAINING

The Learning Center Las Vegas

The best way to prepare for this certification is to take the Cisco-approved training:

Implementing Cisco IP Routing (ROUTE)

Students will learn to plan, configure and verify the implementation of secure enterprise LAN and WAN routing solutions using a range of routing protocols.
» Learn More

Implementing Cisco IP Switched Networks (SWITCH)

Students will learn to plan, configure and verify the implementation of complex enterprise switching solutions using Cisco's Campus Enterprise Architecture.
» Learn More

Troubleshooting and Maintaining Cisco IP Networks (TSHOOT)

Students will learn to (1) plan and perform regular maintenance on complex enterprise routed and switched networks and (2) use technology-based practices and a systematic ITIL-compliant approach to perform network troubleshooting.

Exams & Recommended Training

Required Exam(s)	Recommended Training
300-101 ROUTE	Implementing Cisco IP Routing (ROUTE)
300-115 SWITCH	Implementing Cisco IP Switched Networks (SWITCH)
300-135 TSHOOT	Troubleshooting and Maintaining Cisco IP Networks (TSHOOT)

WHY CHOOSE TLC?

The Learning Center, a division of The Learning Center, has operated for 31 years in IT training and certification field. TLC is an is an Official Training Partner of (ISC)^2, EC-Council Accredited Training Center, ISACA Approved Training Center and CompTIA Alliance member. One of two training organizations certified/approved by 4 out of the 5 global credentialing bodies, a unique distinction. ,

Additionally, TLC has partnered with Merit.edu to deliver "world-class" training and education supported by use of the Michigan Cyber Range. The Michigan Cyber Range is the most mature and robust deliverable training platform in the world today. This partnership enables TLC to uniquely deliver skills-based training, assessment, and certifications in alignment with the National Initiative for Cybersecurity Education (NICE) Framework. Our lab content and assessment services are a one-of-a-kind model for developing performance defined cybersecurity professionals capable of meeting current and future employer demand.

OFFICIAL CYBERSECURITY TRAINING

The Learning Center
Las Vegas

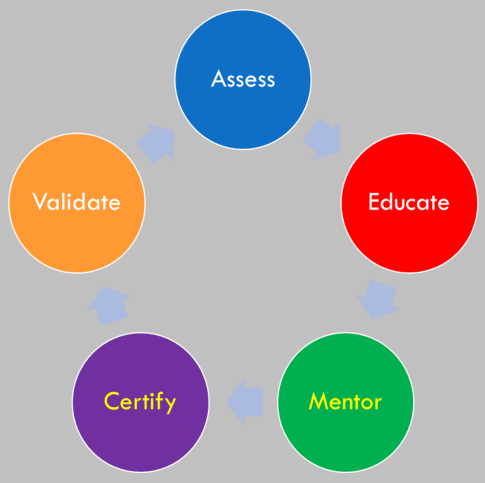
cisco

CCNP Collaboration

Course Description:

For collaboration and unified communications network engineers who want develop advanced collaboration skills designing, deploying, configuring, and troubleshooting Cisco Collaboration and Unified communications applications, devices and networks, the Cisco CCNP Collaboration certification is a job-role focused training and certification program that will expand your skills and ability to deliver business value. Collaboration is becoming a critical necessity for business success and innovation. You can use your knowledge to lead the transformation and increase the effectiveness of your organizations collaboration experience.

The Learning Center Model:



Our unique model follows a streamlined approach to work-force development and skills attainment:

Assess

Assess each individual and teams to determine existing skill sets

Educate

Deliver goal specific training utilizing all delivery modalities

Mentor

Expose students to instructor/mentors with front-line cyber/IT experience

Certify

Certify students with the requisite hands-on skills to perform the tasks related to their functional roles

Validate

Validate students “abilities” through performance analytics and real-world exercises hosted on a cyber range

OFFICIAL CYBERSECURITY TRAINING

The Learning Center Las Vegas

Implementing Cisco IP Telephony & Video, Part 1 (CIPTV1)

This exam tests a candidate's knowledge of implementing a Cisco Unified Collaboration solution in a single-site environment. Candidates will need to show they can configure Cisco Unified Communications Manager, implement gateways and Cisco Unified Border Element, and build dial plans to place on-net and off-net voice and video calls.

» Learn More

Implementing Cisco IP Telephony & Video, Part 2 (CIPTV2)

This exam tests a candidate's knowledge of Cisco Unified Collaboration solutions in a multi-site environment. They will need to be able to describe the role of Cisco Video Communication Server (VCS) Control and the Cisco Expressway Series and how they interact with Cisco Unified Communications Manager.

» Learn More

Troubleshooting Cisco IP Telephony & Video (CTCOLLAB)

This exam assesses a candidate's knowledge and skills to be able to troubleshoot a Cisco Unified Collaboration solution. The exam also covers troubleshooting methodology, triage, resources, and tools.

» Learn More

Implementing Cisco Collaboration Applications (CAPPS)

This exam tests candidates on the integration options of Cisco Unified IM and Presence, Cisco Unity Express, Cisco Unity Connection, Cisco Prime Collaboration, and Cisco TelePresence Management Suite in a Cisco Unified Collaboration solution.

» Learn More

Exams & Recommended Training

Required Exam(s)	Recommended Training
300-070 CIPTV1	Implementing Cisco IP Telephony and Video, Part 1 (CIPTV1)
300-075 CIPTV2	Implementing Cisco IP Telephony and Video, Part 2 (CIPTV2)
300-080 CTCOLLAB	Troubleshooting Cisco IP Telephony and Video (CTCOLLAB)
300-085 CAPPS	Implementing Cisco Collaboration Applications (CAPPS)

NOTE: Other CCNP Voice certification exams can be applied towards the CCNP Collaboration certification.

WHY CHOOSE TLC?

The Learning Center, a division of The Learning Center, has operated for 31 years in IT training and certification field. TLC is an is an Official Training Partner of $(ISC)^2$, EC-Council Accredited Training Center, ISACA Approved Training Center and CompTIA Alliance member. One of two training organizations certified/approved by 4 out of the 5 global credentialing bodies, a unique distinction. ,

Additionally, TLC has partnered with Merit.edu to deliver "world-class" training and education supported by use of the Michigan Cyber Range. The Michigan Cyber Range is the most mature and robust deliverable training platform in the world today. This partnership enables TLC to uniquely deliver skills-based training, assessment, and certifications in alignment with the National Initiative for Cybersecurity Education (NICE) Framework. Our lab content and assessment services are a one-of-a-kind model for developing performance defined cybersecurity professionals capable of meeting current and future employer demand.

OFFICIAL CYBERSECURITY TRAINING

The Learning Center
Las Vegas

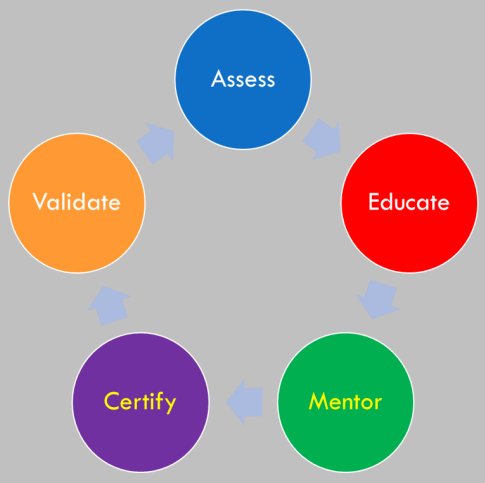
CISCO

CCNP Security

Course Description:

Cisco Certified Network Professional Security (CCNP Security) certification program is aligned specifically to the job role of the Cisco Network Security Engineer responsible for Security in Routers, Switches, Networking devices and appliances, as well as choosing, deploying, supporting and troubleshooting Firewalls, VPNS, and IDS/IPS solutions for their networking environments.

The Learning Center Model:



Our unique model follows a streamlined approach to work-force development and skills attainment:

Assess

Assess each individual and teams to determine existing skill sets

Educate

Deliver goal specific training utilizing all delivery modalities

Mentor

Expose students to instructor/mentors with front-line cyber/IT experience

Certify

Certify students with the requisite hands-on skills to perform the tasks related to their functional roles

Validate

Validate students “abilities” through performance analytics and real-world exercises hosted on a cyber range

OFFICIAL CYBERSECURITY TRAINING

The Learning Center Las Vegas

The best way to prepare for this certification is to take the Cisco-approved training:

Implementing Cisco Secure Access Solutions (SISAS)

This five-day course prepares network security engineers with the skills and knowledge needed to deploy the Cisco Identity Services Engine (ISE) and 802.1X secure network access and to implement and manage network access security by using the Cisco ISE appliance product solution.

» Learn More

AND

Implementing Cisco Edge Network Security Solutions (SENSS)

This five-day course prepares network security engineers with the skills and knowledge needed to configure Cisco perimeter edge security solutions utilizing Cisco switches, Cisco routers, and Cisco Adaptive Security Appliance (ASA) firewalls and to implement and manage security on Cisco ASA firewalls, Cisco routers with the firewall feature set, and Cisco switches.

» Learn More

AND

Implementing Cisco Secure Mobility Solutions (SIMOS)

This five-day course prepares network security engineers with the knowledge and skills needed to protect data traversing a public or shared infrastructure such as the Internet by implementing and maintaining Cisco VPN solutions and troubleshooting remote-access and site-to-site VPN solutions, using Cisco ASA adaptive security appliances and Cisco IOS routers.

» Learn More

AND

Implementing Cisco Threat Control Solutions (SITCS) v1.0

This five-day course prepares network security engineers with the knowledge and skills needed to deploy the Cisco ASA Next-Generation Firewall (NGFW), as well as web security, email security, and cloud web security, and with the capability to implement and manage security on Cisco ASA firewalls utilizing the Cisco Next-Generation product solution.

» Learn More

Exams & Recommended Training

Required Exam(s)	Recommended Training
300-208 SISAS	Implementing Cisco Secure Access Solutions (SISAS)
300-206 SENSS	Implementing Cisco Edge Network Security Solutions (SENSS)
300-209 SIMOS	Implementing Cisco Secure Mobility Solutions (SIMOS)
300-207 SITCS v1.0 Last day to test: March 31, 2017 OR	Implementing Cisco Threat Control Solutions (SITCS)
300-210 SITCS v1.5	Implementing Cisco Threat Control Solutions (SITCS)

WHY CHOOSE TLC?

The Learning Center, a division of The Learning Center, has operated for 31 years in IT training and certification field. TLC is an is an Official Training Partner of $(ISC)^2$, EC-Council Accredited Training Center, ISACA Approved Training Center and CompTIA Alliance member. One of two training organizations certified/approved by 4 out of the 5 global credentialing bodies, a unique distinction. ,

Additionally, TLC has partnered with Merit.edu to deliver “world-class” training and education supported by use of the Michigan Cyber Range. The Michigan Cyber Range is the most mature and robust deliverable training platform in the world today. This partnership enables TLC to uniquely deliver skills-based training, assessment, and certifications in alignment with the National Initiative for Cybersecurity Education (NICE) Framework. Our lab content and assessment services are a one-of-a-kind model for developing performance defined cybersecurity professionals capable of meeting current and future employer demand.

OFFICIAL CYBERSECURITY TRAINING

The Learning Center
Las Vegas

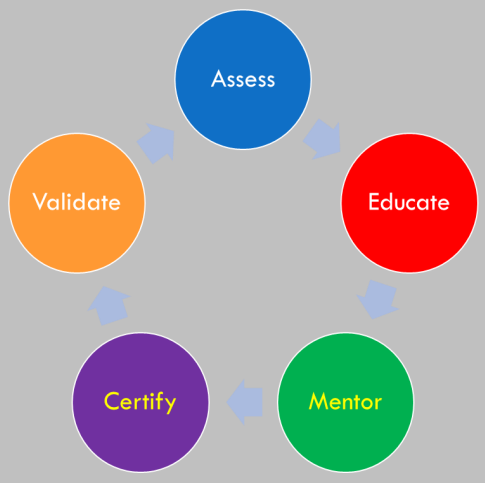
CISCO

CCNP Data Center

Course Description:

The CCNP Data Center certification and training program offers comprehensive certification and Professional-level skills focused on the data center solutions, technologies and best practices to design, implement, and manage a modern data center infrastructure. IT practitioners who are Cisco trained and certified are uniquely qualified for key roles in complex data center environments, with expertise utilizing technologies including policy-driven infrastructure, professionals are highly virtualization, automation and orchestration, unified computing, data center security, and integration of cloud initiatives. CCNP Data Center certified qualified for senior roles chartered with enabling digital business transformation initiatives.

The Learning Center Model:



Our unique model follows a streamlined approach to workforce development and skills attainment:

Assess

Assess each individual and teams to determine existing skill sets

Educate

Deliver goal specific training utilizing all delivery modalities

Mentor

Expose students to instructor/mentors with front-line cyber/IT experience

Certify

Certify students with the requisite hands-on skills to perform the tasks related to their functional roles

Validate

Validate students “abilities” through performance analytics and real-world exercises hosted on a cyber range

OFFICIAL CYBERSECURITY TRAINING

The best way to prepare for this certification is to take the Cisco-approved training:

Implementing Cisco Data Center Unified Computing (DCUCI) v5.0
This course is designed to serve the needs of engineers and technicians who implement Cisco Unified Computing System (UCS) B-Series Blade Servers and Cisco UCS C-Series Rack-Mount Servers.
» Learn More

Implementing Cisco Data Center Unified Fabric (DCUFI) v5.0
This course covers the key components and procedures needed to install, configure, manage and troubleshoot the Cisco Nexus 7000 and 5000 switch in the network and SAN environment.
» Learn More

Designing Cisco Data Center Unified Computing (DCUCD) v5.0
This course covers data center unified computing and virtualization solutions. It explains how to evaluate existing data center computing solution, determine the requirements, and design Cisco data center unified computing solution.
» Learn More

Designing Cisco Data Center Unified Fabric (DCUFD) v5.0
This course enables engineers to choose and design scalable, reliable, and intelligent data center networks.
» Learn More

Troubleshooting Cisco Data Center Unified Computing (DCUCT) v5.0
This course prepares system engineers and implementers with the knowledge and hands-on experience to troubleshoot Cisco UCS B-Series and C-Series servers operating in standalone and integrated modes.
» Learn More

Troubleshooting Cisco Data Center Unified Fabric (DCUFT) v5.0
This course covers how to install, implement, maintain and troubleshoot the Cisco Nexus 7000 Series Switches, the Cisco Nexus 5000 Series Switches, the Cisco Nexus 2000 Fabric Extenders, and the Cisco MDS Series Multilayer Fabric Switches.
» Learn More

Exams & Recommended Training

Required Exam(s)	Recommended Training
642-999 DCUCI Last day to test: July 3, 2017	Implementing Cisco Data Center Unified Computing (DCUCI) v5.0
OR	
300-175 DCUCI	Implementing Cisco Data Center Unified Computing (DCUCI) v6.0
AND	
642-997 DCUFI Last day to test: July 3, 2017	Implementing Cisco Data Center Unified Fabric (DCUFI) v5.0
OR	
300-165 DCII	Implementing Cisco Data Center Infrastructure (DCII) v6.0
AND	
300-170 DCVAI	Implementing Cisco Data Center Virtualization and Automation (DCVAI) v6.0

The Learning Center Las Vegas

Implementing Cisco Data Center Unified Computing (DCUCI) v6.0
The focus of this course is on deploying, securing, operating, and maintaining the Cisco Unified Computing System (UCS) and UCS C-Series Rack Servers fo use in data centers.
» Learn More

Implementing Cisco Data Center Infrastructure (DCII) v6.0
The focus of this course is implementation of LAN, SAN, and Data Center Unified Fabric. The course provides hands-on experience implementing Cisco data center infrastructure.
» Learn More

Implementing Cisco Data Center Virtualization and Automation (DCVAI) v6.0
This course focuses on the implementation and deployment automation of Cisc Application Centric Infrastructure (ACI) and Cisco Nexus switches. It provides rich, hands-on experience building a data center solution.
» Learn More

Designing Cisco Data Center Infrastructure (DCID) v6.0
The focus of this course is data center design based on Cisco solutions. The course includes theoretical content, as well as design-oriented case studies.
» Learn More

Troubleshooting Cisco Data Center Infrastructure (DCIT) v6.0
The focus of this course is troubleshooting of LAN, SAN, Cisco Data Center Unified Fabric, Cisco Unified Computing System (UCS), and Cisco Application Centric Infrastructure (ACI).
» Learn More

AND	
642-998 DCUCD Last day to test: July 3, 2017 AND	Designing Cisco Data Center Unified Computing (DCUCD) v5.0
642-996 DCUFD Last day to test: July 3, 2017	Designing Cisco Data Center Unified Fabric (DCUFD) v5.0
OR	
300-160 DCID	Designing Cisco Data Center Infrastructure (DCID) v6.0
OR	
642-035 DCUCT Last day to test: July 3, 2017 AND	Troubleshooting Cisco Data Center Unified Computing (DCUCT)
642-980 DCUFT Last day to test: July 3, 2017	Troubleshooting Cisco Data Center Unified Fabric (DCUFT)
OR	
300-180 DCIT	Troubleshooting Cisco Data Center Infrastructure (DCIT) v6.0

OFFICIAL CYBERSECURITY TRAINING

The Learning Center
Las Vegas

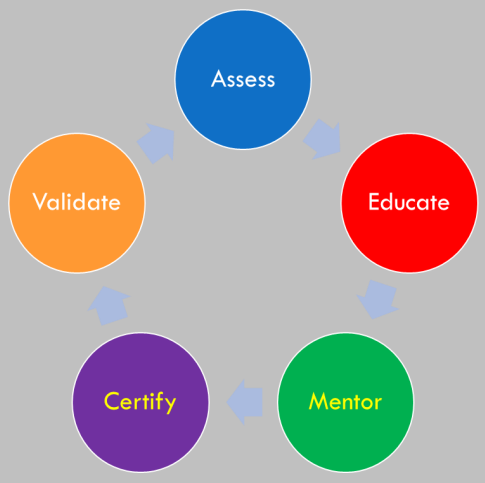
CISCO

CCNP Cloud

Course Description:

Cloud adoption is driving new roles and responsibilities. Cloud engineers need the skills to work with private, public and hybrid cloud models, and leverage Intercloud solutions. The CCNP Cloud certification is a lab based training and certification program that is targeted at Cloud engineers, Cloud Administrators, Cloud Designers, and Architects working in Data Centers. This program delivers the knowledge and skills necessary to design, provision, automate and manage Cloud and Infrastructure-as-a-Service deployments. Learn from the only company that has an end-to-end Cloud and Intercloud story.

The Learning Center Model:



Our unique model follows a streamlined approach to workforce development and skills attainment:

Assess

Assess each individual and teams to determine existing skill sets

Educate

Deliver goal specific training utilizing all delivery modalities

Mentor

Expose students to instructor/mentors with front-line cyber/IT experience

Certify

Certify students with the requisite hands-on skills to perform the tasks related to their functional roles

Validate

Validate students “abilities” through performance analytics and real-world exercises hosted on a cyber range

OFFICIAL CYBERSECURITY TRAINING

The Learning Center
Las Vegas

The best way to prepare for this certification is to take the Cisco-approved training.

Implementing and Troubleshooting the Cisco Cloud Infrastructure (CLDINF)

This course enables cloud support engineers to successfully build, maintain and troubleshoot cloud infrastructure at a cloud service provider.

» Learn More

Designing the Cisco Cloud (CLDDES)

This course is designed to provide students with the necessary knowledge and hands-on skills to design cloud deployments using the Cisco Cloud portfolio.

» Learn More

Automating the Cisco Enterprise Cloud (CLDAUT)

This course provides network professional with the process knowledge of automating and managing private and hybrid clouds using the processes, applications and products of the Cisco ONE Enterprise Cloud Suite.

» Learn More

Building the Cisco Cloud with Application Centric Infrastructure (CLDACI)

This course extensively covers the process of implementing public, private, and hybrid cloud based on Cisco ACI.

» Learn More

Exams & Recommended Training

Required Exam(s)	Recommended Training
300-460 CLDINF	Implementing and Troubleshooting the Cisco Cloud Infrastructure (CLDINF)
300-465 CLDDES	Designing the Cisco Cloud (CLDDES)
300-470 CLDAUT	Automating the Cisco Enterprise Cloud (CLDAUT)
300-475 CLDACI	Building the Cisco Cloud with Application Centric Infrastructure (CLDACI)

WHY CHOOSE TLC?

