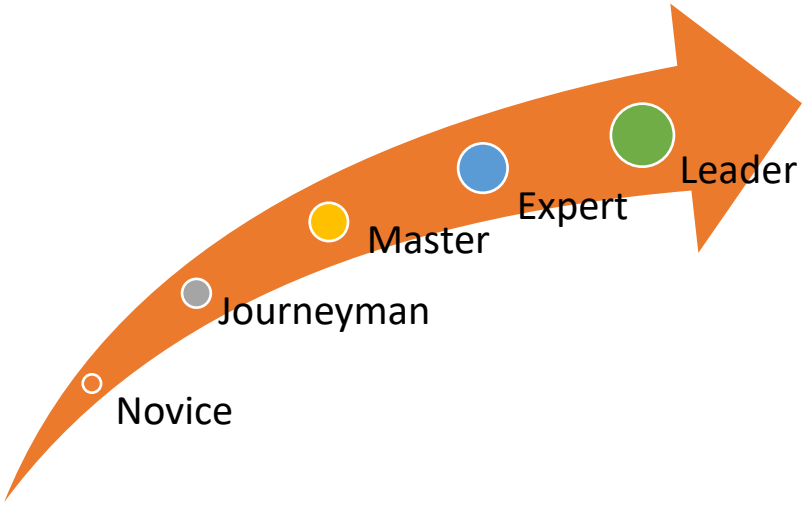
CyberTec® Academy

BOOT CAMP TRAINING CATALOG

2018

Table of Contents

CyberTec® offers world-class globally recognized cybersecurity certification training and skills assessments. Offering a multitude of options that can meet all corporate needs. Our skills training and performance-based assessments provide world-class education & training encompassing the career life-cycle from novice to expert.



Globally Recognized courses that are standardized throughout the world and known for quality and excellence, to include meeting the requirements outlined by all 32 cybersecurity specialty areas. Content aligns to the United States National Cybersecurity Framework categories certifying knowledge, skill, and ability within the following domains:

- Identify
- Protect
- Detect
- Respond
- Recover

Training leverages approved industry recognized certification content, along with experiential learning to develop requisite knowledge, skills, and abilities to ensure clients can perform the tasks required of National Initiative for Cybersecurity Education work roles. Curriculum is conveniently offered via multiple modalities to meet the needs of the corporation:

- Delivered In-Person
- Instructor-Live Online
- On-Demand Distance Learning

Certifications ensure the competence of professionals through a measurement of skills and knowledge. Certification exams go beyond training by providing a measurement of comprehension and expertise. Benefits may include:

- Aids in hiring and promotions
- Keep up with evolving technology and dynamic environment associated with the job
- Validates skills, expertise, and proficiency in a certain area
- Develops knowledge and skills in new and emerging subjects
- Facilitates networking with other IT professionals
- For the individual, it lends credibility and advances career

Specialized Skills Assessments are also available through cutting edge tools that few corporations can provide. Understanding the employees' abilities will allow the corporation to target specific training to an individual's or team's weaknesses. Assessments will aide corporations via:

- Reducing potential liability by ensuring correct talent in place
- Strengthening workforce by developing staff and retaining top talent by measuring competencies
- Individual's skills are that tailored to meet position requirements
- Greater organizational compliance

Globally-Recognized Certifications are a Business Imperative!

Competency is key to cyber-resilience. All business sectors look for individuals with the capability to perform the tasks required of their functional roles. Certifications are aligned to the knowledge, skills, and abilities required of the cybersecurity profession. Competency may facilitate:

- A reduction in the risk associated with a globally-connect economy
- Meet the skills shortage
- Adherence to industry recognized standards and frameworks
- Offers a competitive global advantage
- Individual adaptability in an evolving threat landscape

IT/Cybersecurity Novice (Level One) Courses

CYBR 101) CompTIA A + Certification Bootcamp (48 hours)

CompTIA A+ is a six-day bootcamp. First 3-days is CompTIA A+ 901 covering PC hardware and peripherals, mobile device hardware, networking and troubleshooting hardware and network connectivity issues. The second 3-days is CompTIA A+ 902 covering installing and configuring operating systems including Windows, iOS, Android, Apple OS X and Linux. It also addresses security, the fundamentals of cloud computing and operational procedures.

CTA Staff
Course Delivery: Instructor Live/Hybrid | (meets 6X) |
Training Level: One
Course ID: CYBR 101
Price: $3695 (includes book, exam prep material, certification exam voucher)

(CYBR 102) CompTIA Network + Certification Bootcamp (40 hours)

CompTIA Network+ certification training covers the configuration, management, and troubleshooting of common wired and wireless network devices. Also included are emerging technologies such as unified communications, mobile, cloud, and virtualization technologies.

CTA Staff
Course Delivery: Instructor Live/Hybrid | (meets 5X) |
Training Level: One
Course ID: CYBR 102
Price: $3295 (includes book, exam prep, hands on lab, certification exam voucher)

(CYBR 103) CompTIA Security + Certification Bootcamp (40 hours)

CompTIA Security+ certification training will certify the successful candidate has the knowledge and skills required to install and configure systems to secure applications, networks, and devices; perform threat analysis and respond with appropriate mitigation techniques; participate in risk mitigation activities; and operate with an awareness of applicable policies, laws, and regulations. The successful candidate will perform these tasks to support the principles of confidentiality, integrity, and availability.

CTA Staff
Course Delivery: Instructor Live/Hybrid | (meets 5X) |
Training Level: One
Course ID: CYBR 103
Price: $3495 (includes book, exam prep, hands-on lab, certification exam voucher)

(CYBR 104) CompTIA Server + Certification Bootcamp (40 hours)

Server+ covers server architecture, administration, storage, security, networking, troubleshooting as well as disaster recovery. This course is designed for IT professionals such as PC, desktop, and help desk technicians who have experience supporting PC hardware who wish to make the transition to become server hardware and support specialists. Upon successful completion of this course, you will be able to perform the duties of a server administrator. In this course, you will: 1. Manage server hardware. 2. Install server hardware and operating systems. 3. Configure networking hardware and protocols. 4. Perform basic server configuration tasks. 5. Create a virtual server environment. 6. Administer servers. 7. Implement server storage solutions. 8. Secure the server. - Plan and test disaster recovery. 9. Troubleshoot server issues.

CTA Staff
Course Delivery: Instructor Live/Hybrid | (meets 5X) |
Training Level: One
Course ID: CYBR 104
Price: $2895 (includes book, exam prep, certification exam voucher)

(CYBR 105) CompTIA Cloud + Certification Bootcamp (40 hours)

The new CompTIA Cloud+ certification addresses the increased diversity of knowledge, skills and abilities required of today's systems administrators and systems engineers and validates what is currently necessary to perform effectively on the job. CompTIA Cloud+ covers competency in cloud models, virtualization, infrastructure, security, resource management and business continuity.

CTA Staff
Course Delivery: Instructor Live/Hybrid | (meets 4X) |
Training Level: One
Course ID: CYBR 105
Price: $2595 (includes book, exam prep, certification exam voucher)

CYBR 106) CompTIA Linux+ Certification Bootcamp (40 hours)

The Linux+ certification validates technical competency and provides a broad awareness of Linux operating systems. Those holding the Linux+ certification demonstrate critical knowledge of installation, operation, administration and troubleshooting services. The CompTIA Linux+ [Powered by LPI] certification is a vendor neutral credential. In order to receive CompTIA Linux+ certification, a candidate must pass two exams: LX0-103 and LX0-104. Candidates must pass LX0-103 before taking LX0-104.

