
CHECK POINT
FIRST EDITION
Infinity
Global Services
TRAINING CATALOG
April 2025

TABLE OF CONTENTS

STRENGTHENING CYBER SECURITY THROUGH SKILLS

In today's hyper connected world, cyber threats are always evolving. Check Point Research notes a 30% spike in global cyber attacks in Q2 of 2024—the highest in two years. This surge highlights the need for organizations to invest in security education and proactive defense strategies. A well-informed workforce, backed by advanced security solutions, is the best defense against rising cyber risks.

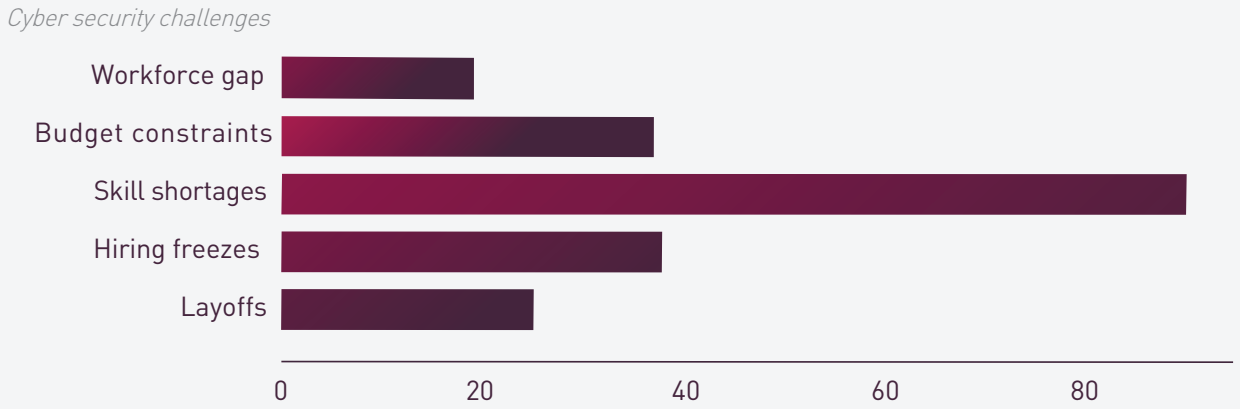
Despite the growing threats, the biggest challenge remains a shortage of skilled cyber security professionals. The 2024 ISC2 Cyber Security Workforce Study reports that while the global workforce holds steady at 5.5 million, the skills gap has grown to 4.8 million - a 19% jump from last year. This gap makes continuous upskilling and reskilling essential if organizations want to maintain their business continuity and growth.

Organizations must prioritize continuous learning to stay ahead of cyber threats. A strong cyber security strategy isn't just about technology—it's about people. Upskilling teams helps businesses keep pace with emerging threats and adapt to new attack techniques. As indicated in the ISC2 study, over 92% of organizations recognize the importance of skill development in maintaining strong cybersecurity defenses. Investing in training boosts security, enhances employee retention, and strengthens overall resilience.

Infinity Global Services (IGS) is helping bridge this gap with training programs that equip professionals with vital cyber security skills. Through hands-on learning and industry-leading expertise, IGS empowers IT teams to strengthen defenses, safeguard assets, and stay ahead of evolving cyber challenges. By fostering continuous skill development, businesses can protect themselves from immediate threats while securing their future in an ever-changing digital landscape.

TOP CYBER SECURITY CHALLENGES IN 2024 (ISC2 STUDY)

Source:
2024 ISC2 Cyber Security Workforce Study



ABOUT INFINITY GLOBAL SERVICES TRAINING PROGRAMS

We understand that staying ahead of emerging threats requires more than just cutting-edge technology—it demands a workforce equipped with the skills and knowledge to proactively identify, mitigate, and respond to risks. Our training programs are designed to provide cyber security professionals, IT teams, and decision-makers with the expertise needed to navigate complex security challenges.

KEY BENEFITS

- **Expert-Led Instruction:** Learn from seasoned industry experts with real-world experience in combating cyber threats.
- **Practical, Hands-On Learning:** Gain actionable skills through immersive labs and simulations based on real-world scenarios.
- **Tailored for All Skill Levels:** Whether you're a beginner or an experienced professional, our diverse course offerings cater to all levels of expertise.
- **Global Recognition:** Earn certifications that are recognized and respected across industries worldwide.

Join the thousands of professionals who have transformed their careers and strengthened their organizations through our training programs. Together, we can build a safer and more resilient digital future.

IGS FLEX CREDITS

Your Gateway to Cyber Security Knowledge

Infinity Global Services (IGS) Credits are the way to consume our diverse cyber security training programs and services. Designed for flexibility and convenience, IGS Credits provide organizations and individuals with a streamlined way to access our comprehensive suite of courses, workshops, and certifications.

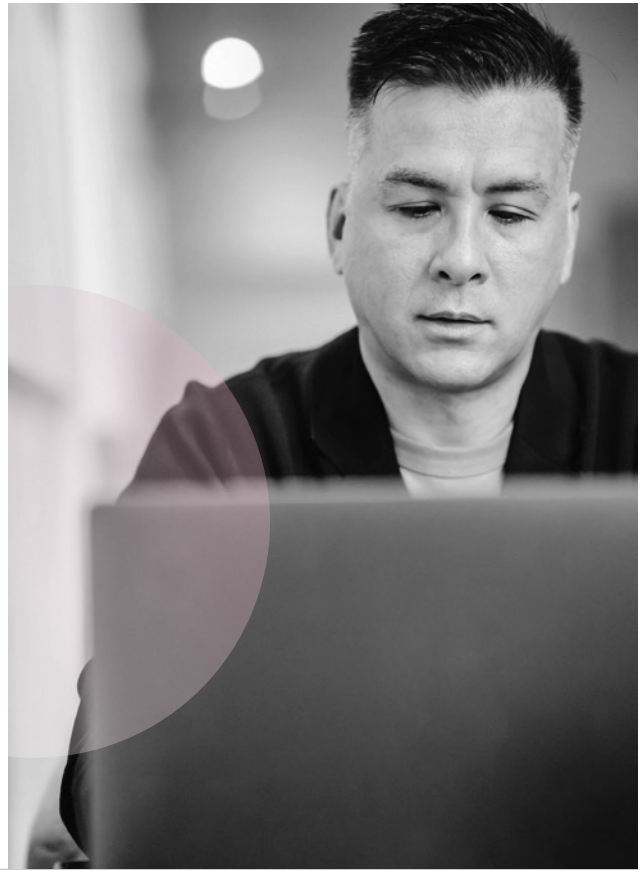
How to Purchase and Redeem IGS Credits?

IGS credits can be purchased through the Check Point Product Catalog. The variety and flexibility of accessible services empower you to make the most of your cyber security investments while meeting your business goals.
To redeem your IGS Credits, please enter the IGS portal.

The IGS Credits Calculator Tool

The IGS Calculator offers a convenient way to pre-determine the number of credits to purchase for your desired services with each service having a specific credit value.

Go to the Calculator



CHECK POINT CERTIFICATIONS

Enabling cyber security professionals to develop the knowledge and skills required to administer, deploy, and manage Check Point solutions.

CERTIFICATION PATHS

YOUR JOURNEY TO CYBER SECURITY MASTERSHIP

CORE CERTIFICATIONS

Certified Security Administrator (CCSA)

This core technical certification course provides an understanding of basic concepts and skills necessary to configure and manage Check Point Security Gateways and Management Software Blades.

Certified Security Expert (CCSE)

This advanced security engineering course provides an in-depth explanation of Check Point technology and an understanding of skills necessary to effectively design, maintain, optimize, and protect your enterprise network from aggressive cyber threats.

SECURITY MASTER CERTIFICATIONS

Check Point Certified Security Master

The CCSM certification recognizes and validates technical mastery of the Check Point Infinity architecture. It is awarded to cyber security professionals with advanced knowledge and expertise in configuring, deploying, managing, and troubleshooting Check Point products and services.

Check Point Certified Security Master Elite

The CCSM Elite certification validates the highest achievement of technical mastery and consists of an elite club of Check Point Certified Security Masters.

*Certification badges are distributed upon course completion and exam

CERTIFICATION PATH TO CYBER SECURITY MASTERY

CHECK POINT CERTIFIED SECURITY MASTER

With Check Point's path to security mastery, you need to achieve 2 Infinity Specialist Accreditations after the CCSE.

CHECK POINT CERTIFIED SECURITY MASTER ELITE

To achieve Check Point's Security Master Elite, you need to pass 2 Infinity Specialist Accreditations after the CCSM.

AUTHORIZED TRAINING CENTER PARTNER PROGRAM

Our global network of certified training partners delivers hands-on, expert-led courses designed to equip professionals with the knowledge and skills needed to protect their organizations. Whether you're looking to achieve Check Point certifications, strengthen your security posture, or stay ahead of evolving threats, our ATC partners provide industry-leading education tailored to your needs.