The Learning Center, a division of The Learning Center, has operated for 31 years in IT training and certification field. TLC is an is an Official Training Partner of $(ISC)^2$, EC-Council Accredited Training Center, ISACA Approved Training Center and CompTIA Alliance member. One of two training organizations certified/approved by 4 out of the 5 global credentialing bodies, a unique distinction. ,

Additionally, TLC has partnered with Merit.edu to deliver “world-class” training and education supported by use of the Michigan Cyber Range. The Michigan Cyber Range is the most mature and robust deliverable training platform in the world today. This partnership enables TLC to uniquely deliver skills-based training, assessment, and certifications in alignment with the National Initiative for Cybersecurity Education (NICE) Framework. Our lab content and assessment services are a one-of-a-kind model for developing performance defined cybersecurity professionals capable of meeting current and future employer demand.

OFFICIAL CYBERSECURITY TRAINING

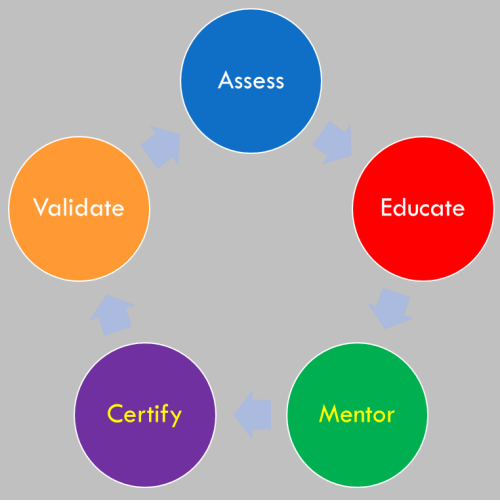
The Learning Center Las Vegas

CCNP Service Provider

Course Description:

The Cisco Certified Network Professional Service Provider (CCNP Service Provider) certification is for service provider network engineers, systems engineers, and network specialists who are responsible for delivering a scalable carrier-grade infrastructure capable of rapid expansion to support ongoing introduction of new managed services and other customer requirements.

The Learning Center Model:



Our unique model follows a streamlined approach to workforce development and skills attainment:

Assess

Assess each individual and teams to determine existing skill sets

Educate

Deliver goal specific training utilizing all delivery modalities

Mentor

Expose students to instructor/mentors with front-line cyber/IT experience

Certify

Certify students with the requisite hands-on skills to perform the tasks related to their functional roles

Validate

Validate students “abilities” through performance analytics and real-world exercises hosted on a cyber range

OFFICIAL CYBERSECURITY TRAINING

The Learning Center Las Vegas

The best way to prepare for this certification is to take the Cisco-approved training:

Deploying Cisco Service Provider Network Routing (SPROUTE)
This instructor-led course will prepare students for the SPROUTE exam required for the new CCNP-SP certification.
» Learn More

Deploying Cisco Service Provider Advanced Routing (SPADVROUTE)
This instructor-led course will prepare students for the SPADVROUTE exam required for the new CCNP-SP certification.
» Learn More

Implementing Cisco Service Provider Next-Generation Core Network Services (SPCORE)
This instructor-led course will prepare students for the SPCORE exam required for the new CCNP-SP certification.
» Learn More

Implementing Cisco Service Provider Next-Generation Edge Network Services (SPEDGE)
This instructor-led course will prepare students for the SPEDGE exam required for the new CCNP-SP certification.
» Learn More

Exams & Recommended Training

Required Exam(s)	Recommended Training
642-883 SPROUTE	Deploying Cisco Service Provider Network Routing (SPROUTE)
642-885 SPADVROUTE	Deploying Cisco Service Provider Advanced Routin((SPADVROUTE)
642-887 SPCORE	Implementing Cisco Service Provider Next-Generation Core Network Services (SPCORE)
642-889 SPEDGE	Implementing Cisco Service Provider Next-Generation Edge Network Services (SPEDGE)

WHY CHOOSE TLC?

The Learning Center, a division of The Learning Center, has operated for 31 years in IT training and certification field. TLC is an is an Official Training Partner of $(ISC)^2$, EC-Council Accredited Training Center, ISACA Approved Training Center and CompTIA Alliance member. One of two training organizations certified/approved by 4 out of the 5 global credentialing bodies, a unique distinction. ,

Additionally, TLC has partnered with Merit.edu to deliver “world-class” training and education supported by use of the Michigan Cyber Range. The Michigan Cyber Range is the most mature and robust deliverable training platform in the world today. This partnership enables TLC to uniquely deliver skills-based training, assessment, and certifications in alignment with the National Initiative for Cybersecurity Education (NICE) Framework. Our lab content and assessment services are a one-of-a-kind model for developing performance defined cybersecurity professionals capable of meeting current and future employer demand.

OFFICIAL CYBERSECURITY TRAINING

The Learning Center Las Vegas

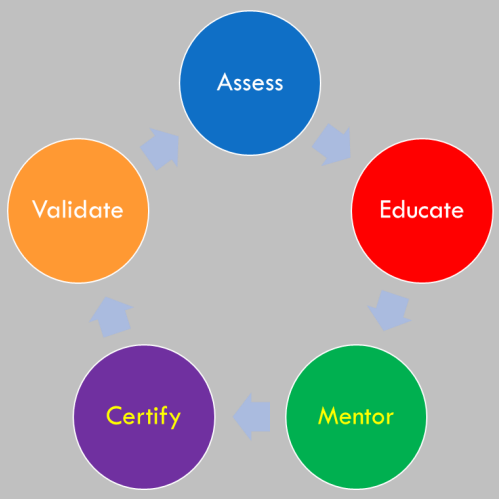
cisco

CCDA Design Associate

Course Description:

Enterprise environments require networks designed for performance, availability, and scalability with the flexibility to meet rapidly evolving demands. To meet these challenges head on, skilled IT professionals are needed with up-to-date, fundamental network design skills. For network design engineers, system engineers, and sales engineers and individuals looking to build and validate Cisco network design fundamental knowledge the Cisco CCDA certification program focuses on design methodologies and objectives, addressing and routing protocols, and network expansion considerations within basic campus, data center, security, voice, and wireless networks.

The Learning Center Model:



Our unique model follows a streamlined approach to workforce development and skills attainment:

Assess

Assess each individual and teams to determine existing skill sets

Educate

Deliver goal specific training utilizing all delivery modalities

Mentor

Expose students to instructor/mentors with front-line cyber/IT experience

Certify

Certify students with the requisite hands-on skills to perform the tasks related to their functional roles

Validate

Validate students “abilities” through performance analytics and real-world exercises hosted on a cyber range

OFFICIAL CYBERSECURITY TRAINING

The Learning Center Las Vegas

The best way to prepare for this certification is to take the Cisco-approved training:

Designing for Cisco Internetwork Solutions (DESGN) v3.0

Designing for Cisco Internetwork Solutions (DESGN) v3.0 course presents a structured and modular approach to designing networks that are scalable, resilient, and have well-defined failure domains. Course discusses routing and switching design of Campus and Enterprise networks in detail. Data center, wireless networking, and real-time traffic infrastructure are introduced and their effects on the core network are discussed from the design perspective.

How You Benefit

- **Drive business outcomes and innovation** by enabling the breadth of Enterprise network capabilities
- **Optimize Enterprise network performance** by gaining Cisco network design expertise to ensure availability, flexibility, and scalability
- **Scale expertise** by building and validating network design skills from entry to architect levels
- **Earn** global recognition from an industry leader for your accomplishments

CCDA Exams & Recommended Training

Required Exam(s)	Recommended Training
200-310 DESGN	Designing for Cisco Internetwork Solutions (DESGN) v3.0

WHY CHOOSE TLC?

The Learning Center, a division of The Learning Center, has operated for 31 years in IT training and certification field. TLC is an is an Official Training Partner of $(ISC)^2$, EC-Council Accredited Training Center, ISACA Approved Training Center and CompTIA Alliance member. One of two training organizations certified/approved by 4 out of the 5 global credentialing bodies, a unique distinction. ,

Additionally, TLC has partnered with Merit.edu to deliver “world-class” training and education supported by use of the Michigan Cyber Range. The Michigan Cyber Range is the most mature and robust deliverable training platform in the world today. This partnership enables TLC to uniquely deliver skills-based training, assessment, and certifications in alignment with the National Initiative for Cybersecurity Education (NICE) Framework. Our lab content and assessment services are a one-of-a-kind model for developing performance defined cybersecurity professionals capable of meeting current and future employer demand.

OFFICIAL CYBERSECURITY TRAINING

The Learning Center
Las Vegas

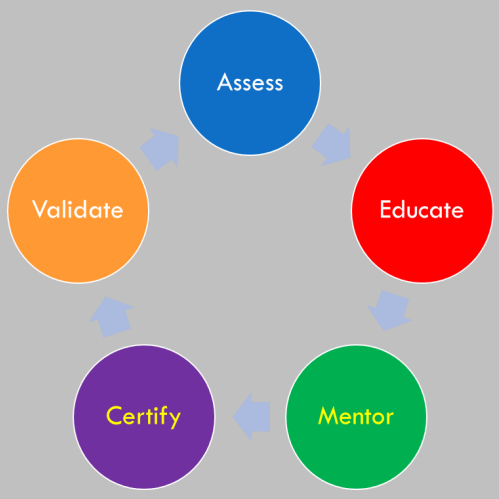
CISCO

CCDP Design Professional

Course Description:

Enterprise environments require networks designed for performance, availability and scalability to achieve outcomes. Seasoned IT professionals with progressive end-to-end network design expertise are crucial to ensure networks deliver to today's requirements while future proofing investments. For Senior Network Design Engineers, Principle System Engineer, Network/Solution Architects and CCDA professionals looking to build upon your fundamental Cisco network design expertise the Cisco CCDP certification program focuses on advanced addressing and routing protocols, WANs, services virtualization, and integration strategies for multi-layered Enterprise architectures.

The Learning Center Model:



Our unique model follows a streamlined approach to workforce development and skills attainment:

Assess

Assess each individual and teams to determine existing skill sets

Educate

Deliver goal specific training utilizing all delivery modalities

Mentor

Expose students to instructor/mentors with front-line cyber/IT experience

Certify

Certify students with the requisite hands-on skills to perform the tasks related to their functional roles

Validate

Validate students “abilities” through performance analytics and real-world exercises hosted on a cyber range

OFFICIAL CYBERSECURITY TRAINING

The Learning Center Las Vegas

The best way to prepare for this certification is to take the Cisco-approved training:

Implementing Cisco IP Routing (ROUTE)

Students will learn to plan, configure and verify the implementation of secure enterprise LAN and WAN routing solutions using a range of routing protocols.
» Learn More

Implementing Cisco IP Switched Networks (SWITCH)

Students will learn to plan, configure and verify the implementation of complex enterprise switching solutions using Cisco's Campus Enterprise Architecture.
» Learn More

Designing Cisco Network Service Architectures (ARCH)

The aim of the course is to enable learners to perform the conceptual, intermediate, and detailed design of a network infrastructure that supports desired network solutions over intelligent network services, in order to achieve effective performance, scalability, and availability.

Exams & Recommended Training

Required Exam(s)	Recommended Training
300-101 ROUTE	Implementing Cisco IP Routing (ROUTE)
300-115 SWITCH	Implementing Cisco IP Switched Networks (SWITCH)
300-320 ARCH	Designing Cisco Network Service Architectures (ARCH)

WHY CHOOSE TLC?

The Learning Center, a division of The Learning Center, has operated for 31 years in IT training and certification field. TLC is an is an Official Training Partner of $(ISC)^2$, EC-Council Accredited Training Center, ISACA Approved Training Center and CompTIA Alliance member. One of two training organizations certified/approved by 4 out of the 5 global credentialing bodies, a unique distinction. ,

Additionally, TLC has partnered with Merit.edu to deliver "world-class" training and education supported by use of the Michigan Cyber Range. The Michigan Cyber Range is the most mature and robust deliverable training platform in the world today. This partnership enables TLC to uniquely deliver skills-based training, assessment, and certifications in alignment with the National Initiative for Cybersecurity Education (NICE) Framework. Our lab content and assessment services are a one-of-a-kind model for developing performance defined cybersecurity professionals capable of meeting current and future employer demand.

OFFICIAL CYBERSECURITY TRAINING

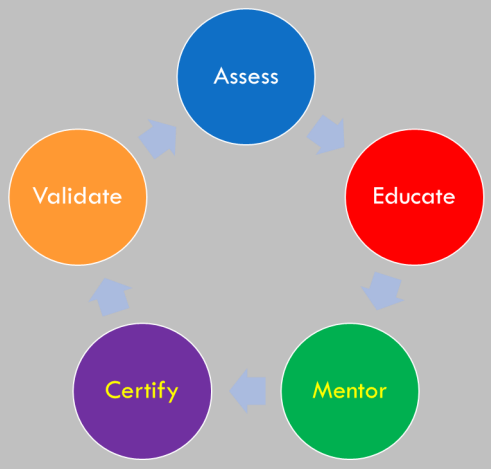
The Learning Center Las Vegas

CCSK Certificate of Cloud Security Knowledge

Cloud Computing Security Knowledge

Course Description: The CCSK - Foundation course is based on V3.0 of the CCSK exam and the CSA Security Guidance for Critical Areas of Cloud Computing V3.0. The Cloud Computing Security Knowledge- Foundation class provides students a comprehensive one day review of cloud security fundamentals and prepares them to take the Cloud Security Alliance CCSK v3.0 certificate exam. Starting with a detailed description of cloud computing, the course covers all major domains in the Guidance v3.0 document from the Cloud Security Alliance, and the recommendations from the European Network and Information Security Agency (ENISA). This class is geared towards security professionals, but is also useful for anyone looking to expand their knowledge of cloud security. (We recommend attendees have at least a basic understanding of security fundamentals, such as firewalls, secure development, encryption, and identity management).

The Learning Center Model:



Our unique model follows a streamlined approach to workforce development and skills attainment:

Assess

Assess each individual and teams to determine existing skill sets

Educate

Deliver goal specific training utilizing all delivery modalities

Mentor

Expose students to instructor/mentors with front-line cyber/IT experience

Certify

Certify students with the requisite hands-on skills to perform the tasks related to their functional roles

Validate

Validate students “abilities” through performance analytics and real-world exercises hosted on a cyber range

OFFICIAL CYBERSECURITY TRAINING

The Learning Center
Las Vegas

As cloud computing shows itself to be the future of information technology, several studies have pointed to the necessity of addressing the IT industry's skills gap and training professionals in both cloud computing and security. Since Cloud Security Alliance first released the Certificate of Cloud Security Knowledge (CCSK) in 2010, thousands of IT and security professionals have taken

- Cloud Architecture
- Governance and Enterprise Risk
- Legal and Electronic Discovery
- Compliance and Audit
- Information Lifecycle Management
- Portability and Interoperability
- Traditional Security, BCM, D/R
- Data Center Operations
- Incident Response
- Application Security
- Encryption and Key Management
- Identity and Access Management
- Virtualization
- Security-as-a-Service
- ENISA Document

CCSK
Certificate of
Cloud Security Knowledge

WHY CHOOSE TLC?

The Learning Center, a division of The Learning Center, has operated for 31 years in IT training and certification field. TLC is an is an Official Training Partner of $(ISC)^2$, EC-Council Accredited Training Center, ISACA Approved Training Center and CompTIA Alliance member. One of two training organizations certified/approved by 4 out of the 5 global credentialing bodies, a unique distinction. ,

Additionally, TLC has partnered with Merit.edu to deliver "world-class" training and education supported by use of the Michigan Cyber Range. The Michigan Cyber Range is the most mature and robust deliverable training platform in the world today. This partnership enables TLC to uniquely deliver skills-based training, assessment, and certifications in alignment with the National Initiative for Cybersecurity Education (NICE) Framework. Our lab content and assessment services are a one-of-a-kind model for developing performance defined cybersecurity professionals capable of meeting current and future employer demand.

OFFICIAL CYBERSECURITY TRAINING

The Learning Center Las Vegas

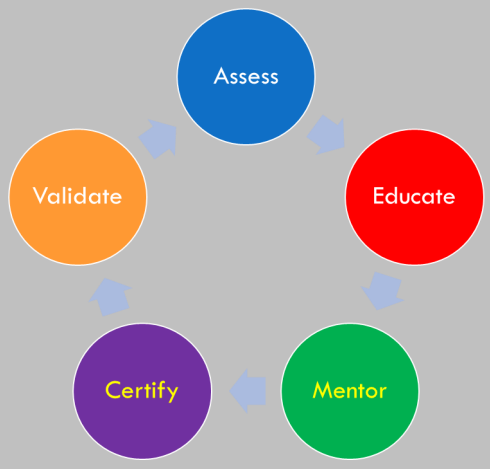
Project Management Institute

Certified Associate in Project Mgmt

Course Description:

Regardless of your career stage, the Certified Associate in Project Management (CAPM)® is an asset that will distinguish you in the job market and enhance your credibility and effectiveness working on — or with — project teams. Organizations with standardized practices attain better results, as shown in our 2015 Pulse of the Profession® report. Because the CAPM® recognizes your knowledge of the profession's preeminent global standard, you'll stand out to employers and be poised to move ahead. Project management is a rapidly growing profession. Through 2020, 1.57 million new jobs will be created each year and qualified practitioners are in demand. With the CAPM, you'll be on the fast track to opportunity.Employers benefit as well. When more than one-third of their project managers are PMP-certified, organizations complete more of their projects on time, on budget and meeting original goals. (Pulse of the Profession® study, PMI, 2015.)

The Learning Center Model:



Our unique model follows a streamlined approach to workforce development and skills attainment:

Assess

Assess each individual and teams to determine existing skill sets

Educate

Deliver goal specific training utilizing all delivery modalities

Mentor

Expose students to instructor/mentors with front-line cyber/IT experience

Certify

Certify students with the requisite hands-on skills to perform the tasks related to their functional roles

Validate

Validate students "abilities" through performance analytics and real-world exercises hosted on a cyber range

OFFICIAL CYBERSECURITY TRAINING

The Learning Center
Las Vegas

CAPM Exam Content Outline
Project Management and Processes in Context (15%)
Understand/recognize project management terminology, process groups, and knowledge areas
Understand the relationships between process groups and knowledge areas
Recognize where outputs from one process become inputs into another
Recognize that the same techniques and tools are used in several places
Project Integration Management (12%)
Define the six processes typically associated with integration management
Identify and describe the ITTOs associated with those six processes
Describe the uses and components of a project management plan
Describe the purpose of, and procedures related to, project change management
Project Scope Management (11%)
Define the six processes typically associated with project scope management
Identify and describe the ITTOs associated with those six processes
Describe the purpose and elements of a Work Breakdown Structure (WBS)
Describe the purpose and elements of a requirements document
Project Time Management (12%)
Define the seven processes typically associated with project time management
Identify and describe the ITTOs associated with those seven processes
Perform simple calculation of activity estimates
Describe the purpose and procedures related to sequencing activities
Interpret various types of network diagrams to identify critical path activities
Project Cost Management (7%)
Define the four processes typically associated with project cost management
Identify and describe the ITTOs associated with those four processes
Understand the concept of Earned Value Management (EVM)
Project Quality Management (6%)
Define the three processes typically associated with project quality management
Identify and describe the ITTOs associated with those three processes
Identify and know when to use quality tools and quality control tools
Apply quality tools to simple scenarios to identify issues, root causes, trends, and/or problems

CAPM Exam Content Outline
Project Human Resource Management (8%)
Define the four processes typically associated with project human resource management
Identify and describe the ITTOs associated with those four processes
Interpret an organization chart and position descriptions for a project team
Identify the specific differences between operational and project team management
Identify and describe the five general techniques for managing conflict
Project Communication Management (6%)
Define the three processes typically associated with project communication management
Identify and describe the ITTOs associated with those three processes
Identify and describe the communications skills necessary for project management
Outline the components contained in a communications management plan
Project Risk Management (9%)
Define the six processes typically associated with project risk management
Identify and describe the ITTOs associated with those six processes
Perform simple qualitative risk calculations
Project Procurement Management (7%)
Define the four processes typically associated with project procurement management
Identify and describe the ITTOs associated with those four processes
Identify various types of fixed-price, cost-reimbursable and Time and Material contractual agreements
Project Stakeholder Management (7%)
Define the four processes typically associated with project stakeholder management
Identify and describe the ITTOs associated with those four processes
Describe the four classification models used for stakeholder analysis

PMI®
Project Management Institute

OFFICIAL CYBERSECURITY TRAINING

The Learning Center Las Vegas

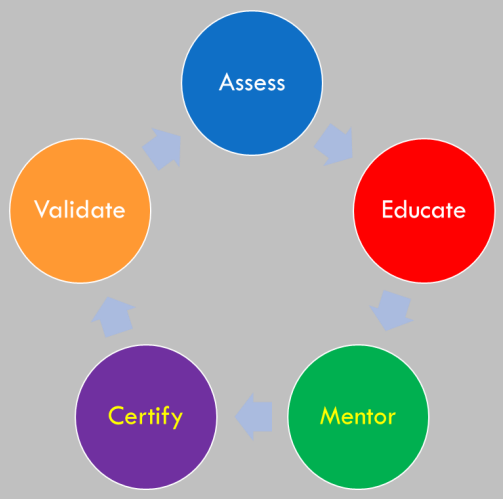
Project Management Institute

PMP Project Mgmt Professional

Course Description:

The Project Management Professional (PMP)® is the most important industry-recognized certification for project managers.
You can find PMPs leading projects in nearly every country and, unlike other certifications that focus on a particular geography or domain, the PMP® is truly global. As a PMP, you can work in virtually any industry, with any methodology and in any location. The PMP can also provide a significant advantage when it comes to salary and earning potential. Among survey respondents to PMI's Earning Power Salary Survey, those with a PMP certification garner a higher salary (20% higher on average) than those without a PMP certification.* Employers benefit as well. When more than one-third of their project managers are PMP-certified, organizations complete more of their projects on time, on budget and meeting original goals. (Pulse of the Profession® study, PMI, 2015.)