CTA Staff
Course Delivery: Instructor Live/Hybrid | (meets 5X) |
Training Level: One
Course ID: CYBR 106
Price: $3495 (includes book, exam prep, certification exam voucher)

IT/Cybersecurity Journeyman (Level Two) Courses

(CYBR 202) CompTIA Cybersecurity Analyst (CSA+) Certification Bootcamp (40 hours)

The Cybersecurity Analyst (CSA+) certification is a vendor-neutral IT professional certification that validates knowledge and skills required to configure and use threat detection tools, perform data analysis, interpreting the results to identify vulnerabilities, threats and risk to an organization with the end goal of securing and protecting applications and systems within an organization. The CSA+ certification applies behavioral analytics to the IT security market to improve the overall state of IT security. Analytics have been successfully integrated in the business intelligence, retail and financial services industries for decades. Analytics are now applied to IT security. Cybersecurity analytics greatly improves threat visibility across a broad attack surface by focusing on network behavior, including an organization's interior network. Threats are better detected using analytics. CSA+ is a vendor-neutral IT professional certification and the recommended first professional-level certification for IT security-analyst professionals. The performance-based CSA+ exam will include hands-on simulations. These simulations require test-takers to perform security analyst job tasks during the exam. To prepare for these performance-based assessments, trainers, educators and publishers should emphasize open-source analytics tools and teamwork. Use net wars or cyberwarfare scenarios with red teams as pen testers, white teams as security analysts, and blue teams as incident responders.

CTA Staff
Course Delivery: Instructor Live/Hybrid | (meets 5X) |
Training Level: Two
Course ID: CYBR 202
Price: $3395 ((includes book, exam prep, hands-on lab, certification exam voucher)

(CYBR 203) EC-Council Certified Ethical Hacker (CEH) Certification Bootcamp (40 hours)

The Certified Ethical Hacker (CEH) Certification Course certifies individuals in the specific network security discipline of Ethical Hacking from a vendor-neutral perspective. CEH certification will fortify the application knowledge of security officers, auditors, security professionals, site administrators, and anyone who is concerned about the integrity of the network infrastructure. A CEH is a skilled professional who understands and knows how to look for the weaknesses and vulnerabilities in target systems and uses the same knowledge and tools as a malicious hacker.

CTA Staff
Course Delivery: Instructor Live/Hybrid | (meets 5X) |
Training Level: Two
Course ID: CYBR 203
Price: $4895 (includes book, exam prep, hands-on lab, certification exam voucher)

(CYBR 204) EC-Council Certified Network Defender (CND) Certification Bootcamp (40 hours lecture)

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 National Cybersecurity Workforce Framework job roles for system/network administrators. The course is designed and developed after extensive market research and surveys.

CTA Staff
Course Delivery: Instructor Live/Hybrid | (meets 5X) |
Training Level: Two
Course ID: CYBR 204
Price: $4395 (includes book, exam prep, hands-on lab, certification exam voucher)

CYBR 205T) CYBRScore TCP/IP Fundamentals (40 hours)

TCP/IP Fundamentals studies traffic analysis and concepts of creating defensive measures based on analyst findings. This course covers collection of network traffic, analysis of individual packets, and setup and configuration of open-source intrusion detection systems (IDS). Additionally, covered are the procedures required for network exploitation analysts to implement traffic statistics methodology, intrusion sensors deployment and report generation utilized by management and administrators. Provide an understanding of TCP/IP fundamentals including where/how to capture and analyze network traffic for summary reporting based on findings and observations. Specific learning objectives include:

- Linux Fundamentals
- Working with Files and Directories & Network Interface
- Installing Software
- Access Control
- Network Fundamentals & Design
- Port Mirroring
- IDS/IPS Architecture
- Snort and SnorbyNetwork devices, packet capturing in a switched environment
- Packet Deconstruction
- Wireshark & Tcpdump
- Application Layer Protocols Staff
- Scans (SYN, SYN/ACK, FIN, Frag, Idle)
- Well-Known Application Ports
- ICMP Time-to Live (TTL)
- OSINT & Google Operators
- Introduction to Attacks
- Kali and Metasploit Framework
- Defense
- Monitoring Networks
- Windows Event Logs, Linux Syslog Logs, DHCP Logs, DNS Logs and Capture Filters
- Analyze network traffic as it is being transmitted live "across the wire"
- Determine the extent and severity of attacks underway
- Analyze attacks and identify potential mitigations

CTA Staff
Course Delivery: Instructor Live/Hybrid | (meets 5X) |
Training Level: Two
Course ID: CYBR 205T
Price: $3295 (includes e-book, labs, certificate of completion)

(CYBR 206T) CYBRScore Fundamentals of Network Forensics (40 hours)

Fundamentals of Network Forensics expands on acquired networking knowledge and extends in to 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. Specific learning objectives include:

- How to recognize exploit traffic
- The difference between attacks and poor network configuration
- Hacker techniques and mindset and steps of an attack
- Tools used for exploitation
- Packet capturing and analysis
- Tools used for network analysis
- 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
- Analyzing Windows & 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

CTA Staff
Course Delivery: Instructor Live/Hybrid | (meets 5X) |
Training Level: Two
Course ID: CYBR 206T
Price: $3295 (includes e-book, labs, certificate of completion)

(CYBR 207T) CYBRScore Fundamentals of Malware Analysis (40 hours)

This course uses a unique method of capability analysis, via pattern recognition, to teach students how to rapidly determine if malware is a threat to operations. This method helps to provide valuable analysis at a quick rate. After determining the threat level, students will learn the how to fix the vulnerabilities and the correct recommendations to make to upper management, while on the job. Specific learning objectives include:

- Overview
- Malware Reverse Engineering Methodology
- Basics of Assembly
- Assembly Instructions
- Malware Fundamentals & Tool Familiarization
- Rapid Malware Identification via reverse engineering
- Identifying Malware Capabilities
- Malware Defensive Techniques
- Web Based Malware
- Malware Incident Prevention
- Prevention
- Eradication

CTA Staff
Course Delivery: Instructor Live/Hybrid | (meets 5X) |
Training Level: Two
Course ID: CYBR 207T
Price: $3295 (includes e-book, labs, certificate of completion)

CISCO Certified Network Associate (CCNA)

(CYBR 208) CCNA Routing and Switching Certification Bootcamp (80 hours)

ICND1: Interconnecting Cisco Network Devices Part 1 (40 hours)

This 40-hour course focuses on providing the skills and knowledge necessary to install, operate, and troubleshoot a small branch office Enterprise network, including configuring a switch, a router, and connecting to a WAN and implementing network security. A Student should be able to complete configuration and implementation of a small branch office network under supervision.

ICND2: Interconnecting Cisco Network Devices Part 2 (40 hours)

This 40-hour course focuses on providing the skills and knowledge necessary to install, operate, and troubleshoot a small to medium-size branch office Enterprise network, including configuring several switches and routers, connecting to a WAN and implementing network security. ICND 1 is a prerequisite.

Staff CK/TRC Staff
Course Delivery: Instructor Live/Hybrid | (meets 10X) |
Training Level: Two
Course ID: CYBR 208
Price: $4495 (includes e-book, labs, exam prep, certification voucher)

(CYBR 209) CCNA Data Center Certification Bootcamp (40 hours)

For data center network administrators who want to save time and money on data center design, equipment installation, and maintenance, the Cisco Certified Network Associate Data Center (CCNA Data Center) certification is a job-role-focused training and certification program that allows you to maximize your investment in your education and increase the value of your data center network. Because of Cisco's leadership in providing data center solutions, this course provides comprehensive training and addresses the key areas of data center network design, implementation, and maintenance.