Link to ATC Locator

Certification Training – Core

CHECK POINT CERTIFIED SECURITY ADMINISTRATOR (CCSA) R81.20

Duration: 3 days

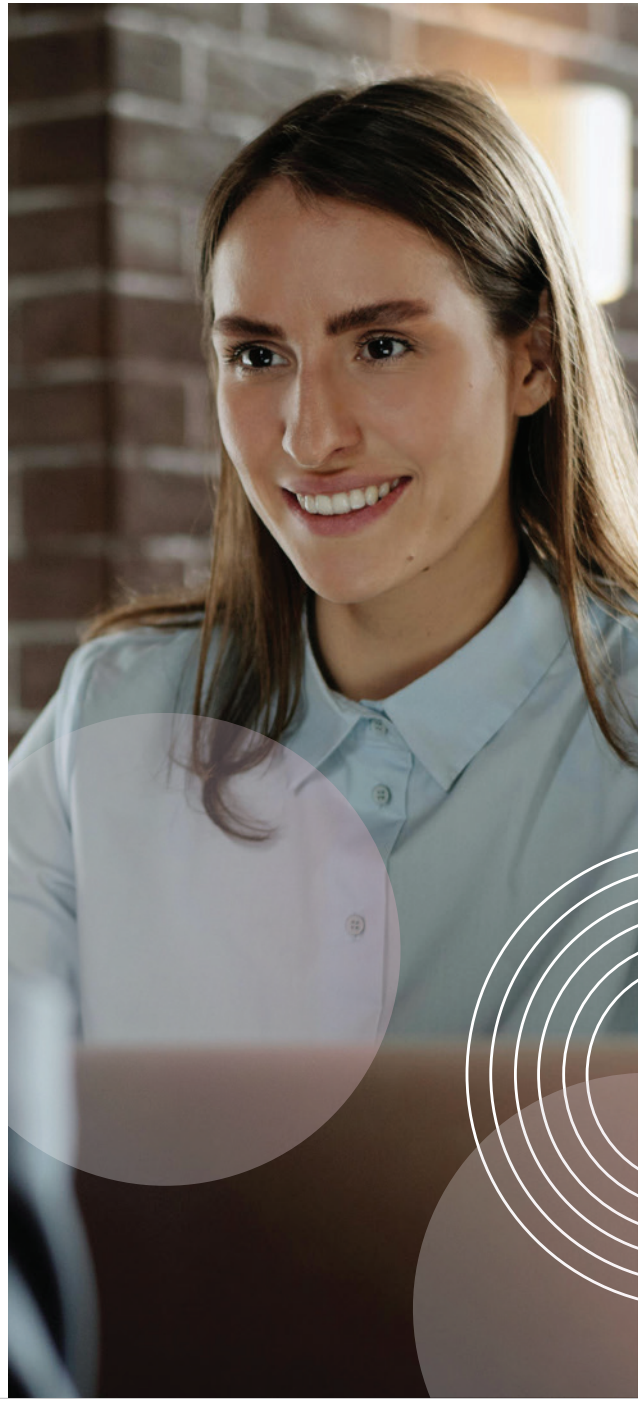
Certification exam: #156-215.81.20
Available on Pearson VUE

Overview:
Learn basic concepts and develop skills necessary to administer essential IT security tasks. This core course covers the fundamentals needed to deploy, configure, and manage daily operations of Check Point Security Gateways and Management Software Blades that run on the Gaia operating system.

Relevant Audience:
Technical professionals who support, install, deploy or administer Check Point products.

Prerequisites:
Working knowledge of Unix-like and Windows operating systems and TCP/IP Networking.

Delivery Method:
Instructor-Led & Virtual Instructor-Led



Link to Enroll

Certification Training – Core

CHECK POINT CERTIFIED SECURITY EXPERT (CCSE) R81.20

Duration: 3 days

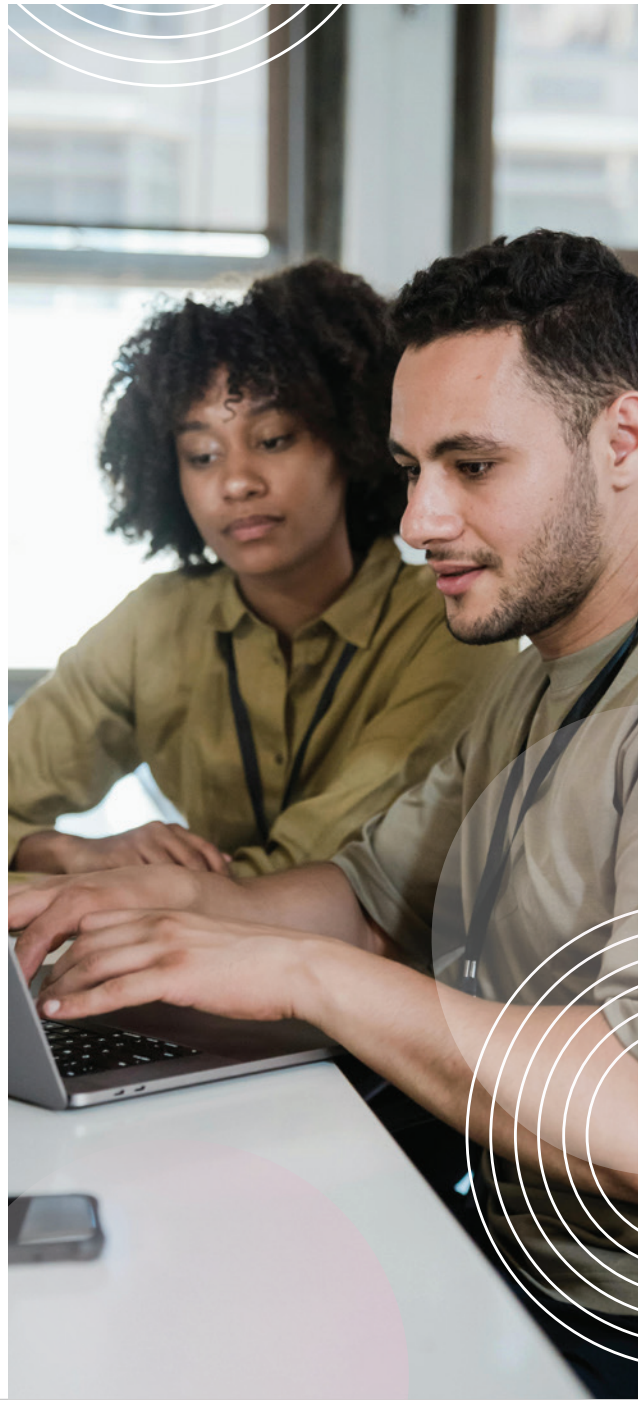
Certification exam: #156-315.81.20
Available on Pearson VUE

Overview:
Gain essential knowledge and hands-on skills to perform fundamental IT security administration tasks. This core course provides the foundation for deploying, configuring, and managing the daily operations of Check Point Security Gateways and Management Software Blades running on the Gaia operating system.

Relevant Audience:
Technical professionals who support, install, deploy or administer Check Point products.

Prerequisites:
Working knowledge of Unix-like and Windows operating systems and TCP/IP Networking. Completion of the Check Point Certified Security Administrator (CCSA) course.

Delivery Method:
Instructor-Led & Virtual Instructor-Led



Link to Enroll

INFINITY SPECIALIST ACCREDITATIONS

CUSTOMIZE YOUR JOURNEY ALONG THE WAY

*Certification badges are distributed upon course completion and exam

THE GATEWAY FOR ADVANCING YOUR CYBER SECURITY SKILLS

Infinity Global Services (IGS) offers a comprehensive suite of Check Point certification courses designed to equip cyber security professionals with the skills to secure, optimize, and manage Check Point security solutions. Our certifications span from core security administration and expert-level troubleshooting to specialized cloud, automation, and threat prevention skills, ensuring that professionals stay ahead in an evolving threat landscape.

These courses and exams focus on emerging technologies and advanced cyber security concepts. The Infinity Specialist Accreditations (ISA) courses enable you to earn ISAs, extending and maintaining the validity of your core certifications. They also serve as a pathway to achieving CCSM and CCSM Elite Security Mastery certifications.

Specialization Tracks

We have specialization tracks that enable you to to focus on key security domains, including:

- Cloud Security (CCCS)
- Endpoint Security (CCES)
- Multi-Domain Security (CCMS)
- Maestro Hyperscale Security (CCME)

Troubleshooting & Performance Optimization

These courses were designed to develop deep technical skills, resolve security issues efficiently (CCTA, CCTE, CCVS) and enhance system performance (Gateway Performance Optimization):

- Resolve security issues efficiently (CCTA, CCTE, CCVS)
- Enhance system performance (Gateway Performance Optimization)

Whether you are installing, configuring, managing, or troubleshooting Check Point security environments, our courses help you gain the technical mastery required to protect today's digital world.

CHECK POINT CERTIFIED AUTOMATION SPECIALIST (CCAS) R81.20

Infinity Specialization Training

Duration: 2 days

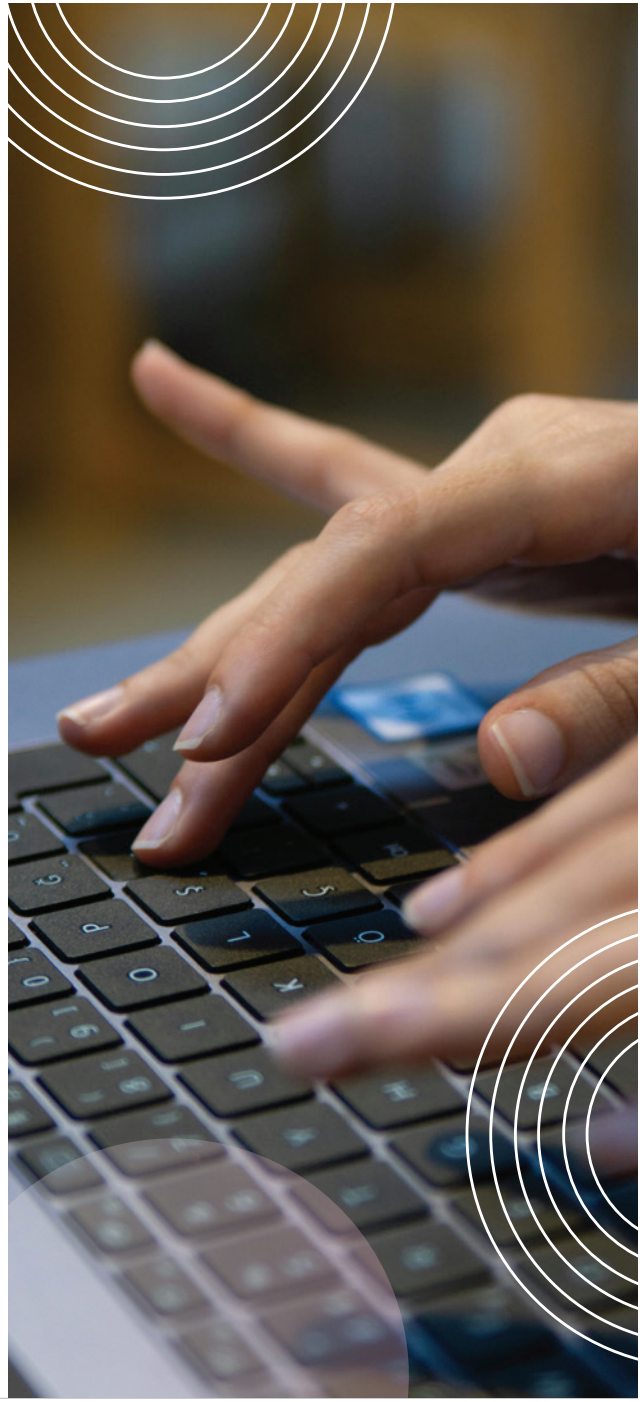
Certification exam: #156-521
Available on Pearson VUE

Overview:
Learn advanced concepts and develop skills necessary to design, deploy, and upgrade Check Point Security environments. This course is recommended for security experts and other technical professionals with prior training and/or practical experience with Check Point Management Servers and Security Gateways that run on the Gaia operating system.