The Learning Center Model:



Our unique model follows a streamlined approach to work-force development and skills attainment:

Assess

Assess each individual and teams to determine existing skill sets

Educate

Deliver goal specific training utilizing all delivery modalities

Mentor

Expose students to instructor/mentors with front-line cyber/IT experience

Certify

Certify students with the requisite hands-on skills to perform the tasks related to their functional roles

Validate

Validate students "abilities" through performance analytics and real-world exercises hosted on a cyber range

OFFICIAL CYBERSECURITY TRAINING

The Learning Center
Las Vegas

DOMAINS, TASKS, AND KNOWLEDGE AND SKILL STATEMENTS

This section of the report contains the domains, tasks, and knowledge and skill statements as defined by the Role Delineation Study.

Each domain contains tasks that are measured through the PMP certification progress. In addition, the domain contains knowledge and skills, which are required to competently perform these tasks. There are also cross-cutting knowledge and skills, which are used in multiple domains and tasks.

I. **Initiating**
II. **Planning**
III. **Executing**
IV. **Monitoring and Controlling**
V. **Closing**

Who Should Apply?

If you're an experienced project manager responsible for all aspects of project delivery, leading and directing cross-functional teams, then the PMP is the right choice for you.

Gain and Maintain Your PMP

- The certification exam has 200 multiple-choice questions, and you have four hours to complete it.
- To maintain your PMP, you must earn 60 professional development units (PDUs) every three years.

PMI® Project Management Institute

WHY CHOOSE TLC?

The Learning Center, a division of The Learning Center, has operated for 31 years in IT training and certification field. TLC is an is an Official Training Partner of $(ISC)^2$, EC-Council Accredited Training Center, ISACA Approved Training Center and CompTIA Alliance member. One of two training organizations certified/approved by 4 out of the 5 global credentialing bodies, a unique distinction. ,

Additionally, TLC has partnered with Merit.edu to deliver "world-class" training and education supported by use of the Michigan Cyber Range. The Michigan Cyber Range is the most mature and robust deliverable training platform in the world today. This partnership enables TLC to uniquely deliver skills-based training, assessment, and certifications in alignment with the National Initiative for Cybersecurity Education (NICE) Framework. Our lab content and assessment services are a one-of-a-kind model for developing performance defined cybersecurity professionals capable of meeting current and future employer demand.

OFFICIAL CYBERSECURITY TRAINING

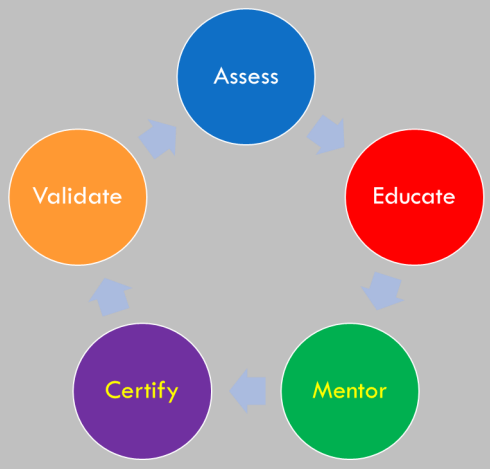
The Learning Center
Las Vegas

CCSK
Certificate of
Cloud Security Knowledge

Cloud Computing Security Knowledge

Course Description: The CCSK - Foundation course is based on V3.0 of the CCSK exam and the CSA Security Guidance for Critical Areas of Cloud Computing V3.0. The Cloud Computing Security Knowledge-Foundation class provides students a comprehensive one day review of cloud security fundamentals and prepares them to take the Cloud Security Alliance CCSK v3.0 certificate exam. Starting with a detailed description of cloud computing, the course covers all major domains in the Guidance v3.0 document from the Cloud Security Alliance, and the recommendations from the European Network and Information Security Agency (ENISA). This class is geared towards security professionals, but is also useful for anyone looking to expand their knowledge of cloud security. (We recommend attendees have at least a basic understanding of security fundamentals, such as firewalls, secure development, encryption, and identity management).

The Learning Center Model:



Our unique model follows a streamlined approach to workforce development and skills attainment:

Assess

Assess each individual and teams to determine existing skill sets

Educate

Deliver goal specific training utilizing all delivery modalities

Mentor

Expose students to instructor/mentors with front-line cyber/IT experience

Certify

Certify students with the requisite hands-on skills to perform the tasks related to their functional roles

Validate

Validate students “abilities” through performance analytics and real-world exercises hosted on a cyber range

OFFICIAL CYBERSECURITY TRAINING

The Learning Center
Las Vegas

As cloud computing shows itself to be the future of information technology, several studies have pointed to the necessity of addressing the IT industry's skills gap and training professionals in both cloud computing and security. Since Cloud Security Alliance first released the Certificate of Cloud Security Knowledge (CCSK) in 2010, thousands of IT and security professionals have taken

- Cloud Architecture
- Governance and Enterprise Risk
- Legal and Electronic Discovery
- Compliance and Audit
- Information Lifecycle Management
- Portability and Interoperability
- Traditional Security, BCM, D/R
- Data Center Operations
- Incident Response
- Application Security
- Encryption and Key Management
- Identity and Access Management
- Virtualization
- Security-as-a-Service
- ENISA Document

CCSK™
Certificate of
Cloud Security Knowledge

OFFICIAL CYBERSECURITY TRAINING

The Learning Center
Las Vegas

ITIL
TRAINING ORGANIZATION ACCREDITED BY
PEOPLECERT ON BEHALF OF AXELOS

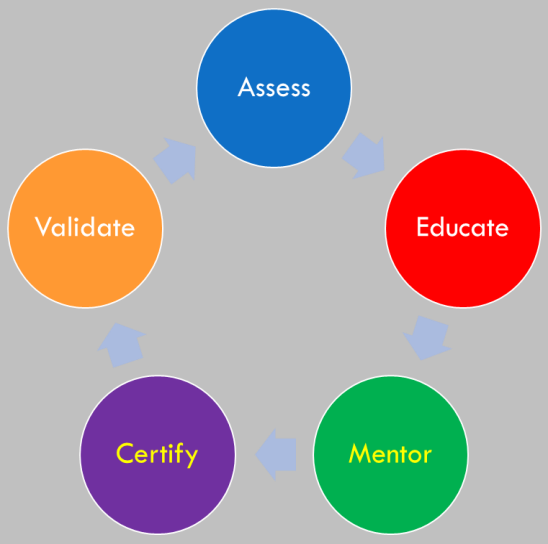
ITIL Foundation

Course Description:

In this exciting and dynamic course, you will get an introduction to the lifecycle of managing IT services to deliver to business expectations. Using an engaging case study, you'll learn the core disciplines of ITIL best practices. Upon completing this course, you'll be well positioned to successfully complete the associated ITIL exam required for entry into the future ITIL intermediate-level training courses.

These disciplines represent a service lifecycle framework that further enhances alignment to the business while demonstrating business value and ROI and enabling IT to solve specific operational needs. This course includes handouts and references useful after the class, as well as practice sessions, quizzes, exam strategies, and test-taking tips.

The Learning Center Model:



Our unique model follows a streamlined approach to workforce development and skills attainment:

Assess

Assess each individual and teams to determine existing skill sets

Educate

Deliver goal specific training utilizing all delivery modalities

Mentor

Expose students to instructor/mentors with front-line cyber/IT experience

Certify

Certify students with the requisite hands-on skills to perform the tasks related to their functional roles

Validate

Validate students “abilities” through performance analytics and real-world exercises hosted on a cyber range

OFFICIAL CYBERSECURITY TRAINING

The Learning Center
Las Vegas

Course Topics:

Key concepts of ITIL

Important principles for improving IT operations

Vital processes and functions

Practical guidance for applying ITIL to everyday IT situations

How to align with business, control costs, and improve IT service quality

Strategies to balance IT resources

Who should attend:

Anyone seeking ITIL Foundation certification and everyone interested in aligning IT with business, controlling or reducing IT costs, improving IT service quality, and balancing IT resources in the most effective manner. All IT professionals, IT project managers, IT managers, IT project or team members, coordinators, network operators, business process analysts, IT architects, consultants, systems integrators, help desk managers and staff, planners, managed service providers, outsourcers, application developers, and other IT-related positions.

ITIL®
TRAINING ORGANIZATION ACCREDITED BY
PEOPLECERT ON BEHALF OF AXELOS

WHY CHOOSE TLC?

The Learning Center, a division of The Learning Center, has operated for 31 years in IT training and certification field. TLC is an is an Official Training Partner of $(ISC)^2$, EC-Council Accredited Training Center, ISACA Approved Training Center and CompTIA Alliance member. One of two training organizations certified/approved by 4 out of the 5 global credentialing bodies, a unique distinction. ,

Additionally, TLC has partnered with Merit.edu to deliver "world-class" training and education supported by use of the Michigan Cyber Range. The Michigan Cyber Range is the most mature and robust deliverable training platform in the world today. This partnership enables TLC to uniquely deliver skills-based training, assessment, and certifications in alignment with the National Initiative for Cybersecurity Education (NICE) Framework. Our lab content and assessment services are a one-of-a-kind model for developing performance defined cybersecurity professionals capable of meeting current and future employer demand.

OFFICIAL CYBERSECURITY TRAINING

The Learning Center
Las Vegas

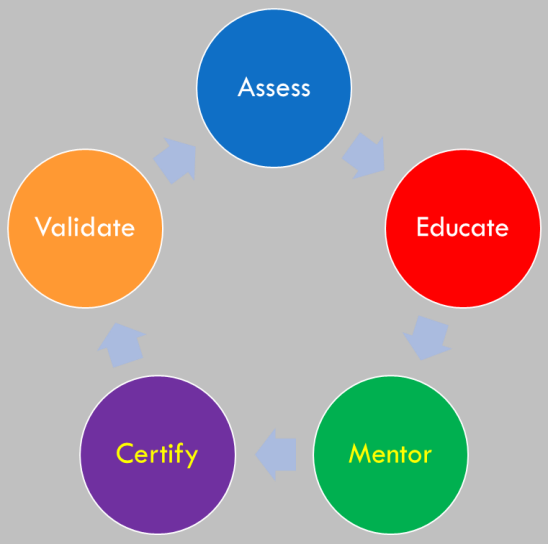
ITIL
TRAINING ORGANIZATION ACCREDITED BY
PEOPLECERT ON BEHALF OF AXELOS

ITIL Intermediate Lifecycle: Service Strategy

Course Description:

In this course, you will be immersed in the overall concepts associated with the service strategy phase of the service lifecycle. You will get an introduction to the key principles of service strategy, and you will learn about the service strategy processes. You will discover the importance of governance and related frameworks, and you will examine implementation considerations and approaches, including organizational design, the role of technology, and service automation. Through lecture, exercises, and scenario-based exam questions, you'll learn the core disciplines of ITIL best practices.

The Learning Center Model:



Our unique model follows a streamlined approach to workforce development and skills attainment:

Assess

Assess each individual and teams to determine existing skill sets

Educate

Deliver goal specific training utilizing all delivery modalities

Mentor

Expose students to instructor/mentors with front-line cyber/IT experience

Certify

Certify students with the requisite hands-on skills to perform the tasks related to their functional roles

Validate

Validate students “abilities” through performance analytics and real-world exercises hosted on a cyber range

OFFICIAL CYBERSECURITY TRAINING

The Learning Center
Las Vegas

Course Topics:

The main process focus areas of this course include:

Strategy management for IT services

Service portfolio management

Financial management for IT services

Demand management

Business relationship management

Key service management concepts

Service strategy principles related to the design of effective service and service management strategies

Service strategy processes, including strategy management for IT services, service portfolio management, financial management for IT services, demand management, and business relationship management

Importance of governance and related frameworks for creating and managing effective service strategies

Relevant organizational and departmental design methods and techniques

Service strategy technologies and service automation to support the service lifecycle

Implementation strategies that follow and support a service lifecycle approach

ITIL®
TRAINING ORGANIZATION ACCREDITED BY
PEOPLECERT ON BEHALF OF AXELOS

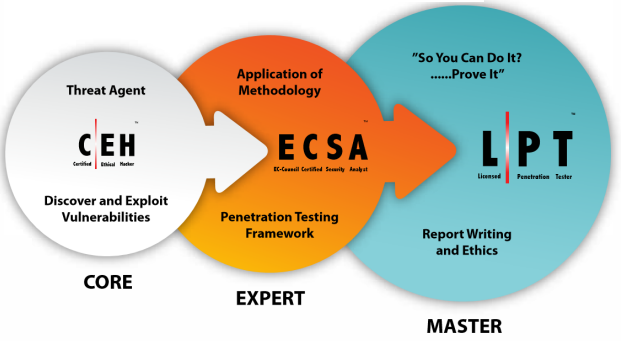
WHY CHOOSE TLC?

The Learning Center, a division of The Learning Center, has operated for 31 years in IT training and certification field. TLC is an is an Official Training Partner of (ISC)^2, EC-Council Accredited Training Center, ISACA Approved Training Center and CompTIA Alliance member. One of two training organizations certified/approved by 4 out of the 5 global credentialing bodies, a unique distinction. ,

Additionally, TLC has partnered with Merit.edu to deliver “world-class” training and education supported by use of the Michigan Cyber Range. The Michigan Cyber Range is the most mature and robust deliverable training platform in the world today. This partnership enables TLC to uniquely deliver skills-based training, assessment, and certifications in alignment with the National Initiative for Cybersecurity Education (NICE) Framework. Our lab content and assessment services are a one-of-a-kind model for developing performance defined cybersecurity professionals capable of meeting current and future employer demand.

OFFICIAL CYBERSECURITY TRAINING

The Learning Center
Las Vegas

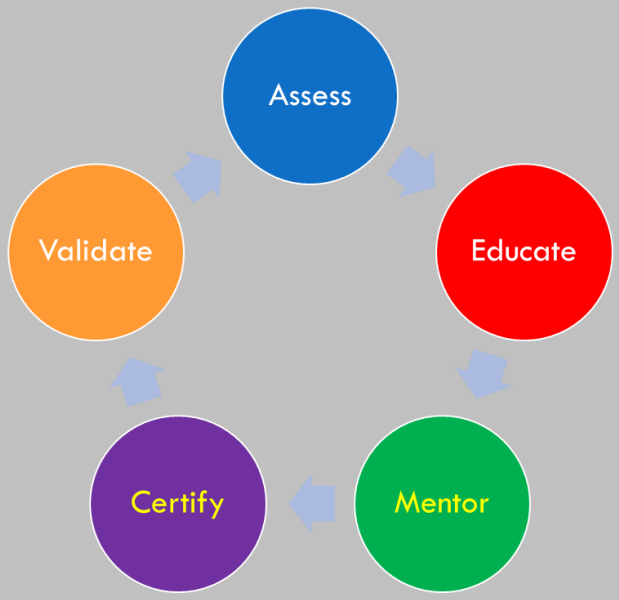


Licensed Penetration Tester Program

Course Description:

This program combines 3 EC-Council courses to create a professional designation leading to Licensed Pen Tester. The CEH provides the foundational skills sets, the ECSA provides the required penetration testing certification , and the LPT provides the licensure as a Penetration Tester. This fully focused program positions an individual with the skills sets to perform at the highest level in penetration testing.

The Learning Center Model:



Our unique model follows a streamlined approach to workforce development and skills attainment:

Assess

Assess each individual and teams to determine existing skill sets

Educate

Deliver goal specific training utilizing all delivery modalities

Mentor

Expose students to instructor/mentors with front-line cyber/IT experience

Certify

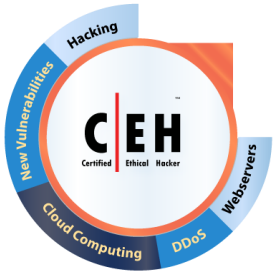
Certify students with the requisite hands-on skills to perform the tasks related to their functional roles

Validate

Validate students “abilities” through performance analytics and real-world exercises hosted on a cyber range

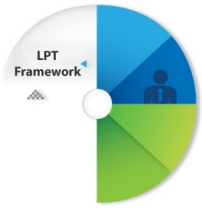
OFFICIAL CYBERSECURITY TRAINING

The Learning Center
Las Vegas ™



ECSA

EC-Council Certified Security Analyst



Course Description:

The goal of this course is to help you master an ethical hacking methodology that can be used in a penetration testing or ethical hacking situation. You walk out the door with ethical hacking skills that are highly in demand, as well as the internationally recognized Certified Ethical Hacker certification! This course prepares you for EC-Council Certified Ethical Hacker exam 312-50.

Course Description:

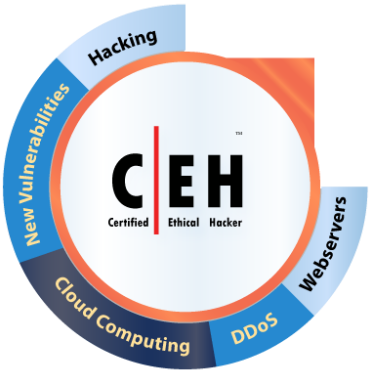
The ECSA penetration testing certification is a security credential like no other! The ECSA penetration testing course provides you with a real world hands-on penetration testing experience and is a globally accepted hacking and penetration testing class available that covers the testing of modern infrastructures, operating systems and application environments while teaching the students how to document and write a penetration testing report.

Course Description:

The goal of this course is to help you master an ethical hacking methodology that can be used in a penetration testing or ethical hacking situation. You walk out the door with ethical hacking skills that are highly in demand, as well as the internationally recognized Certified Ethical Hacker certification! This course prepares you for EC-Council Certified Ethical Hacker exam 312-50.

OFFICIAL CYBERSECURITY TRAINING

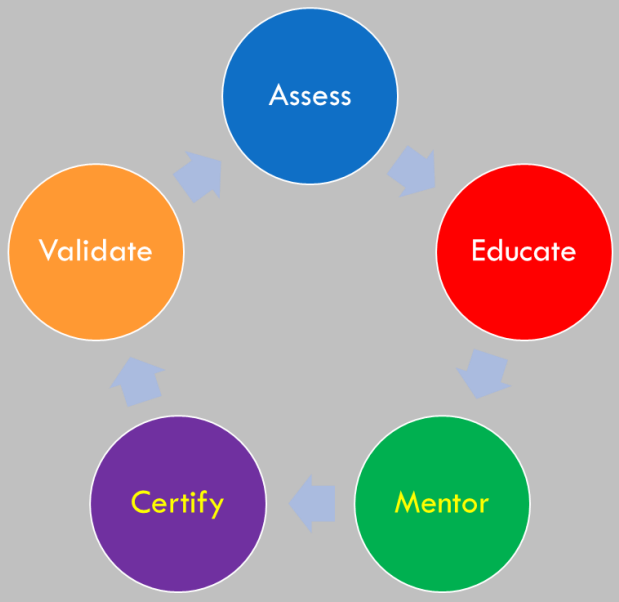
The Learning Center
Las Vegas



Course Description:

The goal of this course is to help you master an ethical hacking methodology that can be used in a penetration testing or ethical hacking situation. You walk out the door with ethical hacking skills that are highly in demand, as well as the internationally recognized Certified Ethical Hacker certification! This course prepares you for EC-Council Certified Ethical Hacker exam 312-50.