Staff CK/TRC Staff
Course Delivery: Instructor Live/Hybrid | (meets 5X) |
Training Level: Two
Course ID: CYBR 209
Price: $3695 (includes e-book, labs, certification voucher)

MCSA Microsoft Certified Solutions Associate

(CYBR 210) Microsoft Certified Solutions Associate Cloud Platform (MCSA) Certification Bootcamp (72 hours)

This instructor-led course is for individuals who are relatively new to IT and interested in expanding their knowledge base and technical skills about for attaining the Microsoft Certified Solutions Associate (MCSA): Cloud Platform certification. This is a step towards growing expertise in Microsoft's Azure and become proficient in mastering key cloud-based solution development skills. This certification demonstrates skills and knowledge in Microsoft cloud-related technologies. CK offers a comprehensive MCSA Cloud Platform certification course which focuses on understanding the deployment, management and application of Windows Azure for developing streamlined cloud-based solutions. The Cloud Platform training from Microsoft certified trainers provides in-depth understanding on leveraging Azure across enterprises. The Cloud Platform certification exam training covers developing and managing web and mobile based applications on Azure. The MCSA Cloud Platform certification is the first step towards achieving the expert-level Microsoft Certified Solutions Expert (MCSE) and grow career opportunities in cloud-related technology. It includes the following courses:

(CYBR 210-1) 20532C (70-532): Developing Microsoft Azure Solutions Course (32 hours)

This course is intended for students who have experience building ASP.NET and C# applications. Students will also have experience with the Microsoft Azure platform and a basic understanding of the services offered. This course offers students the opportunity to take an existing ASP.NET MVC application and expand its functionality as part of moving it to Azure. This course focuses on the considerations necessary when building a highly available solution in the cloud. This course also prepares the students for the 70-532: Developing Microsoft Azure Solutions certification exam. After completing this course, students will be able to:

- Compare the services available in the Azure platform.
- Configure and deploy web applications.
- Creating Azure Web Apps from the gallery.
- Deploying and monitoring Azure Web Apps.
- Creating and configuring Azure Virtual Machines.
- Create and manage a storage account.
- Manage blobs and containers in a storage account.
- Create, configure and connect to a SQL Databases instance.
- Identify the implications of importing a SQL standalone database.
- Manage users, groups and subscriptions in an Azure Active Directory instance.
- Create a virtual network.
- Implement a point-to-site network.

(CYBR 210-2) 20533C (70-533): Implementing Microsoft Azure Infrastructure Solutions Course (40 hours)

his course teaches IT professionals how to provision and manage services in Microsoft Azure. Students will learn how to implement infrastructure components such as virtual networks, virtual machines, containers, web and mobile apps, and storage in Azure. Students also will learn how to plan for and manage Azure AD, and configure Azure AD integration with on-premises Active Directory domains. After completing this course, students will be able to:

- Describe Azure architecture components, including infrastructure, tools, and portals. Implement and manage virtual networking within Azure and configure cross-premises connectivity.
- Plan and create Azure VMs.
- Configure, manage, and monitor Azure VMs to optimize availability and reliability.
- Implement Azure App Service.
- Plan and implement storage, backup, and recovery services.
- Implement container-based workloads in Azure.
- Deploy, configure, monitor, and diagnose cloud services.
- Implement Azure AD.
- Manage an Active Directory infrastructure in a hybrid environment.
- Automate operations in Azure by using Azure Automation runbooks.

CTA Staff
Course Delivery: Instructor Live/Hybrid | (meets 9X) |
Training Level: Two
Course ID: CYBR 210
Price: $3895 (includes e-book, labs, certification voucher)

Amazon Web Services (AWS) Associate

(CYBR 211) AWS Certified Solutions Architect - Associate Certification Bootcamp (24 hours)

Architecting on AWS training covers the fundamentals of building IT infrastructure on AWS. The course is designed to teach solutions architects how to optimize the use of the AWS Cloud by understanding AWS services and how these services fit into cloud-based solutions. This course emphasizes AWS cloud best practices and recommended design patterns to help students think through the process of architecting optimal IT solutions on AWS. Case studies throughout the course showcase how some AWS customers have designed their infrastructures and the strategies and services they implemented. Course Objective include:

- Making decisions based on the AWS-recommended architectural principles and best practices
- Leveraging AWS services to make your infrastructure scalable, reliable, and highly available
- Leveraging AWS managed services to enable greater flexibility and resiliency in an infrastructure
- Making an AWS-based infrastructure more efficient in order to increase performance and reduce costs
- Using the Well-Architected Framework to improve architectures with AWS solutions

CTA Staff
Course Delivery: Instructor Live/Hybrid | (meets 3X) |
Training Level: Two
Course ID: CYBR 211
Price: $3495 (includes e-book, labs, certification voucher)

(CYBR 212) AWS Certified SysOps Administrator - Associate Certification Bootcamp (24 hours)

Systems Operations on AWS training is designed to teach those in a Systems Administrator or Developer Operations (DevOps) role how to create automatable and repeatable deployments of networks and systems on the AWS platform. The course covers the specific AWS features and tools related to configuration and deployment, as well as common techniques used throughout the industry for configuring and deploying systems. Course Objectives include:

- Use standard AWS infrastructure features such as Amazon Virtual Private Cloud (VPC), Amazon Elastic Compute Cloud (EC2), Elastic Load Balancing, and Auto Scaling from the command line
- Use AWS CloudFormation and other automation technologies to produce stacks of AWS resources that can be deployed in an automated, repeatable fashion
- Build functioning virtual private networks with Amazon VPC from the ground up using the AWS Management Console
- Deploy Amazon EC2 instances using command line calls and troubleshoot the most common problems with instances
- Monitor the health of Amazon EC2 instances and other AWS services
- Manage user identity, AWS permissions, and security in the cloud
- Manage resource consumption in an AWS account using tools such as Amazon CloudWatch, tagging, and Trusted Advisor
- Select and implement the best strategy for creating reusable Amazon EC2 instances
- Configure a set of Amazon EC2 instances that launch behind a load balancer, with the system scaling up and down in response to demand
- Edit and troubleshoot a basic AWS CloudFormation stack definition

CTA Staff
Course Delivery: Instructor Live/Hybrid | (meets 3X) |
Training Level: Two
Course ID: CYBR 212
Price: $3495 (includes e-book, exam prep, certification voucher)

(CYBR 213) AWS Certified Developer - Associate Certification Bootcamp (24 hours)

Developing on AWS helps developers understand how to use the AWS SDK to develop secure and scalable cloud applications. The course provides in-depth knowledge about how to interact with AWS using code and covers key concepts, best practices, and troubleshooting tips. Objectives include:

- Install and configure SDKs and IDE toolkits
- Automate basic service operations using C# or Java
- Use security models to manage access to AWS
- Understand deployment models and usage with AWS
- Solve common application problems through testing and debug best practices

CTA Staff
Course Delivery: Instructor Live/Hybrid | (meets 3X) |
Training Level: Two
Course ID: CYBR 213
Price: $3495 (includes e-book, exam prep, certification voucher)

IT/Cybersecurity Master (Level Three) Courses

(CYBR 301) CompTIA Advanced Security Practitioner (CASP) Certification Bootcamp (40 hours)

This course will prepare the successful candidate with the technical knowledge and skills required to conceptualize, design, and engineer secure solutions across complex enterprise environments. The candidate will apply critical thinking and judgment across a broad spectrum of security disciplines to propose and implement solutions that map to enterprise drivers.