Relevant Audience:
Technical professionals who support, install, deploy or administer Check Point products.

Prerequisites:
CCSA training or certification, fundamental Unix and Windows knowledge, certificate management experience, system administration and networking knowledge.

Delivery Method:
Instructor-Led & Virtual Instructor-Led



Link to Enroll

Infinity Specialization Training

CHECK POINT CERTIFIED CLOUD SPECIALIST (CCCS) R81.20

Duration: 2 days

Certification exam: #156-561
Available on Pearson VUE

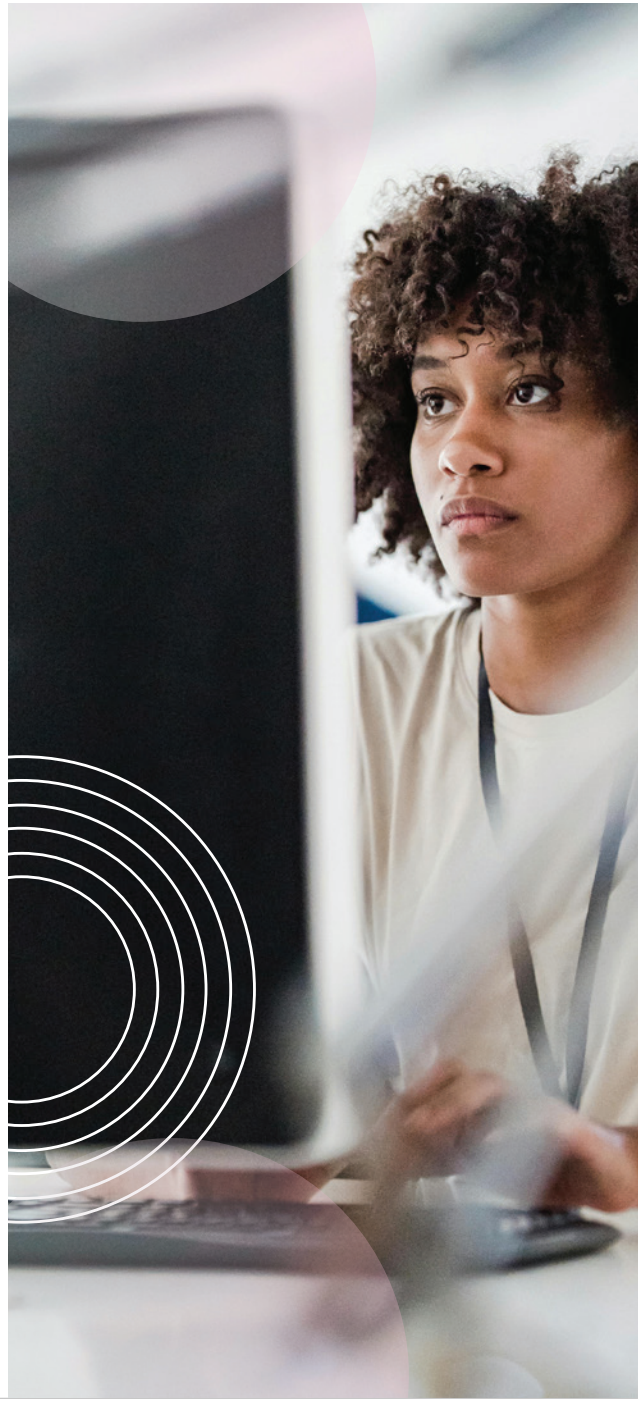
Overview:
Elevate cloud security, block attacks, and significantly reduce risk profile to streamline operational efficiency with our two-day specialist course.

Relevant Audience:
Security professionals looking to deploy and manage the CloudGuard Network Security solutions. It is also useful to prepare for the Check Point Certified Cloud Specialist (CCCS) credential.

Prerequisites:
- Unix-like and/or Windows operating systems
- Internet fundamentals
- Network fundamentals
- Network security
- TCP/IP networking
- System administration
- Cloud-native deployment

Delivery Method:
Instructor-Led & Virtual Instructor-Led

Link to Enroll



Infinity Specialization Training

CHECK POINT HARMONY ENDPOINT SPECIALIST (CCES)

Duration: 2 days

Certification exam: #156-356
Available on Pearson VUE

Overview:
Gain an in depth understanding of the Check Point Harmony Endpoint solution, including its features and capabilities. Apply knowledge and skills gained during training to manage and protect a Harmony Endpoint solution in your organization.

Relevant Audience:
This course is designed for security administrators who are responsible for deploying and managing a Harmony Endpoint security solution.

Prerequisites:
Working knowledge of Unix-like and/or Windows operating systems, networking fundamentals, networking security, TCP/IP networking, administration.

Delivery Method:
Instructor-Led & Virtual Instructor-Led

Link to Enroll

CHECK POINT MAESTRO EXPERT (CCME)

Infinity Specialization Training

Duration: 2 days

Certification exam: #156-836
Available on Pearson VUE

Overview:
Apply knowledge of Maestro implementation, deployment, and capabilities to utilize current hardware investment and maximize appliance capacity. Simplify data center workflow orchestration and scale up existing Check Point security gateways on demand.

Relevant Audience:
Technical professionals who support the Check Point Maestro hyperscale network security solution or who are working towards their Check Point Certified Maestro Expert (CCME) Specialist credential.

Prerequisites:
Before taking this course, we strongly suggests you have the prerequisites listed below:

1. Solid working knowledge of:
- Unix-based and/or Windows OS
- TCP/IP networking
- Check Point API

2. Check Point training/certification:
- Check Point Certified System Administrator (CCSA)
- Check Point Certified Security Expert (CCSE)

Delivery Method:
Instructor-Led & Virtual Instructor-Led

Link to Enroll

CHECK POINT CERTIFIED MULTI-DOMAIN SECURITY MANAGEMENT SPECIALIST R81.1 (CCMS)

Infinity Specialization Training

Duration: 2 days

Certification exam: #156-541
Available on Pearson VUE

Overview:
Gain advanced skills for effectively securing and managing a multi-domain enterprise security network. Apply understanding of open-source and Check Point troubleshooting tools and techniques to investigate and resolve complex issues.

Link to Enroll

Relevant Audience:
Security professionals who install, configure, and manage multiple security domains within their network security environment. It also helps candidates prepare for the Check Point Certified Multi-Domain Security Management Specialist (CCMS) exam.

Prerequisites:
- Solid knowledge of Unix-based and/or Windows OS and TCP/IP Networking.
- Check Point training/ certification: CCSA and CCSE. CCVS and CCAS are useful but not required.

Delivery Method:
Instructor-Led & Virtual Instructor-Led

CHECK POINT THREAT PREVENTION SPECIALIST R81.20 (CTPS)

Infinity Specialization Training

Duration: 2 days

Certification exam: #156-590
Available on Pearson VUE

Overview:
Apply threat prevention technologies to customize and strengthen your security posture and stay ahead of emerging threats.This two-day specialist-level course is designed for security professionals who want to gain the concepts and skills necessary to deploy and manage custom threat prevention within a Check Point Security environment.

Relevant Audience:
Security professionals who want to customize IPS and Anti-Bot/Anti-Virus Protections for specific security needs and identify ways to optimize Threat Prevention performance.

Prerequisites:
Before taking this course, basic knowledge of these topics is strongly encouraged:

- Internet fundamentals
- Networking fundamentals
- Networking security
- System administration
- Check Point training/certification:
  + Check Point Certified Security Administrator (CCSA) - **required**
  + Check Point Certified Security Expert (CCSE) - **recommended**

Delivery Method:
Instructor-Led & Virtual Instructor-Led

Link to Enroll

CHECK POINT CERTIFIED TROUBLESHOOTING ADMINISTRATOR (CCTA) R81.20

Infinity Specialization Training

Duration: 2 days

Certification exam: #156-532
Available on Pearson VUE

Overview:

This course is designed for security administrators who require the fundamental knowledge and skills to troubleshoot basic issues for Check Point Security Gateways and Management Software Blades that run on the Gaia operating system. This course is also useful for candidates who are pursuing the Check Point Certified Troubleshooting Administrator (CCTA) exam.

Relevant Audience:

Security administrators and Check Point resellers who need to manage and monitor issues that may occur within their security management environment.

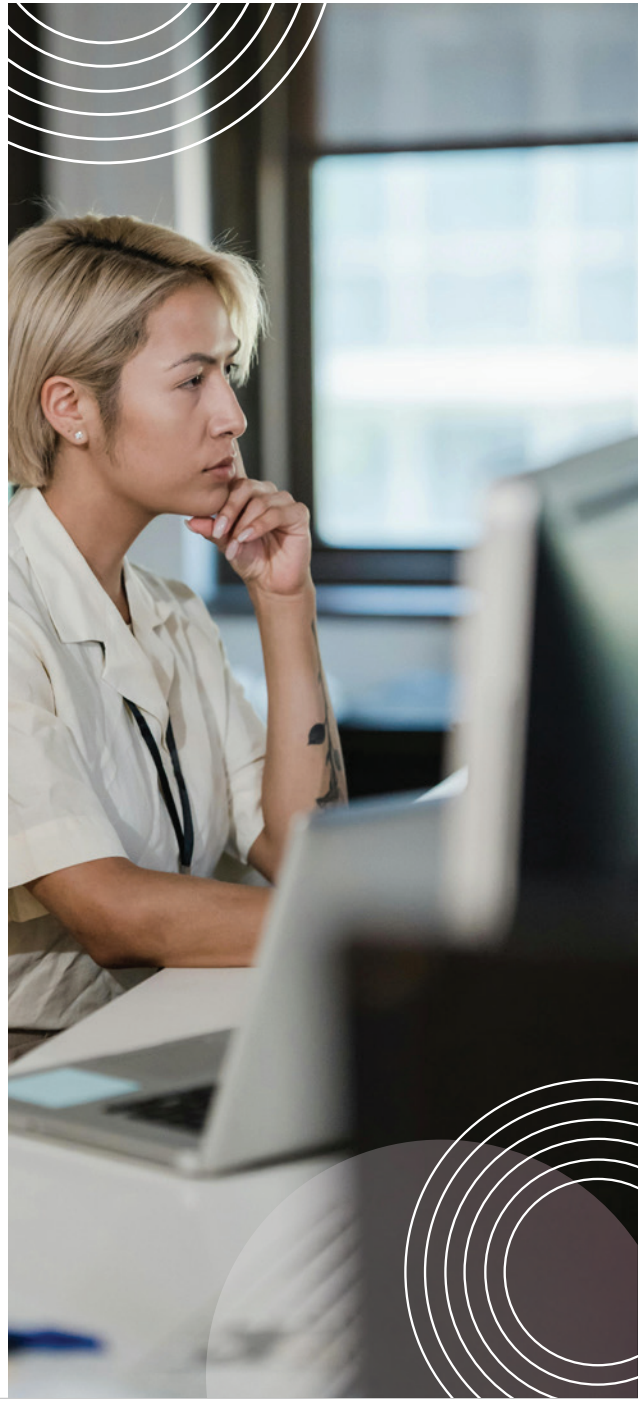
Prerequisites:

- Working knowledge of UNIX and/or Windows operating systems.
- Working knowledge of networking TCP/IP. CCSA training/certification.
- Advanced knowledge of Check Point Security products.

