2022 · Q3 EDITION

COURSE CATALOG

A guide to technical workforce development

FOCAL POINT ACADEMY
A CDW COMPANY

CDW PEOPLE WHO GET IT

2022 · Q3 EDITION

COURSE CATALOG

FOCAL POINT ACADEMY
A CDW COMPANY

CDW PEOPLE WHO GET IT®

2022 COURSE CATALOG

Offensive and Defensive Cybersecurity

OFFENSIVE AND DEFENSIVE CYBERSECURITY | CS-100

Cyber Risk Management Overview

All organizations face cyber risk in today's world. This seminar-style program covers the fundamentals professionals need to operate their organizations securely, embrace disruption safely, and communicate cyber risks effectively within their organizations. Designed with professionals in mind, this program dissects the most important issues in cyber risk management and arms attendees with the tools needed to engage in strategic cyber risk conversations.

1-day course

Challenge level: 1

Key Outcomes

Successful completion of this course will enable students to:

- Express the importance of a sound cybersecurity strategy in attaining the organization's business goals.
- Recognize areas of vulnerability within the organization and the threats that seek to exploit them.
- Identify the cyber risks to the organization and the practices that will mitigate and eliminate them.
- Practice effective personal cyber hygiene.

Prerequisites

This course is intended for executive-level business leaders (e.g., CEO, CFO, VPs)

Capstone Exercise

Individual lab exercises

Pricing

USD	$950
Learning Credits	1

OFFENSIVE AND DEFENSIVE CYBERSECURITY | CS-101

Intro to Security Analysis

Most IT professionals are aware of the importance their jobs play in securing an organization, but many are not adequately trained in this important function and may not know where to begin. This hands-on course gives a jumpstart into the analysis of network intrusions, compromised hosts, and malware. Students will learn what common attacks look like, how to track and analyze malicious activity, and what mitigation steps should be taken.

2-day course

Challenge level: 2

Key Outcomes

Successful completion of this course will enable students to:

- Profile/baseline the hosts, services, and activity in a computer network.
- Perform user-level attribution of unwanted activity in a network.
- Compare observed network traffic to expected topology.
- Identify and observe the core components of an operating system.
- Conduct basic behavioral analysis of malware on a running Windows system.

Prerequisites

A background in IT

A basic understanding of TCP/IP networking

Basic experience with Windows administration and/or the Sys Internals Suite

Capstone Exercise

Individual lab exercises

Pricing

USD	$1,900
Learning Credits	2

OFFENSIVE AND DEFENSIVE CYBERSECURITY | CT-200

Phishing Investigation

This class teaches new security analysts the basics of responding to phishing attempts. Students will start with a primer in command-line basics and network flow concepts, then learn how to reconstruct the path taken by emails, how to analyze email headers for security issues, how to generate indicators of compromise from suspicious emails, and what the effects can be from a successful phish on systems and networks.

3-day course

Challenge level: 2

Key Outcomes

Successful completion of this course will enable students to:

- Analyze flows of network traffic.
- Describe the protocols and infrastructure used to send and receive email.
- Analyze email messages and other network traffic for signs of phishing.
- Identify and observe the core components of an operating system.
- Conduct basic behavioral analysis of malware on a running Windows system.

Prerequisites

IT background

A basic understanding of TCP/IP networking

Basic experience with a protocol analyzer

Capstone Exercise

Individual lab exercises

Pricing

USD	$2,850
Learning Credits	3

OFFENSIVE AND DEFENSIVE CYBERSECURITY | CT-300

Network Forensics and Investigation I

Network Forensics and Investigation I teaches students to differentiate between normal and abnormal network traffic, understand how packets flow through a network, and attribute conversations and actions taken over a network segment to specific hosts or users. This course focuses on research, filtering, and comparative analysis to identify and attribute different types of activity. Students will learn to follow conversations across a wide range of protocols and through redirection, as well as how to develop custom filters for non-dissected protocols.

5 5-day course

3 Challenge level: 3

Key Outcomes

Successful completion of this course will enable students to:

- Create a baseline of the protocols, hosts, and interactions in a network environment.
- Identify anomalous network traffic using a combination of in-depth packet analysis and higher-level statistical analysis.
- Reconstruct event timelines and accurately correlate, or distinguish between, event threads.
- Identify and extract network artifacts for further forensic analysis.
- Compare observed network traffic to expected topology.
- Research and analyze unknown (non-dissected) protocols.
- Track web activity at the user or session level via HTTP header analytics.

Skills Badges and Certifications

Network Traffic Attribution & Reconstruction
Dissection and Analysis of Network Traffic

Prerequisites

Firm understanding of TCP/IP networking

CompTIA Network+, Cisco CNET or similar

Experience with a packet analyzer

CompTIA Security+ or similar

Capstone Exercise

A category-based capture-the-flag challenge that culminates in tracking a simulated SCADA intrusion.

Pricing

USD	$4,750
Learning Credits	5

OFFENSIVE AND DEFENSIVE CYBERSECURITY | CT-301

Network Forensics and Investigation II

Building on Network Forensics and Investigation I, this course teaches students how to use advanced tool features to uncover and investigate complex, multi-stage, and hard-to-detect intrusions. By learning to identify statistical patterns, isolate events of interest, and accurately correlate or distinguish between threads of activity, students will gain the skills needed to perform critical, real-time analysis in a production environment. The course employs several traffic analysis tools including Wireshark, Network Miner and RSA's NetWitness Investigator alongside custom tools and scripts.

5 5-day course

3 Challenge level: 3

Key Outcomes

Successful completion of this course will enable students to:

- Identify and analyze events at all stages of the attack lifecycle.
- Apply threat intelligence feeds to focus monitoring, investigation, and hunt activities.
- Detect and investigate tunneling, botnet command & control traffic, and other forms of covert communications being utilized in a network.
- Employ fingerprinting techniques to detect the use of encrypted traffic flows by malware or an active intruder.
- Accurately correlate and reconstruct multiple stages of malicious activity in order to build a complete picture of the scope and impact of complex network intrusions.

Skills Badges and Certifications

Network IOC Identification & Investigation
Advanced Network Forensic Analysis

Prerequisites

CCNA and/or experience as an Incident Handler or similar

Packet analyzer experience

Knowledge of common Web App functionality and architecture

Capstone Exercise

Investigate a complex, multi-stage intrusion. Prepare a report on the attack, document the hacker's activities, and detail the leaked information.

Pricing

USD	$4,750
Learning Credits	5

OFFENSIVE AND DEFENSIVE CYBERSECURITY | CT-302

Automated Network Defense

An Intrusion Detection/Prevention System (IDS/IPS) can automate the process of identifying attacks among the thousands of connections on a network. Taught by leaders in network defense who work in the cybersecurity industry, this course demonstrates how to defend large-scale network infrastructures by building and maintaining IDS/IPS and mastering advanced signature-writing techniques. With IDS and trained network security auditors, organizations have a reliable means to prioritize and isolate the most critical threats in real time.

5-day course

Challenge level: 3

Key Outcomes

Successful completion of this course will enable students to:

- Recognize the benefits and limitations of different intrusion detection system types (network-based, host-based, and distributed systems).
- Identify optimal sensor placement and gaps in coverage.
- Write basic IDS signatures to identify traffic of interest and tune them to reduce false positives.
- Use reassembly and pre-processing engines to automatically reconstruct streams of network data prior to analysis.
- Apply decoding and other techniques to overcome IDS evasion efforts.
- Develop complex signatures employing rule chaining, event filtering and post-detection analysis to identify distributed attacks, multi-stage events, and other more complex threats.
- Use regular expressions to effectively detect variable or morphing attacks.
- Manage rule sets to reduce redundancy and maintain system efficiency.

Skills Badges and Certifications

IDS Signature Creation and Optimization
Automated Network Threat Mitigation

Prerequisites

A strong understanding of TCP/IP networking

Network Forensics and Investigation I and II

Capstone Exercise

Identify and analyze the elements of a multistage intrusion. Configure and tune an IDS/IPS to detect and mitigate these attacks.

Pricing

USD	$4,750
Learning Credits	5

OFFENSIVE AND DEFENSIVE CYBERSECURITY | OS-300

Endpoint Live Forensics

Endpoint Live Forensics teaches students how to identify abnormal activity and investigate a running system that may have been compromised. In this course, students will learn the most useful commands, tools and techniques that can be employed during investigation to reveal the significant indicators of infiltration, as well as how to create a system baseline to be used for future analysis. This course is focused primarily on the Windows 10 and Linux operating systems.

5-day course

Challenge level: 3

Key Outcomes

Successful completion of this course will enable students to:

- Identify the core components of the operating system and a certain a current state, using built-in or other trusted tools.
- Analyze a running system and detect abnormal behavior relating to operating system components.
- Use event log analysis to verify and correlate the artifacts of anomalous behavior and determine the scope of an intrusion.
- Build or modify PowerShell scripts to Interrogate an operating system and automate repetitive analytic tasks.
- Create and use a system baseline to identify unexpected items, such as rogue accounts or configuration changes.

Skills Badges and Certifications

Live Windows Endpoint Analysis
System & Event Log Analysis

Prerequisites

Familiarity with Windows systems and the command line interface

Understanding of TCP/IP networking

Experience with VMware or other virtualization software

Capstone Exercise

An investigation scenario to remotely analyze a network of systems, identify compromised machines, and remediate as appropriate.

Pricing

USD	$4,750
Learning Credits	5

OFFENSIVE AND DEFENSIVE CYBERSECURITY | HK-300

Hacker Methodologies for the Security Professional

This course teaches the processes threat actors use to break into organizations' networks and steal their most sensitive data. Utilizing Kali Linux and the Metasploit Framework, students will learn to identify, scan, and enumerate target systems, correlate services to vulnerabilities and exploits, employ exploits to gain access to the target systems, elevate privileges, propagate through the network, and cover their tracks within a target network. This course is focused primarily on Linux and Windows operating systems.

5 5-day course

4 Challenge level: 4

Key Outcomes

Successful completion of this course will enable students to:

- Identify the classes of hackers, their motivations, and the methodologies employed by threat actors.
- Use publicly available tools and open-source intelligence techniques to develop a target footprint.
- Scan and enumerate targets to identify target operating systems and services.
- Research and leverage exploits for vulnerable services to achieve access to target systems.
- Identify system configuration weaknesses and viable privilege escalation tactics.
- Analyze exploited systems to identify and remove indications of compromise.
- Employ system tools to exploit additional targets within an internal network.

Skills Badges and Certifications

Windows Exploitation
Linux Exploitation
Land & Expand

Prerequisites

Familiar with the Windows and Linux Command Line Interface and the Windows and Linux operating system components and security features

Capstone Exercise

Red team exercise requiring teams to establish initial access to a DMZ, pivot to other network segments, and retrieve requested information.

Pricing

USD	$4,750
Learning Credits	5

OFFENSIVE AND DEFENSIVE CYBERSECURITY | PY-300

Threat Hunting with Python

This intermediate-level course teaches students how to use threat-hunting hypotheses generated from contextual data or threat intelligence feeds to write Python scripts that interact with various data sources and perform data analytics to determine the validity of those hypotheses. Techniques include the use of advanced data structures, active data gathering using SCAPY and other tools, scripting database or SIEM queries, and more. Successful students will gain the ability to script or automate custom threat hunting tasks.

3-day course

Challenge level: 4

Key Outcomes

Successful completion of this course will enable students to:

- Test cyberthreat hunting hypotheses by creating Python scripts that perform data gathering and analytics.
- Use advanced data structures to store, search, and manipulate data.
- Write Python code to interact with a variety of systems such as SIEM platforms and endpoints, as well as static data sources such as log files and traffic captures.
- Improve the speed and effectiveness of cyberthreat hunting activities through scripting and automation.

Skills Badges and Certifications

Threat Hunting with Python

Prerequisites

Intermediate-level programming experience with Python

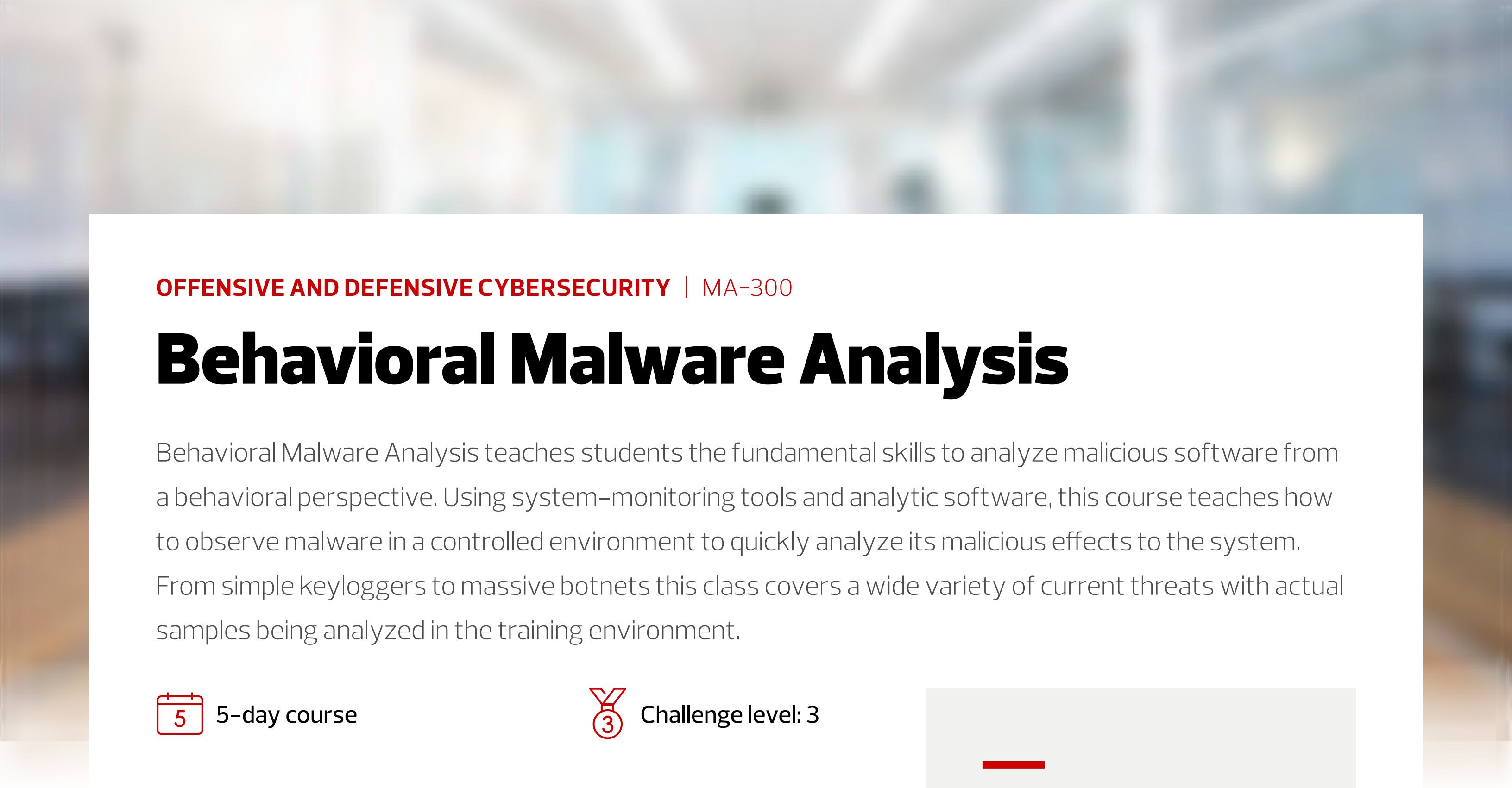
Successful completion of Network Forensics and Investigation II or comparable experience

Capstone Exercise

Given a scenario, develop threat hunting hypotheses, then write Python scripts to gather appropriate data, perform analytics, and produce output.