CTA Staff
Course Delivery: Instructor Live/Hybrid | (meets 5X) |
Training Level: Three
Course ID: CYBR 301
Price: $3795 (includes book, exam prep, hands-on lab, certification exam voucher)

(CYBR 302) ISC² Certified Authorization Professional (CAP—RMF – Risk Management Framework) Certification Bootcamp (40 Hours)

This course is designed for the information security practitioner who champions system security commensurate with an organization's mission and risk tolerance while meeting legal and regulatory requirements. The Certified Authorization Professional (CAP) certification course conceptually mirrors the National Institute of Standards and Technology (NIST) system authorization process in compliance with the Office of Management and Budget (OMB) Circular A-130, Appendix III. Gain the skills needed to categorize, implement, authorize, assess, continuously monitor (real-time risk management), and select security controls for information systems that meets federal mandates on requirements and process guidelines. The RMF credential 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. In this course, you will gain an understanding of the new authorization process and prepare for the CAP certification exam, based on the new SP 800-37 process and the new (ISC)²® Common Body of Knowledge.

CTA Staff
Course Delivery: Instructor Live/Hybrid | (meets 5X) |
Training Level: Three
Course ID: CYBR 302
Price: $3395 (includes book, exam prep, certification exam voucher)

(CYBR 303) EC-Council Computer Hacking Forensic Investigator (CHFI) Certification Bootcamp (40 hours)

During our 5-day EC-Council CHFI Certification Training Camp, students will live, learn, and take the exams at one of our state-of-the- art education centers. This blended-learning course employs outcome-based delivery that focuses on preparing you with the real- world skills required to pass the certification exam.

CTA Staff
Course Delivery: Instructor Live/Hybrid | (meets 5X) |
Training Level: Three
Course ID: CYBR 303
Price: $4195 (includes book, exam prep, hands-on lab, certification exam voucher)

(CYBR 304) EC-Council Certified Incident Handler (ECIH) Certification Bootcamp (40 hours)

ECIH 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 policy related to incident handling. After attending the course, they will be able to create incident handling and response policies and deal with various types of computer security incidents. The IT incident management training program will make students proficient in handling and responding to various security incidents such as network security incidents, malicious code incidents, and insider attack threats. In addition, the students will learn about computer forensics and its role in handling and responding to incidents. The course also covers incident response teams, it incident management training methods, and incident recovery techniques in detail. The ECIH certification will provide professionals greater industry acceptance as the seasoned incident handler

CTA Staff
Course Delivery: Instructor Live/Hybrid | (meets 5X) |
Training Level: Three
Course ID: CYBR 304
Price: $3795 (includes book, exam prep, hands-on lab, certification exam voucher)

(CYBR 305) EC-Council Security Analyst (ECSA) Certification Bootcamp (40 hours)

EC-Council Certified Security Analyst (ECSA) is an advanced ethical hacking certification that complements the Certified Ethical Hacker (CEH) certification by validating the analytical phase of ethical hacking. An ECSA is a step ahead of a CEH by being able to analyze the outcome of hacking tools and technologies. Through groundbreaking network penetration testing methods and techniques, an ECSA can perform intensive assessments required to effectively identify and mitigate risks to the information security of the infrastructure.

CTA Staff
Course Delivery: Instructor Live/Hybrid | (meets 5X) |
Training Level: Three
Course ID: CYBR 305
Price: $3795 (includes book, exam prep, hands-on lab, certification exam voucher)

(CYBR 306) EC-Council Licensed Penetration Tester (LPT) Certification Bootcamp (40 hours)

The LPT (Master) practical exam is the capstone to EC-Council's entire information security track, right from the CEH to the ECSA Program. The LPT (Master) exam covers the entire Penetration Testing process and lifecycle with keen focus on report writing, required to be a true professional Penetration Tester. While the Certified Ethical Hacker course teaches an individual what are the threat agents that can compromise the security posture of an organization and the EC-Council Security Analyst program provides a repeatable and documentable methodology that can be used by a security auditor while analyzing the security status of the organization, the Licensed Penetration Tester exam covers a completely different skill-set that is needed by every penetration tester – Report Writing. Report Writing has been described by many as one of least preferred, yet arguably one of the most critical part of any penetration testing engagement.

CTA Staff
Course Delivery: Instructor Live/Hybrid | (meets 5X) |
Training Level: Three
Course ID: CYBR 306
Price: $3795 (includes book, exam prep, hands-on lab, certification exam voucher)

(CYBR 307) ISACA Cyber Security Nexus (CSX) Practitioner Certification Boot Camp (45 hours)

CSX Practitioner Boot Camp is a 5-day, immersive cyber security training course designed to help you build your technical skillset through true hands-on learning. The Boot Camp is conducted in a live, lab-based network environment – not a simulated environment like other courses. Students go through complex cyber security scenarios based on recent, real-world scenarios and be given live incidents to detect and mitigate. Each day in this immersive training covers complex technical skills and concepts in one of five areas aligned to existing global cyber security frameworks:

- **Identify:** Identification, assessment and evaluation of assets, threats and vulnerabilities in both internal and external networks
- **Protect:** Implementation of cyber security controls to protect a system from identified threats
- **Detect:** Detection of network and system incidents, events and compromise indicators, along with assessment of potential damage
- **Respond:** Execution of comprehensive incident response plans and mitigation of cyber incidents
- **Recover:** Recovery from incidents and disasters, including post incident-response documentation and implementation of continuity plans

CTA Staff
Course Delivery: Instructor Live/Hybrid | (meets 5X) |
Training Level: Three
Course ID: CYBR 307
Price: $6495 (includes book, exam prep, hands-on lab, certification exam voucher)

Amazon Web Services (AWS) Professional

(CYBR 310) AWS Certified Solutions Architect - Professional Certification Bootcamp (24 hours)

Building on concepts introduced in Architecting on AWS, Advanced Architecting on AWS is intended for individuals who are experienced with designing scalable and elastic applications on the AWS platform. In this course, you will cover how to build complex solutions that incorporate data services, governance, and security on AWS. You will get an introduction to specialized AWS services, including AWS Direct Connect and AWS Storage Gateway to support hybrid architecture. You will also cover designing best practices for building scalable, elastic, secure, and highly available applications on AWS. Objectives include:

- Manage multiple AWS accounts
- Connect on-premises datacenter to AWS
- Discuss billing implications of connecting multi-region VPCs
- Move large data from on-premises datacenter
- Design large datastores for AWS cloud
- Understand different architectural designs for scaling a large website
- Protect your infrastructure from DDoS attack
- Secure your data on AWS with encryption
- Design protection of data-at-rest as well as data-in-flight
- Enhance the performance of your solutions

CTA Staff
Course Delivery: Instructor Live/Hybrid | (meets 3X) |
Training Level: Three
Course ID: CYBR 310
Price: $4095 (includes e-book, exam prep, certification exam voucher)

(CYBR 311) AWS Certified DevOps Engineer - Professional Certification Bootcamp (24 hours)

DevOps Engineering on AWS demonstrates how to use the most common DevOps patterns to develop, deploy and maintain applications on AWS. The course covers the core principles of the DevOps methodology and examines a number of use cases applicable to startup, small-medium business, and enterprise development scenarios. Objectives include:

- Use the principal concepts and practices behind the DevOps methodology
- Design and implement an infrastructure on AWS that supports one or more DevOps
- Use AWS CloudFormation and AWS OpsWorks to deploy the infrastructure necessary to create development, test, and production environments for a software development project
- Use AWS CodeCommit and understand the array of options for enabling a Continuous Integration environment on AWS