The Learning Center Model:



Our unique model follows a streamlined approach to workforce development and skills attainment:

Assess

Assess each individual and teams to determine existing skill sets

Educate

Deliver goal specific training utilizing all delivery modalities

Mentor

Expose students to instructor/mentors with front-line cyber/IT experience

Certify

Certify students with the requisite hands-on skills to perform the tasks related to their functional roles

Validate

Validate students "abilities" through performance analytics and real-world exercises hosted on a cyber range

The Learning Center
Las Vegas

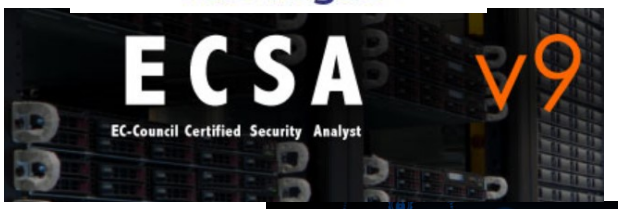
Course Outline Version 9

CEHv9 consists of 20 core modules designed to facilitate a comprehensive ethical hacking and penetration testing training.

Certified Ethical Hacker

OFFICIAL CYBERSECURITY TRAINING

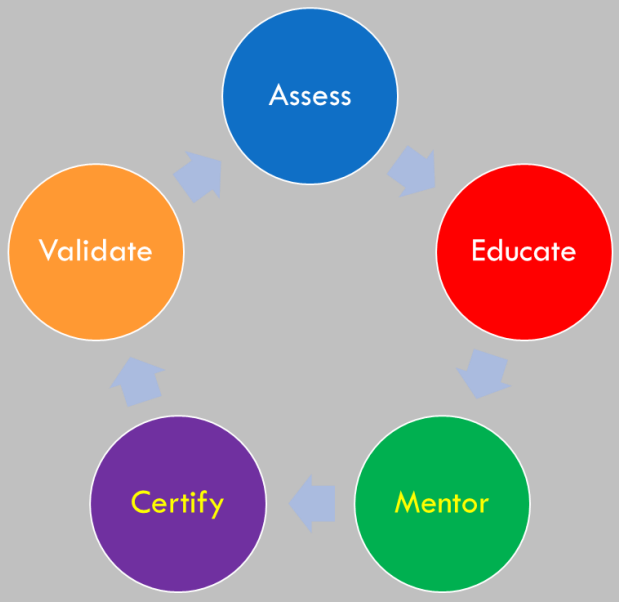
The Learning Center
Las Vegas



Course Description:

The ECSA penetration testing certification is a security credential like no other! The ECSA penetration testing course provides you with a real world hands-on penetration testing experience and is a globally accepted hacking and penetration testing class available that covers the testing of modern infrastructures, operating systems and application environments while teaching the students how to document and write a penetration testing report.

The Learning Center Model:



Our unique model follows a streamlined approach to work-force development and skills attainment:

Assess

Assess each individual and teams to determine existing skill sets

Educate

Deliver goal specific training utilizing all delivery modalities

Mentor

Expose students to instructor/mentors with front-line cyber/IT experience

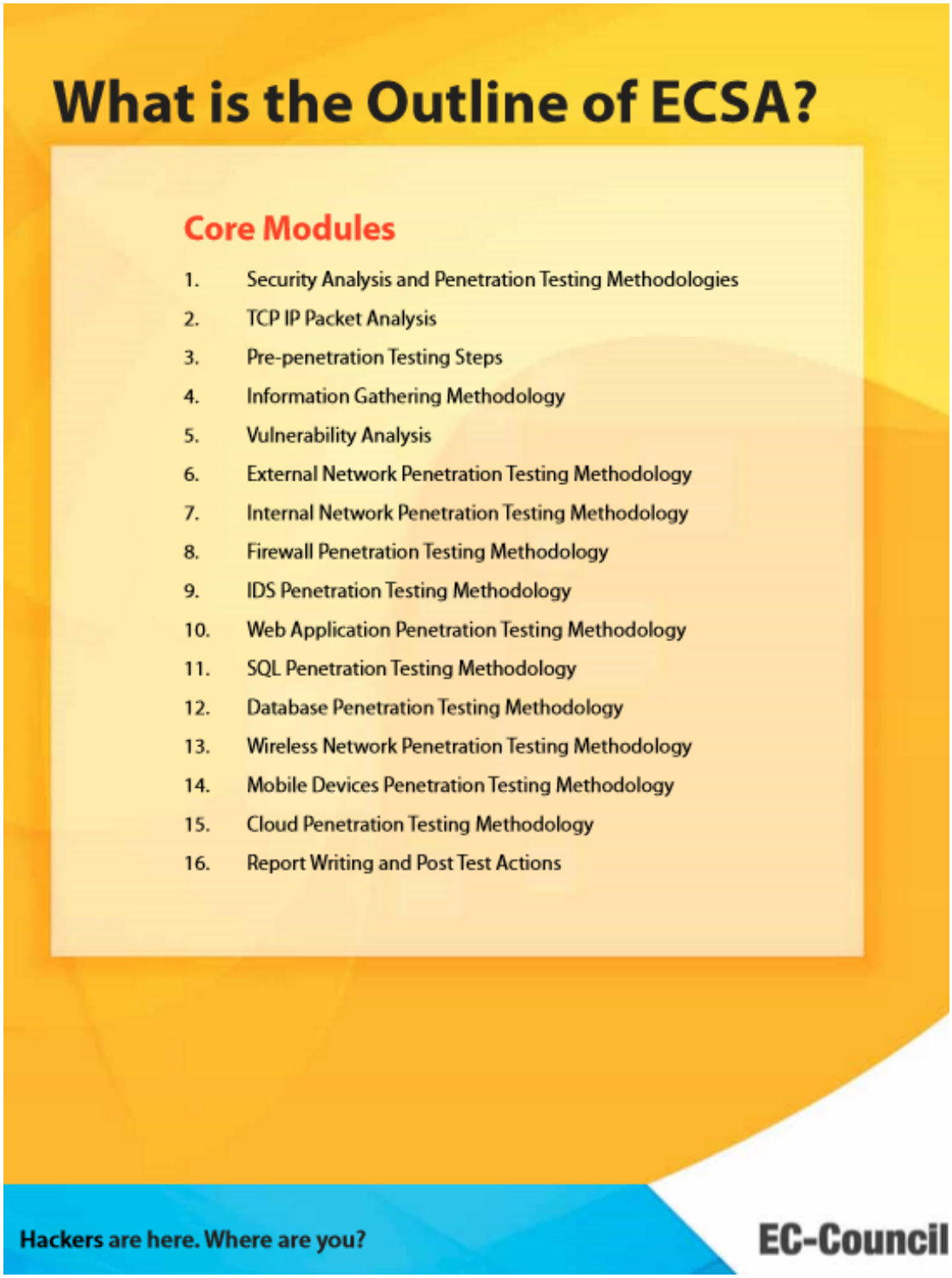
Certify

Certify students with the requisite hands-on skills to perform the tasks related to their functional roles

Validate

Validate students "abilities" through performance analytics and real-world exercises hosted on a cyber range

The Learning Center
Las Vegas



OFFICIAL CYBERSECURITY TRAINING

The Learning Center
Las Vegas

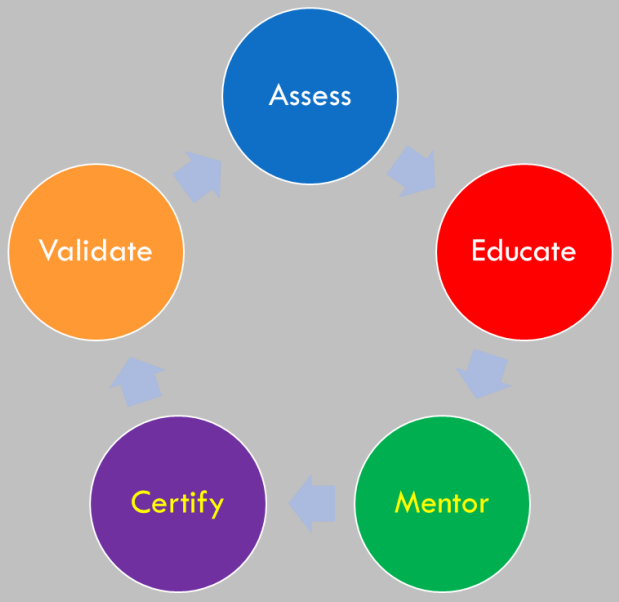
L|P T

Licensed Penetration Tester

Course Description:

To earn the prestigious EC-Council LPT (Master) Credential, you must successfully pass our most challenging practical exam available. The LPT (Master) practical exam is the capstone to EC-Council's entire information security track; from the Certified Ethical Hacker Program (C|EH) to the EC-Council Certified Security Analyst (E|CSA) Program. It all culminates with the ultimate test of your career as a penetration tester – the Licensed Penetration Tester practical exam.

The Learning Center Model:



Our unique model follows a streamlined approach to workforce development and skills attainment:

Assess

Assess each individual and teams to determine existing skill sets

Educate

Deliver goal specific training utilizing all delivery modalities

Mentor

Expose students to instructor/mentors with front-line cyber/IT experience

Certify

Certify students with the requisite hands-on skills to perform the tasks related to their functional roles

Validate

Validate students "abilities" through performance analytics and real-world exercises hosted on a cyber range

The Learning Center
Las Vegas

To successfully pass the LPT (Master) practical, you must fully document your penetration test in a complete, professional penetration test report. This report will follow formats learned in the ECSA program, following industry acceptable, penetration testing and reporting procedures used by only the top professionals in the industry. This report will be reviewed and scored based on a complex rubric by other penetration testing professionals dedicating to upholding the value of EC-Council's LPT (Master) Credential, and enhancing the professionalization of cyber security as a field penetration tester.

While the Certified Ethical Hacker course teaches threat agents that can compromise the security posture of an organization, and the EC-Council Security Analyst program provides a repeatable and documentable methodology for deep analysis of an organizations security posture, the Licensed Penetration Tester exam tests the mastery of the skill-sets required to be a true professional penetration tester – Technical Analysis and Report Writing.

To build on the technical skills taught in the Certified Ethical Hacking course, the EC-Council Certified Security Assessment course emphasizes application of a suitable methodology and report writing. The LPT (Master) practical exam thoroughly tests the application of this knowledge and the skills required in an examination that even our reviewers have called **"extremely challenging"**. There is no course for the LPT (Master) exam. The Licensed Penetration Tester (Master) certification Exam is the final step after the intense training and certification that you would have received in the Certified Ethical Hacker and the EC-Council Certified Security Analyst programs.

Many have described report writing as one of least preferred, yet arguably one of the most critical parts of any penetration testing engagement. While so many cyber security courses are offered globally to cover various subjects in the information security realm, hardly any are dedicated to this very important skill, especially almost since half of all time spent at any penetration testing engagement can revolve around writing and reporting the core findings of the engagement to the client. Explaining a highly technical finding in an elaborate penetration test engagement to someone not technical like the CEO of a company, the senior management or even the board of directors can be very challenging and frustrating at times. Mastery of communication, research and

OFFICIAL CYBERSECURITY TRAINING

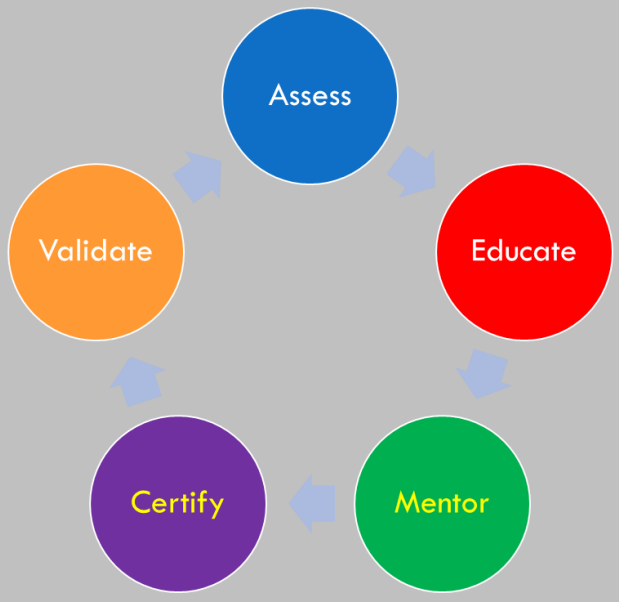
The Learning Center
Las Vegas

E|C I H™
EC-Council Certified Incident Handler

Course Description:

The goal of this course is to help you master an ethical hacking methodology that can be used in a penetration testing or ethical hacking situation. You walk out the door with ethical hacking skills that are highly in demand, as well as the internationally recognized Certified Ethical Hacker certification! This course prepares you for EC-Council Certified Ethical Hacker exam 312-50.

The Learning Center Model:



Our unique model follows a streamlined approach to workforce development and skills attainment:

Assess

Assess each individual and teams to determine existing skill sets

Educate

Deliver goal specific training utilizing all delivery modalities

Mentor

Expose students to instructor/mentors with front-line cyber/IT experience

Certify

Certify students with the requisite hands-on skills to perform the tasks related to their functional roles

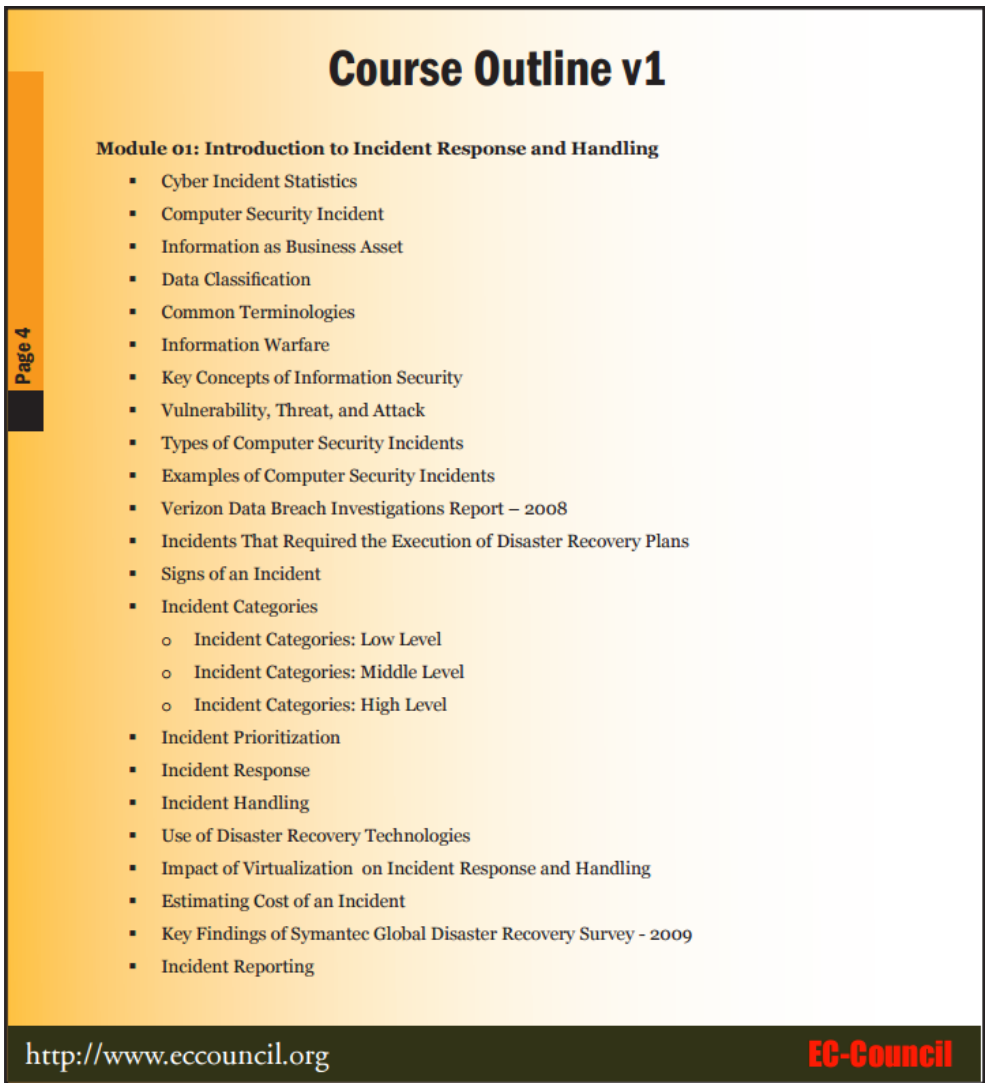
Validate

Validate students "abilities" through performance analytics and real-world exercises hosted on a cyber range

The Learning Center
Las Vegas

The EC-Council Certified Incident Handler (ECIH) program is designed to provide the fundamental skills to handle and respond to the computer security incidents in an information system. The course addresses various underlying principles and techniques for detecting and responding to current and emerging computer security threats. Students will learn how to handle various types of incidents, risk assessment methodologies, and various laws and policies related to incident handling. After attending this course, they will be able to create incident handling and response policies as well as deal with various types of computer security incidents.

The IT incident management training program will enable students to be proficient in handling and responding to various security incidents such as network security incidents, malicious code incidents, and insider attack threats. In addition, students will learn about computer forensics and its role in handling and responding to incidents. The course also covers incident response teams, incident management training methods, and incident recovery techniques in detail. The ECIH certification will provide professionals greater industry acceptance as the seasoned incident handler.



OFFICIAL CYBERSECURITY TRAINING

The Learning Center
Las Vegas

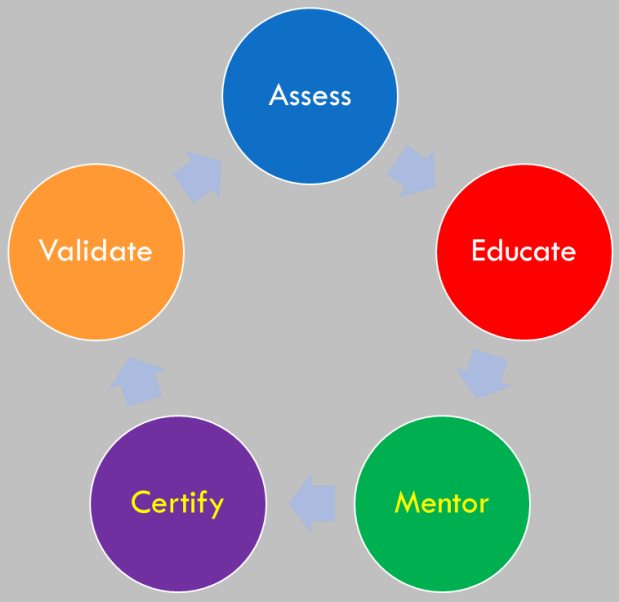
C|ND™
Certified Network Defender

Course Description:

Organizational focus on cyber defense is more important than ever as cyber breaches have a far greater financial impact and can cause broad reputational damage.

Despite best efforts to prevent breaches, many organizations are still being compromised. Therefore organizations must have, as part of their defense mechanisms, trained network engineers who are focused on protecting, detecting, and responding to the threats on their networks.

The Learning Center Model:



Our unique model follows a streamlined approach to workforce development and skills attainment:

Assess

Assess each individual and teams to determine existing skill sets

Educate

Deliver goal specific training utilizing all delivery modalities

Mentor

Expose students to instructor/mentors with front-line cyber/IT experience

Certify

Certify students with the requisite hands-on skills to perform the tasks related to their functional roles

Validate

Validate students "abilities" through performance analytics and real-world exercises hosted on a cyber range

OFFICIAL CYBERSECURITY TRAINING

Course Description

Certified Network Defender (CND) is a vendor-neutral, hands-on, instructor-led comprehensive network security certification training program. It is a skills-based, lab intensive program based on a job-task analysis and cybersecurity education framework presented by the National Initiative of Cybersecurity Education (NICE). The course has also been mapped to global job roles and responsibilities and the Department of Defense (DoD) job roles for system/network administrators. The course is designed and developed after extensive market research and surveys.