Pricing

USD	$2,850
Learning Credits	3



OFFENSIVE AND DEFENSIVE CYBERSECURITY | MA-300

Behavioral Malware Analysis

Behavioral Malware Analysis teaches students the fundamental skills to analyze malicious software from a behavioral perspective. Using system-monitoring tools and analytic software, this course teaches how to observe malware in a controlled environment to quickly analyze its malicious effects to the system. From simple keyloggers to massive botnets this class covers a wide variety of current threats with actual samples being analyzed in the training environment.

5-day course

Challenge level: 3

Key Outcomes

Successful completion of this course will enable students to:

- Identify, classify, and document malware and its capabilities.
- Create and customize a virtualized analysis environment.
- Employ common tools to characterize malware samples quickly.
- Identify obfuscation methods used by attackers to escape detection.

Skills Badges and Certifications

Malware Classification
Behavioral Malware Analysis

Prerequisites

Understanding of Windows Operating System administration

Firm understanding of operating system internals

Knowledge of common malware types and exploit vectors

Capstone Exercise

Analyze a current piece of Windows malware and produce a thorough report on its capabilities, system impact, and means of persistence.

Pricing

USD	$4,750
Learning Credits	5

OFFENSIVE AND DEFENSIVE CYBERSECURITY | RE-300

Assembly for Reverse Engineers

Designed for malware analysts and code developers alike, Assembly for Reverse Engineers will equip students with the know-how to effectively read Assembly, review statements, understand program flow, identify the influence of different compilers, and reverse machine code back to its higher-level equivalent. Learn and practice development techniques to improve the speed and quality of static analysis during this weeklong, lab-intensive course.

5 5-day course

3 Challenge level: 3

Key Outcomes

Successful completion of this course will enable students to:

- Describe how code execution works.
- Understand the components of the x86 instruction set.
- Apply demonstrated analysis techniques to the reverse engineering of Windows executables.
- Use IDA Pro's powerful Assembly markup features to optimize analysis.
- Use static and dynamic analysis to interpret and document program flow.

Skills Badges and Certifications

Reverse Engineering User-Mode x86 Windows Binaries
Static Reverse Engineering I

Prerequisites

Knowledge of operating system internals

Experience with C programming in a Windows environment

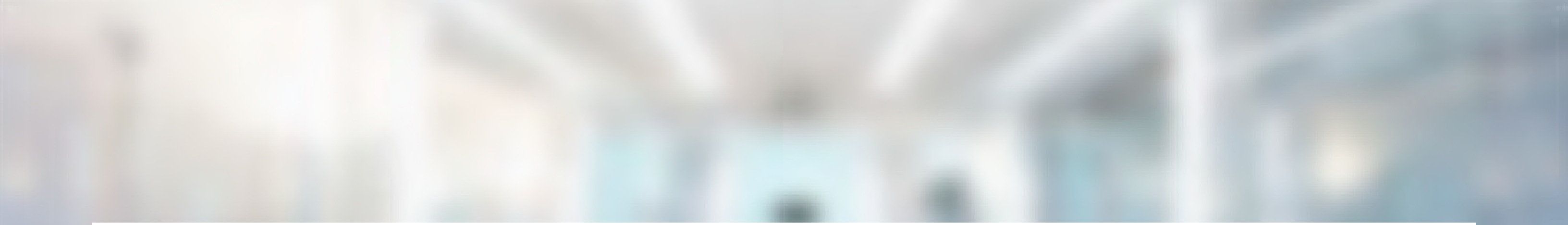
Experience with VMware software is an advantage

Capstone Exercise

A manual stack trace exercise and a reverse engineering assignment to discover and document the function of a given binary.

Pricing

USD	$4,750
Learning Credits	5



OFFENSIVE AND DEFENSIVE CYBERSECURITY | RE-400

Malware Reverse Engineering

This course teaches students how to perform advanced analysis of real-world malware samples using disassembly and debugging techniques. The course also covers data decoding and binary obfuscation to bypass protections and perform effective analysis on hardened samples and how to defeat anti-debugging and other anti-analysis techniques. We will use IDA Pro Disassembler, OllyDbg, and x64dbg, to demonstrate how to accomplish common analysis tasks, overcome malware analysis roadblocks, and achieve a more complete understanding of a malicious sample's functionality.

5 5-day course

Challenge level: 5

Key Outcomes

Successful completion of this course will enable students to:

- Use IDA Pro, OllyDbg, x64dbg and other tools to analyze and debug malware, and report on its capabilities.
- Describe in detail the structure and functions of the Portable Executable (PE) header, and analyze PE headers to aid in malware characterization.
- Apply techniques for identifying, analyzing, and bypassing data obfuscation.
- Understand the structure and use of Dynamic Linked Libraries (DLLs) and apply reverse engineering skills to DLL analysis.
- Identify and overcome a range of anti-debugging and anti-analysis techniques used in modern malware.
- Identify developer code in a compiled binary.

Skills Badges and Certifications

Reverse Engineering User-Mode Windows Malware
Static Reverse Engineering II
Dynamic Reverse Engineering

Prerequisites

Successful completion of Assembly for Reverse Engineers

Understanding of operating system internals

Experience in C and Python programming is recommended

Capstone Exercise

Reverse engineering assignment to analyze and report on a real-world malware sample that employs anti-analysis techniques.

Pricing

USD	$5,700
Learning Credits	6

OFFENSIVE AND DEFENSIVE CYBERSECURITY | RE-500

Python for Reverse Engineers

This course is geared toward the reverse engineer. It introduces a student to the Python language with a focus on using it to accelerate, automate, and optimize reverse engineering tasks. The course starts with an introduction to the Python language, a review of object types and flow statements, then delves into file operations, modules, working with the CTypes library for interaction with Windows operating systems, debugging, and IDA scripting.

5-day course

Challenge level: 4

Key Outcomes

Successful completion of this course will enable students to:

- Write and implement Python scripts used in reverse engineering.
- Use Python to interact with the Windows operating system using the Windows API.
- Create custom event handlers to automate debugging tasks.
- Use Python to automate tasks to debug malware and report on its activities.
- Automate disassembly tasks using IDAPython and other available modules.

Prerequisites

Successful completion of Malware Reverse Engineering

Familiarity with programming/scripting

Experience writing or editing Python scripts

Capstone Exercise

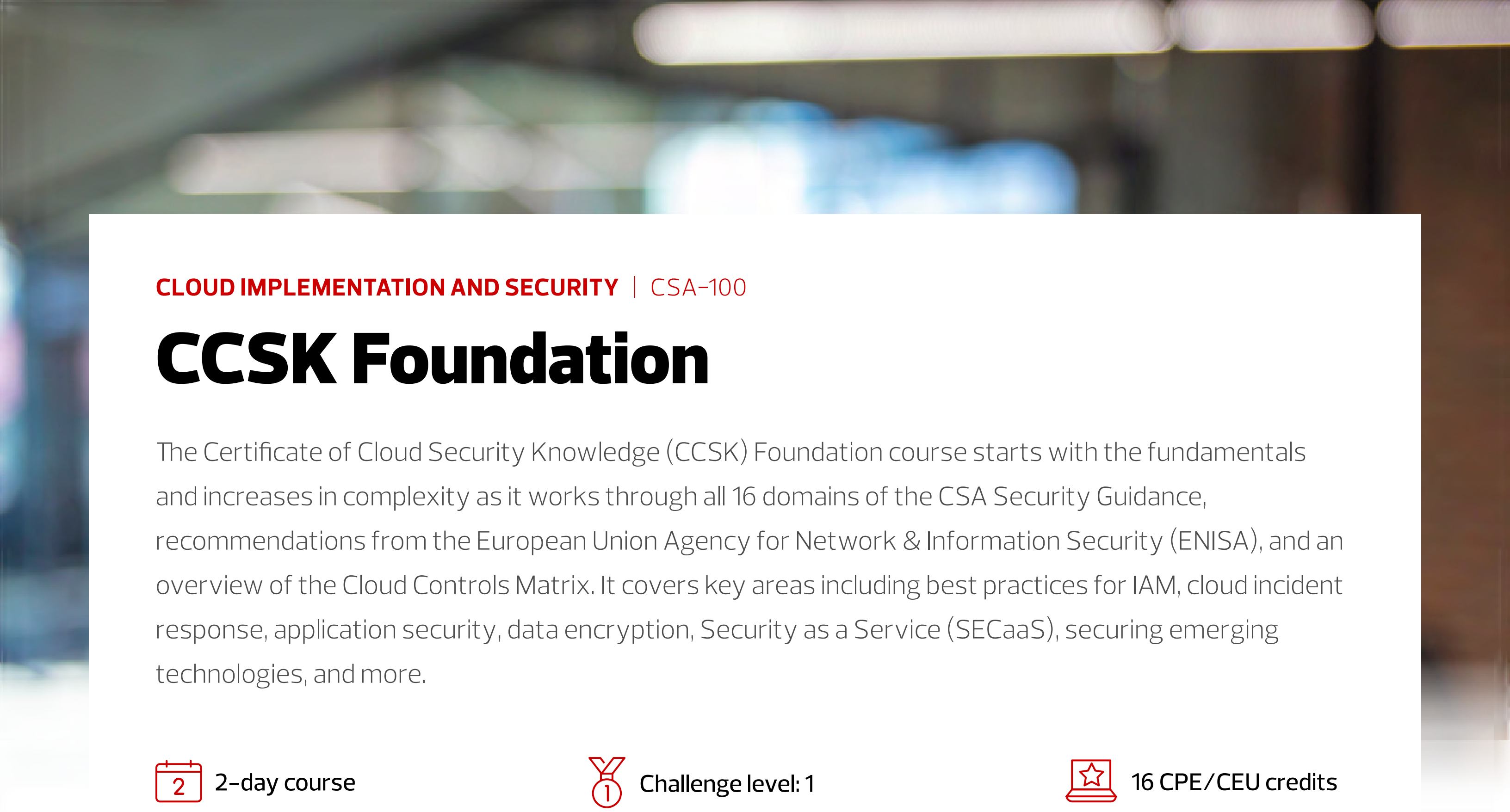
Individual Lab Exercises

Pricing

USD	$5,700
Learning Credits	6

2022 COURSE CATALOG

Cloud Implementation and Security



CLOUD IMPLEMENTATION AND SECURITY | CSA-100

CCSK Foundation

The Certificate of Cloud Security Knowledge (CCSK) Foundation course starts with the fundamentals and increases in complexity as it works through all 16 domains of the CSA Security Guidance, recommendations from the European Union Agency for Network & Information Security (ENISA), and an overview of the Cloud Controls Matrix. It covers key areas including best practices for IAM, cloud incident response, application security, data encryption, Security as a Service (SECaaS), securing emerging technologies, and more.

2-day course

Challenge level: 1

16 CPE/CEU credits

Key Outcomes

Successful completion of this course will enable students to:

- Apply Cloud Security Alliance Security Guidance, Cloud Controls Matrix, and other research to a cloud security program.
- Evaluate how to secure the cloud management plane and ensure business continuity for cloud computing.
- Compare the effectiveness of different access controls and cloud encryption models.
- Develop Security as a Service (SECaaS) recommendations based on organizational requirements and legal obligations.

Skills Badges and Certifications

The Certificate of Cloud Security Knowledge can be obtained by passing the 60-question exam. An exam voucher allowing two attempts is included.

Prerequisites

None

Capstone Exercise

CCSK Exam (Optional)

Pricing

USD	$1,900
Learning Credits	2

CLOUD IMPLEMENTATION AND SECURITY | CSA-200

CCSK Plus – AWS

The CCSK Plus – AWS course covers the foundational content from CCSK Foundation (CSA-100), but also includes hands-on labs and activities that reinforce classroom instruction and build applicable skills. Students engage in a scenario of bringing a fictional organization securely into the cloud, which gives them the opportunity to apply their knowledge by performing a series of activities that would be required in a real-world environment. **This course covers the AWS cloud platform.**

3-day course

Challenge level: 2

24 CPE/CEU credits

Key Outcomes

Successful completion of this course will enable students to:

- Apply Cloud Security Alliance Security Guidance, Cloud Controls Matrix, and other research to a cloud security program in AWS.
- Evaluate how to secure the cloud management plane and ensure business continuity for cloud computing in AWS.
- Compare the effectiveness of different access controls and cloud encryption models in AWS.
- Develop Security as a Service (SECaaS) recommendations based on organizational requirements and legal obligations.

Skills Badges and Certifications

The Certificate of Cloud Security Knowledge can be obtained by passing the 60-question exam. An exam voucher allowing two attempts is included.

Prerequisites

None

Capstone Exercise

CCSK Exam (Optional)

Pricing

USD	$2,850
Learning Credits	3

CLOUD IMPLEMENTATION AND SECURITY | CSA-201

CCSK Plus – Azure

The CCSK Plus – Azure course covers the foundational content from CCSK Foundation (CSA-100), but also includes hands-on labs and activities that reinforce classroom instruction and build applicable skills. Students engage in a scenario of bringing a fictional organization securely into the cloud, which gives them the opportunity to apply their knowledge by performing a series of activities that would be required in a real-world environment. **This course covers the Azure cloud platform.**

3-day course

Challenge level: 2

24 CPE/CEU credits

Key Outcomes

Successful completion of this course will enable students to:

- Apply Cloud Security Alliance Security Guidance, Cloud Controls Matrix, and other research to a cloud security program in Azure.
- Evaluate how to secure the cloud management plane and ensure business continuity for cloud computing in Azure.
- Compare the effectiveness of different access controls and cloud encryption models in Azure.
- Develop Security as a Service (SECaaS) recommendations based on organizational requirements and legal obligations.

Skills Badges and Certifications

The Certificate of Cloud Security Knowledge can be obtained by passing the 60-question exam. An exam voucher allowing two attempts is included.

Prerequisites

None

Capstone Exercise

CCSK Exam (Optional)

Pricing

USD	$2,850
Learning Credits	3

2022 COURSE CATALOG

AppDev, Programming, Secure Coding, and DevSecOps

APPDEV, PROGRAMMING, SECURE CODING, AND DEVSECOPS | SC-200

Securing Web Applications Overview

This course is geared for web developers and technical stakeholders who need to produce secure web applications and integrate security measures into the development process. This overview explores core concepts and challenges in web application security, showcasing current, real-world examples that illustrate the potential consequences of not following these best practices. The final portion of this course builds on the previously learned mechanics for building defenses by exploring how design and analysis can be used to build stronger applications from the beginning of the software lifecycle.

2-day course

Challenge level: 2

16 CPE/CEU credits

Key Outcomes

Successful completion of this course will enable students to:

- Use various tools and techniques to determine a web application's operational environment and determine its vulnerabilities.
- Detect, attack, and implement defenses for authentication, authorization, functionality, and services as well as XSS and Injection attacks.
- Assess the risks associated with XML processing, file uploads, and server-side interpreters and how to best eliminate or mitigate those risks.
- Identify the strengths, limitations, and uses for tools such as code scanners, dynamic scanners, and web application firewalls (WAFs).
- Apply techniques and measures that can be used to harden web and application servers as well as other components in your infrastructure.

Prerequisites

Experience deploying and/or supporting web applications

Prior programming experience is highly recommended

Capstone Exercise

Individual lab exercises

Pricing

USD	$1,900
Learning Credits	2

APPDEV, PROGRAMMING, SECURE CODING, AND DEVSECOPS | SC-201

Exploring the OWASP Top Ten

Exploring the OWASP Top Ten is a series of quick, hard-hitting sessions that set the context for and walks through the OWASP vulnerabilities. Each session provides a solid set of information for developers, testers, and other stakeholders about understanding, identifying, and mitigating a vulnerability. This course provides an understanding of the recently updated OWASP Top Ten with useful insights, discussions, and, in many cases, demonstrations of the application vulnerabilities that are plaguing the industry.