- Implement several common Continuous Deployment use cases using AWS, including blue/green deployment and A/B testing
- Distinguish between the array of application deployment technologies available on AWS (including AWS CodeDeploy, AWS Opsworks, AWS Elastic Beanstalk, Amazon EC2 Container Service, Container Registry)
- Fine-tune the applications you deliver on AWS

CTA Staff
Course Delivery: Instructor Live/Hybrid | (meets 3X) |
Training Level: Three
Course ID: CYBR 311
Price: $3695 (includes book, exam prep, certification exam voucher)

IT/Cybersecurity Expert/Manager (Level Four) Courses

(CYBR 401) ISC² Certified Information Systems Security Professional (CISSP) Certification Bootcamp (40 hours)

A CISSP is an information assurance professional who defines the architecture, design, management and/or controls that assure the security of business environments. The vast breadth of knowledge and the experience it takes to pass the exam is what sets the CISSP apart. The credential demonstrates a globally recognized standard of competence provided by the (ISC)²® CBK which covers critical topics in security today, including cloud computing, mobile security, application development security, risk management and more. The CISSP was the first credential in the field of information security to meet the stringent requirements of ISO/IEC Standard 17024. CISSP certification is not only an objective measure of excellence, but is also a globally recognized standard of achievement.

CTA Staff
Course Delivery: Instructor Live/Hybrid | (meets 5X) |
Training Level: Four
Course ID: CYBR 401
Price: $4295 (includes book, exam prep, hands-on lab, certification exam voucher)

(CYBR 402) ISC² Certified Cloud Security Professional (CCSP) Certification Bootcamp (40 hours)
As powerful as cloud computing is for the organization, understanding its information security risks and mitigation strategies is critical. Legacy approaches are inadequate, and organizations need competent, experienced professionals equipped with the right cloud security knowledge and skills to be successful. They need CCSPs. 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 information security and cloud computing. CCSPs professionals have achieved the highest standard for cloud security expertise and enable any organization to benefit from the power of cloud computing while keeping sensitive data secure.

CTA Staff
Course Delivery: Instructor Live/Hybrid | (meets 5X) |
Training Level: Four
Course ID: CYBR 402
Price: $3595 (includes book, exam prep, certification exam voucher)

(CYBR 403) ISACA Certified in Risk & Information Control (CRISC) Certification Bootcamp (40 hours)

This 5-day ISACA Certified in Risk and Information Systems Control Bootcamp equips information professionals with the knowledge and technical skills required for proficiency in the most current and rigorous assessment available to evaluate the risk management proficiency of IT professionals and other employees within an enterprise or financial institution. IS audit, control, monitoring, and assessing. CRISC-certified professionals manage risk, design and oversee response measures, monitor systems for risk, and ensure the organization's risk management strategies are met. Organizations look for employees with the CRISC credential for jobs such as IT security analyst, security engineer or architect, information assurance program manager and senior IT auditor. The CRISC exam covers four domains that are periodically updated to reflect the changing needs of the profession:

- Domain 1: Risk Identification
- Domain 2: Risk Assessment
- Domain 3: Risk Response and Mitigation
- Domain 4: Risk and Control Monitoring and Reporting

CTA Staff
Course Delivery: Instructor Live/Hybrid | (meets 3X) |
Training Level: Four
Course ID: CYBR 403
Price: $4195 (includes book, exam prep, certification exam voucher)

(CYBR 404) ISACA Certified Information Security Manager (CISM) Certification Bootcamp (40 hours)

This 5-day ISACA Certified Information Security Manager (CISM) training course equips information security professionals with the knowledge and technical skills required for proficiency in building and managing enterprise information security. This exam benchmarks the understanding of essential concepts in many Information Security job practice areas. With the help of prominent industry leaders, subject matter experts and industry practitioners, ISACA has put together this exam to define what security managers do and what they need to know. The DoD's IA professionals are classified into two categories-information assurance technical (IAT) and information assurance managerial (IAM)-that are each divided into three levels. CISM is an approved certification for professionals in IAM Levels II and III.

CTA Staff
Course Delivery: Instructor Live/Hybrid | (meets 4X) |
Training Level: Four
Course ID: CYBR 404
Price: $4595 (includes book, exam prep, hands-on lab, certification exam voucher)

(CYBR 405) ISACA Certified Governance of Enterprise IT (CGEIT) Certification Bootcamp (40 hours)

This 5-day ISACA Certified in the Governance of Enterprise IT (CGEIT) Boot Camp equips information professionals with the knowledge and technical skills required for proficiency in enterprise governance of IT systems. The Certified in the Governance of Enterprise IT (CGEIT) credential is geared toward professionals who play a significant role in managing, advising and/or assuring IT governance. Typical job roles include senior security analyst and chief information security officer—the upper echelon of the organization chart. ISACA's CGEIT exam covers five domains that address various aspects of governance and risk management:

- Domain 1: Framework for the Governance of Enterprise IT
- Domain 2: Strategic Management
- Domain 3: Benefits Realization
- Domain 4: Risk Optimization
- Domain 5: Resource Optimization

CTA Staff
Course Delivery: Instructor Live/Hybrid | (meets 2X) |
Training Level: Four
Course ID: CYBR 405
Price: $4695 (includes book, exam prep, certification exam voucher)

(CYBR 406) ISACA Certified Information Systems Auditor (CISA) Certification Bootcamp (40 hours)

This 5-day ISACA Certified Information Systems Auditor (CISA) Boot Camp equips information professionals with the knowledge and technical skills required for proficiency in IS audit, control, monitoring, and assessing. The CISA designation is a globally recognized certification for IS audit control, assurance and security professionals. CISA-certified individuals demonstrate that they have audit experience, skills and knowledge. They are also capable of managing vulnerabilities, ensuring compliance and instituting controls within the enterprise.

CTA Staff
Course Delivery: Instructor Live/Hybrid | (meets 4X) |
Training Level: Four
Course ID: CYBR 406
Price: $4595 (includes book, exam prep, certification exam voucher)

(CYBR 408T) CYBRScore Python for Network Security Administrators (40 hours)

Python for Network Security Administrators is a fast-paced boot camp-style introductory course for Python security and networking topics. The course will expose students to common Python types, data manipulation, networking, command-line scripting, and parallel processing. Additionally, this 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. Specific learning objectives include:

- Command-Line Python
- Screen Output
- Main Functions in Python
- String I/O and manipulation
- Converting Strings and Numbers
- Python Lists, Dictionaries
- Loops
- Writing Functions, Packing Objects
- Unit testing
- File I/O, Error Handling
- SQLite
- Pickling & Un-pickling
- ICMP Scanner
- TCP Port Scanner
- Chat Client and Server
- Dictionary-Based Password Cracking
- Parallel Processing ICMP Scanner
- Parallel Processing TCP Scanner
- Parallel Processing Password Cracker
- Clear Windows Event Log Using C-Types and the Windows AP
- Packet Crafting Using Scapy
- Network-Based File Transfer

CTA Staff
Course Delivery: Instructor Live/Hybrid | (meets 5X) |
Training Level: Four
Course ID: CYBR 408T
Price: $3895 (includes e-book, labs, certificate of completion)

(CYBR 409T) CYBRScore Pen Testing & Network Exploitation (40 hours)

Pen Testing & 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. Provides 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. Specific learning objectives include:

- Linux & Windows Command Line Review
- PowerShell Introduction
- Scanning LAN Hosts
- Scanning & Enumeration of Windows Hosts & Linus Hosts
- Exploits Searching Based on Scanning & Enumeration
- SQL Injection
- Cross Site Scripting
- Routed Scanning & Discovery
- Understanding Firewalls & NAT Devices
- SSH Forwarding & Brute-Forcing SSH
- Adding Routes
- Privilege Escalation Discovery
- Post-Exploitation Pillaging
- Breaking Web Apps
- Using PowerShell Over Pivoted SSH Tunnels
- Creating Backdoors

CTA Staff
Course Delivery: Instructor Live/Hybrid | (meets 5X) |
Training Level: Four
Course ID: CYBR 409T
Price: $3895 (includes e-book, labs, certificate of completion)

(CYBR 410T) CYBRScore Wireless Security & Testing (40 hours)

Wireless Pen Testing 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. This course provides in-depth exposure to all facets of 802.11 penetration testing, encryption cracking, post-exploitation pillaging and report writing. Specific learning objectives include:

- Scoping and Planning WiFi Penetration Tests
- 802.11 Protocols and Standards
- Authentication vs Association
- WiFi Security Solutions & Hacking Hardware
- Connectors and Drivers
- Recon and Custom Password
- Generation with Cupp and CeWL
- 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 & Bypassing MAC Filters
- GISKimset to Database Survey Information and create GISKismet .kml files
- Creating Custom SQL Queries
- AWK Tool to Format Output from SQL Queries for Reporting
- Stream and Block Ciphers, Block Cipher Modes
- WPA2 AES-CCMP Security Process
- Cowpatty to Recover WPA2 Passphrase
- Pyrit to Survey and Attack Encryption
- Data basing and Recovering WPA2 Passphrases
- 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
- Custom Ettercap Filters & Ettercap to Poison ARP Cache on WiFi Network & Conduct Attacks Against Clients
- Rusty Cobra Tool to Automate WiFi Survey
- Visualization, Database Management and Report File Creation

CTA Staff
Course Delivery: Instructor Live/Hybrid | (meets 5X) |
Training Level: Four
Course ID: CYBR 410T
Price: $3895 (includes e-book, labs, certificate of completion)

(CYBR 411T) CYBRScore Incident Response (40 hours)

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 environment. Specific learning objectives include:

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

CTA Staff
Course Delivery: Instructor Live/Hybrid | (meets 5X) |
Training Level: Four
Course ID: CYBR 411T
Price: $3895 (includes e-book, labs, certificate of completion)

(CYBR 412T) CYBRScore Reverse Engineering Malware (25 hours lecture; 15 hours Lab)

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, and identify common malware functionality, in addition to reversing covert and encoded malware. Specific learning objectives include:

- Windows API
- Handles & file system functions
- Common registry functions & autoruns
- Networking APIs
- Processes, threads & mutexes
- COM objects
- Kernel vs. User-mode debugging
- Software & hardware breakpoints
- Modifying program execution & patching
- OllyDbg overview
- Memory maps
- Executing code, breakpoints & tracing
- OllyDbg plugins
- Kernel debugging with WinDbg
- Configuring kernel debugging environment
- Analyzing functions, structures and driver objects
- Rootkit analysis
- Downloaders, launchers & backdoors
- Analyzing various persistence mechanisms & usermode rootkits
- Covert malware
- Abusing resource section of PE file
- Process injection & process replacement
- Windows hooks & detours
- APC injection from kernel space
- Analyzing encoding algorithms
- XOR, BASE64 & custom encoding
- Common crypto algorithms
- KANAL
- Custom decoding scripts in Python
- Instrumentation for generic decryption

CTA Staff
Course Delivery: Instructor Live/Hybrid | (meets 5X) |
Training Level: Four
Course ID: CYBR 411T
Price: $3895 (includes e-book, labs, certificate of completion)

(CYBR 412T) CYBRScore Advanced Malware Analysis (40 hours)

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. Provide an in-depth understanding of identifying & analyzing the presence of advanced packers, polymorphic malware, encrypted malware & malicious code. Specific learning objectives include:

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

CTA Staff
Course Delivery: Instructor Live/Hybrid | (meets 5X) |
Training Level: Four
Course ID: CYBR 412T
Price: $3895 (includes e-book, labs, certificate of completion)

(CYBR 413) CompTIA Certified Technical Trainer (40 hours)

The CTT+ certificate is a cross-industry credential that provides recognition that an instructor has attained a standard of excellence in the training industry. The examinations are based on a set of objectives designed to measure the core knowledge and skills that competent instructors must successfully demonstrate to complete an instructional assignment successfully both in a classroom and a virtual classroom environment. This certification is targeted towards all training professionals and can be applied to all industries that provide technical and non-technical training and education. This is CK's Train the Trainer Program.

CTA Staff
Course Delivery: Instructor Live/Hybrid | (meets 5X) |
Training Level: Four
Course ID: CYBR 413
Price: $4795 (includes e-book, certification voucher)

MCSE Microsoft Certified Solutions Expert

(CYBR 414) Microsoft Certified Solutions Expert--Cloud Platform and Infrastructure (MCSE) (96 hours)

This instructor-led course is for individuals who are relatively new to IT and interested in expanding their knowledge base and technical skills about for attaining the Microsoft Certified Solutions Expert (MCSE): Cloud Platform and Infrastructure certification validates an IT professional's skills in managing and running a highly efficient modern data center. Getting certified in MCSE: Cloud Platform and Infrastructure demonstrates the skills of the IT professional in various expertise, including cloud technology, systems management, identity management, storage, virtualization and networking. This expert-level certification is the subsequent path to Associate level certifications (MCSA) for specializations ranging from Windows Server, Linux to Cloud Platform. Upon qualification, the candidate can work as a computer support specialist, cloud architect, cloud administrator and IT security analyst. CK offers comprehensive training for MCSE: Cloud and Infrastructure course, providing complete learning support for achieving MCSE qualification. The learners can opt from a range of training delivery mediums: Microsoft - Cloud Platform and Infrastructure boot camp training, ILT or online training.

(CYBR 414-1) 20744A (70-744): Securing Windows Server 2016 Boot Camp Course (40 hours)

This five-day, instructor-led course teaches IT professionals how they can enhance the security of the IT infrastructure that they administer. This course begins by emphasizing the importance of assuming that network breaches have occurred already, and then teaches you how to protect administrative credentials and rights to ensure that administrators can perform only the tasks that they need to, when they need to. This course also details how you can mitigate malware threats, identify security issues by using auditing and the Advanced Threat Analysis feature in Windows Server 2016, secure your virtualization platform, and use new deployment options, such as Nano server and containers to enhance security. The course also explains how you can help protect access to files by using encryption and dynamic access control, and how you can enhance your network's security. After completing this course, students will be able to:

- Secure Windows Server.
- Secure application development and a server workload infrastructure.
- Manage security baselines.
- Configure and manage just enough and just-in-time (JIT) administration.
- Manage data security.
- Configure Windows Firewall and a software-defined distributed firewall.
- Secure network traffic.
- Secure your virtualization infrastructure.
- Manage malware and threats.
- Configure advanced auditing.
- Manage software updates.
- Manage threats by using Advanced Threat Analytics (ATA) and Microsoft Operations Management Suite (OMS).