Delivery Method:

Instructor-Led & Virtual Instructor-Led

Link to Enroll



CHECK POINT CERTIFIED TROUBLESHOOTING EXPERT (CCTE) R81.20

Infinity Specialization Training

Duration: 2 days

Certification exam: #156-587
Available on Pearson VUE

Overview:
This course is designed to provide security experts and Check Point resellers with advanced troubleshooting skills to investigate and resolve more complex issues that may occur while managing their Check Point security environment.

Relevant Audience:
Security experts and Check Point resellers looking to gain the necessary knowledge to perform more advanced troubleshooting skills while managing their security environments. It is also useful for security professionals who are pursuing the Check Point Certified Troubleshooting Expert (CCTE) certification.

Prerequisites:

- Working knowledge of UNIX and/or Windows operating systems.
- Working knowledge of networking TCP/IP. CCSA training/certification.
- Advanced knowledge of Check Point security products.

Delivery Method:
Instructor-Led & Virtual Instructor-Led

Link to Enroll

CHECK POINT CERTIFIED VSX SPECIALIST R81.1 (CCVS)

Infinity Specialization Training

Duration: 2 days

Certification exam: #156-551
Available on Pearson VUE

Overview:
Gain the fundamental knowledge and skills needed to install, configure, and manage a Check Point Virtual Security Extension (VSX) solution within a network security environment. Identify and use the appropriate commands and techniques to troubleshoot VSX deployments, routing, and provisioning issues.

Relevant Audience:
Technical professionals who support a Check Point Virtual Security Extension (VSX) solution within their network security environment. It is also recommended for candidates who are preparing for the Check Point Certified Virtual System Extension Specialist (CCVS) credential.

Prerequisites:
Before taking this course, we strongly suggest that you have the following prerequisites:

1. Solid working knowledge of:
   - Unix-based and/or Windows OS
   - TCP/IP networking
   - Check Point API
2. Check Point training/certification:
   - Check Point Certified System Administrator (CCSA)
   - Check Point Certified Security Expert (CCSE)

Delivery Method:
Instructor-Led & Virtual Instructor-Led

Link to Enroll

Infinity Specialization Training

GATEWAY PERFORMANCE OPTIMIZATION

Duration: 2 days

Overview:
This two-day course covers everything you need to know to squeeze every last bit of performance out of your Check Point Security Gateways without compromising security. Through a series of break/fix lab exercises, you will become familiar with gateway optimization strategies, while running speed tests every step of the way to see the dramatic results of your tuning adjustments.

Relevant Audience:
Advanced level security professionals interested in improving the performance of their security gateways.

Prerequisites:
CCSE certification plus 3 years of Check Point production experience or minimum 5 years of Check Point production experience with SecureXL/ CoreXL knowledge.

Delivery Method:
Instructor-Led & Virtual Instructor-Led

Link to Enroll

HARMONY EMAIL & COLLABORATION

Infinity Specialization Training

Duration: 365 days

Overview:
This course is designed for Security Administrators and Partners who manage or support the Harmony Email & Collaboration solution, including System Administrators, Support Analysts, Network Engineers, and Communications Security Administrators. Students will gain an understanding of the Check Point Harmony Email & Collaboration product, including how it works, how it is configured, and how it can be used to secure cloud-based email, file sharing, and communication tools. Online course access is available for 1 year.

Relevant Audience:
Security Administrators and other technical professionals who manage or support the Harmony Email & Collaboration solution, including System Administrators, Support Analysts, Network Engineers, and Communications Security Administrators.

Prerequisites:
- Before taking this course, Check Point strongly suggests you have a working knowledge of the following
- Fundamental understand of network security
- Fundamental understanding of applications in cloud-based communication suites

Delivery Method:
Self-paced learning platform

Link to Enroll

CLOUDGUARD CNAPP POSTURE MANAGEMENT SPECIALIST (CPMS)

Infinity Specialization Training

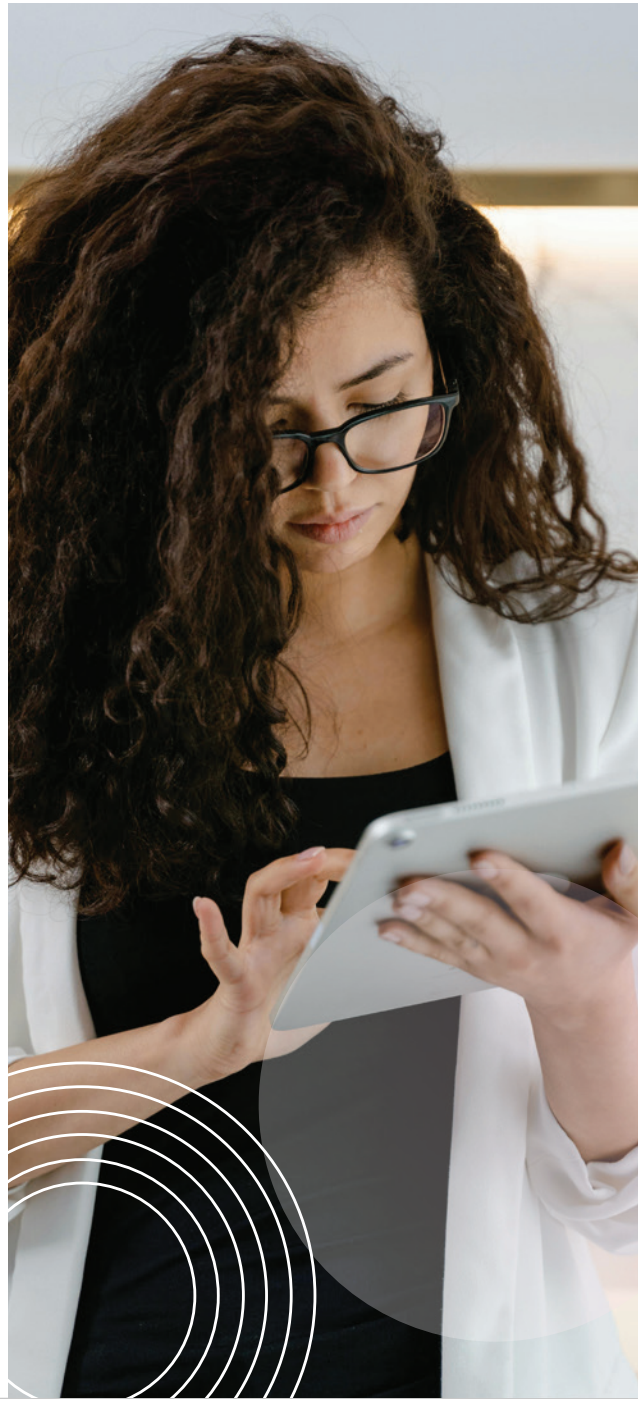
Duration: 365 days

Overview:
This course describes the CloudGuard Posture Management product, the product features and benefits, architecture, and role-based use cases. Online course access is available for 1 year. Please allow up to two business days after placing order to receive additional information to access the course.

Relevant Audience:
This course is designed for Security Administrators who are responsible for managing a CloudGuard Posture Management security solution.

Prerequisites:
Working knowledge of Unix and/or Windows operating systems, Working knowledge of Networking, TCP/IP, CCSE training/ certification, Advanced knowledge of Check Point Security Products.

Delivery Method:
Self-paced learning platform



Link to Enroll

QUANTUM ROLE-BASED LEARNING PATHS

QUANTUM SPECIALTY TRAINING OFFERINGS

Providing a continuous learning journey for all roles and experience levels

DEPLOYMENT

GPDA

Coming Soon

ADMINISTRATION

CCSA CCSE

DEPLOYMENT + ADMINISTRATION

GPDA CCSA CCSE

Coming Soon

ADMINISTRATION + TROUBLESHOOTING

CCSA CCTA CCSE CCTE

SPECIALTY: MAESTRO

CCSA CCSE CCME

SPECIALTY: THREAT PREVENTION

CCSA CCSE CTPS

SPECIALTY: AUTOMATION

CCSA CCSE CCAS

SPECIALTY: VPN

CCSA CCSE GDPS

Available in 2026

HACKING POINT

A global education program to help master Pen Testing techniques and cyber security skills.

HACKING POINT

Hacking Point is a global training program designed for security professionals to master advanced penetration testing techniques and essential cyber security skills. The courses provide in-depth training on the latest threats, equipping students with the expertise needed to defend against real-world cyber attacks. Upon completion, participants will have a deeper understanding of how to protect corporate networks and critical resources effectively.

WORLD-CLASS INSTRUCTORS

Gain expertise in cyber security threats from world-class instructors and trainers.

HIGH-QUALITY TRAINING

Receive top-quality, agnostic training from official Check Point partners and providers to enhance your expertise in cyber security practices and pen-testing methods.

LEARN FROM ANYWHERE

Convenient remote training for most courses allows easy access from any office across the globe.