2-day course

Challenge level: 2

16 CPE/CEU credits

Key Outcomes

Successful completion of this course will enable students to:

- Identify and describe the mechanism by which each of the top ten vulnerabilities is exploited.
- Determine the prevalence of each vulnerability, including characteristics to focus on during design and code reviews to help detect potential issues.
- Describe the type and severity of potential consequences when a successful exploit occurs.
- Differentiate the appropriate detection, mitigation, or prevention techniques for each potential exploited vulnerability.
- Assess and outline the relative effectiveness of scanners and other tools in detecting Top Ten vulnerabilities.
- Explore and examine generic and code-specific references that can be used in defensive efforts.

Prerequisites

Real-world programming experience is highly recommended, but not required

Capstone Exercise

Individual lab exercises

Pricing

USD	$1,900
Learning Credits	2

APPDEV, PROGRAMMING, SECURE CODING, AND DEVSECOPS | SC-300

Attacking and Securing Java/JEE Web Applications

Attacking and Securing Java/JEE Web Applications provides unique coverage of Java application security. This course covers penetration testing, hunting for bugs in Java web applications, best practices for defensively coding web applications, and the OWASP Top Ten. Participants will be able to recognize actual and potential software vulnerabilities and implement defenses for those vulnerabilities. Each vulnerability is examined from a Java/JEE perspective by describing the threat and attack mechanisms; recognizing associated vulnerabilities; and designing, implementing, and testing effective defenses.

4-day course

Challenge level: 4

32 CPE/CEU credits

Key Outcomes

Successful completion of this course will enable students to:

- Detect and avoid common mistakes that are made in bug hunting and vulnerability testing.
- Explain concepts and terminology behind defensive, secure coding.
- Configure and test web applications with various attack techniques to determine the existence and effectiveness of layered defenses.
- Identify and implement effective defenses against vulnerabilities associated with untrusted data, XSS and Injection attacks.
- Formulate and employ techniques and measures to harden web and application servers.

Prerequisites

Real-world programming experience is highly recommended

Experience with and working knowledge of Java and JEE

Capstone Exercise

Individual lab exercises

Pricing

USD	$3,800
Learning Credits	4

APPDEV, PROGRAMMING, SECURE CODING, AND DEVSECOPS | SC-301

Secure Web App Development Lifecycle – Java/JEE

This course is geared for web developers and technical stakeholders who need to produce secure web applications by integrating security measures into the development process. This overview explores core concepts and challenges in web application security, showcasing real-world examples that illustrate the potential consequences of not following these best practices. The final portion explores how design and analysis can be used to build stronger applications from the beginning of the software lifecycle.

5-day course

Challenge level: 4

40 CPE/CEU credits

Key Outcomes

Successful completion of this course will enable students to:

- Identify defect/bug reporting mechanisms within their organizations.
- Define concepts and terminology behind defensive, secure coding including the phases and goals of a typical exploit.
- Detect, attack, and implement defenses for vulnerabilities associated with authentication and authorization functionality and services.
- Harden the web and application servers as well as other components in your infrastructure.
- Build, utilize and apply defensive options to an asset inventory for a software application.

Prerequisites

Real-world programming experience is highly recommended, but not required

Capstone Exercise

Individual lab exercises

Pricing

USD	$4,750
Learning Credits	5

APPDEV, PROGRAMMING, SECURE CODING, AND DEVSECOPS | PY-200

Intro to Python Programming

Intro to Python Programming is a hands-on course to help students learn the fundamentals of writing and running basic Python scripts. The course focuses on advanced features such as file operations, regular expressions, working with binary data, and using the extensive functionality of Python modules. Emphasis is placed on features unique to Python, such as tuples, array slices, and output formatting. The course also teaches students to automate or simplify common tasks with scripts for basic web development projects.

3-day course

Challenge level: 2

24 CPE/CEU credits

Key Outcomes

Successful completion of this course will enable students to:

- Create working Python scripts following best practices.
- Configure Python data types appropriately.
- Read and write files with both text and binary data.
- Search and replace text using regular expressions.
- Recognize the standard library and its work-saving modules.
- Create "real-world," professional Python applications.
- Recognize when to use collections such as lists, dictionaries, and sets.
- Determine Pythonic features such as comprehensions and iterators.
- Write robust code, using exception handling.

Prerequisites

Basic familiarity with any programming or scripting language

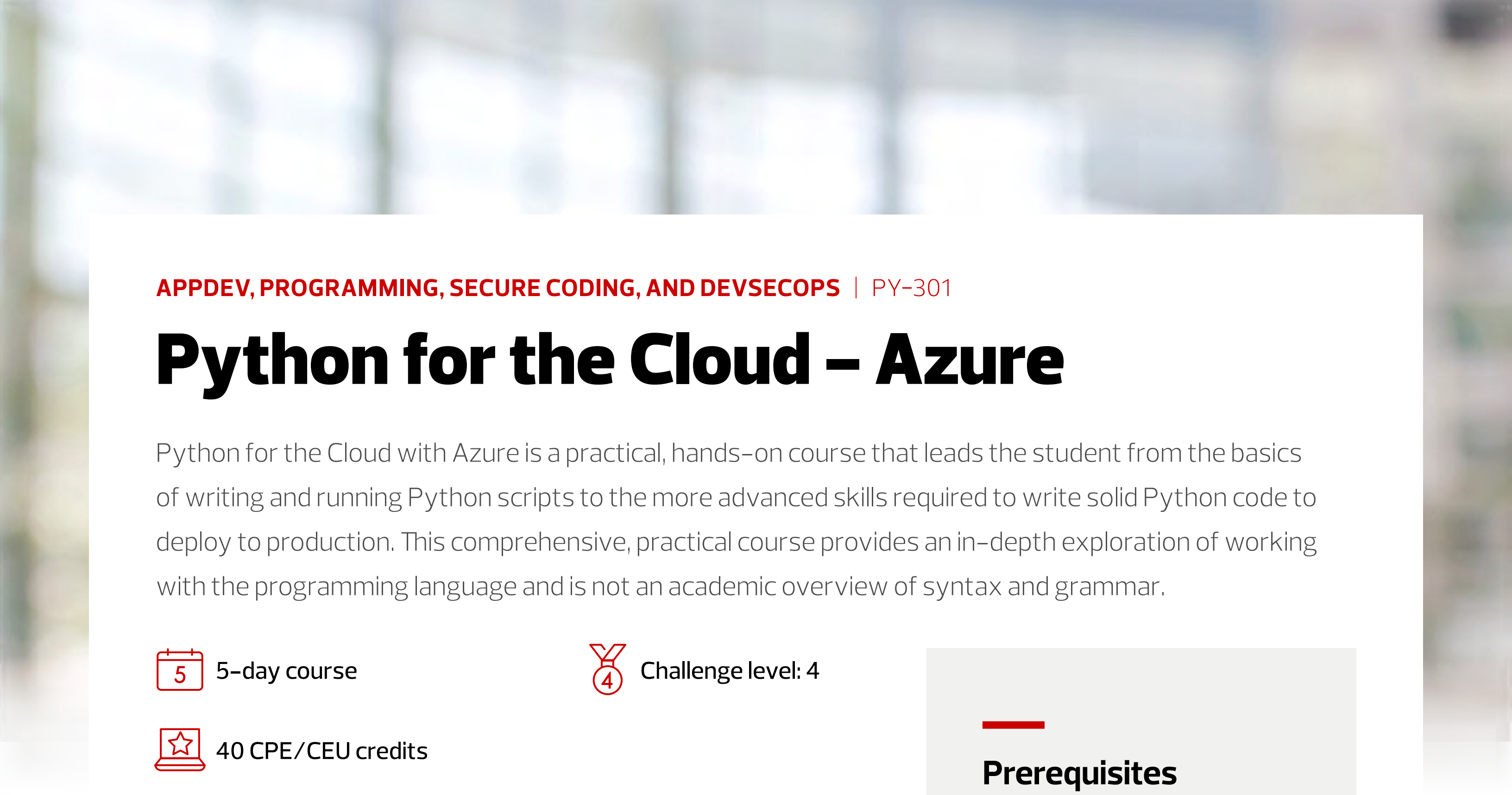
Students should have a working, user-level knowledge of Unix/Linux, Mac, or Windows

Capstone Exercise

Individual lab exercises

Pricing

USD	$1,900
Learning Credits	2



APPDEV, PROGRAMMING, SECURE CODING, AND DEVSECOPS | PY-301

Python for the Cloud – Azure

Python for the Cloud with Azure is a practical, hands-on course that leads the student from the basics of writing and running Python scripts to the more advanced skills required to write solid Python code to deploy to production. This comprehensive, practical course provides an in-depth exploration of working with the programming language and is not an academic overview of syntax and grammar.

5-day course

Challenge level: 4

40 CPE/CEU credits

Key Outcomes

Successful completion of this course will enable students to:

- Perform introductory level Python for analytics with NumPy and Pandas.
- Identify data movement, errors, expectations, and code optimization.
- Describe how to pack and ship code into services and cloud, or container or VM.
- Effectively use the Azure API to interact with Azure in Python.

Prerequisites

Basic familiarity with any programming or scripting language

Working knowledge of Unix/Linux, Mac, or Windows

Comfortable using a command line interface

Capstone Exercise

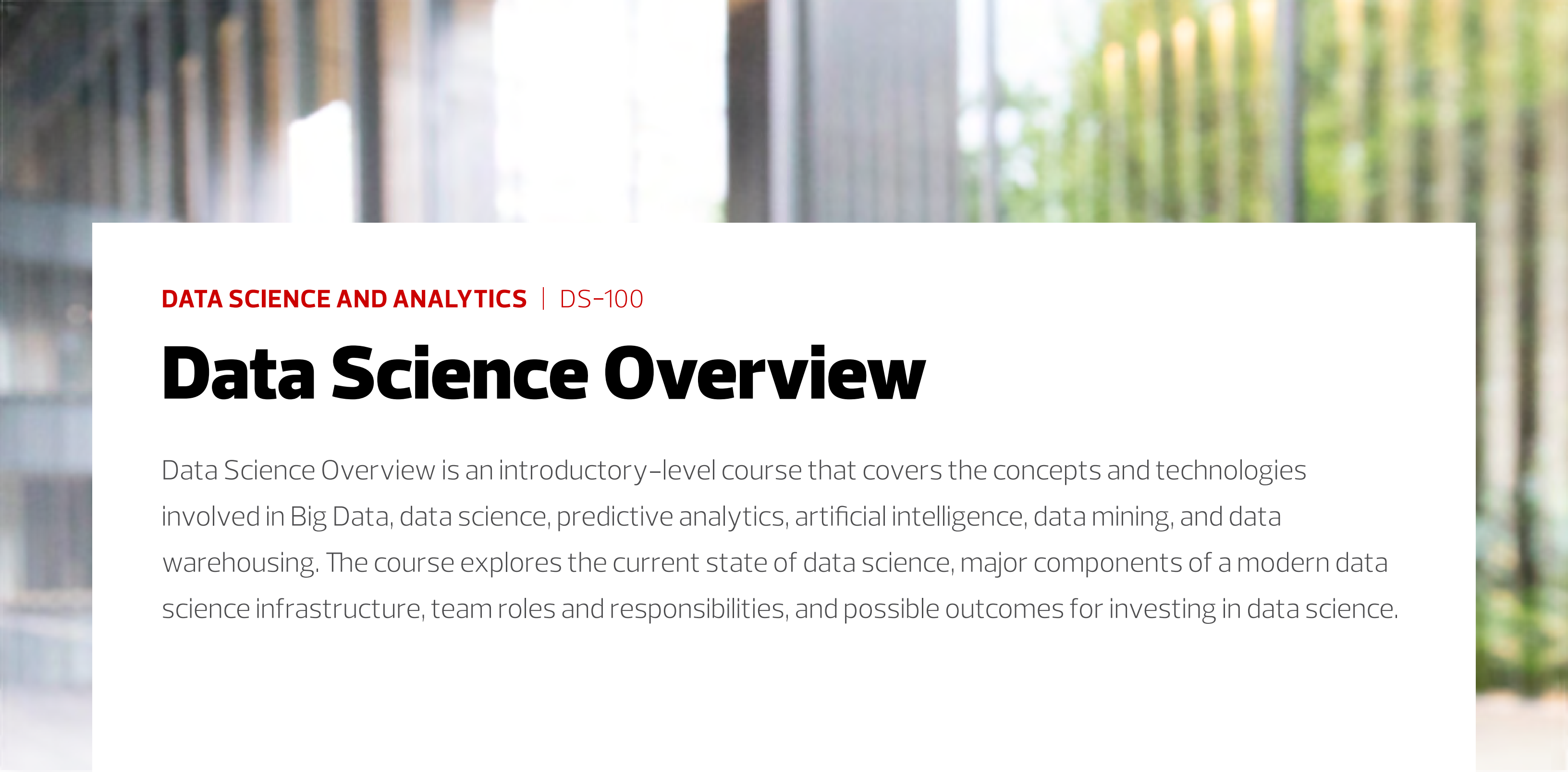
Leverage the skills from throughout the course to create, deliver, and present (optional) a complete, tested solution.

Pricing

USD	$2,850
Learning Credits	3

2022 COURSE CATALOG

Data Science and Analytics



DATA SCIENCE AND ANALYTICS | DS-100

Data Science Overview

Data Science Overview is an introductory-level course that covers the concepts and technologies involved in Big Data, data science, predictive analytics, artificial intelligence, data mining, and data warehousing. The course explores the current state of data science, major components of a modern data science infrastructure, team roles and responsibilities, and possible outcomes for investing in data science.

1-day course

Challenge level: 1

8 CPE/CEU credits

Key Outcomes

Successful completion of this course will enable students to:

- Identify the elements of the Hadoop Ecosystem: HDFS, Resource Navigators, MapReduce, Spark, Distributions.
- Define data science types and terms and explain ETL (Exchange, Transform, Load).
- Summarize data handling, including the common tools used.
- Identify the languages, libraries, and frameworks used in the Hadoop Ecosystem including R, Python, Java, Scala, Pig, and BPMN.
- Apply artificial intelligence principles in business systems.
- Differentiate between the evolving roles and functions in data science.

Prerequisites

Attendees should have prior exposure to enterprise information technology and be familiar with relational databases

Pricing

USD	$950
Learning Credits	1

DATA SCIENCE AND ANALYTICS | DS-200

R Programming for Data Science and Analytics

R Programming for Data Science and Analytics examines components of a statistical programming environment and enables students to describe generic programming language concepts as they are implemented in R. The course focuses on the basics of statistical computing, which includes programming in R, reading data into R, accessing R packages, writing R functions, and visualizing data with R.

3-day course

Challenge level: 3

24 CPE/CEU credits

Key Outcomes

Successful completion of this course will enable students to:

- Identify and define R programming variables, types, loops, scalars, vectors, and matrices.
- Perform string and text manipulation in R.
- Identify and employ R lists and functions.
- Use R data frames and file I/O.
- Read data from files and perform data preparation.
- Perform data visualization using a range of plotting functions.
- Use Dplyr for data exploration.
- Create statistical models with R.
- Use linear and logistic regressions.