(CYBR 414-2) 55224A-1/52242A ((70-475): Microsoft Azure Big Data Analytics Solutions Boot Camp Course (32 hours)

55224A-1 is a two-day instructor-led course is intended for data professionals who want to expand their knowledge about creating big data analytic solutions on Microsoft Azure. Students will learn how to design solutions for batch and real-time data processing. Different methods of using Azure will be discussed and practiced in lab exercises, such Azure CLI, Azure PowerShell and Azure Portal. 55224A-1 labs & exercises cover the first two objectives of exam 70-475 (Designing Big Data batch, interactive & real-time solutions). The other two objectives (Designing Machine Learning and cloud analytics solutions) are covered in 55224A-2. *52242A* is a two-day instructor-led course intended for data professionals who want to expand their knowledge about creating big data analytic solutions on Microsoft Azure. Students will learn how to operationalize end-to-end cloud analytics solutions using the Azure Portal and Azure PowerShell. It can be used on its own or with 552241A, Microsoft Azure Big Data Analytics, to prepare for exam 70-475.

(CYBR 414-3) 40441 (70-473): Designing and Implementing Cloud Data Platform Solutions Boot Camp Course (24 hours)

The focus of this three-day instructor-led Microsoft Training course is on designing and implementing cloud data platform solutions with the Microsoft Data Platform by using SQL Server on-premises, hybrid and cloud data platform solutions. It describes how to design and implement and optimize workloads in hybrid scenarios with both on-premises and Microsoft Azure cloud-based solutions, and how to implement high availability and disaster recovery solutions. After completing this course, students will be able to:

- Position Microsoft Cloud Data Platform Solutions
- Design and implement solutions on Azure using SQL Server
- Design and implement solutions on Azure using SQL Database
- Design and implement security, access and auditing for cloud data platform solutions
- Design highly scalable mission critical solutions using the Microsoft Data Platform
- Design and implement cloud data platform solutions.

CTA Staff
Course Delivery: Instructor Live/Hybrid | (meets 12X) |
Training Level: Four
Course ID: CYBR 414
Price: $6295 (includes e-book, certification voucher)

(CYBR 415) Microsoft Solutions Expert-Mobility (MSCE)

Microsoft Certified Solutions Expert (MCSE) is an expert-level certification from Microsoft. This globally recognized standard for IT professionals validates expertise to build innovative on-premises and cloud solutions across multiple technologies. MCSE Mobility certification from Microsoft qualifies a candidate who has gained knowledge and skills to manage devices in Bring-Your-Own-Device (BYOD) enterprise environment. Microsoft MCSE Mobility is the subsequent credential building on the foundational Windows 10 skills developed at the MCSA certification level. After passing the relative MCSE: Mobility 2016 certification exam, an aspirant is qualified to work in different roles, ranging from desktop support technician to enterprise management of BYOD apps and devices. CK offers a structured and qualitative learning support to interested candidates who are looking to get trained in Microsoft technologies and become MCSE certified. The advanced MCSE: Mobility 2016 certification training courses are delivered by Microsoft certified trainers on Windows Client and Enterprise.

(CYBR 415-1) 20695C (70-695): Deploying Windows Desktops and Enterprise Applications Course Bootcamp Course (40 hours)

This course describes how to assess operating system and application deployment options, determine the most appropriate deployment strategy, and then implement a deployment solution for Windows devices and apps that meets your environment's needs. Solutions that this course details include operating system deployment scenarios ranging from high-touch solutions to zero-touch solutions. It also discusses the technologies that you use to implement these solutions, including the MDT and Configuration Manager. Objectives include:

- Assess the network environment to support operating system and application deployment tasks.
- Identify the most appropriate operating system deployment strategy based upon organizational requirements.
- Assess application compatibility issues and identify mitigation solutions to ensure that applications function successfully after an operating system deployment.
- Describe and configure strategies to migrate user state during operating system deployments.
- Determine the most appropriate image management strategy to support operating system and application deployments.
- Describe and use the tools provided in the Windows ADK to prepare for and support automated deployment strategies.
- Identify solutions to support PXE-initiated and multicast solutions when performing operating system deployment tasks.
- Configure an operating system deployment strategy by using the MDT.
- Configure an operating system deployment strategy using Configuration Manager.
- Integrate the MDT with Configuration Manager to support operating system deployment procedures.
- Implement volume license activation and configuration settings for client computers.
- Customize and deploy Microsoft Office 2016 to an enterprise network environment and describe how to use the Windows ICD.

(CYBR 415-2) 20696C (70-696): Administering System Center Configuration Manager and Intune Bootcamp Course (40hours)

Get expert instruction and hands-on practice configuring and managing clients and devices by using Microsoft System Center v1511 Configuration Manager, Microsoft Intune, and their associated site systems. In this five-day course, you will learn day-to-day management tasks, including how to manage software, client health, hardware and software inventory, applications, and integration with Intune. You also will learn how to optimize System Center Endpoint Protection, manage compliance, and create management queries and reports. Additionally, this course, in conjunction with Microsoft Official Course 20695, also helps certification candidates prepare for Exam 70-696: Managing Enterprise Devices and Apps. Objectives include:

- Describe the features Configuration Manager and Intune include, and explain how you can use these features to manage PCs and mobile devices in an enterprise environment
- Prepare a management infrastructure, including configuring boundaries, boundary groups, and resource discovery, and integrating mobile-device management with Microsoft Exchange Server
- Deploy and manage the Configuration Manager client
- Configure, manage, and monitor hardware and software inventory, and use Asset Intelligence and software metering
- Identify and configure the most appropriate method to distribute and manage content used for deployments
- Distribute, deploy, and monitor applications for managed users and systems
- Maintain software updates for PCs that Configuration Manager manages
- Use Configuration Manager to implement Endpoint Protection
- Manage configuration items, baselines, and profiles to assess and configure compliance settings and data access for users and devices
- Configure an operating-system deployment strategy by using Configuration Manager
- Manage mobile devices by using Configuration Manager and Intune
- Manage and maintain a Configuration Manager site

(CYBR 415-3) 20398 (70-398): Planning for and Managing Devices in the Enterprise Course (40 hours)

This course teaches IT professionals how to use the Enterprise Mobility Suite to manage devices, users, and data. In addition, this course teaches students how to use other technologies, such as Group Policy and other Windows Server–based technologies, to manage devices and secure data. Aspirants will learn how to design and implement cloud-based and on-premises solutions for managing Windows-based, iOS, and Android devices, and they will learn how to provide secure and efficient access to data and applications.

- Use devices in the enterprise environment
- Implement and administer Microsoft Azure Active Directory (Azure AD)
- Connect AD DS with Azure AD
- Manage devices in Microsoft Office 365
- Plan and implement Intune
- Use Intune to manage devices
- Plan and implement app support
- Use Intune to manage applications and Resource Access
- Plan and implement Microsoft Azure Rights Management (Azure RMS)
- Plan and implement Remote Access
- Plan and implement Dynamic Access Control and auditing
- Plan and protect data
- Recover data and operating systems

CTA Staff
Course Delivery: Instructor Live/Hybrid | (meets 15X) |
Training Level: Four
Course ID: CYBR 415
Price: $7395 (includes e-book, certification voucher)

IT/Cybersecurity Leader (Level Five) Courses

(CYBR 501) EC-Council Certified Chief Information Security Officer (C-CISO) Certification Bootcamp (40 hours)

EC-Council's C|CISO Program has certified leading information security professionals around the world. A core group of high-level information security executives, the C|CISO 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 C|CISO program is the first of its kind training and certification program aimed at producing top-level information security executives. The C|CISO 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.