PROUD TO PARTNER WITH:

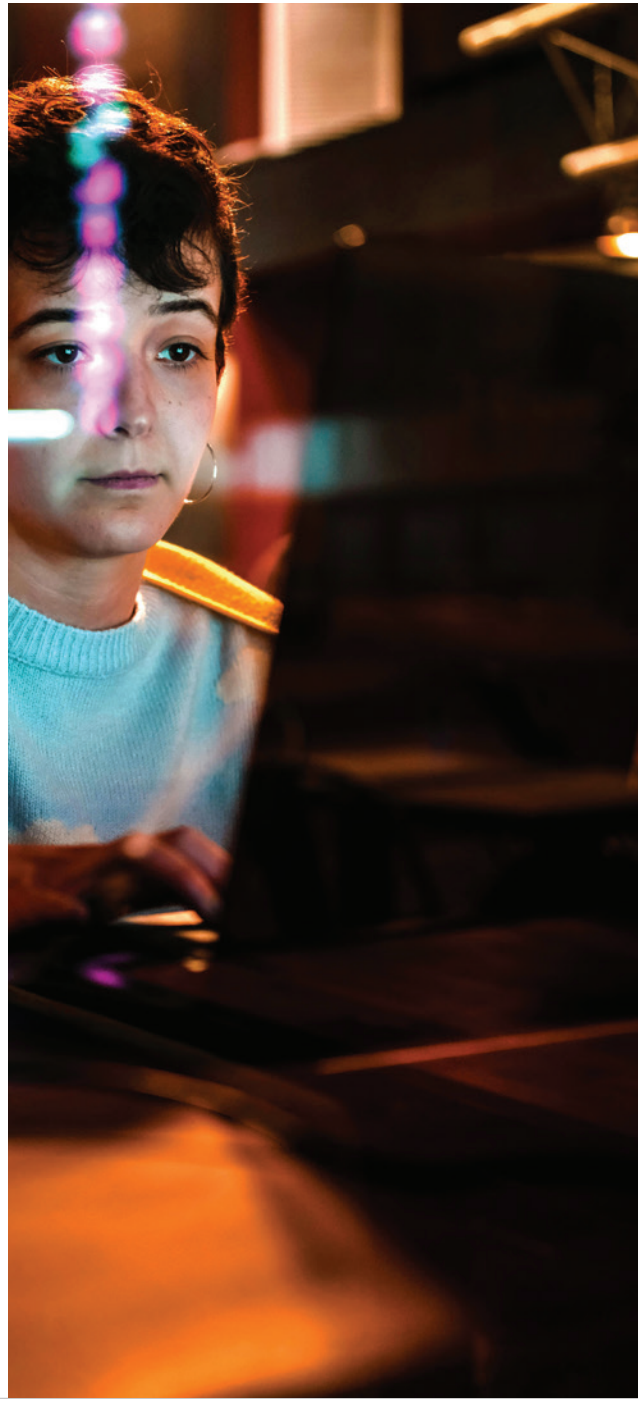
OffSec
The Path to a Secure Future

Payatu

NotSoSecure part of claranet cyber security

CYBRARY

MONNAPPA K A

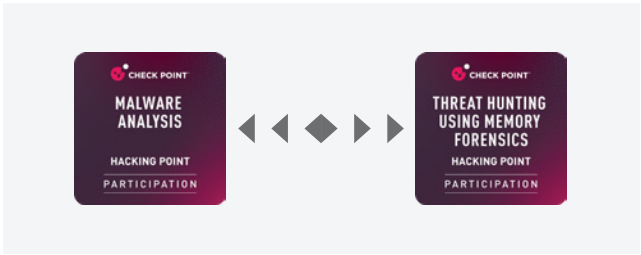


Go to Hacking Point

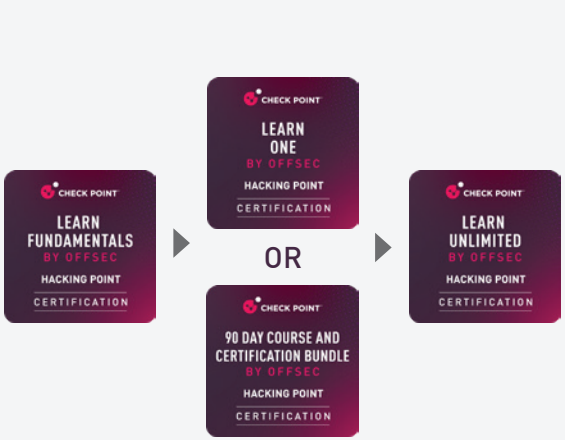
RECOMMEND LEARNING PATHS

PEN TESTING EXPERT - ZERO TO HERO

PRACTICAL APPLICATIONS FOR CYBER THREAT ANALYSTS



CYBER SECURITY MASTRY AT YOUR OWN PACE



SHIFT LEFT WITH SECURE CODE TRAINING

HACKING 101

BY NotSoSecure part of claranet cyber security

Hacking Point

Duration: 1 day

Certification exam: #156-401
Available on Pearson VUE

Overview:

Explore the fundamentals of Penetration Testing and learn how to identify and exploit vulnerabilities across various technologies. This introductory course provides an understanding of Pen Testing, covering risks, system vulnerabilities, and the hacker mindset. Participants will also gain access to an online course platform to practice hands-on techniques learned during the training.

Relevant Audience:

- Network admins: understand how your environment could be attacked
- Developers: see how real cyber criminals might target your applications
- Students and graduates: improve your employability and enhance your CV
- Career changers: get a taste of what it's like to work as a penetration tester

Prerequisites:

- A genuine interest in cyber security and a desire to develop your skills
- Basic knowledge of common command line syntax

Delivery Method:

Virtual Instructor-Led

Link to Enroll

INFRASTRUCTURE HACKING

BY NotSoSecure part of claranet cyber security

Hacking Point

Duration: 3 days

Certification exam: #156-402
Available on Pearson VUE

Course certification qualifies as a specialty course towards receiving or extending the validity of Check Point's CCSM or CCSM Elite validity.

Overview:

This ideal introductory/intermediate training class is designed to teach the fundamentals of what Pen Testing is all about. The hands-on training was written to address the market need around the world for a real hands-on, practical, and hack-lab experience that focuses on what is really needed when conducting a penetration test. While a variety of tools are used, these are the key tools in any penetration tester's kit bag. This, when combined with a sharp focus on methodology, will give you what is necessary to start or formalize your testing career.

Link to Enroll

Relevant Audience:

- Students and graduates: improve your employability and enhance your CV
- Infrastructure Penetration Testers (1-2 years' experience): build up your ability with the guidance of experienced Pen Testers and researchers
- Penetration Testers in other fields (e.g., web, mobile): develop your infrastructure hacking skills and knowledge
- Network Admins: understand how your environment could be attacked
- SOC Analysts and Engineers: develop your awareness of potential indicators of compromise (IoCs) and more complex malicious behaviors
- Security/IT Managers and Team Leads: update your knowledge of the threat landscape

Prerequisites:

- Basic knowledge of infrastructure application security (at least 1 year experience)
- Basic familiarity with common command line syntax

Delivery Method:

Virtual, Live Instructor-Led Training

ADVANCED INFRASTRUCTURE HACKING

BY NotSoSecure part of claranet cyber security

Overview:
IT infrastructure is more complex and dynamic than it's ever been, demanding comprehensive, up-to-date, and well-rehearsed security skills to match. Join this hands-on, 5-day course to push your infrastructure hacking to the next level and widen your career prospects.

Link to Enroll

Hacking Point

Duration: 5 days

Certification exam: #156-409
Available on Pearson VUE

Course certification qualifies as a specialty course towards receiving or extending the validity of Check Point's CCSM or CCSM Elite validity.

Relevant Audience:

- Penetration Testers and Red Teamers
- Security Consultants and Architects
- Network Admins with security experience
- CSIRT/SOC Teams/Blue Teamers
- Security/IT Managers and Team Leads

Prerequisites:

- Intermediate knowledge of infrastructure application security (at least 2 years experience)
- Common command line syntax competency
- Experience using virtual labs for Pen Testing and/or offensive research

Delivery Method:
Virtual, Live Instructor-Led Training

WEB HACKING

BY NotSoSecure part of claranet cyber security

Hacking Point

Duration: 2 days

Certification exam: #156-403
Available on Pearson VUE

Course certification qualifies as a specialty course towards receiving or extending the validity of Check Point's CCSM or CCSM Elite validity.

Overview:

This foundation course of "Web Hacking" familiarises the attendees with the basics of web application and web application security concerns. A number of tools and techniques, backed up by a systematic approach on the various phases of hacking will be discussed during this 2-day course

Relevant Audience:

- Security enthusiasts
- Anybody who wishes to make a career in this domain and gain some knowledge of networks and applications
- Web Developers
- System Administrators
- SOC Analysts
- Network Engineers
- Pen Testers who are wanting to level up their skills

Prerequisites:

- Basic knowledge of web application security
- Basic familiarity with common command line syntax
- Basic knowledge of Burp Suite

Delivery Method:

Virtual, Live Instructor-Led Training

Link to Enroll

ADVANCED WEB HACKING

BY NotSoSecure part of claranet cyber security

Hacking Point

Duration: 5 days

Certification exam: #156-408
Available on Pearson VUE

Overview:

Web application security is one of the biggest and fastest moving specializations within cyber security today. Only with a comprehensive, well-rehearsed arsenal of modern ethical hacking skills can it be mastered. Join this hands-on, 5-day course to push your web hacking to the next level and widen your career prospect.

Relevant Audience:

- Penetration Testers and Red Teamers
- Security Consultants and Architects
- CSIRT/SOC Analysts and Engineers/ Blue Teams
- Developers with in-depth security experience
- Security/IT Managers and Team Leads

Prerequisites:

- Intermediate knowledge of web application security (at least 2 years experience)
- Common command line syntax competency
- Experience using virtual labs for Pen Testing and/or offensive research
- Basic working knowledge of Burp Suite

Delivery Method:

Virtual, Live Instructor-Led Training

Link to Enroll

CLOUD SECURITY

BY NotSoSecure part of claranet cyber security

Hacking Point

Duration: 2 days

Certification exam: #156-406
Available on Pearson VUE

Course certification qualifies as a specialty course towards receiving or extending the validity of Check Point's CCSM or CCSM Elite validity.

Overview:

As cloud innovation gives birth to new technologies and new threats, now is the time to modernize your cloud security skills and bring them up to the industry standard. Join this hands-on, two day course to push your cloud hacking and vulnerability remediation skills to the next level and widen your career prospects.