Prerequisites

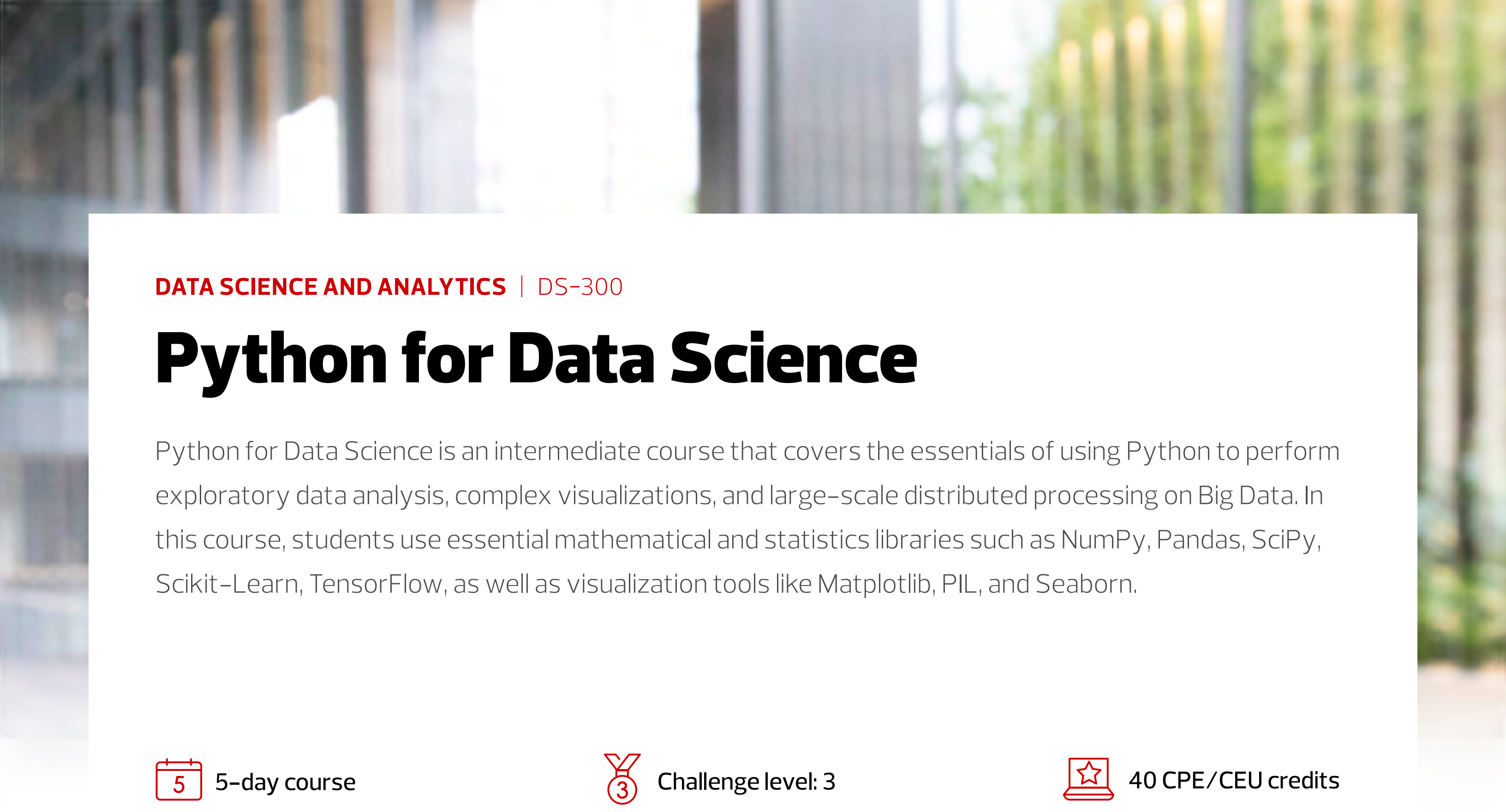
Students should have intermediate-level experience in their field and prior experience working with programming languages

Capstone Exercise

Individual lab exercises

Pricing

USD	$2,850
Learning Credits	3



DATA SCIENCE AND ANALYTICS | DS-300

Python for Data Science

Python for Data Science is an intermediate course that covers the essentials of using Python to perform exploratory data analysis, complex visualizations, and large-scale distributed processing on Big Data. In this course, students use essential mathematical and statistics libraries such as NumPy, Pandas, SciPy, Scikit-Learn, TensorFlow, as well as visualization tools like Matplotlib, PIL, and Seaborn.

5-day course

Challenge level: 3

40 CPE/CEU credits

Key Outcomes

Successful completion of this course will enable students to:

- Write and run Python code in a data science context.
- Create and process images with PIL.
- Apply and visualize with Seaborn.
- Identify Key features of SciPy and Scikit-Learn.
- Interact with Spark using DataFrames.
- Perform Big Data analytics with SparkSQL, MLib, and Streaming.

Prerequisites

Students must have a background in basic Python development skills

Capstone Exercise

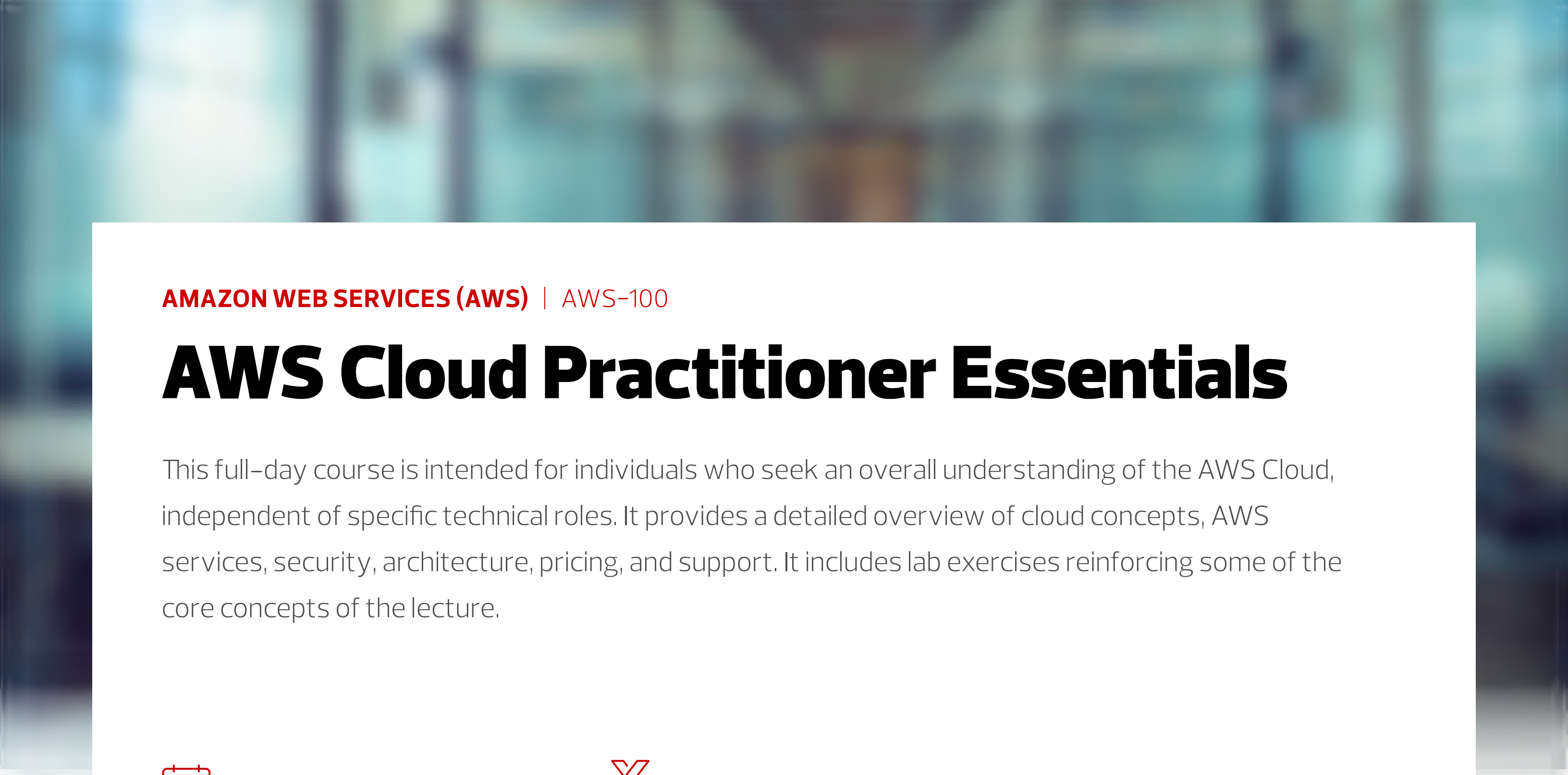
Individual lab exercises

Pricing

USD	$4,750
Learning Credits	5

2022 COURSE CATALOG

Amazon Web Services (AWS)



AMAZON WEB SERVICES (AWS) | AWS-100

AWS Cloud Practitioner Essentials

This full-day course is intended for individuals who seek an overall understanding of the AWS Cloud, independent of specific technical roles. It provides a detailed overview of cloud concepts, AWS services, security, architecture, pricing, and support. It includes lab exercises reinforcing some of the core concepts of the lecture.

1-day course

Challenge level: 2

Key Outcomes

Successful completion of this course will enable students to:

- Differentiate between cloud computing and deployment models.
- Describe the AWS Cloud value proposition.
- Describe the basic global infrastructure of the cloud.
- Compare the different methods of interacting with AWS.
- Describe and differentiate between AWS service domains.
- Describe basic AWS Cloud architectural principles.
- Describe security services with the AWS cloud.

Prerequisites

General IT technical knowledge

Pricing

USD	$675
Learning Credits	0.75

Skills Badges and Certifications

This course helps students prepare for the AWS Certified Cloud Practitioner exam.

AMAZON WEB SERVICES (AWS) | AWS-101

AWS Technical Essentials

In this course, students will learn about AWS products, services, and common solutions. Students will learn the fundamentals of identifying AWS services so that they can make informed decisions about IT solutions based on business requirements.

1 1-day course

2 Challenge level: 2

Key Outcomes

Successful completion of this course will enable students to:

- Create an Amazon Machine Image (AMI) from a running instance.
- Create a load balancer.
- Create a launch configuration and an Auto Scaling group.
- Automatically scale new instances within a private subnet.
- Create Amazon CloudWatch alarms and monitor performance of your infrastructure.

Prerequisites

General IT technical knowledge

Pricing

USD	$675
Learning Credits	0.75

AMAZON WEB SERVICES (AWS) | AWS-300

Security Engineering on AWS

This course demonstrates how to efficiently use AWS security services to stay secure in the AWS Cloud. The course focuses on the security practices that AWS recommends for enhancing the security of your data and systems in the cloud. The course highlights the security features of AWS key services including compute, storage, networking, and database services. You will also learn how to leverage AWS services and tools for automation, continuous monitoring and logging, and responding to security incidents.

3-day course

Challenge level: 3

Key Outcomes

Successful completion of this course will enable students to:

- Assimilate and leverage the AWS shared security responsibility model.
- Architect and build AWS application infrastructures that are protected against the most common security threats.
- Protect data at rest and in transit with encryption.
- Apply security checks and analyses in an automated and reproducible manner.

Skills Badges and Certifications

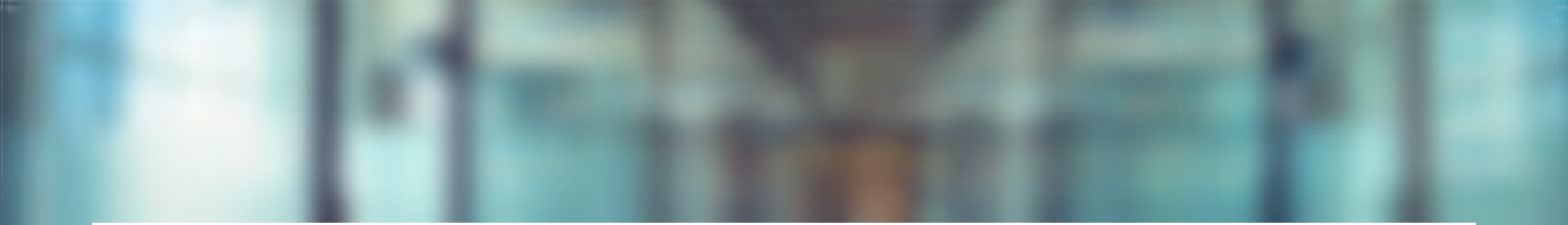
This course helps students prepare for the AWS Certified Security – Specialty exam.

Prerequisites

Working knowledge of IT infrastructure, security, and cloud computing concepts

Pricing

USD	$2,025
Learning Credits	2



AMAZON WEB SERVICES (AWS) | AWS-301

Architecting on AWS

This course covers the fundamentals of building IT infrastructure on the AWS platform. Students learn how to optimize the AWS Cloud by understanding how AWS services fit into cloud-based solutions. In addition, students explore AWS Cloud best practices and design patterns for architecting optimal IT solutions on AWS, and build a variety of infrastructures in guided, hands-on activities. The course also covers how to create fledgling architectures and build them into robust and adaptive solutions.

3-day course

Challenge level: 3

Key Outcomes

Successful completion of this course will enable students to:

- Make architectural decisions based on AWS architectural principles and best practices.
- Leverage AWS services to make your infrastructure scalable, reliable, and highly available.
- Leverage AWS Managed Services to enable greater flexibility and resiliency in an infrastructure.
- Make an AWS-based infrastructure more efficient to increase performance and reduce costs.
- Use the Well Architected Framework to improve architectures with AWS solutions.

Skills Badges and Certifications

This course helps students prepare for the AWS Certified Solutions Architect – Associate exam.

Prerequisites

AWS Cloud Practitioner Essentials

Pricing

USD	$2,025
Learning Credits	2

AMAZON WEB SERVICES (AWS) | AWS-302

System Operations on AWS

This course teaches systems operators and anyone performing system operations functions how to install, configure, automate, monitor, secure, maintain, and troubleshoot the services, networks, and systems on AWS necessary to support business applications. The course also covers specific AWS features, tools, and best practices related to these functions.

3-day course

Challenge level: 3

Key Outcomes

Successful completion of this course will enable students to:

- Automate resource deployment using AWS services such as AWS CloudFormation and AWS Service Catalog.
- Use AWS services to manage AWS resources through SysOps lifecycle processes such as deployments and patches.
- Use Amazon CloudWatch and associated features such as alarms, dashboards, and widgets to monitor your cloud environment.
- Manage permissions and track activity in your cloud environment using AWS services such as AWS CloudTrail and AWS Config.

Skills Badges and Certifications

This course helps students prepare for the AWS Certified SysOps Administration – Associate exam.