The program prepares network administrators on network security technologies and operations to attain Defense-in-Depth network security preparedness. It covers the protect, detect and respond approach to network security. The course contains hands-on labs, based on major network security tools and techniques which will provide network administrators real world expertise on current network security technologies and operations. The study-kit provides you with over 10 GB of network security best practices, assessments and protection tools. The kit also contains templates for various network policies and a large number of white papers for additional learning.

Course Duration: 5 days

The Learning Center
Las Vegas

"While there will be over 1.5 million cyber security jobs that remain unfilled by 2019, millions of IT and Network administrators remain untrained on network defense techniques"

- Michael Brown, CEO at Symantec, the world's largest security software vendor.

OFFICIAL CYBERSECURITY TRAINING

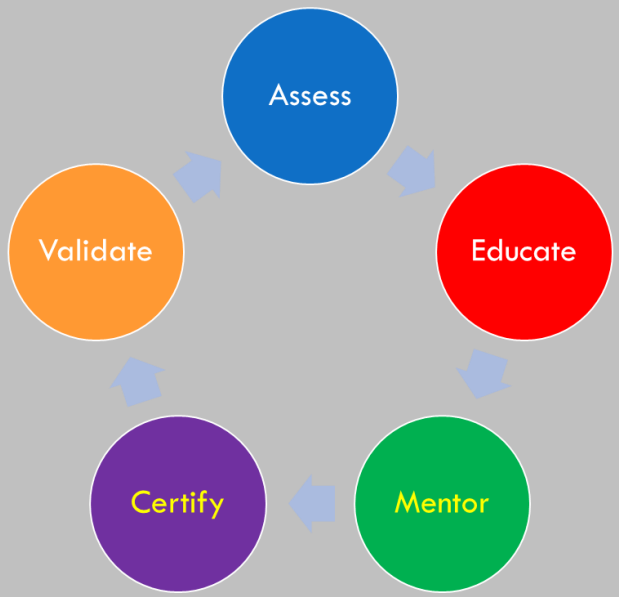
The Learning Center
Las Vegas

C|HFI™
Computer Hacking Forensic INVESTIGATOR

Course Description:

The CHFI Program certifies individuals in the specific security discipline of computer forensics from a vendor-neutral perspective. The CHFI certification will fortify the application knowledge of law enforcement personnel, system administrators, security officers, defense and military personnel, legal professionals, bankers, security professionals, and anyone who is concerned about the integrity of the network infrastructure.

The Learning Center Model:



Our unique model follows a streamlined approach to work-force development and skills attainment:

Assess

Assess each individual and teams to determine existing skill sets

Educate

Deliver goal specific training utilizing all delivery modalities

Mentor

Expose students to instructor/mentors with front-line cyber/IT experience

Certify

Certify students with the requisite hands-on skills to perform the tasks related to their functional roles

Validate

Validate students "abilities" through performance analytics and real-world exercises hosted on a cyber range

The Learning Center
Las Vegas

Course Outline Version 8

CHFIv8 curriculum consists of 22 instructor-led training modules.

1. Computer Forensics in Today's World
2. Computer Forensics Investigation Process
3. Searching and Seizing Computers
4. Digital Evidence
5. First Responder Procedures
6. Computer Forensics Lab
7. Understanding Hard Disks and File Systems
8. Windows Forensics
9. Data Acquisition and Duplication
10. Recovering Deleted Files and Deleted Partitions
11. Forensics Investigation Using AccessData FTK
12. Forensics Investigation Using EnCase
13. Steganography and Image File Forensics
14. Application Password Crackers
15. Log Capturing and Event Correlation
16. Network Forensics, Investigating Logs and Investigating Network Traffic
17. Investigating Wireless Attacks
18. Investigating Web Attacks
19. Tracking Emails and Investigating Email Crimes
20. Mobile Forensics
21. Investigative Reports
22. Becoming an Expert Witness

"CHFI is a certification that gives a complete overview of the process that a forensic investigator must follow when investigating a cybercrime. It includes not only the right treatment of the digital evidence in order to be accepted in the Courts but also useful tools and techniques that can be applied to investigate an incident."

- Virginia Aguilar, CHFI, KPMG, Madrid.

EC-Council | Computer Hacking Forensic Investigator

OFFICIAL CYBERSECURITY TRAINING

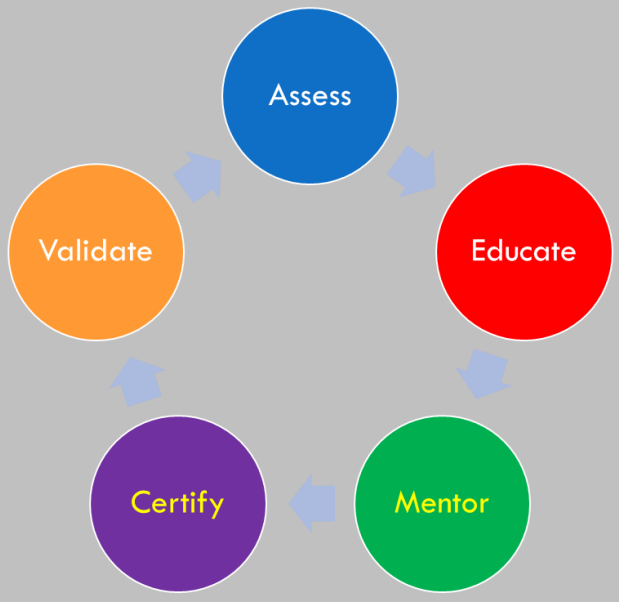
The Learning Center
Las Vegas

C|CISO

Course Description:

EC-Council's CCISO Program has certified leading information security professionals around the world. A core group of high-level information security executives, the CCISO Advisory Board, contributed by forming the foundation of the program and outlining the content that would be covered by the exam, body of knowledge, and training. Some members of the Board contributed as authors, others as exam writers, others as quality assurance checks, and still others as trainers. Each segment of the program was developed with the aspiring CISO in mind and looks to transfer the knowledge of seasoned professionals to the next generation in the areas that are most critical in the development and maintenance of a successful information security program.

The Learning Center Model:



Our unique model follows a streamlined approach to workforce development and skills attainment:

Assess

Assess each individual and teams to determine existing skill sets

Educate

Deliver goal specific training utilizing all delivery modalities

Mentor

Expose students to instructor/mentors with front-line cyber/IT experience

Certify

Certify students with the requisite hands-on skills to perform the tasks related to their functional roles

Validate

Validate students "abilities" through performance analytics and real-world exercises hosted on a cyber range

OFFICIAL CYBERSECURITY TRAINING

The Learning Center
Las Vegas

EC-Council's CCISO Program has certified leading information security professionals around the world. A core group of high-level information security executives, the CCISO Advisory Board, contributed by forming the foundation of the program and outlining the content that would be covered by the exam, body of knowledge, and training. Some members of the Board contributed as authors, others as exam writers, others as quality assurance checks, and still others as trainers. Each segment of the program was developed with the aspiring CISO in mind and looks to transfer the knowledge of seasoned professionals to the next generation in the areas that are most critical in the development and maintenance of a successful information security program.

The Certified CISO (CCISO) program is the first of its kind training and certification program aimed at producing top-level information security executives. The CCISO does not focus solely on technical knowledge but on the application of information security management principles from an executive management point of view. The program was developed by sitting CISOs for current and aspiring CISOs.

In order to sit for the CCISO exam and earn the certification, candidates must meet the basic CCISO requirements. Candidates who do not yet meet the CCISO requirements but are interested in information security management can pursue the EC-Council Information Security Management (EISM) certification.

OFFICIAL CYBERSECURITY TRAINING

The Learning Center
Las Vegas

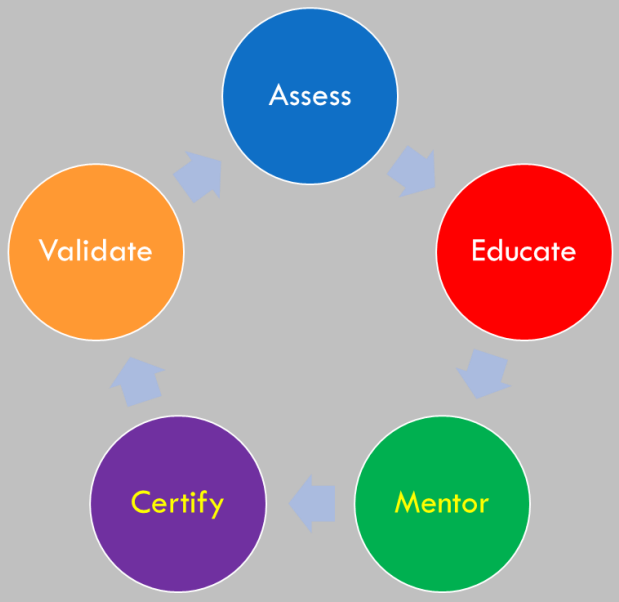
Basic Digital Media Forensics

Course Description:

Basic Digital Media Forensics provides an introduction to media collection, imaging and analysis. Students will discuss file systems, partition structures and data storage to better understand how and where data is stored on multiple types of digital media, as well as the best methods to access it.

The course is an optimal starting point for individuals looking to expand their forensic knowledge and outlines a number of ways to achieve forensic goals while ensuring all processes are completed in a forensically-sound manner. Chain of custody and evidence handling is addressed, as well as what to do and what not to do when dealing with 'live' evidence.

The Learning Center Model:



Our unique model follows a streamlined approach to workforce development and skills attainment:

Assess

Assess each individual and teams to determine existing skill sets

Educate

Deliver goal specific training utilizing all delivery modalities

Mentor

Expose students to instructor/mentors with front-line cyber/IT experience

Certify

Certify students with the requisite hands-on skills to perform the tasks related to their functional roles

Validate

Validate students "abilities" through performance analytics and real-world exercises hosted on a cyber range

OFFICIAL CYBERSECURITY TRAINING

The Learning Center
Las Vegas

DAY 1

During the first lesson, students will learn about setting up a Forensic workspace. In addition, students will learn about preparing target media to ensure a forensically sound process prior to imaging.

Topics List

- Preparation of target media/wiping using dc3dd
- Forensic imaging using FTK Imager
- Identification and discussion of various digital media that has been and could be useful in a forensic investigation

DAY 2

A lesson consisting of Incident response and acquisition. Students will also learn about forensic tools, windows file systems, and partition structures.

Topics List

- Forensic imaging of different media using FTK Imager
- Forensic analysis of a raw image using autopsy
- Exifdata analysis

DAY 3

Students will become more familiar with Forensics for Windows , and learn the value of metadata, and exifdata in forensic analysis.

Topics List

- Forensic analysis of a raw image using autopsy
- Exifdata analysis
- Viewing of data in a hex editor

DAY 4

Students will learn the proper techniques for Forensic reporting and documentation.

Topics List

- Lab will begin by conducting analysis on another dd image
- Answering a line of questions that pertains to that provided image
- Conduct imaging and analysis of a smaller image
- Draft a comprehensive forensic report

DAY 5

Review all submitted forensic reports at the end of Day 4 and discuss items of concern within both the processes and the reporting.

Capstone Exercise

Students will conduct a forensically-sound acquisition and analysis of assigned media. After which, they will be required to write a comprehensive forensic report.

TARGET AUDIENCE

Professionals looking to broaden their cyber skills or begin developing a strong skill set within the forensic community

OBJECTIVE

Provide a solid understanding of what is considered valuable digital media used as forensic evidence for an investigation, including how data is stored, retrieved and analyzed

OFFICIAL CYBERSECURITY TRAINING

The Learning Center Las Vegas

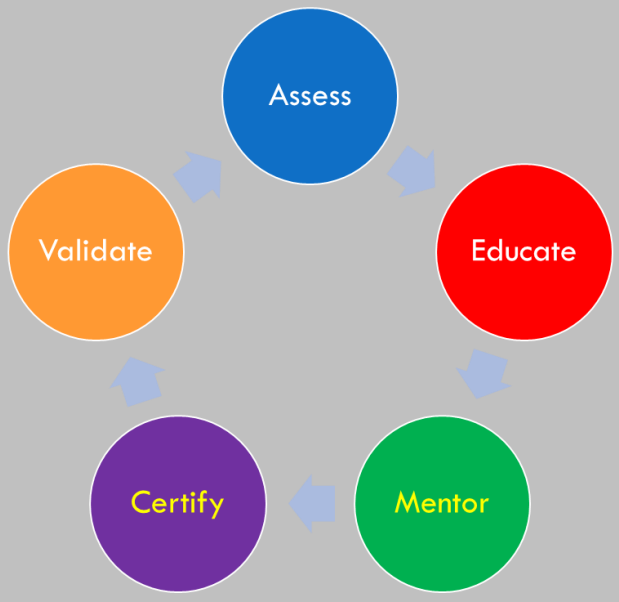
Fundamentals of Network Forensics

Course Description:

Fundamentals of Network Forensics expands on acquired networking knowledge and extends into the computer forensic mindset. Students will learn about common devices used in computer networks and where useful data may reside. Students will also learn how to collect that data for analysis using hacker methodology.

Additionally, the course covers information related to common exploits involved in Windows server systems and common virus exploits. Students will learn how to recognize exploit traffic, and the difference between attacks and poor network configuration.

The Learning Center Model:



Our unique model follows a streamlined approach to workforce development and skills attainment:

Assess

Assess each individual and teams to determine existing skill sets

Educate

Deliver goal specific training utilizing all delivery modalities

Mentor

Expose students to instructor/mentors with front-line cyber/IT experience

Certify

Certify students with the requisite hands-on skills to perform the tasks related to their functional roles

Validate

Validate students "abilities" through performance analytics and real-world exercises hosted on a cyber range

OFFICIAL CYBERSECURITY TRAINING

The Learning Center
Las Vegas

DAY 1

Students will learn to understand and demonstrate the use of a standard methodology for exploitation, the concepts of various software threats and the techniques expected of a professional hacker.

Topics List

- Hacker mindset and steps of an attack
- Hacker techniques
- Tools used for exploitation
- Packet capturing and analysis
- Tools used for network analysis

DAY 2

Students will identify protocols helpful when performing network forensics. Students will gain an understanding of filters and how they can help identify specific packets of interest. Students will setup Ethernet ports for capturing data and analyze traffic using Snort to identify malicious activity.

Topics List

- Filtering traffic and protocol analysis
- Comparing file hashes to identify malicious files
- Parsing network traffic to identify malicious files and attacker activity
- Network devices, packet capturing in a switched environment
- Configuring Ethernet ports on an IDS
- Advantages of internal and external IDS placement
- Running Snort
- Examining Snort rules and using Snort to analyze packet capture files

DAY 3

Students will learn how to edit Snort configuration files to use local rules, edit rules files and write custom rules to detect malicious activity, command shells and malware. Students analyze traffic using Snort as an intrusion detection system. Students will learn to recognize anomalous activity in web, FTP authentication and access logs in Linux and Windows.

Topics List

- Editing Snort configuration files
- Editing Snort rules files
- Writing custom Snort rules to detect malicious activity
- Analyzing traffic using Snort as an IDS
- Recognizing anomalous activity in Linux and Windows logs

DAY 4

Students will learn how to recognize anomalous activity in Linux and Windows. Student will understand how to detect evidence of an attack using incident response toolkits as well as native tools to view process lists, established connections, scheduled jobs, and account activity.

Topics List

- Analyzing Windows incident response data
- Analyzing Linux incident response data
- Using visualization tools to recognize anomalous communications
- Correlating data from established connections processes and traffic
- Using Sawmill to analyze Snort logs
- Recognizing internal and external threats

DAY 5

Students will demonstrate the ability to identify attacker IP addresses, exfiltrated data, malware, method of compromise, accounts used, and document observed activity in an executive summary and timeline of events.

Capstone Exercise

Students will be required to assign attribution to an attack and final exercise.

OFFICIAL CYBERSECURITY TRAINING

The Learning Center Las Vegas

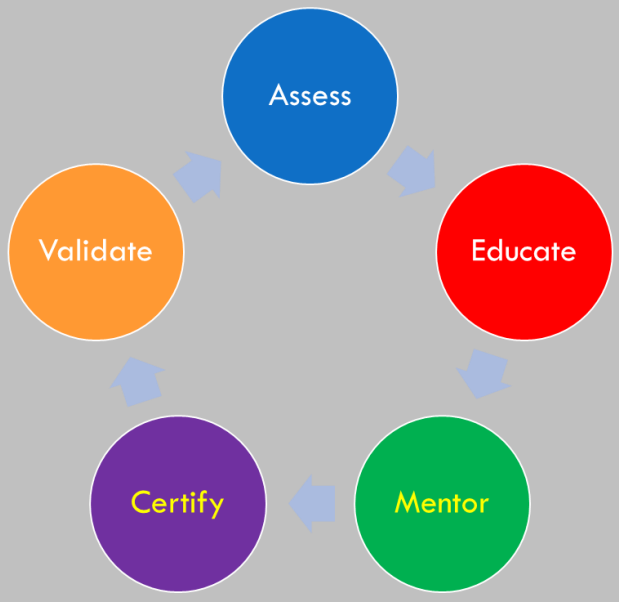
Mobile Device Forensics

Course Description:

Mobile Device Forensics provides an introduction to mobile devices and the value that they offer in forensic investigations. The class addresses the methods used to store data, as well as the areas of the mobile device where data is stored and how to access it. The class will also discuss mobile device removable media and the role it plays with the mobile device.

Students will cover network technology as well as three tools specifically designed for mobile device acquisition. Upon completion of an extensive hands-on experience, the student will draft a comprehensive forensic report, ensuring all actions were documented and conducted in a forensically sound manner.

The Learning Center Model:



Our unique model follows a streamlined approach to work-force development and skills attainment:

Assess

Assess each individual and teams to determine existing skill sets

Educate

Deliver goal specific training utilizing all delivery modalities

Mentor

Expose students to instructor/mentors with front-line cyber/IT experience

Certify

Certify students with the requisite hands-on skills to perform the tasks related to their functional roles

Validate

Validate students "abilities" through performance analytics and real-world exercises hosted on a cyber range

OFFICIAL CYBERSECURITY TRAINING

The Learning Center
Las Vegas

DAY 1

Students will be introduced to mobile device hardware and architecture.

Topics List

- Using faraday
- Preparing target media using dc3dd
- Acquiring a SIM card and saving to target media
- Creating a forensic image of removable media using dc3dd

DAY 2

Students will learn about cell phone acquisition and exploitation and become familiar with various mobile device acquisition tools.

Topics List

- Exifdata analysis
- Viewing data in hex editor
- Conducting forensic analysis on previously imaged media

DAY 3

Students will learn the correct methods for Forensic reporting and documentation.

Topics List

- Device acquisitions following forensically sound methodologies
- Drafting of forensic report

DAY 4

Students will review the results from the forensic reports that have been submitted and acquisitions completed. Students will also go through a review of the course material.

Capstone Exercise

Students will utilize the knowledge and skills acquired throughout the course, in a hands on lab exercise.

TARGET AUDIENCE

Professionals looking to broaden their cyber forensics skills or individuals that will begin working with mobile devices and acquiring data from them, as well as their removable components

OBJECTIVE

Provide students with an understanding of how mobile devices actually work and store data, and what data can be of forensic value, as well as how certain types of damage can determine what data can be acquired from the device

OFFICIAL CYBERSECURITY TRAINING

The Learning Center Las Vegas

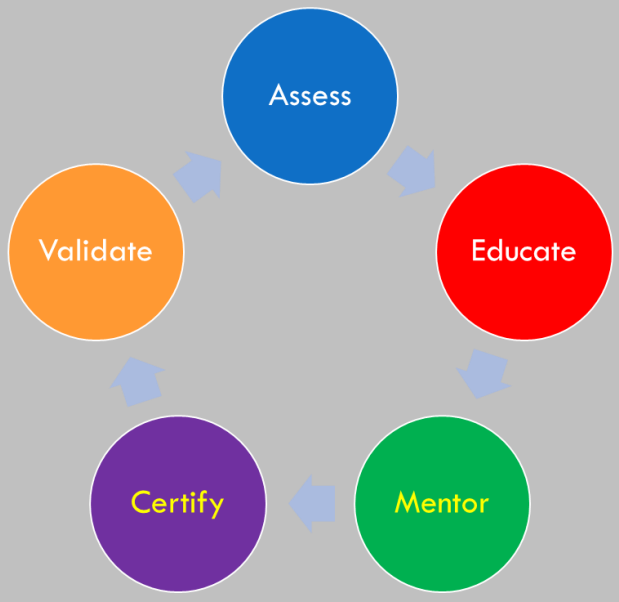
Advanced Digital Media Forensics

Course Description:

Advanced Digital Media Forensics provides an in-depth look at forensic acquisition and analysis of multiple types of media. The course outlines a number of ways to achieve forensic goals while ensuring all processes are completed in a forensically-sound manner, and covers advanced automated tools, as well as manual tools and methodologies.