Relevant Audience:

- Security enthusiasts
- Anybody who wishes to make a career in this domain and gain some knowledge of networks and applications
- Web Developers
- System Administrators
- SOC Analysts
- Network Engineers
- Pen Testers who are wanting to level up their skills

Prerequisites:

- Basic to intermediate knowledge of cyber security (1.5+ years experience)
- Experience with common command line syntax

Delivery Method:

Virtual, Live Instructor-Led Training

Link to Enroll

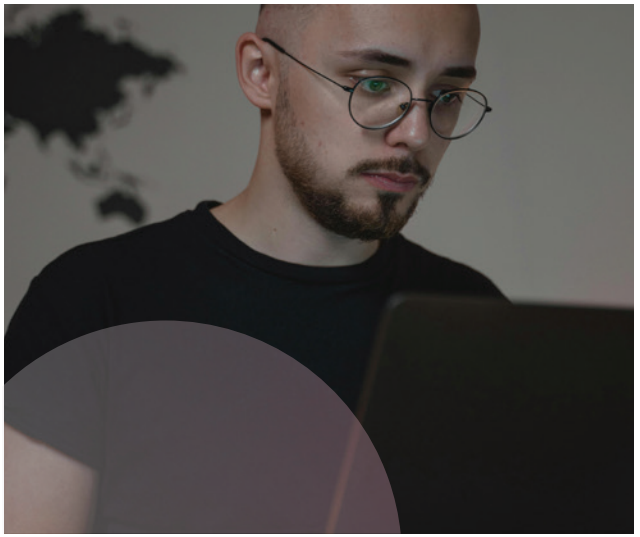
DEVSECOPS

BY NotSoSecure part of claranet cyber security

Hacking Point

Duration: 2 days

Certification exam: #156-407
Available on Pearson VUE



Overview:

Keep up with DevOps modernization and widen your career prospects. This practical course will help you build your own DevSecOps pipeline so you can make products secure by design. Get your hands dirty with our popular virtual labs and learn from experienced, practicing penetration testers with a legacy of training at Black Hat. Learn how to use and automate the most popular and effective security tools and practices, overcome common DevSecOps challenges, instil security culture within your team, and more.

Relevant Audience:

- Developers
- DevOps/DevSecOps Engineers
- Application Security Engineers
- Ops teams
- CISOs

Prerequisites:

- Basic DevOps knowledge – Familiarity with DevOps workflows and CI/CD pipelines is beneficial.
- Fundamental security concepts – Understanding of security principles and common vulnerabilities.
- Technical Background – Ideal for developers, DevOps Engineers, and security professionals with hands on experience in coding or system administration.

Delivery Method:

Virtual, Live Instructor-Led Training

Link to Enroll

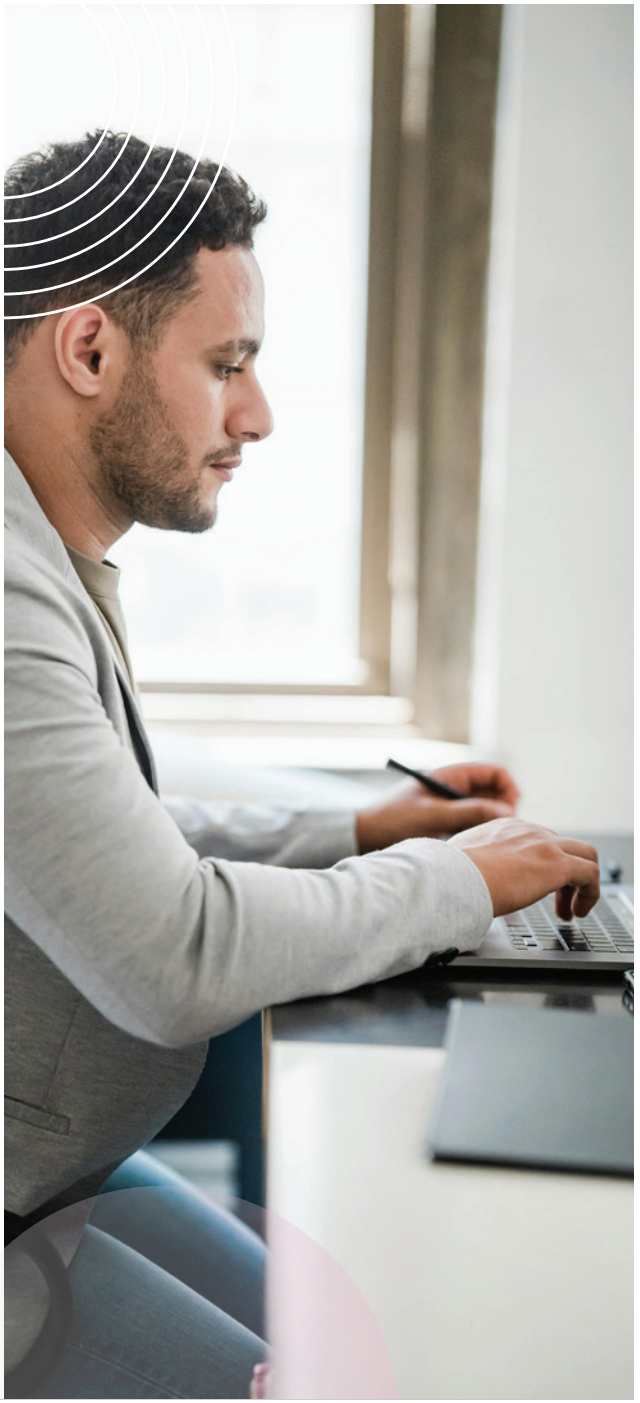
CHECK POINT
MALWARE ANALYSIS
HACKING POINT
PARTICIPATION

MALWARE ANALYSIS

BY MONNAPPA K A

Hacking Point

Duration: 2 days



Overview:

This hands-on training teaches the concepts, tools, and techniques to analyze and determine the behavior and capability of malware. The course will introduce you to the concept of Malware Analysis and Reverse Engineering. Additionally, you will learn to perform static, dynamic, and code analysis to determine the inner workings of the binary.

Relevant Audience:

SOC Analysts, Incident Responders, Cyber Security Investigators, Security Researchers, System Administrators, Software Developers, Students, and curious security professionals who would like to learn Malware analysis.

Prerequisites:

- Basic Malware Analysis Concepts
- Understanding of Windows OS
- Familiarity with basic analysis Tools:
- General cyber security and Incident Response concepts

Delivery Method:

Virtual, Live Instructor-Led Training

Link to Enroll

CHECK POINT
APPSEC FOR DEVELOPERS
CCPE
HACKING POINT
CERTIFICATION

APPSEC FOR DEVELOPERS

BY NotSoSecure part of claranet cyber security

Hacking Point

Duration: 2 days

Overview:

The AppSec for Developers course equips you with essential application security skills through immersive, hands-on labs guided by industry experts. Over two days, you'll learn to identify and remediate code vulnerabilities, integrate DevSecOps practices, and build a security-first mindset for your team. Using a unique Defense by Offense approach, this course is perfect for developers of all experience levels who are ready to secure modern applications and drive meaningful change in software security.

Relevant Audience:

- Software Developers (beginner to advanced)
- Development team leads

This course is suitable for developers and development teams who want to build and maintain secure software. The syllabus considers different application development strategies, from preserving legacy applications to developing new products.

Prerequisites:

- Basic Understanding of Software Development
- Familiarity with Web Technologies

Delivery Method:

Virtual, Live Instructor-Led Training

Link to Enroll

HACKING IOT

BY Payatu

Hacking Point

Duration: 1 day

Overview:

Hacking IoT is a unique workshop that offers security professionals an understanding of the IoT technology suite. These hands-on labs include IoT protocols, hardware, and their underlying weaknesses.

Relevant Audience:

- Penetration Testers tasked with auditing IoT
- Bug hunters who want to find new bugs in IoT products
- Government officials from defensive or offensive units
- Red Team members tasked with compromising the IoT infrastructure
- Security professionals who want to build IoT security skills
- Embedded security enthusiasts
- IoT Developers and testers
- Anyone interested in IoT security

Prerequisites:

- Basic knowledge of web and mobile security
- Knowledge of Linux OS
- Basic knowledge of programming with Python

Delivery Method:

Virtual, Live Instructor-Led Training

Link to Enroll

CYBRARY

BY CYBRARY

Hacking Point

Duration: 365-day subscription

Certification exam: In-platform training assessments

Overview:

Cybrary for Teams is the leading choice for cyber security skills development programs that build mission-ready teams. With a future-proof, cyber security-focused platform, Cybrary provides timely, expert-curated content. Labs based on real-world enterprise scenarios and skills assessments ensure your staff is prepared to succeed against evolving threats.

Relevant Audience:

- Cyber security and IT teams: providing structured career paths and hands on technical training to enhance team capabilities.
- Organizations seeking to align with industry frameworks: offering training aligned with frameworks like MITRE ATT&CK and NICE cyber security workforce framework.
- Businesses aiming to benchmark and develop employee skills: utilizing assessments to evaluate and improve team members' knowledge and skills.

Prerequisites:

None. The platform features self-paced foundational training alongside prep training for the most advanced cyber security and cyber management certifications

Delivery Method:

Self-paced learning platform

Link to Enroll

CHECK POINT
LEARN FUNDAMENTALS
BY OFFSEC
HACKING POINT
CERTIFICATION

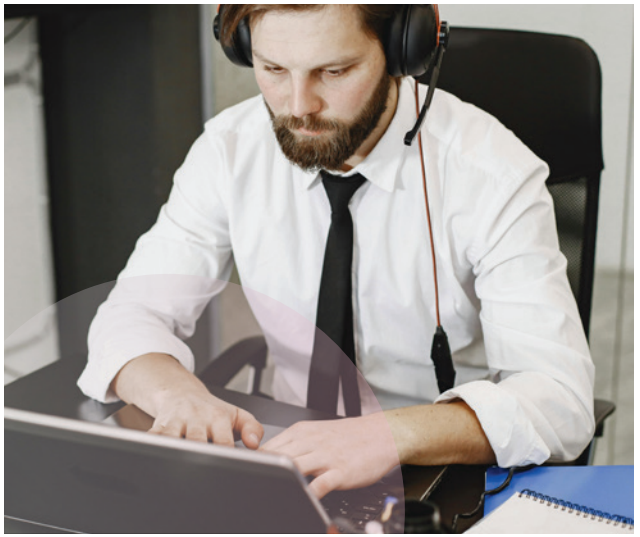
LEARN FUNDAMENTALS

BY OffSec
The Path to a Secure Future

Hacking Point

Duration: 365-day subscription

Certification exam: Included
Available at the OffSec Platform



Overview:

Learn Fundamentals, OffSec's entry-level or beginner training plan, is designed to help students learn basic technical adjacent concepts, cultivate the mindset necessary for a successful cyber security career, and provide the prerequisites for advanced courses. Learn Fundamentals includes access to: PEN-100, SOC-100, WEB-100, CLD-100 and EXP-100. Assessments and badges are available upon successful completion.