Prerequisites

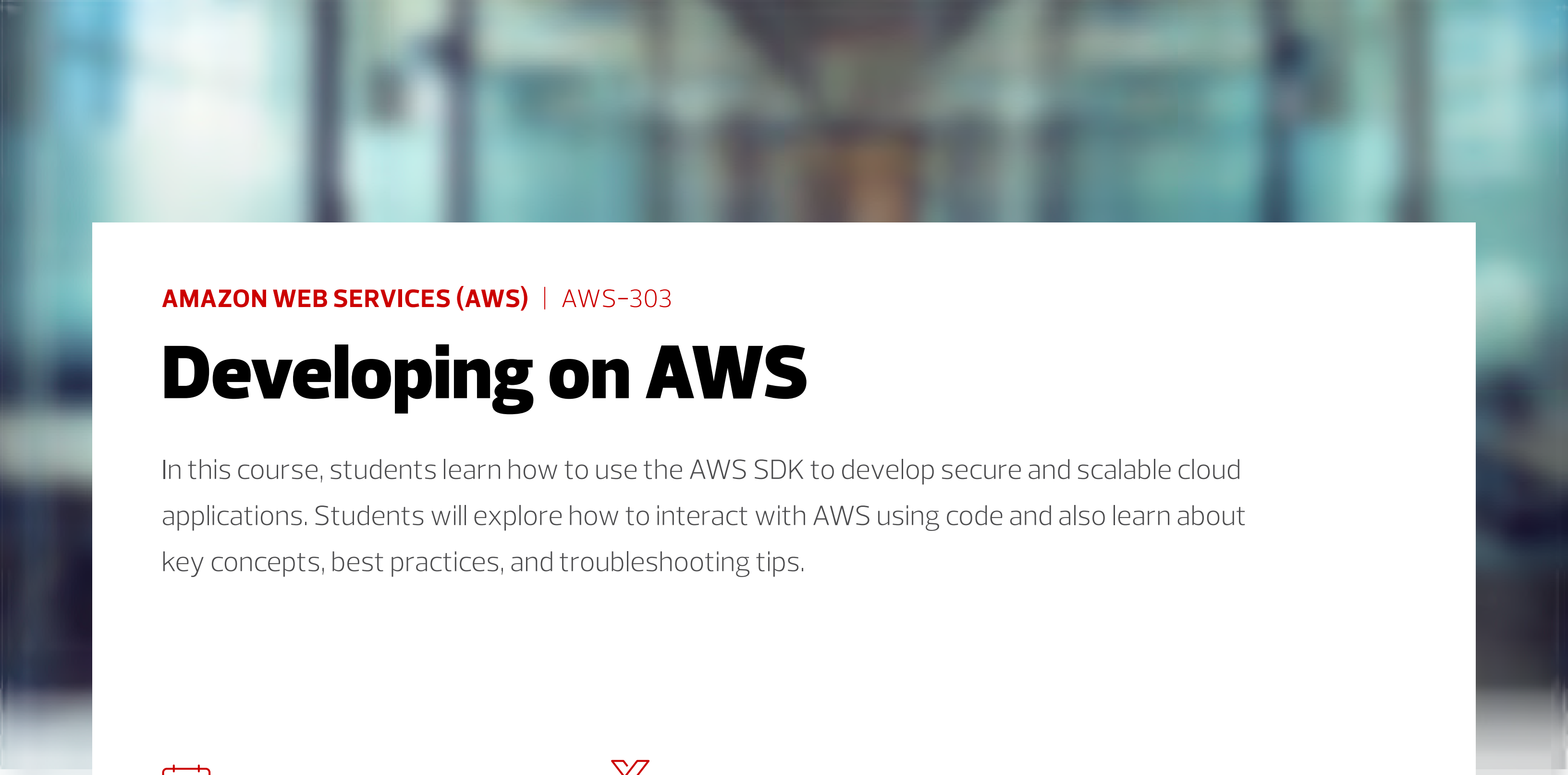
AWS Technical Essentials

Proficiency in managing systems at the command line

Basic knowledge of networking protocols

Pricing

USD	$2,025
Learning Credits	2



Developing on AWS

In this course, students learn how to use the AWS SDK to develop secure and scalable cloud applications. Students will explore how to interact with AWS using code and also learn about key concepts, best practices, and troubleshooting tips.

3-day course

Challenge level: 3

Key Outcomes

Successful completion of this course will enable students to:

- Set up the AWS SDK and developer credentials for Java, C#/.NET, Python, and JavaScript.
- Interact with AWS services and develop solutions by using the AWS SDK.
- Use AWS Identity and Access Management (IAM) for service authentication.
- Use containers in the development process.
- Leverage the CI/CD pipeline to deploy applications on AWS.

Skills Badges and Certifications

This course helps students prepare for the AWS Certified Developer – Associate exam.

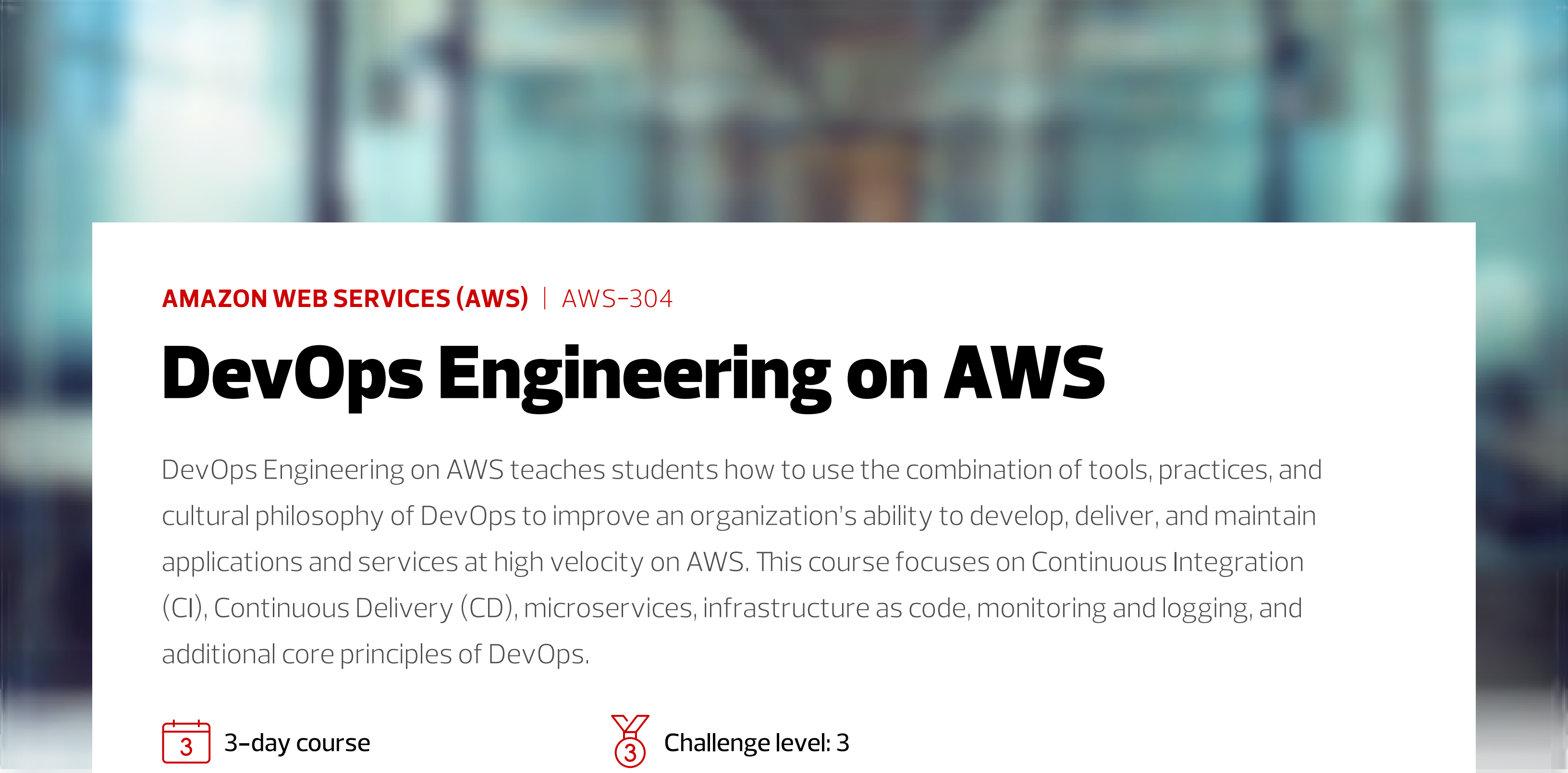
Prerequisites

Expertise in at least one high-level programming language

Working knowledge of core AWS services

Pricing

USD	$2,025
Learning Credits	2



AMAZON WEB SERVICES (AWS) | AWS-304

DevOps Engineering on AWS

DevOps Engineering on AWS teaches students how to use the combination of tools, practices, and cultural philosophy of DevOps to improve an organization's ability to develop, deliver, and maintain applications and services at high velocity on AWS. This course focuses on Continuous Integration (CI), Continuous Delivery (CD), microservices, infrastructure as code, monitoring and logging, and additional core principles of DevOps.

3-day course

Challenge level: 3

Key Outcomes

Successful completion of this course will enable students to:

- 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, AWS CodeBuild, AWS CodePipeline, and AWS CodeStar.
- Implement several common continuous deployment (CD) use cases using AWS technologies.
- Distinguish between the array of application deployment technologies available on AWS, including AWS CodeDeploy, AWS OpsWorks, AWS Elastic Beanstalk, Amazon Elastic Container Service (Amazon ECS), and Amazon Elastic Container Registry (Amazon ECR).
- Leverage automated testing in different stages of a CI/CD pipeline.

Skills Badges and Certifications

This course helps students prepare for the AWS Certified DevOps Engineer – Professional exam.

Prerequisites

Systems Operations on AWS or Developing on AWS

Experience administering Linux or Windows systems at the command-line level

Pricing

USD	$2,025
Learning Credits	2

AMAZON WEB SERVICES (AWS) | AWS-400

Advanced Architecting on AWS

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. This course covers how to build complex solutions which incorporate data services, governance, and security on AWS, and introduces specialized AWS services, including AWS Direct Connect and AWS Storage Gateway to support Hybrid architecture.

3-day course

Challenge level: 4

Key Outcomes

Successful completion of this course will enable students to:

- Connect on-premises data center to AWS cloud.
- Move large data from on-premises data center to AWS.
- Understand different architectural designs for scaling.
- 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.

Skills Badges and Certifications

This course helps students prepare for the AWS Certified Solutions Architect – Professional exam.

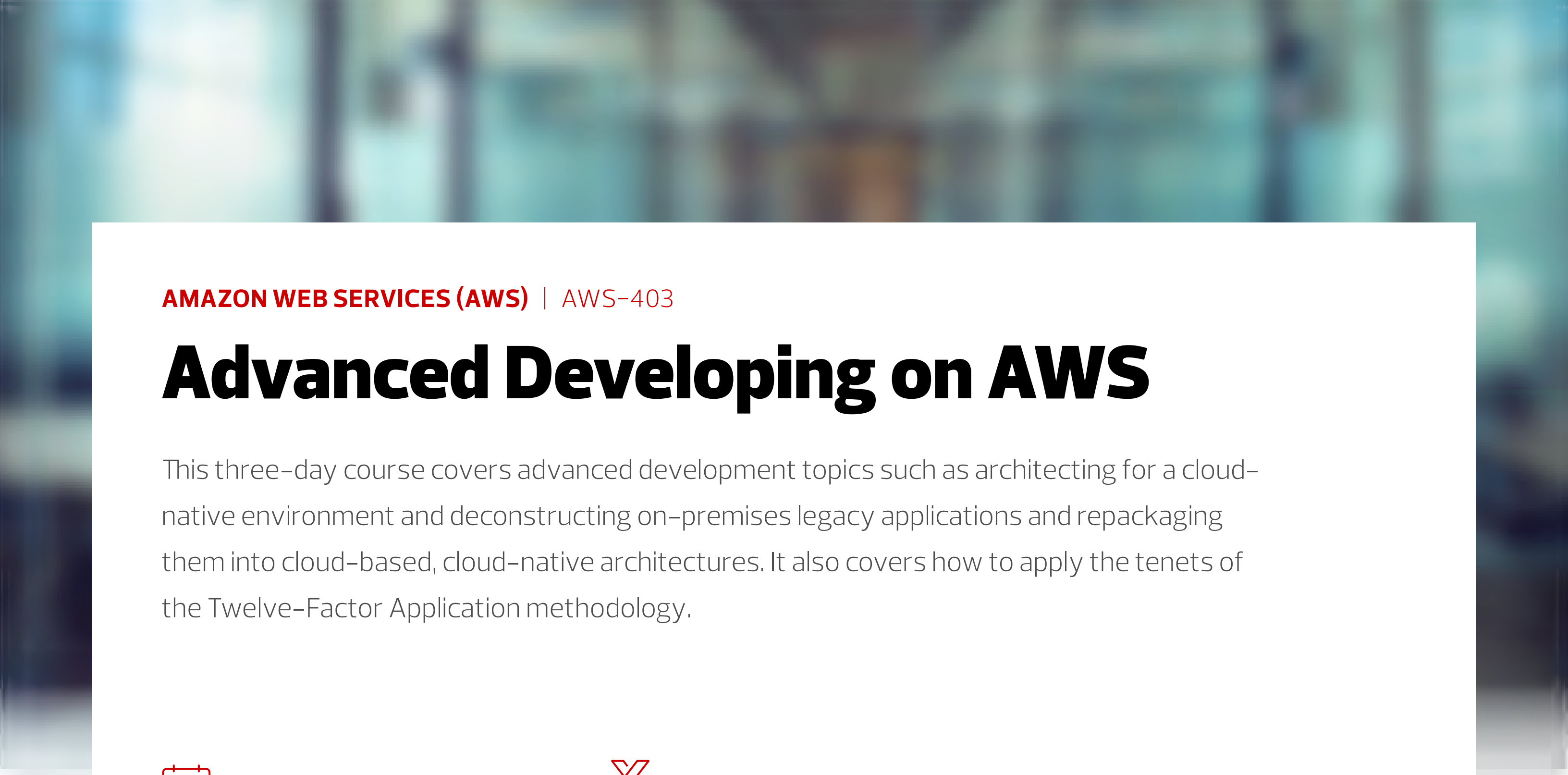
Prerequisites

Architecting on AWS

Achieved AWS Certified Solution Architect – Associate

Pricing

USD	$2,025
Learning Credits	2



AMAZON WEB SERVICES (AWS) | AWS-403

Advanced Developing on AWS

This three-day course covers advanced development topics such as architecting for a cloud-native environment and deconstructing on-premises legacy applications and repackaging them into cloud-based, cloud-native architectures. It also covers how to apply the tenets of the Twelve-Factor Application methodology.

3 3-day course

4 Challenge level: 4

Key Outcomes

Successful completion of this course will enable students to:

- Analyze a monolithic application architecture to determine logical or programmatic break points where the application can be broken up across different AWS services.
- Apply Twelve-Factor Application manifesto concepts and steps while migrating from a monolithic architecture.
- Recommend the appropriate AWS services to develop a microservices-based, cloud-native application.
- Use the AWS API, CLI, and SDKs to monitor and manage AWS services.

Prerequisites

Developing on AWS plus 6 months of real-world experience with the concepts covered

Pricing

USD	$2,025
Learning Credits	2

Skills Badges and Certifications

This course helps students prepare for the AWS Certified DevOps Engineer – Professional exam.

2022 COURSE CATALOG

Cisco

CISCO | CBROPS

Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)

Understanding Cybersecurity Operations Fundamentals (CBROPS) teaches the fundamentals of network infrastructure devices, operations, and vulnerabilities of Transmission Control Protocol/Internet Protocol (TCP/IP). Students will learn basic security concepts, common network application operations and attacks, Windows and Linux operating systems, and the types of data used to investigate security incidents. Following this course, students can perform the job role of an associate-level cybersecurity analyst in a security operations center. This course prepares students for the Cisco Certified CyberOps Associate certification.

5-day course

Challenge level: 2

30 CPE/CEU credits

Key Outcomes

Successful completion of this course will enable students to:

- Explain how a SOC operates and describe the different types of services that are performed from a Tier-1 SOC analyst's perspective.
- Explain Network Security Monitoring (NSM) tools that are available to the network security analyst.
- Describe security flaws in the TCP/IP protocol and how they can be used to attack networks and hosts.
- Understand common endpoint security technologies.
- Understand the kill chain and the diamond models for incident investigations, and the use of exploit kits by threat actors.
- Identify resources for hunting cyberthreats.
- Explain the use of a workflow management system and automation to improve the effectiveness of the SOC.
- Describe a typical incident response plan and the functions of a typical CSIRT.
- Explain the use of VERIS to document security incidents in a standard format.

Skills Badges and Certifications

This course helps prepare students for the following certifications:
Cisco Certified CyberOps Associate

Prerequisites

Implementing and Administering Cisco Solutions (CCNA) course or equivalent

Familiarity with Ethernet and TCP/IP and security concepts

Knowledge of the Windows and Linux

Capstone Exercise

Cisco Certified CyberOps Associate exam (optional)

Pricing

USD	$3,800
Learning Credits	4

CISCO | DCIUCS

Introducing Cisco Unified Computing System (DCIUCS)

The Introducing Cisco Unified Computing System (DCIUCS) v1.0 is an introductory course that shows students how to deploy, secure, operate, and maintain the Cisco Unified Computing system (Cisco UCS®) B-Series blade servers, Cisco UCS C-Series and S-Series rack servers, and Cisco HyperFlex™ product family for use in data centers. Students will gain hands-on practice on basic Cisco UCS server configuration, performing backup and restore activities, and more.