Advanced Digital Media Forensics focuses on a variety of Windows Internet, Chat, and Social Media artifacts. Additional topic discussions include data obfuscation and obtaining and analyzing intentionally hidden, overwritten, or deleted data. Students will also consider deploying discussed forensic methodologies in both a proactive and reactive manner.

The Learning Center Model:



Our unique model follows a streamlined approach to workforce development and skills attainment:

Assess

Assess each individual and teams to determine existing skill sets

Educate

Deliver goal specific training utilizing all delivery modalities

Mentor

Expose students to instructor/mentors with front-line cyber/IT experience

Certify

Certify students with the requisite hands-on skills to perform the tasks related to their functional roles

Validate

Validate students "abilities" through performance analytics and real-world exercises hosted on a cyber range

OFFICIAL CYBERSECURITY TRAINING

The Learning Center Las Vegas

DAY 1

During the first lesson, students will learn about incident response and memory analysis.

Topics List

- Memory Analysis
- Live Memory Capture
- Typical Windows Functionality
- Windows Event Logs

DAY 2

Students will learn about advanced automated tools, advanced filtering, creating and using custom filters, manual, data carving, fuzzy hashing and rolling hashes.

Topics List

- Manual Data Carving
- Setting Custom/Advanced Filters
- SSdeep

DAY 3

Students will learn advanced Windows forensics, data hiding and obfuscation (how to detect, protect, and create), application artifacts and cryptography.

Topics List

- Alternate Data Streams
- Creating and Detection
- Deleted Partition Recovery
- Volume Shadow Copy/Restore Point Analysis
- Password Cracking

DAY 4

Students will learn about forensic reporting and documentation. Student will review all the course modules and labs and work through a practical lab. The practical will encompass a multitude of methodologies learned throughout the course in order to apply all techniques simultaneously.

DAY 5

Review all submitted forensic reports at the end of Day 4 and discuss items of concern within both the processes and the reporting.

Capstone Exercise

Conduct forensically sound memory acquisition and answer a line of questions. Furthermore, complete the rest of the investigation using all of the discussed and practiced skills throughout the class. The student must successfully complete the investigation and answer any corresponding questions while effectively reporting on the appropriate steps taken to achieve said goal

TARGET AUDIENCE

Professionals looking to expand their digital forensic knowledge and obtain a better understanding of tips, tricks, and methodologies for data locations and recovery. This class is for the examiner/investigator that may face a multitude of examination requirements

OBJECTIVE

Provide an advanced analytical perspective on data considered to have forensic value

OFFICIAL CYBERSECURITY TRAINING

The Learning Center Las Vegas

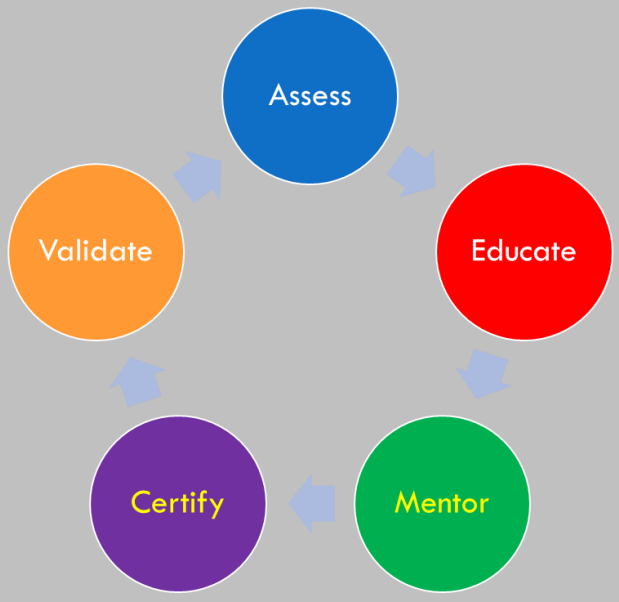
Incident Response

Course Description:

Incident Response equips students with the needed tools to implement robust defense-in-depth practices within the workplace. IR provides detailed training on proper documentation and planning for computer network defense.

The course exposes students to a variety of real-world scenarios and provides hands-on experience in event detection and recovery in an enterprise envi-

The Learning Center Model:



Our unique model follows a streamlined approach to work-force development and skills attainment:

Assess

Assess each individual and teams to de-termine existing skill sets

Educate

Deliver goal specific training utilizing all delivery modalities

Mentor

Expose students to instructor/mentors with front-line cyber/IT experience

Certify

Certify students with the requisite hands-on skills to perform the tasks related to their functional roles

Validate

Validate students "abilities" through per-formance analytics and real-world exer-cises hosted on a cyber range

OFFICIAL CYBERSECURITY TRAINING

The Learning Center
Las Vegas

DAY 1

Day 1 introduces students to sound IR concepts focusing on proper awareness of information systems and networks, clear and up-to-date documentation and effective use of risk management theory.

Topics List

- IR today
- Network mapping and awareness
- Standard documentation requirements and options
- System and network baselining practices
- Wisdom of security auditing
- Proactive vs. reactive action
- Risk management and defense

DAY 2

Students use the tools learned on Day 1 to detect a possible incident and conduct a full-spectrum analysis on a selection of corporate network systems in order to judge impact and threat to business or company data.

Topics List

- Incident detection approaches
- Baselining saves the day
- Practices for analyzing an incident
- Approaches for confirming an incident
- Using all logs for impact analysis
- Techniques for analyzing files

DAY 3

Students learn to formulate a fully-realized recovery plan based on data received on a confirmed cyber incident on their company network. They will contain and eradicate threats to the network and use security auditing tools to verify success . Recovery efforts will be completed by verifying no new vulnerabilities were introduced to the network. Day 3 ends with students reporting on details of the event identification, response and recovery to organizational management.

Topics List

- Incident Recovery Plans
- Testing recovery options before/after rollout
- Standard Operating Procedures and Recovery Plans
- Approaches for confirming an incident
- Using all logs for impact analysis
- Techniques for analyzing files
- Reporting to management

DAY 4

Students apply forensically-sound principles to image a machine and recover useful information from additional imaged systems. Students participate in the recovery experience and are required to update a response plan.

Topics List

- Real world recoveries
- Forensic imaging and analysis
- Maintaining clear communications
- Post-incident actions and lessons learned
- Updating documentation to prep for the next cycle

DAY 5

Day 5 comprises a full-spectrum IR scenario that requires students to recover from a series of attacks discovered on a corporate network. They must scope the impacted systems, create a mitigation plan, harden weak defenses and conduct recovery efforts. This final exercise replicates a variety of network services, hardware, and configurations. The capstone reinforces exposure to tools and techniques learned during the previous four days.

Capstone Exercise

All the material covered in the course will be put to use in the final exercise.

TARGET AUDIENCE

IT and Cyber Security professionals looking to acquire hands-on experience, in the identification of and recovery from security events, and to establish and maintain a robust computer network defense posture

OBJECTIVE

Provide in-depth exposure to network and systems intrusion protection methods, what to do before, during and after an event,, and how to recover from events and strengthen organizational security

OFFICIAL CYBERSECURITY TRAINING

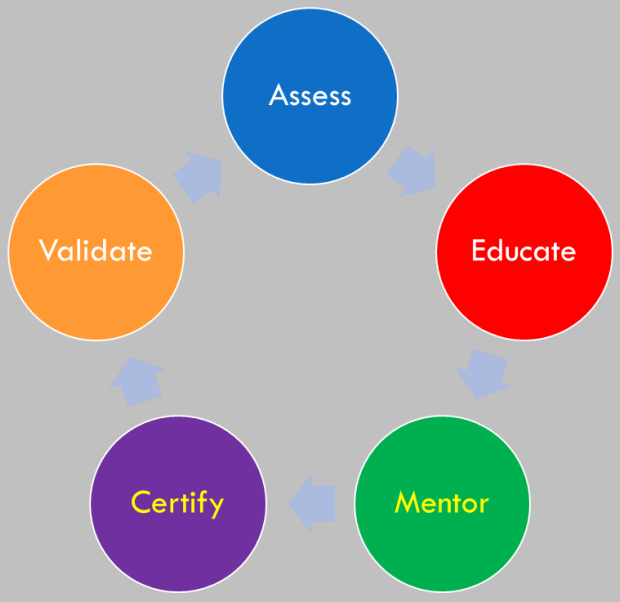
The Learning Center
Las Vegas

CSX Practitioner Bootcamp

Course Description:

Practitioner Boot Camp is a five-day, intensive cyber security training course focused on more complex, technical cyber skills and scenarios. CSXP Boot Camp is an accelerated alternative to our more comprehensive three-week CSX Practitioner course series. CSXP Boot Camp is conducted in an adaptive, live cyber lab environment, enabling students to build critical technical skills by learning complex concepts and practice applying industry-leading methods. They will learn to utilize the latest open-source tools within actual, real-world scenarios. CSXP Boot Camp is an ideal way to build complex and advanced technical skills essential for career advancement and will help students in preparing for the CSXP certification exam.

The Learning Center Model:



Our unique model follows a streamlined approach to workforce development and skills attainment:

Assess

Assess each individual and teams to determine existing skill sets

Educate

Deliver goal specific training utilizing all delivery modalities

Mentor

Expose students to instructor/mentors with front-line cyber/IT experience

Certify

Certify students with the requisite hands-on skills to perform the tasks related to their functional roles

Validate

Validate students "abilities" through performance analytics and real-world exercises hosted on a cyber range

OFFICIAL CYBERSECURITY TRAINING

The Learning Center Las Vegas

ISACA® Trust in, and value from, information systems

DAY 1

LESSON	LAB	ASSOCIATED TOPICS
» Hardware Software Identification & Documentation	» Preliminary Scanning	» Identity
» Network Discovery Tools	» Additional Scanning Options	
» Sensitive Information Discovery	» Sensitive Information Identification	
» Vulnerability Assessment Process	» Vulnerability Scanner Set-up & Configuration	
» Patch Upgrade Configure Vulnerability Scanners	» Vulnerability Scanner Set-up & Configuration, Part 2	

DAY 2

LESSON	LAB	ASSOCIATED TOPICS
» Specific Cyber Controls	» System Hardening	» Protect
» Collecting Event Data	» Firewall Setup & Configuration	
» Verifying the Effectiveness of Controls	» Microsoft Baseline Security Analyzer	
» Monitoring Controls	» IDS Setup	
» Updated Cyber Security Controls	» Personal Security Products	
» Patch Management	» Linux Users & Groups	
» Verifying Identities & Credentials		
» Cyber Security Procedures Standards		

DAY 3

LESSON	LAB	ASSOCIATED TOPICS
» Cyber Security Control Introduction & Explanation	» Network Reconnaissance	» Detect
» Cyber Security Control Evaluation & Configuration	» Security Control Assessment	
» Threat Data Collection & Amalgamation	» Log Analysis & Collection	
» Threat Log Parsing & Maintenance	» Threat Log Parsing & Maintenance	
» Incident Escalation Reporting	» Performing Network Packet Analysis	
» Change Implementation Escalation		

DAY 4

LESSON	LAB	ASSOCIATED TOPICS
» Defined Response Plan Execution	» Incident Detection & Identification	» Respond
» Network Isolation	» Remove Trojan	
» Disable User Accounts	» Block Incoming Traffic on Known Port	
» Blocking Traffic	» Implement Single-System Changes in Firewall	
» Documentation	» Conduct Supplemental Monitoring	
» Incident Report	» Create Custom Snort Rules	

DAY 5

LESSON	LAB	ASSOCIATED TOPICS
» Industry Best Practices	» Comprehensive Lab Response	» Recover
» Disaster Recovery & BC Plans	» Patches & Updates	
» Cyber System Restoration	» Data Backup & Recovery	
» Data Backup & Restoration Key Concepts	» Recovering Data & Data Integrity Checks	
» Actualizing Data Backups & Recovery	» Post-Incident Service Restoration	
» Implementing Patches & Updates		
» Ensuring Data Integrity		
» Post-Incident Review		

OFFICIAL CYBERSECURITY TRAINING

The Learning Center
Las Vegas

CSX Practitioner
Level 1:
Identify/Protect
Identify

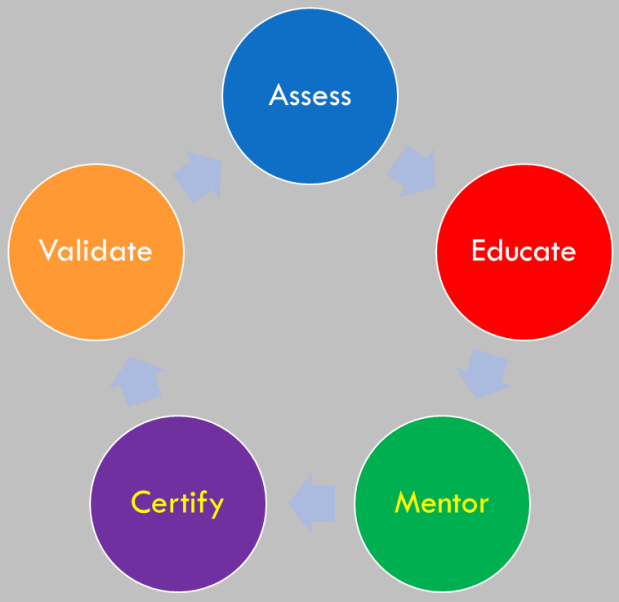
ISACA®
Trust in, and value from, information systems

Course Description:

Identify/Protect provides individuals newly initiated to Incident Response (IR) an introductory experience in the theoretical concepts and practical applications of cyber security. Through multiple lab-reinforced courses, students gain a hands-on education in identifying key networks of responsibility and implementing applicable protection mechanisms.

Uniquely crafted by ISACA® for individuals with little to no previous experience in cyber security, students are provided the optimal experiential environment that includes traditional classroom education, with an emphasis on practical lab exercises. The goal is to begin the student transformation process from novice to valuable team member in corporate or government IR groups.

The Learning Center Model:



Our unique model follows a streamlined approach to workforce development and skills attainment:

Assess

Assess each individual and teams to determine existing skill sets

Educate

Deliver goal specific training utilizing all delivery modalities

Mentor

Expose students to instructor/mentors with front-line cyber/IT experience

Certify

Certify students with the requisite hands-on skills to perform the tasks related to their functional roles

Validate

Validate students "abilities" through performance analytics and real-world exercises hosted on a cyber range

OFFICIAL CYBERSECURITY TRAINING

The Learning Center Las Vegas

DAY 1

LESSON	LAB	ASSOCIATED TOPICS
» Network Reconnaissance	» Network Reconnaissance	» C.I.A. » Active / Passive Scanning » Availability / Authenticity » Asset Classification » Network Devices » OSI Model
» Software / Hardware Scanning	» Network and System Scanning	
» Asset Validation / Anomaly Assessment		
» Network Mapping	» Network Topology Generation	

DAY 2

LESSON	LAB	ASSOCIATED TOPICS
» Introduction to Vulnerability Scanning		» Scanning, Enumeration, Penetration Testing, » Fingerprinting
» Vulnerability Scanning Preparation / Configuration	» Vulnerability Scanner Differentiation / Configuration	
» Asset Validation / Anomaly Assessment	» Vulnerability Scanning	
» Vulnerability Scan Assessment / Evaluation	» Vulnerability Scanner Log Evaluation	

DAY 3

LESSON	LAB	ASSOCIATED TOPICS
» Cybersecurity Control Introduction and Explanation	» Network Reconnaissance	» Cryptographic Controls » NSIT / ISO Documentation » Network / Host Prevention Systems » Internal Log Processes » External Documentation
» Cybersecurity Control Evaluation and Configuration	» Security Control Assessment	
» Threat Data Collection and Amalgamation	» Log Analysis and Collection	
» Threat Log Parsing and Maintenance	» Threat Log Parsing and Maintenance	

DAY 4

LESSON	LAB	ASSOCIATED TOPICS
» Control Vulnerability Scanning and Assessment	» IDS Installation, Configuration, Implementation	» Host Logs » Activity Logs » Network Logs » Firewall Logs » IDS Logs » Encryption
» Control Monitoring and Assessment	» IDS Control Testing	
» Control Change Implementation	» IDS Control Reconfiguration	
» Control Documentation Maintenance		

DAY 5

LESSON	LAB	ASSOCIATED TOPICS
» Control Patch Implementation / Dissemination	» IDS Patching	» Non-repudiation » Multiple Factor Authentication » Information Classification » File System Access Control Mechanisms » Mobile Device Management Policy » Remote Access Solutions

OFFICIAL CYBERSECURITY TRAINING

The Learning Center Las Vegas

CSX Practitioner

Level 1: Detect

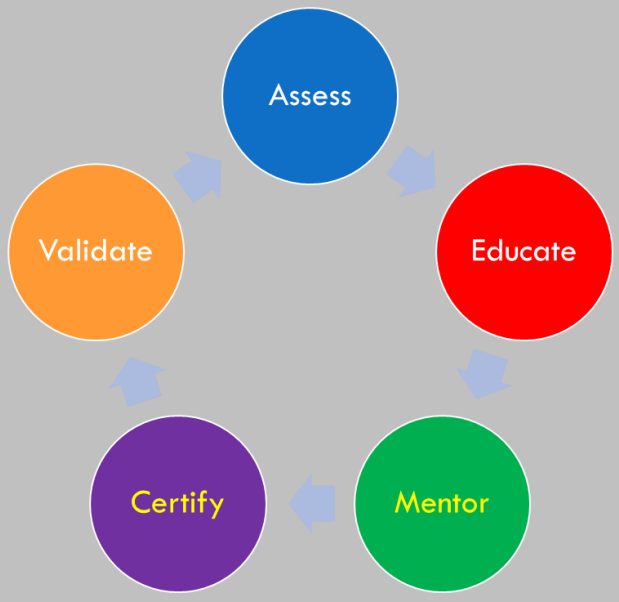
Identify

Course Description:

Detect continues providing individuals newly initiated to IR an introductory experience in the theoretical concepts and practical applications of cyber security. Through multiple lab-reinforced courses, students gain a hands-on education in the detection of potential events and incidents that occur on their networks of responsibility.