Relevant Audience:

- Beginners in cyber security – Ideal for individuals starting their cyber security journey.
- IT and Security Professionals – Those looking to strengthen foundational security knowledge.
- Aspiring Ethical Hackers & Pen Testers – Prepares learners for advanced cyber security roles and certifications.

Prerequisites:

Students looking to enter the cyber security job force, and cyber security adjacent professionals looking to upskill their security training, including IT Engineers (Developers, System Administrators, Cloud Engineers, DevOps, etc.). No prerequisites are required for PEN-100, WEB-100, SOC-100, EXP-100, PEN-103 or PEN-210. For CLD-100, students should have knowledge of cyber security adjacent concepts such as Linux and Networking.

Delivery Method:

Self-paced learning platform

Link to Enroll

CHECK POINT
LEARN ONE
BY OFFSEC
HACKING POINT
CERTIFICATION

LEARN ONE

BY OffSec
The Path to a Secure Future

Hacking Point

Duration: 365-day subscription

Certification exam: Included
Available at the OffSec Platform

Overview:

Learn One is perfect for beginners or anyone progressing through OffSec courses, offering a full year of lab access to balance learning with life. Monthly content updates and two exam attempts provide ongoing support and a second chance to succeed.

Relevant Audience:

Ideal for anyone looking to start their cyber security journey through our Learn Fundamentals content and/or work through an advanced level course, including cyber security professionals and IT specialists in cyber adjacent roles.

Prerequisites:

No prerequisites are required for taking the Learn One subscription by OffSec. The platform provides foundational learning paths, making it accessible to those without prior cyber security experience.

Delivery Method:

Self-paced learning platform

Link to Enroll

CHECK POINT
LEARN UNLIMITED
BY OFFSEC
HACKING POINT
CERTIFICATION

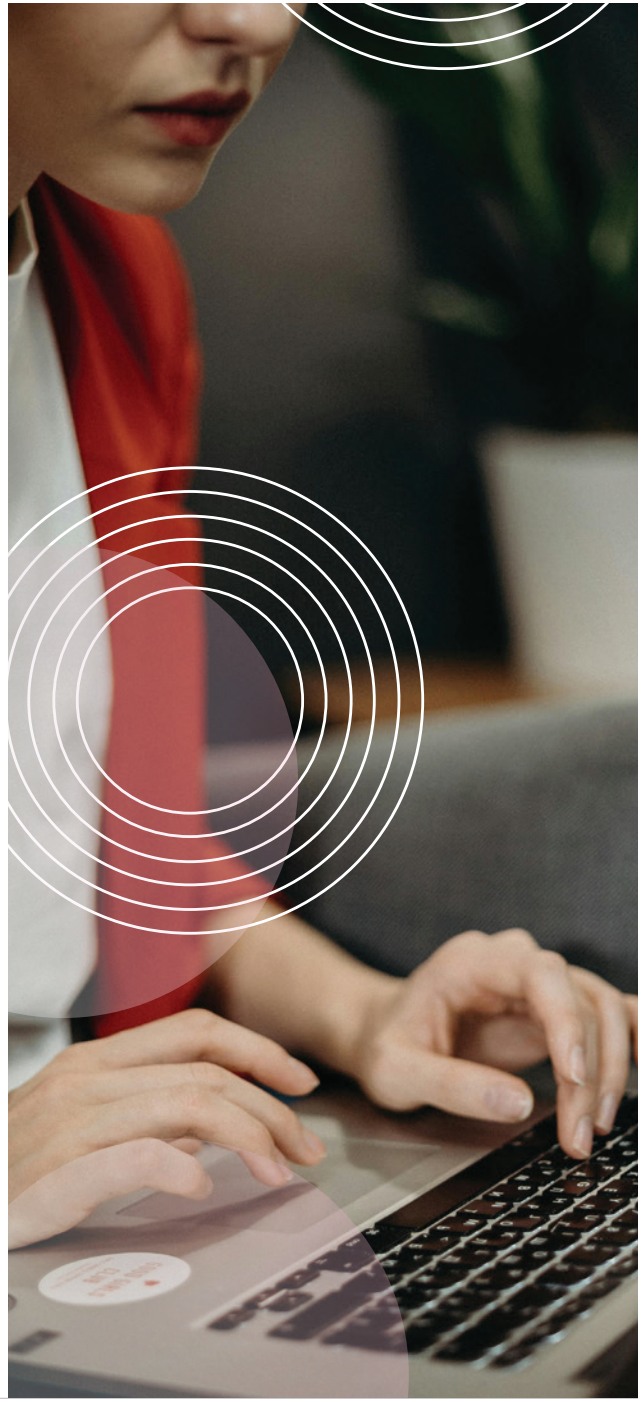
LEARN UNLIMITED

BY OffSec
The Path to a Secure Future

Hacking Point

Duration: 365-day subscription

Certification exam: Included
Available at the OffSec Platform



Overview:

OffSec Learn Unlimited provides full access to Offensive Security's complete training library and Proving Grounds Practice for one year, enabling learners to engage with beginner to advanced cyber security topics. This subscription includes unlimited exam attempts, allowing participants to develop comprehensive skills across multiple domains, including Penetration Testing, Security Operations, Web Security, and Cloud Security.

Relevant Audience:

- Cyber security professionals aiming for continuous learning and certification
- IT specialists looking to gain expertise across multiple cyber security domains
- Professionals preparing for advanced roles in cyber security, such as SOC Analysts, Penetration Testers, and Security Engineers

Prerequisites:

Basic to intermediate cyber security knowledge:

- Understanding of IT infrastructure
- Willingness to tackle advanced topics

Delivery Method:

Self-paced learning platform

Link to Enroll

90 DAY COURSE AND CERTIFICATION BUNDLE

BY OffSec
The Path to a Secure Future

Hacking Point

Duration: 90-day subscription

Certification exam: Included
Available at the OffSec Platform

Overview:

The OSCP / OSEP / OSDA Course & Certification Bundle provides 90 days of access to one advanced cyber security course and lab environment, along with one exam attempt, enabling students to build expertise in specific areas such as Penetration Testing, Security Operations, Web Application Security, and Exploit Development. This bundle is designed for intermediate learners seeking hands-on experience and certification to advance their cyber security careers.

Relevant Audience:

Intermediate cyber security professionals and practitioners, Soc Analysts and Threat Hunters, Web Application Security Specialists and Penetration Testers, IT professionals looking to specialize in Exploit Development and offensive security techniques.

Prerequisites:

- Intermediate understanding of cyber security concepts
- Technical skills in IT and Network Security
- Programming knowledge (recommended for advanced courses)

Delivery Method:

Self-paced learning platform

Link to Enroll

LEARN ENTERPRISE SINGLE USER & 5-USERS LICENSE

BY OffSec
The Path to a Secure Future

Hacking Point

Duration: 365-day subscription

Certification exam: Included
Available at the OffSec Platform

Overview:

OffSec Learn Enterprise is a comprehensive cyber security training solution designed to address workforce development needs by providing access to OffSec's full learning library, including courses, labs, and the exclusive OffSec Cyber Range. This solution allows enterprises to enhance their team's skills through real-world simulations, continuous training, and certification opportunities.

Relevant Audience:

- Cyber security teams in enterprise settings
- Organizations aiming to upskill and retain cyber security talents
- IT and security managers responsible for team training and skills development
- Enterprises focused on addressing cyber security skills gaps

Prerequisites:

No prerequisites are required for taking the Learn Enterprise subscription by OffSec. This subscription is designed for both beginners and highly advanced professionals in adjacent IT roles looking to upskill. The platform provides foundational learning paths, making it accessible to those with and without prior cyber security experience.

Delivery Method:

Self-paced learning platform

Link to Enroll

CISO ACADEMY

A program for C-Level executives and aspiring leaders to enhance security while balancing tactical and strategic responsibilities.

CISO ACADEMY

CYBER SECURITY TRAINING FOR C-LEVEL EXECUTIVES

CISO Academy is a premier global education program designed for C-level executives or those building up to it. It helps master all types of cyber security practices while learning to balance the handling of tactical issues with strategic leadership responsibilities.

WORLD-CLASS INSTRUCTORS

Gain expertise in cyber security from industry leading instructors and trainers.

HIGH-QUALITY TRAINING

Receive the highest quality training with official Check Point training partners and providers to facilitate the learning of cyber security technologies by Check Point.