2-day course

Challenge level: 2

12 CPE/CEU credits

Key Outcomes

Successful completion of this course will enable students to:

- Describe Cisco UCS server hardware and connectivity.
- Describe the Cisco HyperFlex Data Platform, its data writing and reading processes, and data optimization.
- Describe and configure Cisco UCS service profiles and profile templates.
- Describe and implement Internet Small Computer Systems Interface (iSCSI) on Cisco UCS.
- Describe and implement Cisco UCS firmware updates and backups.

Prerequisites

General knowledge of servers, routing and switching, storage area networking, and server virtualization

Capstone Exercise

Individual lab exercises

Pricing

USD	$2,850
Learning Credits	3

CISCO | CLCOR

Implementing and Operating Cisco Collaboration Core Technologies (CLCOR)

Implementing Cisco Collaboration Core Technologies (CLCOR) v1.0 helps students prepare for the Cisco® CCNP® Collaboration and CCIE® Collaboration certifications, and advanced-level roles focused on the implementation and operation of Cisco collaboration solutions. Students will gain the knowledge and skills needed to implement and deploy core collaboration and networking technologies, including infrastructure and design, protocols, codecs, and endpoints, Cisco Internetwork Operating System (IOS®) XE gateway and media resources, call control, Quality of Service (QoS), and additional Cisco collaboration applications.

5-day course

Challenge level: 2

64 CPE/CEU credits

Key Outcomes

Successful completion of this course will enable students to:

- Describe the Cisco Collaboration solutions architecture.
- Compare the IP Phone signaling protocols of Session Initiation Protocol (SIP), H323, Media Gateway Control Protocol (MGCP), and Skinny Client Control Protocol (SCCP).
- Integrate and troubleshoot Cisco Unified Communications Manager with LDAP for user synchronization and user authentication.
- Implement Cisco Unified Communications Manager provisioning features and calling privileges.
- Implement and troubleshoot media resources in Cisco Unified Communications Manager.
- Analyze traffic patterns and quality issues in converged IP networks supporting voice, video, and data traffic.
- Define QoS and its models.
- Configure classification and marking options on Cisco Catalyst® switches.

Skills Badges and Certifications

This course helps prepare students for the following certifications:

CCNP Collaboration
CCIE Collaboration
Cisco Certified Specialist - Collaboration Core

Prerequisites

Knowledge of basic terms of computer networking

Basics of digital interfaces, PSTNs, and VoIP

Knowledge of converged voice and data networks and Cisco Unified Communications Manager

Capstone Exercise

Implementing Cisco Collaboration Core Technologies (350-801 CLCOR) exam (optional)

Pricing

USD	$3,800
Learning Credits	4

CISCO | DCACI

Implementing Cisco Application Centric Infrastructure (DCACI)

Implementing Cisco Application Centric Infrastructure (DCACI) v1.0 shows students how to deploy and manage the Cisco® Nexus® 9000 Series Switches in Cisco Application Centric Infrastructure (Cisco ACI®) mode. The course gives students the knowledge and skills to configure and manage Cisco Nexus 9000 Series Switches in ACI mode, connect the Cisco ACI fabric to external networks and services, and to support Virtual Machine Manager (VMM) integration. Students will exercise key capabilities such as fabric discovery, policies, connectivity, and VMM integration.

5-day course

Challenge level: 2

40 CPE/CEU credits

Key Outcomes

Successful completion of this course will enable students to:

- Describe Cisco ACI Fabric Infrastructure and basic Cisco ACI concepts.
- Describe Cisco ACI policy model logical constructs.
- Describe Cisco ACI basic packet forwarding.
- Describe external network connectivity.
- Describe VMM Integration.
- Describe Layer 4 to Layer 7 integrations.
- Explain Cisco ACI management features.

Skills Badges and Certifications

This course helps prepare students for the following certifications:
CCNP Data Center
Cisco Certified Specialist – Data Center ACI Implementation

Prerequisites

Understanding of networking protocols, routing, and switching

Familiarity with ethernet switching products

Understanding of data center architecture

Familiarity with virtualization

Capstone Exercise

Implementing Cisco Application Centric Infrastructure (300-620 DCACI) exam (optional)

Pricing

USD	$3,800
Learning Credits	4

CISCO | DCACIA

Implementing Cisco Application Centric Infrastructure–Advanced

Implementing Cisco Application Centric Infrastructure – Advanced (DCACIA) v1.0 shows students how to integrate the capabilities of the Cisco® Nexus® 9000 Series Switches in Cisco Application Centric Infrastructure (Cisco ACI®) mode. The course covers how to use Cisco ACI as a policy-driven solution that integrates software and hardware, and how to implement Cisco ACI Multi-Pod and Multi-Site deployments. Students will implement advanced ACI capabilities such as Rogue Endpoint Feature, Transit Routing, VRF Route Leaking, Contracts, and Zoning Rules, and Cisco ACI® Multi-Site Orchestrator.

5-day course

Challenge level: 3

40 CPE/CEU credits

Key Outcomes

Successful completion of this course will enable students to:

- Explain Cisco ACI advanced fabric packet forwarding.
- Explain advanced ACI policy and tenant configuration.
- Describe Cisco ACI Multi-Pod deployment.
- Explain the details and consideration of implementing and integrating the traditional network with Cisco ACI.
- Describe Cisco ACI Service Graph Policy-Based Redirect (PBR).
- Describe Cisco ACI Multi-Site deployment.

Prerequisites

Basic understanding of Cisco ACI

Understanding of Cisco data center architecture

Familiarity with virtualization fundamentals

Capstone Exercise

Individual lab exercises

Pricing

USD	$3,800
Learning Credits	4

CISCO | CCNA

Implementing and Administering Cisco Solutions (CCNA)

Through a combination of lecture and hands-on labs, Implementing and Administering Cisco Solutions (CCNA) v1.0 teaches students how to install, operate, configure, and verify basic IPv4 and IPv6 networks. The course covers configuring network components such as switches, routers, and wireless LAN controllers; managing network devices; and identifying basic security threats. The course also provides a foundation in network programmability, automation, and software-defined networking. This course helps students prepare to take the 200-301 Cisco Certified Network Associate (CCNA) exam.

5-day course

Challenge level: 3

30 CPE/CEU credits

Key Outcomes

Successful completion of this course will enable students to:

- Describe the TCP/IP Internet layer, IPv4, its addressing scheme, and subnetting.
- Install a switch and perform the initial configuration.
- Identify and resolve common switched network issues and common problems associated withIPv4 addressing.
- Describe the application and configuration of inter-VLAN routing.
- Explain the basics of dynamic routing protocols and describe components and terms of Open Shortest Path First (OSPF).
- Explain how Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP) work.
- Configure Internet access using Dynamic Host Configuration Protocol (DHCP) clients and explain and configure network address translation (NAT) on Cisco routers.
- Describe the concepts of wireless networks, which types of wireless networks can be built, and how to use Wireless LAN Controllers (WLCs).
- Describe network and device architectures and introduce virtualization.

Skills Badges and Certifications

This course helps prepare students for the following certifications:

Certified Network Associate (CCNA)

CISCO CERTIFIED CCNA 200-301

Prerequisites

Basic computer literacy

Basic PC operating system navigation skills

Knowledge of TCP/IP networking is recommended

Capstone Exercise

CCNA exam (optional)

Pricing

USD	$3,800
Learning Credits	4

CISCO | ENCOR

Implementing and Operating Cisco Enterprise Network Core Technologies (ENCOR)

The Implementing and Operating Cisco Enterprise Network Core Technologies (ENCOR) v1.0 course gives students the knowledge and skills needed to configure, troubleshoot, and manage enterprise wired and wireless networks. Students will also learn to implement security principles within an enterprise network and how to overlay network design by using solutions such as SD-Access and SD-WAN.

5-day course

Challenge level: 3

64 CPE/CEU credits

Key Outcomes

Successful completion of this course will enable students to:

- Illustrate the hierarchical network design model and architecture using the access, distribution, and core layers.
- Compare and contrast the various hardware and software switching mechanisms and operation.
- Implementing internet connectivity within enterprise using static and dynamic Network Address Translation (NAT).
- Describe how APs communicate with WLCs to obtain software, configurations, and centralized management.
- Configure and verify Extensible Authentication Protocol (EAP), WebAuth, and Pre-shared Key (PSK) wireless client authentication on a WLC.
- Explain the use of available network analysis and troubleshooting tools.
- Configure secure administrative access for Cisco IOS devices.
- Explain the purpose, function, features, and workflow of Cisco DNA Center™ Assurance for Intent-Based Networking, for network visibility, proactive monitoring, and application experience.
- Define the components and features of Cisco SD-WAN solutions.

Skills Badges and Certifications

This course helps prepare students for the following certifications:

CCNP® Enterprise
CCIE® Enterprise Infrastructure
CCIE Enterprise Wireless
Cisco Certified Specialist – Enterprise Core

Prerequisites

Basic understanding of enterprise routing and wireless connectivity, Python scription, and enterprise LAN network implementation

Capstone Exercise

This course helps students prepare for the 350-401 Implementing Cisco® Enterprise Network Core Technologies (ENCOR) exam.

Pricing

USD	$3,800
Learning Credits	4

CISCO | SCOR

Implementing and Operating Cisco Security Core Technologies (SCOR)

In this course, students will master the skills and technologies needed to implement core Cisco security solutions to provide advanced threat protection. Students will learn security for networks, cloud and content, endpoint protection, secure network access, visibility, and enforcement. Students will get extensive hands-on experience deploying Cisco Firepower Next-Generation Firewall and Cisco ASA Firewall. Students will get introductory practice on Cisco Stealthwatch Enterprise and Cisco Stealthwatch Cloud.

5-day course

Challenge level: 3

64 CPE/CEU credits

Key Outcomes

Successful completion of this course will enable students to:

- Implement access control on the Cisco ASA appliance and Cisco Firepower Next-Generation Firewall.
- Describe and implement basic email content security features and functions provided by the Cisco Email Security Appliance.
- Describe Cisco Umbrella security capabilities, deployment models, policy management, and Investigate console.
- Describe Cisco secure site-to-site connectivity solutions and explain how to deploy Cisco IOS VTI-based point-to-point IPsec VPNs, and point-to-point IPsec VPN on the Cisco ASA and Cisco Firepower NGFW.
- Describe and deploy Cisco secure remote access connectivity solutions and describe how to configure802.1X and EAP authentication.
- Examine various defenses on Cisco devices that protect the control and management plane.
- Configure and verify Cisco IOS Software Layer 2 and Layer 3 Data Plane Controls.
- Describe Cisco Stealthwatch Enterprise and Stealthwatch Cloud solutions.

Skills Badges and Certifications

This course helps prepare students for the following certifications:

CCNP Security
CCIE Security
Cisco Certified Specialist - Security Core

Prerequisites

Implementing and Administering Cisco Solutions (CCNA) or equivalent

Familiarity with Ethernet, TCP/IP, network security, Windows OS, and Cisco IOS

Capstone Exercise

This course prepares students for the Implementing and Operating Cisco Security Core Technologies (350-701 SCOR) exam.

Pricing

USD	$3,800
Learning Credits	4

CISCO | SCOR

Implementing and Configuring Cisco Identity Services Engine (SISE)

This course shows students how to deploy and use Cisco® Identity Services Engine (ISE) v2.4. This hands-on course provides students with the knowledge and skills to implement and use Cisco ISE, including policy enforcement, profiling services, web authentication and guest access services, BYOD, endpoint compliance services, and TACACS+ device administration. Students will learn how to use Cisco ISE to gain visibility into what is happening in the network, streamline security policy management, and contribute to operational efficiency.

5-day course | Challenge level: 3 | 40 CPE/CEU credits

Key Outcomes

Successful completion of this course will enable students to:

- Describe Cisco ISE deployments, including core deployment components and how they interact to create a cohesive security architecture.
- Describe concepts and configure components related to 802.1X and MAC Authentication Bypass (MAB) authentication, identity management, and certificate services.
- Describe how Cisco ISE policy sets are used to implement authentication and authorization.
- Describe and configure Cisco ISE profiling services, and understand how to monitor these services to enhance your situational awareness about network-connected endpoints. Describe best practices for deploying this profiler service in your specific environment.
- Describe endpoint compliance, compliance components, posture agents, posture deployment and licensing, and the posture service in Cisco ISE.
- Describe and configure TACACS+ device administration using Cisco ISE.
- Migrate TACACS+ functionality from Cisco Secure Access Control System (ACS) to Cisco ISE.

Prerequisites

Familiarity with the Cisco IOS® Software command-line interface (CLI); Cisco AnyConnect® Secure Mobility Client; Microsoft Windows OS; and 802.1X

Capstone Exercise

Individual lab exercises

Pricing

USD	$3,800
Learning Credits	4

CISCO | SSNGFW

Securing Networks with Cisco Firepower Next-Generation Firewall (SSNGFW)

This course introduces the features of Cisco Firepower Threat Defense, including VPN configuration, traffic control, NAT configuration, SSL decryption, and advanced NGFW and NGIPS tuning and configuration. Students will learn how to use and configure Cisco Firepower Threat Defense technology, beginning with initial device setup and configuration. The course will then explore how to implement advanced Next-Generation Firewall (NGFW) and Next-Generation Intrusion Prevention System (NGIPS) features. Students will also learn how to configure site-to-site VPN, remote-access VPN, and SSL decryption.

5 5-day course

3 Challenge level: 3

40 CPE/CEU credits

Key Outcomes

Successful completion of this course will enable students to:

- Describe key concepts of NGIPS and NGFW technology and the Cisco Firepower Threat Defense system, and identify deployment scenarios.
- Perform initial Firepower Threat Defense device configuration and setup tasks.
- Describe how to manage traffic and implement Quality of Service (QoS) using Cisco Firepower Threat Defense.
- Perform an initial network discovery, using Cisco Firepower to identify hosts, applications, and services.
- Describe the behavior, usage, and implementation procedure for access control policies.
- Describe Cisco AMP for Networks and the procedures for implementing file control and Advanced Malware Protection.
- Implement and manage intrusion policies.
- Describe and configure a remote-access SSL VPN that uses Cisco AnyConnect.
- Describe SSL decryption capabilities and usage.

Prerequisites

Technical understanding of TCP/IP networking and network architecture

Basic familiarity with firewall, VPN, and IPS concepts

Capstone Exercise

Individual lab exercises

Pricing

USD	$3,800
Learning Credits	4

CISCO | DEVASC

Developing Applications and Automating Workflows Using Cisco Core Platforms (DEVASC)

The Developing Applications and Automating Workflows Using Cisco Platforms (DEVASC) v1.0 course helps students prepare for the Cisco® DevNet Associate certification and for associate-level network automation engineer roles. Students will learn how to implement basic network applications using Cisco platforms as a base, and how to implement automation workflows across network, security, collaboration, and computing infrastructure. The course gives students hands-on experience solving real-world problems using Cisco Application Programming Interfaces (APIs) and modern development tools.

5-day course

Challenge level: 4

48 CPE/CEU credits

Key Outcomes

Successful completion of this course will enable students to:

- Describe the importance of APIs and use of version control tools in modern software development.
- Describe HTTP concepts and how they apply to network-based APIs.
- Apply Representational State Transfer (REST) concepts to integration with HTTP-based APIs.
- Describe programmability features of different Cisco platforms.
- Describe basic networking concepts and interpret simple network topology.
- Describe interaction of applications with the network and tools used for troubleshooting issues.
- Apply concepts of model-driven programmability to automate common tasks with Python scripts.
- Identify common application deployment models and components in the development pipeline.
- Describe common security concerns and types of tests, and utilize containerization for local development.
- Utilize tools to automate infrastructure through scripting and model-driven programmability.