Uniquely crafted by ISACA® for individuals with little to no previous experience in cyber security, students are provided the optimal experiential environment that includes traditional classroom education, with an emphasis on practical lab exercises. The goal is to begin the student transformation process from novice to valuable team member in cor-

The Learning Center Model:



Our unique model follows a streamlined approach to workforce development and skills attainment:

Assess

Assess each individual and teams to determine existing skill sets

Educate

Deliver goal specific training utilizing all delivery modalities

Mentor

Expose students to instructor/mentors with front-line cyber/IT experience

Certify

Certify students with the requisite hands-on skills to perform the tasks related to their functional roles

Validate

Validate students "abilities" through performance analytics and real-world exercises hosted on a cyber range

OFFICIAL CYBERSECURITY TRAINING

The Learning Center Las Vegas

DAY 1

LESSON	LAB	ASSOCIATED TOPICS
» Network Reconnaissance	» Network Reconnaissance	» Traffic Flow Analysis » IR Resources
» Software / Hardware Scanning	» Network and System Scanning	
» Asset Validation / Anomaly Assessment		
» Network Mapping	» Network Topology Generation	

DAY 2

LESSON	LAB	ASSOCIATED TOPICS
» Introduction to Vulnerability Scanning		» Scanning, Enumeration, Penetration Testing, » Fingerprinting
» Vulnerability Scanning Preparation / Configuration	» Vulnerability Scanner Differentiation / Configuration	
» Asset Validation / Anomaly Assessment	» Vulnerability Scanning	
» Vulnerability Scan Assessment / Evaluation	» Vulnerability Scanner Log Evaluation	

DAY 3

LESSON	LAB	ASSOCIATED TOPICS
» Cybersecurity Control Introduction and Explanation	» Network Reconnaissance	» Cryptographic Controls » NSIT / ISO Documentation » Network / Host Prevention Systems » Internal Log Processes » External Documentation
» Cybersecurity Control Evaluation and Configuration	» Security Control Assessment	
» Threat Data Collection and Amalgamation	» Log Analysis and Collection	
» Threat Log Parsing and Maintenance	» Threat Log Parsing and Maintenance	

DAY 4

LESSON	LAB	ASSOCIATED TOPICS
» Control Vulnerability Scanning and Assessment	» IDS Installation, Configuration, Implementation	» Host Logs » Activity Logs » Network Logs » Firewall Logs » IDS Logs » Encryption
» Control Monitoring and Assessment	» IDS Control Testing	
» Control Change Implementation	» IDS Control Reconfiguration	
» Control Documentation Maintenance		

DAY 5

LESSON	LAB	ASSOCIATED TOPICS
» Control Patch Implementation / Dissemination	» IDS Patching	» Non-repudiation » Multiple Factor Authentication » Information Classification » File System Access Control Mechanisms » Mobile Device Management Policy » Remote Access Solutions

TARGET AUDIENCE

Individuals new to the field of cyber security who are expected to perform basic to intermediate IR tasks

OBJECTIVE

Equip students with fundamental understanding of issues faced by cyber security professionals in the Detect domain

OFFICIAL CYBERSECURITY TRAINING

The Learning Center Las Vegas

CSX Practitioner

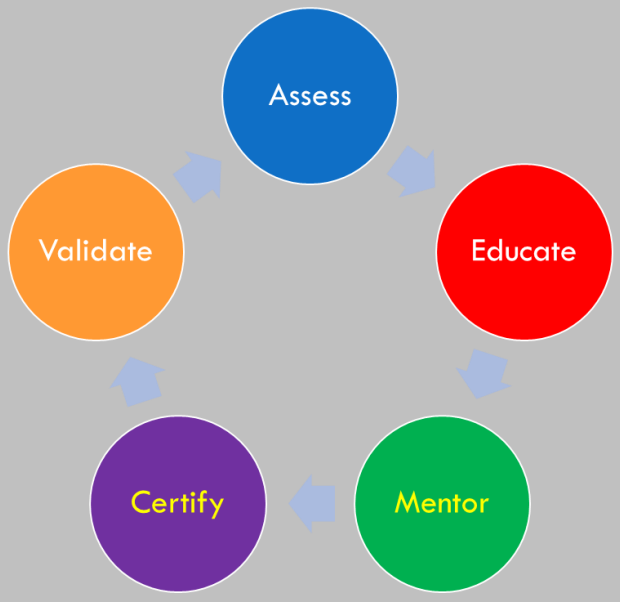
Level 1:

Respond/Recover

Course Description:

Respond/Recover continues providing individuals newly initiated to IR an introductory experience in the theoretical concepts and practical applications of cyber security with a focus on tasks and responsibilities found in the Respond and Recover domains. Through multiple lab-reinforced courses, students gain a hands-on education in incident and disaster response and recovery when occurring on a network of responsibility. Uniquely crafted by ISACA® for individuals with little to no previous experience in cyber security, students are provided the optimal experiential environment that includes traditional classroom education, with an emphasis on practical lab exercises. The goal is to begin the student transformation process from novice to valuable team member in corporate or government IR groups.

The Learning Center Model:



Our unique model follows a streamlined approach to workforce development and skills attainment:

Assess

Assess each individual and teams to determine existing skill sets

Educate

Deliver goal specific training utilizing all delivery modalities

Mentor

Expose students to instructor/mentors with front-line cyber/IT experience

Certify

Certify students with the requisite hands-on skills to perform the tasks related to their functional roles

Validate

Validate students "abilities" through performance analytics and real-world exercises hosted on a cyber range

OFFICIAL CYBERSECURITY TRAINING

The Learning Center
Las Vegas

DAY 1

LESSON	LAB	ASSOCIATED TOPICS
» IRP Execution	» IRP Component Assessment	» IR Reputation Databases
» System Containment Response	» Compromised Assets Containment	» IR Procedure
» Asset Quarantine	» Compromised Assets Quarantine	» Real Time Blacklists, Whitelists
» Network Mapping	» Network Topology Generation	

DAY 2

LESSON	LAB	ASSOCIATED TOPICS
» Incident Response Documentation	» Incident Response Component Identification	» IR Procedure
» Incident Response Protocol Procedure	» Incident Response Procedure identification	» IR Drafting
» Incident Response Drafting	» Incident Response Draft Generation	» IR Framework

DAY 3

LESSON	LAB	ASSOCIATED TOPICS
» DRP / BCP Task Identification		» Business Unit Integration
» System Restore Processes	» System Restoration	» Third-Party Connection Mechanisms
» Site Configuration		» Warm Site / Cold Site Configurations
» System Backup	» System Backup Procedure	» Data Preservation

DAY 4

LESSON	LAB	ASSOCIATED TOPICS
» System Restoration		» Host Logs
» Network Backup Procedures	» Network Backup Procedures	» Activity Logs
» Data Integrity Check	» Integrity check Process	» Network Logs
» Procedures / Documentation		» Firewall Logs
		» IDS Logs
		» Encryption

DAY 5

LESSON	LAB	ASSOCIATED TOPICS
» Post-Incident Review Process	» After-Action Report Generation	» NIST Procedures
		» ISO Procedures
		» Team Input
		» AAR Generation

TARGET AUDIENCE

Individuals new to the field of cyber security who are expected to perform basic to intermediate IR tasks

OBJECTIVE

quip students with fundamental understanding of issues faced by cyber security professionals in the Respond & Recover domains

OFFICIAL CYBERSECURITY TRAINING

The Learning Center Las Vegas

CISA
Certified Information Systems Auditor

ISACA

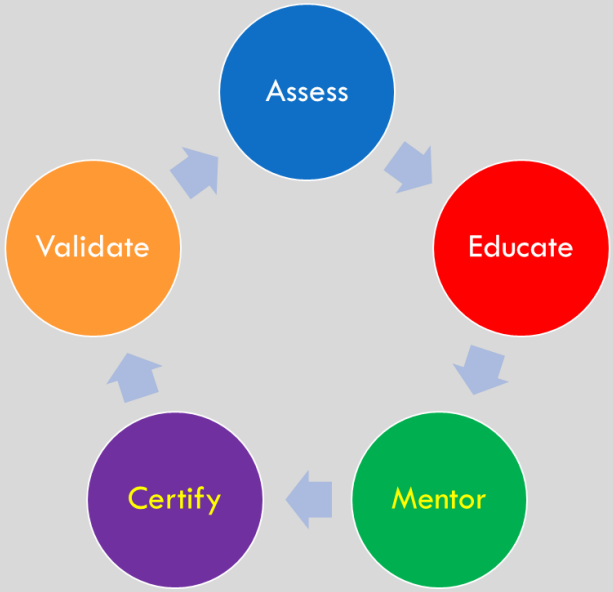
CISA

Certified Information Systems Auditor

Course Description:

Students will perform evaluations of organizational policies, procedures, and processes to ensure that an organization's information systems align with overall business goals and objectives. You will evaluate the security and controls of business structure and governance methods; the policies, procedures, and guidelines used; and the overall security of the business environment. Also, this course will help you prepare for the ISACA® CISA® certification exam.

The Learning Center Model:



Our unique model follows a streamlined approach to work-force development and skills attainment:

Assess

Assess each individual and teams to determine existing skill sets

Educate

Deliver goal specific training utilizing all delivery modalities

Mentor

Expose students to instructor/mentors with front-line cyber/IT experience

Certify

Certify students with the requisite hands-on skills to perform the tasks related to their functional roles

Validate

Validate students "abilities" through performance analytics and real-world exercises hosted on a cyber range

OFFICIAL CYBERSECURITY TRAINING

The Learning Center

1. The Information Systems Audit Process

- ISACA Information Systems Auditing Standards and Guidelines
- Develop and Implement an Information Systems Audit Strategy
- Plan an Audit
- Conduct an Audit
- The Evidence Lifecycle
- Communicate Issues, Risks, and Audit Results
- Support the Implementation of Risk Management and Control Practices

2. IT Governance

- Evaluate the Effectiveness of IT Governance
- Evaluate the IT Organizational Structure
- Evaluate the IT Strategy
- Evaluate IT Policies, Standards, and Procedures for Compliance
- Ensure Organizational Compliance
- IT Resource Investment, Use, and Allocation Practices
- Evaluate IT Contracting Strategies and Policies
- Evaluate Risk Management Practices
- Performance Monitoring and Assurance Practices

3. Systems and Infrastructure Lifecycle Management

- Determine the Business Case for Change
- Evaluate Project Management Frameworks and Governance Practices
- Perform Periodic Project Reviews
- Evaluate Control Mechanisms for Systems
- Evaluate Development and Testing Processes
- Evaluate Implementation Readiness
- Evaluate a System Migration

4. Systems and Infrastructure Lifecycle Maintenance

- Perform a Post-Implementation System Review
- Perform Periodic System Reviews
- Evaluate the Maintenance Process
- Evaluate the Disposal Process

5. IT Service Delivery and Support

- Evaluate Service Level Management Practices
- Evaluate Operations Management
- Evaluate Data Administration Practices
- Evaluate the Use of Capacity and Performance Monitoring Methods
- Evaluate Change, Configuration, and Release Management Practices
- Evaluate Problem and Incident Management Practices
- Evaluate the Functionality of the IT Infrastructure

6. Protection of Information Assets

- Information Security Design
- Encryption Basics
- Evaluate the Design, Implementation, and Monitoring of Logical Access Controls
- Evaluate the Design, Implementation, and Monitoring of Physical Access Controls
- Evaluate the Design, Implementation, and Monitoring of Environmental Controls
- Evaluate Network Infrastructure Security
- Evaluate the Confidential Information Processes and Procedures

7. Business Continuity and Disaster Recovery

- Evaluate the Adequacy of Backup and Restore
- Evaluate the BCP and DRP

CISA

Certified Information Systems Auditor

OFFICIAL CYBERSECURITY TRAINING

The Learning Center
Las Vegas

CISM
Certified Information Security Manager

ISACA

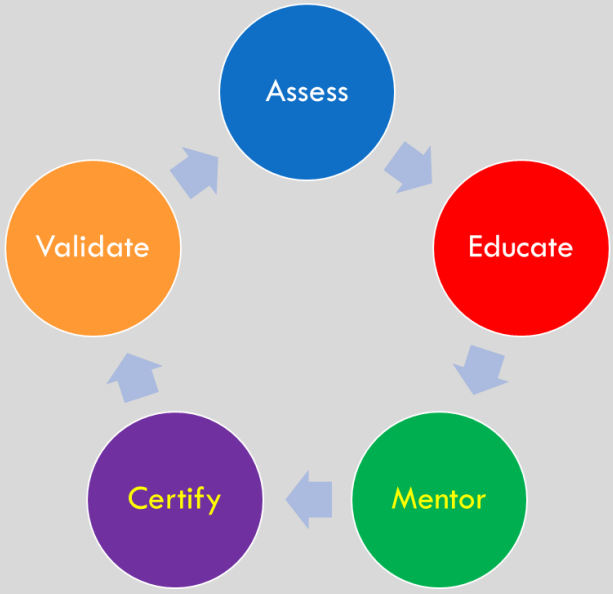
CISM

Certified Information Systems Manager

Course Description:

CISM certification program was developed by the Information Systems Audit and Control Association (ISACA) for experienced Information security management professionals with work experience in developing and managing information security programs and who understand the programs relationship with the overall business goals. The CISM exam is offered three times a year (June, September, and December), consisting of 200 multiple-choice questions that cover the four CISM domains. The American National Standards Institute (ANSI) has accredited the CISM certification program under ISO/IEC 17024:2003, General Requirements for Bodies Operating Certification Systems of Persons.

The Learning Center Model:



Our unique model follows a streamlined approach to workforce development and skills attainment:

Assess

Assess each individual and teams to determine existing skill sets

Educate

Deliver goal specific training utilizing all delivery modalities

Mentor

Expose students to instructor/mentors with front-line cyber/IT experience

Certify

Certify students with the requisite hands-on skills to perform the tasks related to their functional roles

Validate

Validate students "abilities" through performance analytics and real-world exercises hosted on a cyber range

OFFICIAL CYBERSECURITY TRAINING

The Learning Center
Las Vegas

1. Testing-Taking Tips and Study Techniques

- Preparation for the CISM exam
- Submitting Required Paperwork
- Resources and Study Aids
- Passing the Exam the First Time

2. Information Security Governance

- Asset Identification
- Risk Assessment
- Vulnerability Assessments
- Asset Management

3. Information Risk Management

- Asset Classification and Ownership
- Structured Information Risk Assessment Process
- Business Impact Assessments
- Change Management

4. Information Security Program Development

- Information Security Strategy
- Program Alignment of Other Assurance Functions
- Development of Information Security Architectures
- Security Awareness, Training, and Education
- Communication and Maintenance of Standards, Procedures, and Other Documentation
- Change Control
- Lifecycle Activities
- Security Metrics

5. Information Security Program Management

- Security Program Management Overview
- Planning
- Security Baselines
- Business Processes
- Security Program Infrastructure
- Lifecycle Methodologies
- Security Impact on Users
- Accountability
- Security Metrics
- Managing Resources

6. Incident Management and Response

- Response Management Overview
- Importance of Response Management
- Performing a Business Impact Analysis
- Developing Response and Recovery Plans
- The Incident Response Process
- Implementing Response and Recovery Plans
- Response Documentation
- Post-Event Reviews

CISM®
Certified Information Security Manager®

OFFICIAL CYBERSECURITY TRAINING

The Learning Center
Las Vegas

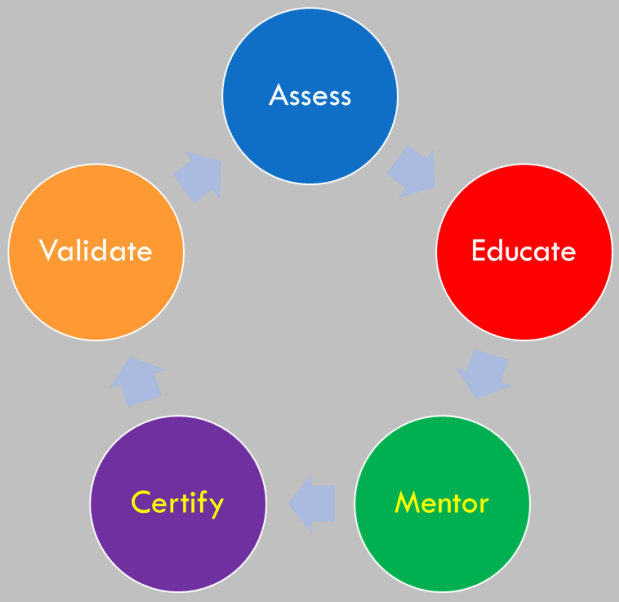
Fundamentals of Malware Analysis

Course Description:

Fundamentals of Malware Analysis is an introductory course that exposes students to the theoretical knowledge and hands-on techniques for analyzing malware.

Students will learn how to identify and analyze software that causes harm to users, computers and networks as part of an overall cyber defense and incident response plan. Understanding how malware works and what it was designed to do is crucial to thwarting future attacks.

The Learning Center Model:



Our unique model follows a streamlined approach to workforce development and skills attainment:

Assess

Assess each individual and teams to determine existing skill sets

Educate

Deliver goal specific training utilizing all delivery modalities

Mentor

Expose students to instructor/mentors with front-line cyber/IT experience

Certify

Certify students with the requisite hands-on skills to perform the tasks related to their functional roles

Validate

Validate students "abilities" through performance analytics and real-world exercises hosted on a cyber range

OFFICIAL CYBERSECURITY TRAINING

The Learning Center
Las Vegas

DAY 1

Introduction to the overall malware analysis process and methodology. Students define terminology, learn specific malware types and cover fundamental approaches of analysis, in addition to learning how to effectively analyze program code/structure to determine function. Students are challenged with three labs.

Day 1 ends with a detailed overview of setting up and using a safe virtual environment for malware analysis.

Topics List

- Malware analysis techniques
- Identification via antivirus tools and hashing
- Analyzing strings, functions, and headers
- Use a variety of virtual machines, settings and configurations

DAY 2

Day 2 focuses on easy-to-use techniques to dynamically analyze malicious programs by running them in a lab. Students learn to observe true behavior of malware and determine its purpose and functionality via live demos and three challenging specimens they must analyze.

Day 2 centers around how malware interacts with the victim's OS by looking at network activity, registry changes and interactions with the file system.

Topics List

- Use of Procmon, Process Explorer and Regshot to understand malicious behavior
- Fake network services to aid analysis
- Traffic analysis
- Network connections
- X86 architecture

DAY 3

Day 3 closes behavioral analysis and ends with a final fourth lab.

Students then begin X86 assembly language. This module is crucial for learning follow-on analysis techniques using debuggers and disassemblers. Students learn key concepts in assembly language to assist follow-on analysis with IDA Pro. IDA Pro is introduced as a disassembler and reverse engineering tool.

Considerable time is spent on familiarization with the UI and IDA's numerous features. Plenty of code snippets, demos and two IDA familiarization labs help the student understand both assembly language and how to use IDA Pro.

Topics List

- Stack vs. Heap
- Registers, flags & basic instructions
- Conditionals, flow control instructions & jumps
- IDA Pro UI intro
- Disassembly window (Text vs. Graph Mode)
- Jumping to memory addresses

DAY 4

IDA Pro Introductions continues on Day 4 with the identification and analysis of more complex functions. Students are gradually exposed to more complex malware and its disassembly to build confidence and skills. Students learn techniques needed to identify, categorize and analyze high-level functionality of assembly code. Two labs challenge students to identify a variety of C code constructs in malware specimens as part of an overarching analysis strategy.

Topics List

- Cross-references in code
- Function identification, analysis & renaming
- Imports, exports & structs
- Searching through disassembly
- Code & data redefinition
- Deeper function analysis

DAY 5

Students spend their final day analyzing two malicious programs to further solidify analysis skills focusing on the identification of C code constructs in assembly, and how these high-level constructs correlate to other aspects of the program and its behavior. An instructor-led review of all major topics will be conducted and any final questions will be answered.

After the course, students have 90 days to challenge the optional CYBRScore-enabled certification associated with MAL400. The certification presents a malware specimen to the challenger that must be analyzed using the techniques and tools learned in this course. Our behind-the-scenes scoring engine will track progress throughout against a rubric of core skills that must be demonstrated in the hands-on analysis.

TARGET AUDIENCE

New malware analysts looking to increase their arsenal of techniques, or others looking to break into the malware analysis field

OBJECTIVE

To obtain the basic skills needed for the identification and analysis of software that causes harm to users, computers and networks

OFFICIAL CYBERSECURITY TRAINING

The Learning Center Las Vegas

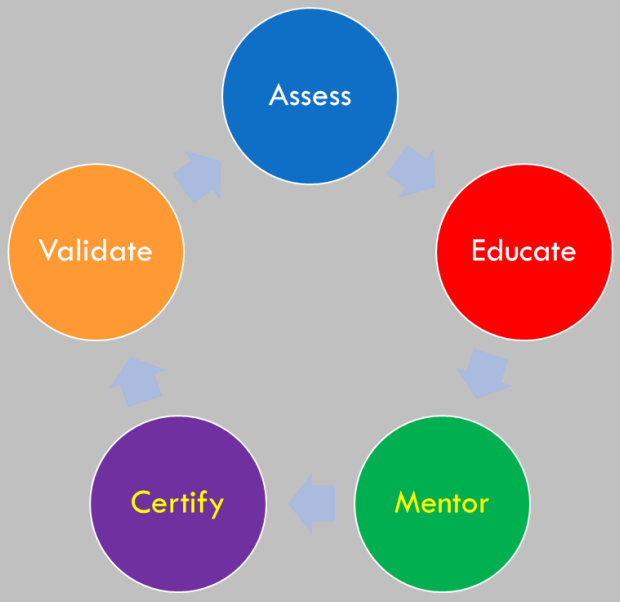
Reverse Engineering Malware

Course Description:

Reverse Engineering Malware is an intermediate course that exposes students to the theoretical knowledge and hands-on techniques to analyze malware of greater complexity.

Students will learn to analyze malicious Windows programs, debug user-mode and kernel-mode malware with WinDbg, identify common malware functionality, in addition to reversing covert and encoded malware.