CTA Staff
Course Delivery: Instructor Live/Hybrid | (meets 4X) |
Training Level: Five
Course ID: CYBR 501
Price: $6095 (includes book, exam prep, certification exam voucher)

CYBR 502) TRC Cybersecurity Risk for Executives Bootcamp (24 hours lecture)

Organizations, leaders, managers and information security personnel across every business sector are increasingly concerned about cybersecurity and the business risk associated with a cybersecurity breach. Everyday organizations face an onslaught of attack on their information systems targeting critical information and data. New government laws and regulations place a premium on cybersecurity controls. Customers, shareholders, and investors are demanding effective controls to ensure protection of sensitive information, especially personal and financial data. Organizations struggle to balance effective information protection without breaking the bank. This 3-day course examines cybersecurity as a business imperative through the eyes of the executive leaders and senior managers not the technologist. Simply, cybersecurity is an organizational risk management function. The primary objective of the course is to teach students how to establish a planning process and examine key policy practices that will enable the integration of cybersecurity as a primary component of an organizations' risk management strategy.

CTA Staff
Course Delivery: Instructor Live/Hybrid | (meets 3X) |
Training Level: Five
Course ID: CYBR 502
Price: $4995 (includes book, certificate of completion)

IT/Cybersecurity Skills Assessments

(CYBR 601) CYBRSCORE System Administrator Assessment (Level One) (4 hours)

System Administrator skills assessment is designed to assess the knowledge, skills and abilities required by the System Administration specialty area as defined by the NICE Cybersecurity Workforce Framework. Individuals in this role should have a comprehensive understanding of installing, configuring, troubleshooting and maintaining server configurations (hardware and software) to ensure their confidentiality, integrity, and availability. They should also be able to manage accounts, firewalls, and patches, and be responsible for access control, passwords, and account creation and administration. This assessment targets CK/TRC Level One clients currently in or candidates for the following roles:

- LAN Administrator
- Platform Specialist
- Security Administrator
- Server Administrator
- Systems Operations Personnel
- Systems Administrator
- Website Administrator

CTA Staff
Assessment Delivery: Online | (meets 1X) |
Training Level: One
Course ID: CYBR 601
Price: $595 (includes assessment voucher)

(CYBR 602) CYBRSCORE Defense Analyst Assessment (Level Two/Three) (2-3 hours each)

Cyber Defense Analyst is designed to assess an individual's knowledge, skills and abilities related to using data collected from cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze events that occur within their environments for mitigating threats. Cyber Defense Analysts are assessed in five specific areas:

1. **Protocol Analysis (CYBR 602-1)**: Evaluates an individual's ability to use a network protocol analyzer to examine network traffic, discover malicious activity, and report their findings. *OS/Tools used: Security Onion / Wireshark, tcpdump.*
2. **Intrusion Detection (CYBR 602-2): E**valuates an individual's ability to monitor events that occurred on a computer network and to review and interpret captured traffic for signs of incidents that could be considered an imminent threat or violation of security policies, standard security practices, or acceptable use policies. OS/Tools used: *Security Onion / Wireshark, Snort.*
3. **Incident Handling Methodology (CYBR 602-3)**: Evaluates an individual's ability to gather information on an incident, to understand the importance of following industry standard reporting techniques, to comprehend commonly utilized attack types, and to perform analysis and response tasks for a sample incident. *OS/Tools used: Security Onion, Windows / Wireshark, Microsoft Baseline Security Analyzer.*
4. **Network Defense Analysis (CYBR 602-4)**: Evaluates an individual's ability to define, identify, and classify weaknesses or vulnerabilities that exist in a system or networked environment. *OS/Tools used: Kali Linux / network scanners.*
5. **Network Attack Analysis (CYBR 602-5)**: Evaluates an individual's ability to exploit previously identified weaknesses or vulnerabilities on a system or network environment. *OS/Tools used: Kali Linux / Metasploit, network scanners.*

This assessments targets CK/TRC Level Two/Three clients currently in or candidates for the following roles:

- CND Analyst (Cryptologic)
- Cyber Security Intelligence Analyst
- Focused Operations Analyst
- Incident Analyst
- Network Defense Technician
- Network Security Engineer
- Security Analyst
- Security Operator
- Sensor Analyst

CTA Staff
Assessment Delivery: Online | (meets up to 1X) |
Training Level: Two & Three
Course ID: CYBR 602
Price: $295 each or $1195 for all five (includes assessment voucher(s))

(CYBR 603) CYBRSCORE Vulnerability and Management Assessment (Level Three/Four) (4 hours)

Vulnerability and Management assessment is designed to assess the knowledge, skills and abilities required by the Vulnerability and Management specialty areas as defined by the NICE Cybersecurity Workforce Framework. Individuals in this role should have a comprehensive understanding of the tools and techniques to detect and exploit security vulnerabilities in web-based applications, networks, and computer systems that use the Windows and Linux OS, as well as recommend mitigation countermeasures.

This assessments targets CK/TRC Level Three and Four clients currently in or candidates for the following roles:

- Blue Team Technician
- Certified TEMPEST Professionals/Technicians
- Close Access Technician
- CND Auditor/Compliance Manager
- Ethical Hacker
- Governance Manager
- Information Security Engineer
- Internal Enterprise Audit
- Penetration Tester
- Red Team Technician
- Reverse Engineer
- Risk/Vulnerability Analyst
- Technical Surveillance Countermeasures Technician
- Vulnerability Assessment Analyst/Manager

CTA Staff
Assessment Delivery: Online | (meets 1X) |
Training Level: Two & Three
Course ID: CYBR 602
Price: $595 (includes assessment voucher)

About CyberTec

ABOUT CYBERTEC ACADEMY®: CyberTec Academy® is a full-service IT/Cyber certification training organization, it is a division of Titan Rain Cybersecurity, LLC. CyberTec® partners with industry leading organizations to deliver the world's first experiential-based, certification-driven cybersecurity training and workforce development program. CyberTec's mission is to provide IT/Cyber education and training programs that ensures individuals and teams gain the requisite knowledge, skills, and abilities to perform the requisite tasks require of their roles and responsibilities within any organization—CyberTec® certifies competency. Programs combine the requirements of the global certification bodies, hands-on skills labs/scenarios, and skills assessments to ensure client ability to meet employer skill-demand. Training is delivered in three modalities to meet client demand—classroom live, synchronous instructor led, or asynchronous on-demand. CyberTec partners will key industry leaders, such as The Global McDuffie Group and the Global Institute for Cyber Security Resilience to develop agile, competent cybersecurity professionals.

ABOUT TITAN RAIN CYBERSECURITY, LLC: Titan Rain Cybersecurity (TRC) is a cutting-edge cybersecurity education, training, and workforce development provider; in addition, a full-service cyber risk, governance, advisory, international standards, and policy consulting firm. Titan Rain's CyberTec Academy® delivers IT/Cyber Security training and education to increase professional competency through classroom instruction, hands-on labs, and skills assessment. CyberTec® ensure graduates have the requisite knowledge, skill and ability to perform the tasks aligned to the National Cybersecurity Workforce Framework functional roles. TRC leads the globe in providing "Big 3" cyber consulting quality at a fiscally responsible price. TRC's unique approach to client-first consulting service ensure organizations get best-in-value solutions to address current and future needs related to cyber resiliency, risk management, IT governance, cyber policy, IT/cybersecurity framework integration, workforce development, and general/specific training. TRC solutions to increase cyber resilience across the healthcare, transportation, defense, information technology, energy, communications, chemical, financial, manufacturing, agriculture, federal/state/local government, emergency services, water, and academic sectors.

"We Develop Agile, Competent Cybersecurity Professionals"