Skills Badges and Certifications

This course helps prepare students for the following certifications:

Cisco DevNet Associate

Prerequisites

Basic computer literacy

Basic PC operating system navigation skills

Hands-on experience with a programming language (specifically Python)

Capstone Exercise

DevNet Associate exam (optional)

Pricing

USD	$3,800
Learning Credits	4

CISCO | DCIT

Troubleshooting Cisco Data Center Infrastructure (DCIT)

The Troubleshooting Cisco Data Center Infrastructure (DCIT) v7.0 course shows students how to troubleshoot LAN, SAN, Cisco Data Center Unified Fabric, Cisco Unified Computing System (UCS), and Cisco Application-Centric Infrastructure (ACI). Students will learn methodologies and tools to identify issues that may occur in data center network architecture. Students will get extensive hands-on practice troubleshooting installation, configuration and interconnectivity issues on Cisco MDS switches, Cisco Nexus switches, Cisco Fabric Extenders (FEXs), Cisco UCS, Cisco ACI, and more.

5-day course

Challenge level: 4

50 CPE/CEU credits

Key Outcomes

Successful completion of this course will enable students to:

- Identify and resolve issues that are related to: VLANs and PVLANs; port channels and virtual port channels; OTV; and VXLAN.
- Troubleshoot routing protocols such as OSPF, EIGRP, and PIM.
- Identify and resolve Fibre Channel switching issues when the Cisco NX-OS Software is used in switched mode, and in NPV mode.
- Identify and resolve issues that are related to FIP and FCoE.
- Describe Cisco UCS configuration and troubleshoot related issues.
- Describe Cisco IMC tools for validating performance and facilitating data-gathering activities for Cisco UCSC-Series server troubleshooting, and the troubleshooting approach for hardware and firmware failures.
- Define the proper procedures for configuring LAN and SAN connectivity, avoiding issues with the VIC, and troubleshooting connectivity issues.
- Troubleshoot Cisco UCS C-Series server integration with Cisco UCS Manager.
- Describe how to troubleshoot automation, scripting tools, and programmability.

Skills Badges and Certifications

This course helps prepare students for the following certifications:

CCNP Data Center

Cisco Certified Specialist - Data Center Operations

Prerequisites

Ability to configure, secure, and maintain LAN and SAN-based on Cisco Nexus and MDS switches; Cisco Unified Computing System; and Cisco ACI

Capstone Exercise

This course prepares students for the Troubleshooting Cisco Data Center Infrastructure (300-615 DCIT) exam (optional).

Pricing

USD	$3,800
Learning Credits	4

2022 COURSE CATALOG

CompTIA

COMPTIA | TIA-201

CompTIA Security+

The Official CompTIA Security+ Student Guide (SY0-601) has been developed for the CompTIA® certification candidate. This course provides the knowledge and skills required to assess the security posture of an enterprise environment and recommend and implement appropriate security solutions, monitor and secure hybrid environments, operate with an awareness of applicable laws and policies, and identify and respond to security incidents.

5-day course

Challenge level: 2

Key Outcomes

Successful completion of this course will enable students to:

- Compare security roles and controls.
- Explain various threat actors, vectors, and intelligence sources.
- Compare and contrast types of social engineering and malware techniques.
- Implement authentication and authorization solutions, identity and account management controls, secure network designs and network security appliances.
- Differentiate risk management concepts.
- Determine the importance of cybersecurity resilience and physical security controls.

Skills Badges and Certifications

This course helps prepare students for the following certifications: CompTIA Security+

Prerequisites

Basic Windows user skills and an understanding of computer and networking concepts

Experience in networking including configuring security parameters

Capstone Exercise

CompTIA Security+ exam (optional). Exam voucher included.

Pricing

USD	$2,850
Learning Credits	3

COMPTIA | TIA-300

CompTIA Advanced Security Practitioner (CASP+)

CompTIA® Advanced Security Practitioner (CASP+) allows application of critical thinking and judgment across a broad spectrum of security disciplines. It proposes and implements sustainable security solutions that map to organizational strategies and translate business needs into security requirements. It supports IT governance, risk management, security architecture, incident response, and more. This course provides the information and activities to develop that needed skill set to confidently perform as an advanced security practitioner.

5-day course

Challenge level: 3

Key Outcomes

Successful completion of this course will enable students to:

- Support IT governance in the enterprise with an emphasis on managing risk.
- Secure the enterprise through research and analysis.
- Integrate advanced authentication and authorization techniques.
- Implement security controls for hosts and mobile device as well as the network security.
- Examine security in the systems and software development lifecycle.
- Integrate hosts, storage, networks, applications, virtual environments, and cloud technologies in a secure enterprise architecture.

Skills Badges and Certifications

This course helps prepare students for the following certifications:
CompTIA CASP+

Prerequisites

Foundational knowledge of identity and access management (IAM), cryptography, computer networking, and common security technologies used to safeguard the enterprise

Capstone Exercise

CompTIA CASP+ exam (optional). Exam voucher included.

Pricing

USD	$3,800
Learning Credits	4

COMPTIA | TIA-301

CompTIA Cyber Security Analyst (CySA+)

CompTIA Cyber Security Analyst (CySA+) covers the duties of cybersecurity analysts who are responsible for monitoring and detecting security incidents and for executing a proper response to such incidents. The course introduces tools and tactics to manage cybersecurity risks, identify various types of common threats, evaluate the organization's security, collect, and analyze cybersecurity intelligence, and handle incidents as they occur. Ultimately, the course promotes a comprehensive approach to security aimed toward those on the front lines of defense.

5-day course

Challenge level: 3

Key Outcomes

Successful completion of this course will enable students to:

- Assess information security risk in computing and network environments.
- Examine reconnaissance threats to computing and network environments.
- Investigate attacks and analyze post-attack on computing and network environments.
- Implement a vulnerability management program.
- Assess data collected from security and event logs and perform active analysis on assets and networks and respond and investigate cybersecurity incidents.

Skills Badges and Certifications

This course helps prepare students for the following certifications: CompTIA CySA+

Prerequisites

IT background

A basic understanding of TCP/IP networking

Basic experience with a protocol analyzer

Capstone Exercise

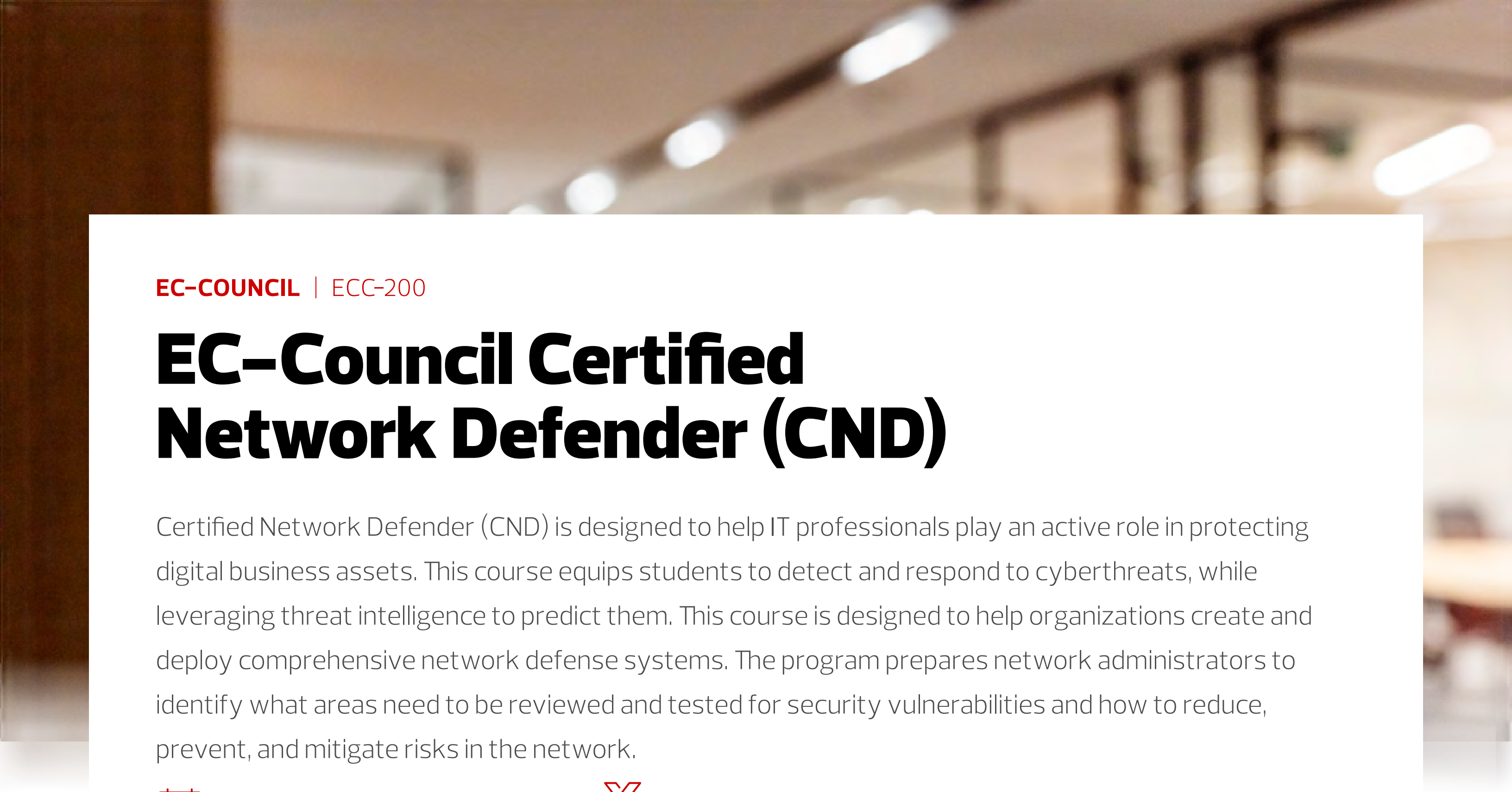
CompTIA CySA+ exam (optional). Exam voucher included.

Pricing

USD	$3,800
Learning Credits	4

2022 COURSE CATALOG

EC-Council



EC-COUNCIL | ECC-200

EC-Council Certified Network Defender (CND)

Certified Network Defender (CND) is designed to help IT professionals play an active role in protecting digital business assets. This course equips students to detect and respond to cyberthreats, while leveraging threat intelligence to predict them. This course is designed to help organizations create and deploy comprehensive network defense systems. The program prepares network administrators to identify what areas need to be reviewed and tested for security vulnerabilities and how to reduce, prevent, and mitigate risks in the network.

5-day course

Challenge level: 3

Key Outcomes

Successful completion of this course will enable students to:

- Recognize network security management, policies, and procedures.
- Apply data security techniques.
- Deploy risk assessment tools.
- Recognize the indicators of compromise, attack, and exposures (IoC, IoA, IoE).
- Establish network authentication, authorization, and accounting (AAA).

Skills Badges and Certifications

This course includes a test voucher for the CND certification exam.

Prerequisites

Basic network and host operations knowledge

Experience commensurate with one to five years of network, host, or application administration

Capstone Exercise

CND exam (optional)

Pricing

USD	$3,800
Learning Credits	4

EC-COUNCIL | ECC-201

EC-Council Certified Ethical Hacker (CEH)

The Certified Ethical Hacker (CEH) provides an in-depth understanding of ethical hacking phases, various attack vectors, and preventive countermeasures. It teaches students how hackers think and act, so that they are better positioned to set up security infrastructure and defend against future attacks. CEH is very hands-on and systematically walks across every ethical hacking domain and methodology, equipping students with the knowledge and skills needed to perform the job of an ethical hacker.

5-day course

Challenge level: 3

Key Outcomes

Successful completion of this course will enable students to:

- Demonstrate an understanding of attack vectors.
- Employ the appropriate tools and techniques to effectively find, exploit, gain access, and pivot on/through target hosts and networks.
- Conduct a variety of web server and web application attacks, including directory traversal, parameter tampering, XSS, etc.
- Perform SQL injection attacks and various types of cryptography attacks.
- Implement a vulnerability analysis to identify security loopholes in a target organization's network, communication infrastructure, end systems, etc.

Skills Badges and Certifications

This course includes a test voucher for the CEH certification exam.

Prerequisites

Minimum two years of IT security experience

A strong working knowledge of TCP/IP

Security+ Prep Course is highly recommended

Capstone Exercise

CEH exam (optional)

Pricing

USD	$3,800
Learning Credits	4

EC-COUNCIL | ECC-202

EC-Council Computer Hacking Forensic Investigator (CHFI)

The Computer Hacking Forensic Investigator (CHFI) course covers major forensic investigation scenarios. It provides a hands-on experience for the forensic investigation techniques and standard tools necessary to successfully carry out a computer forensic investigation. This course helps students to excel in digital evidence acquisition, handling, and analysis in a forensically sound manner. Acceptable in a court of law, these skills will lead to successful prosecutions in various types of security incidents such as data breaches, corporate espionage, insider threats, and other cases involving computer systems.

5-day course

Challenge level: 3

Key Outcomes

Successful completion of this course will enable students to:

- Explain the computer forensic investigation process and the various legal issues involved.
- Perform evidence searching, seizing, and acquisition methodologies in a legally and forensically sound manner.
- Collect data using forensic technology methods in accordance with evidence handling procedures.
- Differentiate between the types of digital evidence, rules of evidence, digital evidence examination process, and electronic crime and digital evidence consideration by crime category.

Skills Badges and Certifications

This course includes a test voucher for the CHFI certification exam.

EC-Council CERTIFIED C|HFI

Prerequisites

None

Capstone Exercise

CHFI exam (optional)

Pricing

USD	$3,800
Learning Credits	4

2022 COURSE CATALOG

(ISC)^2

(ISC)² | ISC-200

Certified Information Systems Security Professional (CISSP)

(ISC)²'s Certified Information Systems Security Professional (CISSP) course is a comprehensive review of information security concepts and industry best practices. This course covers the eight domains of the official CISSP CBK (Common Body of Knowledge). Students will gain knowledge in information security that will increase their ability to successfully implement and manage security programs in any organization or government entity.

5-day course

Challenge level: 2

Key Outcomes

Successful completion of this course will enable students to:

- Apply concepts of confidentiality, integrity, availability, and security governance principles and compliance.
- Align overall organizational operational goals with security functions and implementations.
- Apply appropriate security controls and countermeasures to optimize an organization's operation function and capacity while mitigating risk.
- Assess information systems risks to an organization's operational endeavors.

Skills Badges and Certifications

This course helps prepare students for the CISSP exam.

Prerequisites

CISSP candidates must meet specific requirements, as established by (ISC)²

Capstone Exercise

CISSP exam (optional)

Pricing

USD	$2,850
Learning Credits	3

2022 COURSE CATALOG

Palo Alto Networks

PALO ALTO NETWORKS | EDU-210

Firewall Essentials: Configuration and Management

Firewall Essentials: Configuration and Management is a five-day, instructor-led course that will enhance students' understanding of how to configure and manage Palo Alto Networks Next-Generation Firewalls. The course includes hands-on experience configuring, managing and monitoring a firewall in a lab environment.

5-day course

Challenge level: 3

Key Outcomes

Successful completion of this course will enable students to:

- Configure and manage the essential features of Palo Alto Networks Next-Generation Firewalls.
- Configure and manage Security and NAT policies to enable approved traffic to and from zones.
- Configure and manage Threat Prevention strategies to block traffic from known and unknown IP addresses, domains and URLs.
- Monitor network traffic using the interactive web interface and firewall reports.

Skills Badges and Certifications

This course includes a test voucher for the PCNSA certification exam.