The Learning Center Model:



Our unique model follows a streamlined approach to workforce development and skills attainment:

Assess

Assess each individual and teams to determine existing skill sets

Educate

Deliver goal specific training utilizing all delivery modalities

Mentor

Expose students to instructor/mentors with front-line cyber/IT experience

Certify

Certify students with the requisite hands-on skills to perform the tasks related to their functional roles

Validate

Validate students "abilities" through performance analytics and real-world exercises hosted on a cyber range

OFFICIAL CYBERSECURITY TRAINING

The Learning Center
Las Vegas

DAY 1

Malware targeting Windows victims is prolific, and understanding how this malware interacts with the complex Windows operating system and API is a challenge not to be taken lightly.

In the first part of this course, students dive straight into Windows API and its myriad functions, inputs, and outputs as they relate to reverse engineering malware targeted against Windows victims. Networking APIs, as well as threads and mutexes are examined in-depth. The day is spent trying to solve the Gordian knot that is Windows malware.

Topics List

- Windows API
- Handles & file system functions
- Common registry functions & autoruns
- Networking APIs
- Processes, threads & mutexes
- COM objects

DAY 2

Being able to debug a program is crucial to reverse engineering and malware analysis. On Day 2 students are introduced to the concept of debugging and extensively exposed to OllyDbg, its functionality, tools and plugins. Breakpoints, and tracing are used as part of the overall reversing process to unravel complex malware specimens.

Topics List

- Kernel vs. User-mode debugging
- Software & hardware breakpoints
- Modifying program execution & patching
- OllyDbg overview
- Memory maps
- Executing code, breakpoints & tracing
- OllyDbg plugins

DAY 3

On Day 3, students are introduced to the broad and complex topic of kernel debugging. This includes core principles of this interesting sub-topic, as well as a demonstration of how to configure an environment, analyze kernel objects, and look at rootkits. Day 3 closes with the discovering and reversing of a variety of malicious functionality malware executes across several labs.

Topics List

- Kernel debugging with WinDbg
- Configuring kernel debugging environment
- Analyzing functions, structures and driver objects
- Rootkit analysis
- Downloaders, launchers & backdoors
- Analyzing various persistence mechanisms & user-mode rootkits

DAY 4

Day 4 switches gears and delves into the complex world of covert malware. Students learn about a variety of techniques malware uses to hide its activities, and how to identify indicators of this type of activity. Process injection, hooks, and detours are looked at as part of this interesting module of the course.

Topics List

- Covert malware
- Abusing resource section of PE file
- Process injection & process replacement
- Windows hooks & detours
- APC injection from kernel space

DAY 5

On the final day of class, students learn how malware authors use a variety of encoding mechanisms to obfuscate data, and how to analyze them. XOR, BASE64 and custom encoding mechanisms are explored and analyzed.

After the course, students have 90 days to challenge the optional CYBRScore-enabled certification associated with MAL400. The certification presents a malware specimen to the challenger that must be analyzed using the techniques and tools learned in this course. Our behind-the-scenes scoring engine will track progress throughout against a rubric of core skills that must be demonstrated in the hands-on analysis.

Topics List

- Analyzing encoding algorithms
- XOR, BASE64 & custom encoding
- Common crypto algorithms
- KANAL
- Custom decoding scripts in Python
- Instrumentation for generic decryption

TARGET AUDIENCE

Junior malware analysts and reverse engineers who want to increase their skills to better understand more complex malicious code

OBJECTIVE

Provide students with a working knowledge of analyzing malicious Windows programs, debugging user-mode & kernel-mode malware, identifying common malware functionality, & other related topics

OFFICIAL CYBERSECURITY TRAINING

The Learning Center Las Vegas

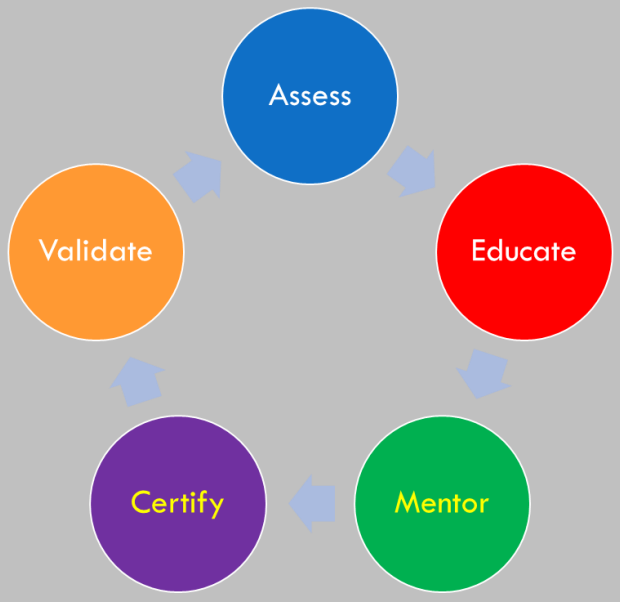
Advanced Malware Analysis

Course Description:

Advanced Malware Analysis is an advanced course that exposes students to the theoretical knowledge and hands-on techniques to reverse engineer malware designed to thwart common reverse engineering techniques.

Students will learn how to identify and analyze the presence of advanced packers, polymorphic malware, encrypted malware, and malicious code that has been armored with cryptors, anti-debugging and anti-reverse engineering.

The Learning Center Model:



Our unique model follows a streamlined approach to work-force development and skills attainment:

Assess

Assess each individual and teams to determine existing skill sets

Educate

Deliver goal specific training utilizing all delivery modalities

Mentor

Expose students to instructor/mentors with front-line cyber/IT experience

Certify

Certify students with the requisite hands-on skills to perform the tasks related to their functional roles

Validate

Validate students "abilities" through performance analytics and real-world exercises hosted on a cyber range

OFFICIAL CYBERSECURITY TRAINING

The Learning Center
Las Vegas

DAY 1

The course begins by examining a variety of network signatures associated with malware. Understanding the networking aspect is important because malware almost always uses network connectivity to infect, persist, receive command and control instructions, and exfiltrate data.

Students are asked to spend a significant amount of time reversing malicious command and control structure parsing routines to better understand the overall network activity, and how to identify and stop it.

Topics List

- Indications of malware activity
- Network countermeasures
- Snort & complex signatures
- Hiding in the noise by mimicking existing protocols
- Client initiated beacons
- Networking code & encoding data
- Networking from an attacker's perspective

DAY 2

Day 2 focuses on anti-disassembly techniques employed by malware authors to thwart analysis. Students learn about various techniques, like jump instructions with the same target, jump instructions with a constant condition and more. More complex techniques like return pointer abuse and misusing structured exception handlers give the student new conceptual knowledge.

This knowledge will help complete three complex hands-on challenges: identifying false conditional branches, improperly disassembled code, and return pointer abuse.

Topics List

- Defeating disassembly algorithms
- Same target jumps & constant condition jumps
- Rogue opcodes
- Multi-level inward jumping sequences
- Patching binaries to defeat return pointer abuse
- SEH abuse
- Reversing armored code designed to thwart stack frame analysis

DAY 3

Anti-debugging is used by malware authors to determine when their malware is under the control of a debugger or to thwart debugging efforts. On Day 3 students learn how Windows API can be used to detect debugger use, and how malware manually checks structs. Checking the ProcessHeap and NTGlobal flags is reviewed, as well as how some malware checks the analysis system for debugging tool residue in the registry.

The module concludes with a discussion of TLS callbacks, and exceptions to disrupt debugger use.

Topics List

- Using Windows API functions to detect debuggers
- PEB checks, ProcessHeap flag & NTGlobal flag
- TLS Callbacks
- Exceptions and Interrupts
- PE Header vulnerabilities
- OutputDebugString vulnerability

DAY 4

Although the presence of anti-virtual machine techniques seems to be declining, Day 4 is spent discussing how to identify various methods used by malware authors.

Students also learn how to manually unpack malware by finding tail jumps, the original entry point (OEP) and rebuilding Import Address Tables (IAT).

Topics List

- Anti-VM techniques & memory artifacts
- Red pill & no pill techniques
- Unpacking stub, tail jump, OEP & import resolution
- Manual IAT rebuilds
- Tips & tricks for dealing with several common packers

DAY 5

On the final day of class, students learn how to identify and reverse C++ code, in addition to conducting shellcode analysis. Virtual functions and the concept of polymorphism are discussed to prepare students to identify and reverse vtables using their cross references.

Position-independent shellcode is examined, as well as how to identify execution location. Day 5 ends with a look at 64-bit malware and the challenges analysts face when reversing this type of code.

Topics List

- Shellcode analysis, position independent-code & call/pop
- Shellcode use of LoadLibraryA & GetProcAddress for dynamic function location
- C++ Analysis
- Overloading functions, mangling and vtables
- Challenges of identifying inheritance between classes
- 64-bit malware, general-purpose & special-purpose registers
- X64 calling convention & exception handling

TARGET AUDIENCE

Mid-level malware analysts & reverse engineers, as well as programmers who want a different professional perspective as a means of better protect their tools & intellectual property

OBJECTIVE

Provide an in-depth understanding of identifying & analyzing the presence of advanced packers, polymorphic malware, encrypted malware & malicious code

OFFICIAL CYBERSECURITY TRAINING

The Learning Center Las Vegas

Pentesting &

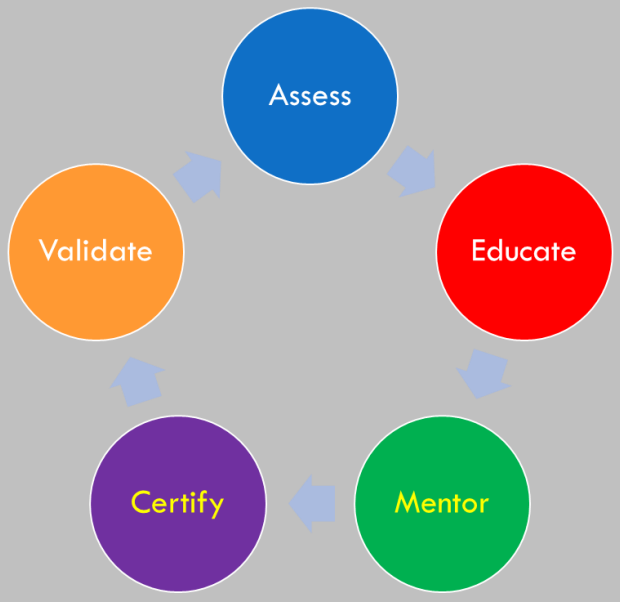
Network Exploitation

Course Description:

Pentesting & Network Exploitation exposes students to all manner of reconnaissance, scanning, enumeration, exploitation and pillaging for 802.3 networks.

Topics expose students to a variety of recon, discovery, scanning, enumeration, exploitation, post-exploitation, pillaging, covering one's tracks and persistence.

The Learning Center Model:



Our unique model follows a streamlined approach to work-force development and skills attainment:

Assess

Assess each individual and teams to determine existing skill sets

Educate

Deliver goal specific training utilizing all delivery modalities

Mentor

Expose students to instructor/mentors with front-line cyber/IT experience

Certify

Certify students with the requisite hands-on skills to perform the tasks related to their functional roles

Validate

Validate students "abilities" through performance analytics and real-world exercises hosted on a cyber range

OFFICIAL CYBERSECURITY TRAINING

The Learning Center Las Vegas

DAY 1

Day 1 introduces students to host target analysis. Topics include Linux command line, bash scripting and simple programming to enumerate, attack and exploit Linux hosts later in the course. Once Linux is complete, students begin learning basic through intermediate Windows Command Line skills, PowerShell cmdlets and the PowerShell attack framework called PowerPreter.

Topics List

- Linux administration tools
- Navigation of *nix file systems
- Bash scripts writing for pentesting engagements
- Python socket program writing to connect to remote server
- Basic C programs in *nix environment compliation and modification
- Windows command line administration tools
- Windows file systems navigation
- PowerShell use for conducting enumeration and analysis of targets
- Nishang and PowerPreter for enumerating, attacking and deploying persistence on targets boxes

DAY 2

Students learn how to conduct basic service scans and exploit vulnerable hosts on internal networks through hands-on challenges that force them to replicate a real-world penetration test. They learn how to map, discover and exploit web applications, which requires the tester to understand how they communicate and the role the server plays in the relationship. Students learn how to conduct reconnaissance against a web server, followed by mapping its architecture. They're also challenged with discovering vulnerabilities and misconfigurations for follow-on exploitation.

Topics List

- Discovering live hosts
- Scaning hosts to find vulnerabilities and misconfigurations with Nmap and manual techniques
- Determination of which ports are open and what services are running
- Use of Metasploit to scan and database target information
- Choosing exploit and payload for target host
- Use of various post-exploitation Meterpreter scripts to steal information from victim
- How web applications operate
- How HTTP operates
- Headers and session management techniques
- Authentication and post-authentication role assignment
- OWASP Top 10
- Web app recon, mapping, discovery and exploitation process
- Differentiation of URI, URL and URN
- Differences between server-side and client-side code
- Nikto for discovery of web app vulnerabilities and misconfigurations
- Code snippet analysis (HTML, PHP, JavaScript, JSON Arrays, AJAX, etc.)
- Manual SQL injection and XSS scripting attack techniques

DAY 3

Students learn how to simulate an insider threat and escape restricted environments by abusing native services and functionality. Students then move to routed attacks against clients that have NAT devices, firewalls and DMZs deployed. They learn how to exploit a variety of web-facing services and gain access to the DMZ. Once in the DMZ they are asked to pillage the hosts and find additional information to assist in pivoting deeper into the network and into network segments that don't touch the web directly.

Topics List

- Escaping restricted Windows desktop environments
- Spawning unauthorized browsers for Internet access
- Enumerating firewalls and web-facing services with Nmap, Nikto and Dirbuster
- Burp Suite to proxy web application traffic to and from victim web server
- Accessing demilitarized zone
- Pillaging hosts to find additional information
- Moving files onto victim boxes using Netcat and Meterpreter
- Stealing files from victim boxes using Netcat and Meterpreter

DAY 4

On Day 4 students learn how to create and host malicious binaries on their own webserver to facilitate network penetration with purpose-built shellcode. Building on techniques and access gained into the DMZ, students are challenged to burrow further into the victims network by adding routes and pivoting into internal network segments by exploiting additional victims. Having exploited a variety of hosts throughout the network deploying persistence is then taught to maintain hard earned access.

Topics List

- Using MSFvenom to create purpose-built binaries with a variety of payloads
- Hosting malware on web server for easy delivery to victims
- Adding routes to additional network segments to facilitate pivoting
- Using post-exploitation Meterpreter tools to pillage various hosts
- Deploying Visual Basic Script for persistence on various victims
- Modifying persistence mechanism to survive reboot

DAY 5

Day 5 deals exclusively with hands-on challenges. Using all the skills, techniques and tools learned during the previous four days to lay waste to the company's network and computers, students will be tasked with owning "the CEO's" computer, and stealing as much sensitive information from the notional corporation as possible. The company's computers contain a wide variety of PII, corporate information and intellectual property for the taking. Can they own the CEO's box? Can they gain access to and modify the company's firewall settings?

Topics List

- Obtaining sensitive, non-public information from the company's computer
- Modifying the company's firewall settings
- Pwning the CEO's computer

TARGET AUDIENCE

Penetration testers looking to broaden their overall penetration testing skill set, network engineers, system administrators, developers

OBJECTIVE

Provide in-depth exposure and hands-on practice with all facets of 802.3 hacking, vulnerability research, pivoting, exploitation, password/hash cracking, post-exploitation pillaging and methods of setting up persistence on a victim's network

OFFICIAL CYBERSECURITY TRAINING

The Learning Center Las Vegas

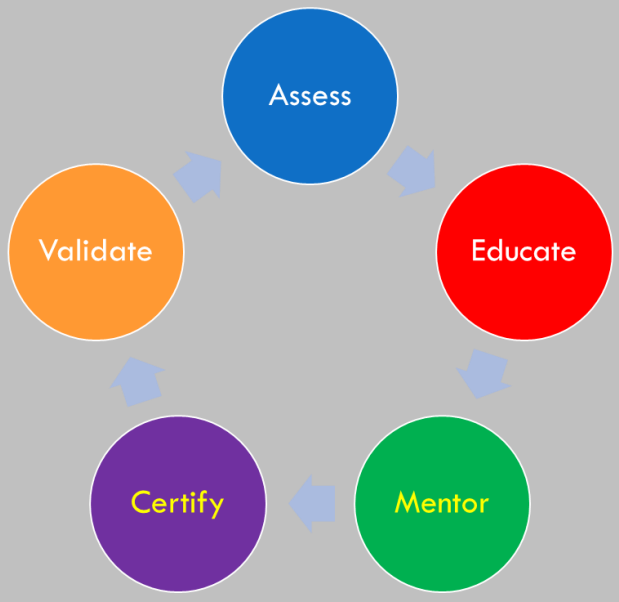
Wireless Pentesting & Network Exploitation

Course Description:

Wireless Pentesting and Network Exploitation introduces students to all manner of reconnaissance, scanning, enumeration, exploitation and reporting for 802.11 networks.

The lab topics expose students to a variety of survey, database creation, scripting, and attack methods that can be used to gain a foothold in to a client's network during a penetration test.

The Learning Center Model:



Our unique model follows a streamlined approach to work-force development and skills attainment:

Assess

Assess each individual and teams to determine existing skill sets

Educate

Deliver goal specific training utilizing all delivery modalities

Mentor

Expose students to instructor/mentors with front-line cyber/IT experience

Certify

Certify students with the requisite hands-on skills to perform the tasks related to their functional roles

Validate

Validate students "abilities" through performance analytics and real-world exercises hosted on a cyber range

OFFICIAL CYBERSECURITY TRAINING

The Learning Center
Las Vegas

DAY 1

Students will learn how to conduct wireless penetration tests using open source tools against 802.11 a/b/g/n networks. In addition, students will identify characteristics and common vulnerabilities associated with WiFi.

Topics List

- Scoping and Planning WiFi Penetration Tests
- 802.11 Protocols and Standards
- Authentication vs Association
- WiFi Security Solutions
- WiFi Hacking Hardware
- Connectors and Drivers
- Recon and Custom Password Generation with Cupp and CeWL

DAY 2

Students will learn to use open source tools and hardware to conduct both mobile and static 802.11 a/b/g/n surveys. Planning and executing surveys will be covered in depth as well as data management and database management techniques.

Topics List

- Conducting Surveys Using Airodump-ng and Kismet
- Creating SQL Databases of Survey Data
- Specialized SQL and AWK Commands to Manipulate Data for Reporting
- Cracking WEP
- Setting Up MAC Filters
- Bypassing MAC Filters

DAY 3

Students continue their use of Kismet and Airodump-ng to conduct mobile surveys, database the information and create .kml files in order to visualize survey data. Students are then exposed to an in-depth discussion on advanced encryption security processes followed by learning how to use open source tools to exploit the security process.

Topics List

- Planning and Conducting Mobile WiFi Survey
- GISKimset to Database Survey Information
- Creating Custom SQL Queries
- AWK Tool to Format Output from SQL Queries for Reporting
- GISKismet to Create .kml Files
- Stream and Block Ciphers, Block Cipher Modes
- WPA2 AES-CCMP Security Process
- Cowpatty to Recover WPA2 Passphrase
- Pyrit to Survey and Attack Encryption
- Databasing and Recovering WPA2 Passphrases

DAY 4

Building on the skills learned in the first three days, the students will learn how to conduct Man-in-the-Middle attack using easy-creds and a fake access point. Students will learn how to conduct various types of attacks, traffic capture, and credential harvesting once a victim connects.

Topics List

- Man-in-the-Middle Attack Theory
- Attacking Preferred Network Lists via Rogue AP
- Easy-Creds to set up Fake AP
- SSLStrip to Conduct Attack Against SSL Traffic
- URLSnarf to Capture Victim HTTP Traffic
- Ettercap to Poison ARP Cache on WiFi Network and Conduct Various Attacks Against Clients
- Custom Ettercap Filters
- Rusty Cobra Tool to Automate WiFi Survey
- Visualization, Database Management and Report File Creation

DAY 5

The last day of the course comprises a full-spectrum WiFi penetration test that the students must scope, plan and conduct. Final exercise serves to replicate a variety of network hardware, services and configurations, target website for recon, with multiple WiFi access points and clients using a variety of security mechanisms as provided.

Capstone Exercise

All the material covered in the course will be put to use in the final exercise.

TARGET AUDIENCE

Penetration testers looking to broaden their overall penetration testing skill set, wireless engineers, system administrators and developers

OBJECTIVE

Provide in-depth exposure to all facets of 802.11 penetration testing, encryption cracking, post-exploitation pillaging and report writing