Prerequisites

Basic familiarity with common networking and security concepts

Capstone Exercise

Individual lab exercises

Pricing

USD	$5,000
PAN TC*	50

*Palo Alto Networks Training Credits are purchased through Palo Alto Networks and can be redeemed for CDW courses.

PALO ALTO NETWORKS | EDU-220

Panorama: Managing Firewalls at Scale

Palo Alto Panorama 10.1: Managing Firewalls at Scale is a two-day, instructor-led course that helps students gain in-depth knowledge about how to configure and manage a Palo Alto Networks Panorama management server. Administrators that complete this course will become familiar with the Panorama management server's role in managing and securing the overall network. Students will be shown how to use Panorama aggregated reporting to get a holistic view of a network of Palo Alto Networks Next-Generation Firewalls.

2-day course

Challenge level: 3

Key Outcomes

Successful completion of this course will enable students to:

- Learn how to configure and manage the next-generation Panorama management server.
- Gain experience configuring templates (including template variables) and device groups.
- Gain experience with administration, log collection, and logging and reporting.
- Become familiar with planning and design considerations for Panorama deployment.

Prerequisites

Completion of Firewall Essentials: Configuration and Management (EDU-210)

Basic knowledge of networking concepts

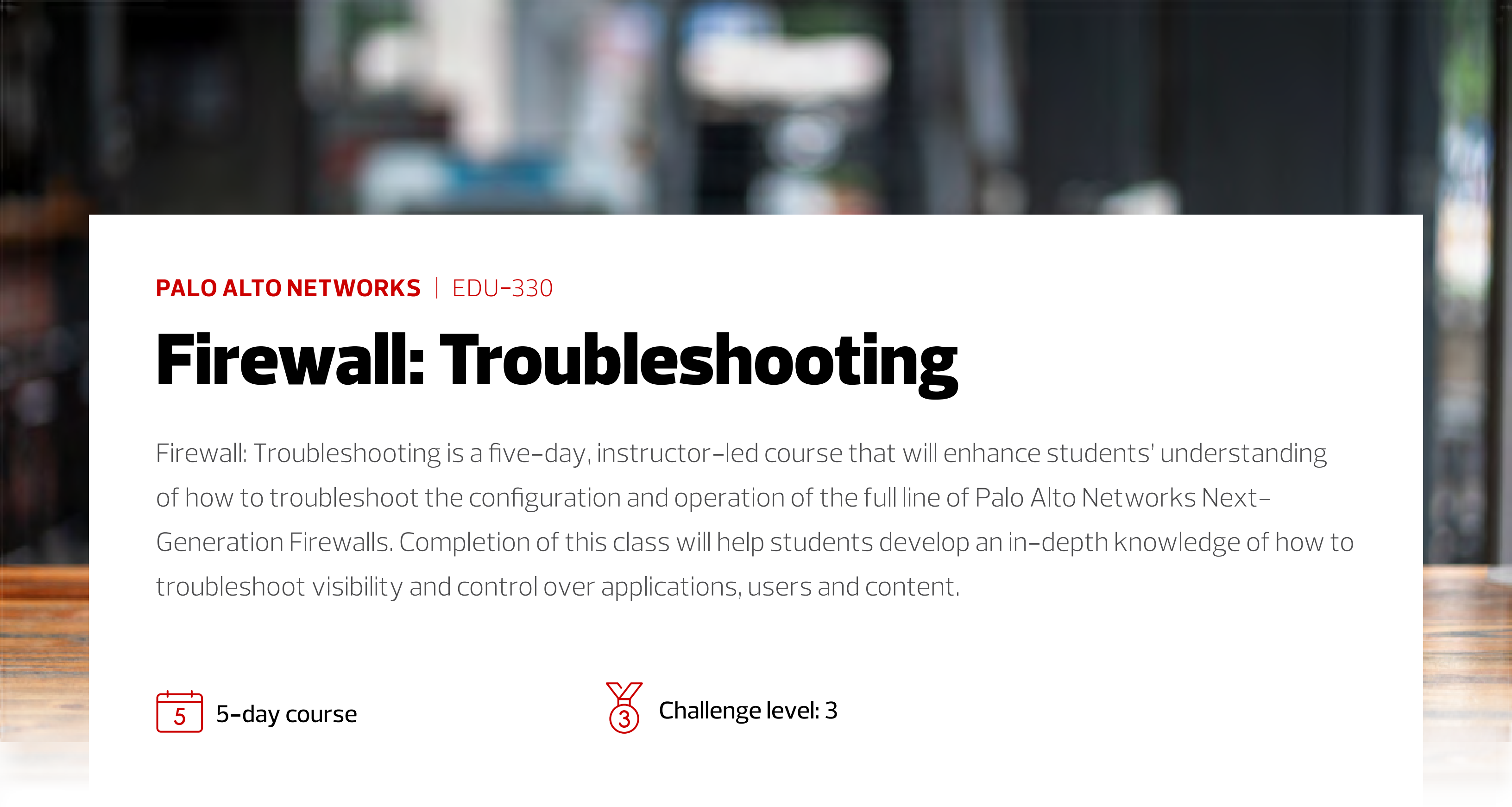
Capstone Exercise

Individual lab exercises

Pricing

USD	$2,000
PAN TC*	20

*Palo Alto Networks Training Credits are purchased through Palo Alto Networks and can be redeemed for CDW courses.



PALO ALTO NETWORKS | EDU-330

Firewall: Troubleshooting

Firewall: Troubleshooting is a five-day, instructor-led course that will enhance students' understanding of how to troubleshoot the configuration and operation of the full line of Palo Alto Networks Next-Generation Firewalls. Completion of this class will help students develop an in-depth knowledge of how to troubleshoot visibility and control over applications, users and content.

5-day course

Challenge level: 3

Key Outcomes

Successful completion of this course will enable students to:

- Use firewall tools, including the CLI, to investigate networking issues.
- Follow proven troubleshooting methodologies that are specific to individual features.
- Analyze advanced logs to resolve various real-life scenarios.
- Solve advanced, scenario-based challenges.

Prerequisites

Completion of Firewall Essentials: Configuration and Management (EDU-210)

Strong practical knowledge of network security concepts

Six months of on-the-job experience with Palo Alto Networks firewalls

Capstone Exercise

Individual lab exercises

Pricing

USD	$5,000
PAN TC*	50

*Palo Alto Networks Training Credits are purchased through Palo Alto Networks and can be redeemed for CDW courses.

PALO ALTO NETWORKS | EDU-238

Prisma SD-WAN: Design and Operation

The Palo Alto Networks Prisma SD-WAN: Design and Operation course describes the next-generation Prisma SD-WAN solution, its capability and the value it provides over legacy WAN and SD-WAN implementations. The five-day, instructor-led course also covers how to configure, operate and troubleshoot the solution. This course is intended for people who must configure, maintain and use wide-area networks, from data centers, to branches, to the cloud.

5-day course

Challenge level: 3

Key Outcomes

Successful completion of this course will enable students to:

- Enhance your understanding of how to design, implement and effectively operate a Prisma SD-WAN solution.
- Configure Prisma SD-WAN with a branch and data center.
- Configure and implement policies.
- Use Prisma SD-WAN services.

Prerequisites

1+ year of
networking experience

Familiarity with
monitoring tools like
LiveAction and Splunk

Experience with DNS, DHCP,
and IP Management Tools

Capstone Exercise

Individual lab exercises

Pricing

USD	$5,000
PAN TC*	50

*Palo Alto Networks Training Credits are purchased through Palo Alto Networks and can be redeemed for CDW courses.

PALO ALTO NETWORKS | EDU-318

Prisma Access SASE Security: Design and Operation

Palo Alto Networks Prisma Access SASE Security: Design and Operation is a four-day, instructor-led course that will help students enhance their understanding of how to better protect applications, remote networks and mobile users using Prisma Access Secure Access Service Edge (SASE) implementation. Students will get hands-on experience configuring, managing and troubleshooting Prisma Access in a lab environment.

4-day course

Challenge level: 4

Key Outcomes

Successful completion of this course will enable students to:

- Learn how to use Prisma Access SASE Security to better protect your applications, remote networks, and mobile users.
- Gain hands-on experience configuring, managing, and troubleshooting Prisma Access in a lab environment.

Prerequisites

Completion of Firewall Essentials: Configuration and Management (EDU-210) and Panorama: Managing Firewalls at Scale course (EDU-220) or have equivalent experience

Capstone Exercise

Individual lab exercises

Pricing

USD	$4,000
PAN TC*	40

*Palo Alto Networks Training Credits are purchased through Palo Alto Networks and can be redeemed for CDW courses.

PALO ALTO NETWORKS | EDU-260

Cortex XDR: Prevention and Deployment

The Palo Alto Networks Cortex XDR: Prevention and Deployment course helps students gain in-depth knowledge about how to configure and manage a Palo Alto Networks Panorama management server. Administrators who complete this course should become familiar with the Panorama management server's role in managing and securing the overall network. Network professionals will be shown how to use Panorama aggregated reporting to provide themselves with a holistic view of a network of Palo Alto Networks Next-Generation Firewalls.

3-day course

Challenge level: 4

Key Outcomes

Successful completion of this course will enable students to:

- Differentiate the architecture and components of Cortex XDR and work with the Cortex XDR management console.
- Differentiate exploit and malware attacks, describe how Cortex XDR blocks them, and perform appropriate response actions.
- Describe the Cortex XDR causality analysis and analytics concepts.
- Manage Cortex XDR rules and investigate threats through the Query Center.

Prerequisites

Familiarity with basic networking concepts

Completion of Firewall Essentials: Configuration and Management (EDU-210)

Capstone Exercise

Individual lab exercises

Pricing

USD	$3,000
PAN TC*	30

*Palo Alto Networks Training Credits are purchased through Palo Alto Networks and can be redeemed for CDW courses.

PALO ALTO NETWORKS | EDU-262

Cortex XDR: Investigation and Response

Palo Alto Networks Cortex XDR: Investigation and Response is a two-day, instructor-led course that teaches students how to use the Incidents pages of the Cortex XDR management console to investigate attacks. It explains causality chains, detectors in the Analytics Engine, alerts versus logs, log stitching and the concepts of causality and analytics.

2-day course

Challenge level: 4

Key Outcomes

Successful completion of this course will enable students to:

- Differentiate the architecture and components of Cortex XDR and learn to investigate and manage incidents.
- Work with Cortex XDR Pro actions such as remote script execution.
- Create and manage the Cortex XDR rules BIOC and IOC.
- Work with Cortex XDR assets and inventories.
- Write XQL queries to search data sets and visualize the result sets.

Prerequisites

Completion of Cortex XDR: Prevention and Deployment (EDU-260)

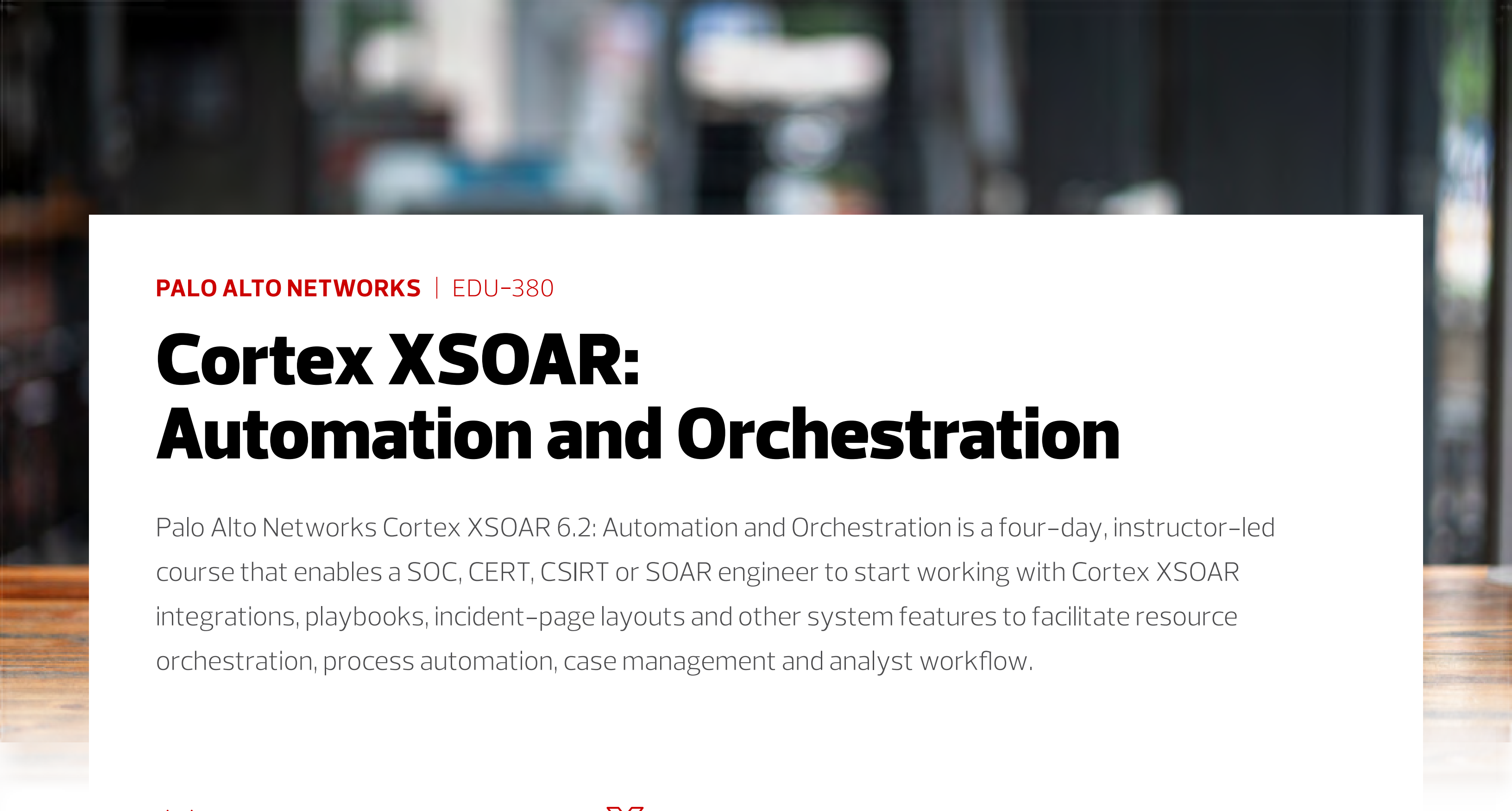
Capstone Exercise

Individual lab exercises

Pricing

USD	$2,000
PAN TC*	20

*Palo Alto Networks Training Credits are purchased through Palo Alto Networks and can be redeemed for CDW courses.



PALO ALTO NETWORKS | EDU-380

Cortex XSOAR: Automation and Orchestration

Palo Alto Networks Cortex XSOAR 6.2: Automation and Orchestration is a four-day, instructor-led course that enables a SOC, CERT, CSIRT or SOAR engineer to start working with Cortex XSOAR integrations, playbooks, incident-page layouts and other system features to facilitate resource orchestration, process automation, case management and analyst workflow.

4-day course

Challenge level: 5

Key Outcomes

Successful completion of this course will enable students to:

- Configure integrations, create tasks, and develop playbooks
- Build incident layouts that enable analysts to triage and investigate incidents efficiently.
- Identify how to categorize event information and map that information to display fields.
- Develop automations, manage content, indicator data, and artifact stores, schedule jobs, organize users and user roles, oversee case management, and foster collaboration.

Prerequisites

Completion of the Cortex XSOAR Analyst digital learning

Python and JavaScript knowledge is useful but not required

Capstone Exercise

Individual lab exercises

Pricing

USD	$4,000
PAN TC*	40

*Palo Alto Networks Training Credits are purchased through Palo Alto Networks and can be redeemed for CDW courses.

FOCAL POINT

ACADEMY

A CDW® COMPANY