LEARN FROM ANYWHERE

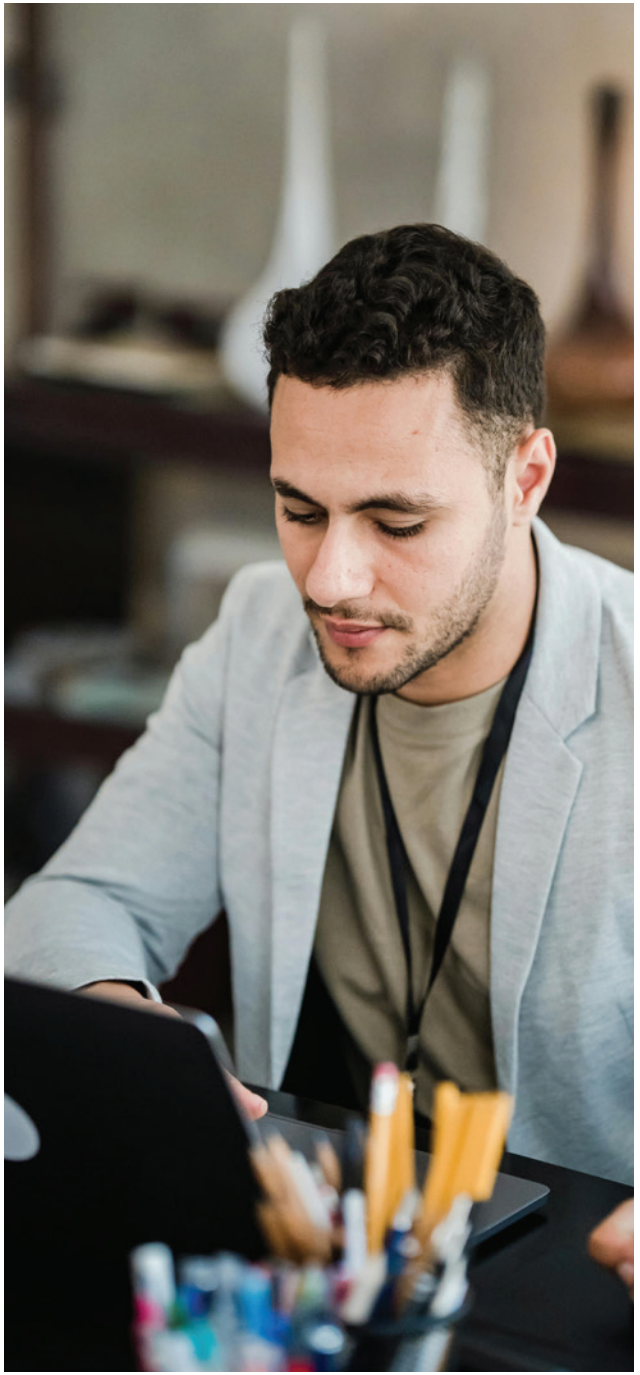
Convenient remote training for most courses allows easy access from any office across the globe.

PROUD TO PARTNER WITH:

ISC2

ISACA

NotSoSecure part of claranet cyber security



Go to Ciso Academy

CISO Academy

8-WEEKS / 5-DAYS / SELF PACED

CCSP

BY ISC2

Duration Options:

- 5-days training
- 8-weeks, twice a week training
- Self paced course

Overview:

The CCSP certification training provides a detailed review of essential cloud security concepts, including cloud architecture, data security, and compliance. Covering six domains of the CCSP Common Body of Knowledge (CBK), this course is designed for experienced IT and security professionals who want to deepen their understanding of cloud security risks, controls, and strategies.

Links to enroll:

8 Weeks | 5 Days | Self paced

Relevant Audience:

- Security Management and Systems Architecture
- Systems and Security Engineering
- Enterprise and Security Architecture
- Security Administration
- Cloud Security Consulting

Prerequisites:

- Five years of full-time IT experience
- Foundational knowledge of cloud computing
- Basic understanding of security and compliance

Delivery Method:

5-DAYS: Virtual, Instructor Led-Training

8-WEEKS: Virtual, Live Instructor-Led Training

SELF PACED: Self-paced Learning

CISO Academy

8-WEEKS / 5-DAYS / SELF PACED

CISSP

BY ISC2

Overview:

The CISSP certification training provides a thorough overview of the principles and practices necessary for designing, managing, and securing an organization's overall security framework. Covering the eight domains of the CISSP Common Body of Knowledge (CBK), this course is ideal for seasoned security professionals seeking to deepen their knowledge and prepare for the CISSP exam, enhancing their credibility and career prospects in information security.

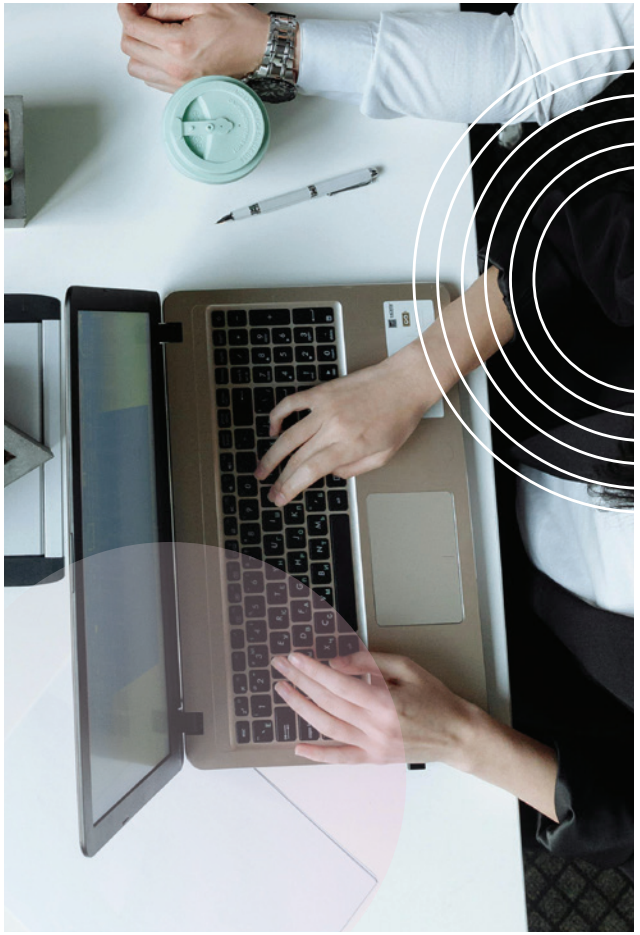
Links to enroll:

8 Weeks | 5 Days | Self paced

CISO Academy

Duration Options:

- 5-days training
- 8-weeks, twice a week training
- Self paced course



Relevant Audience:

Security Consultant roles, Security Managers and IT Managers, Security Architects and Analysts, Chief Information Security Officers (CISO), Security Systems Engineers, Network and Security Architects, Security Directors and Auditors.

Prerequisites:

- Minimum of five years of work experience
- Strong knowledge of security principles
- Basic understanding of IT infrastructure

Delivery Method:

5-DAYS: Virtual, Instructor Led-Training

8-WEEKS: Virtual, Live Instructor-Led Training

SELF PACED: Self-paced Learning

CISO Academy

5-DAYS / SELF PACED

SSCP

BY ISC2

Overview:

The SSCP certification training provides in-depth knowledge and skills necessary to implement, monitor, and manage an IT infrastructure aligned with information security policies. Covering seven domains of the SSCP Common Body of Knowledge (CBK), the course is aimed at security practitioners in operational roles who seek to advance their practical security skills and prepare for the SSCP exam, focusing on areas like Risk Management, Cryptography, and Incident Response.

Links to enroll:

5 Days | Self Paced

CISO Academy

Duration Options:

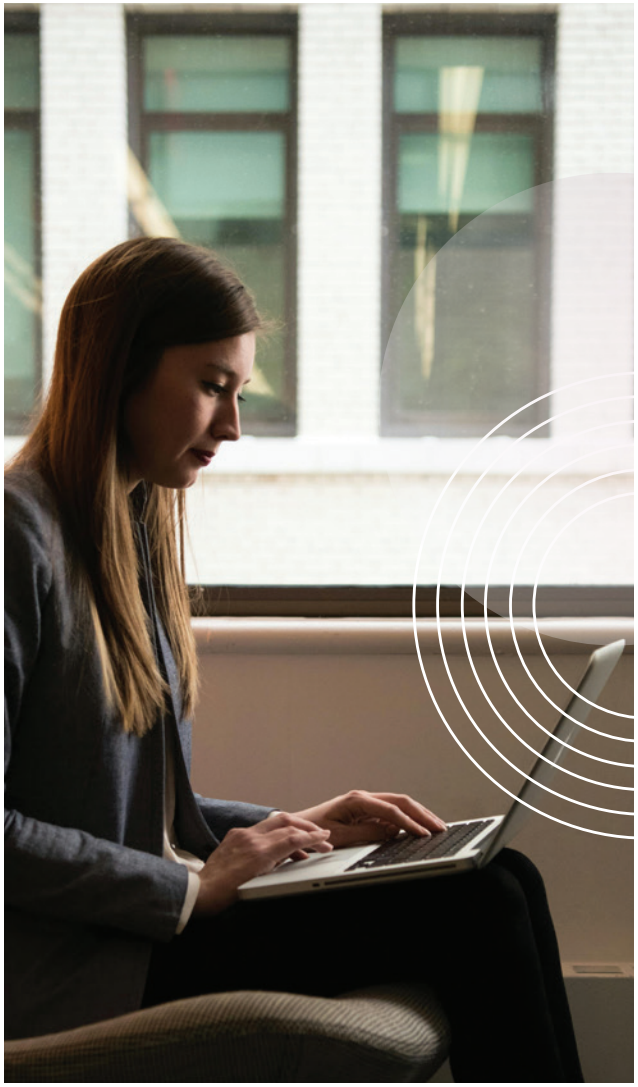
- 5-days training
- Self paced course

Relevant Audience:

Network Security Engineers, Systems/Network Administrators, Security Analyst, Systems Engineers, Security Consultants/Specialists, Security Administrators, Database Administrators.

Prerequisites:

- Minimum of one year of professional experience in IT security
- Understanding of security operations and infrastructure
- Comfort with technical and hands-on security tasks



Delivery Method:

5-DAYS: Virtual, Instructor Led-Training

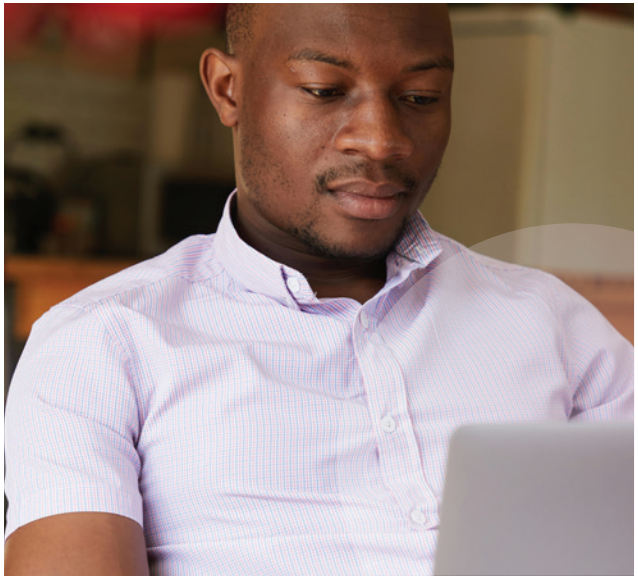
SELF PACED: Self-paced Learning

CISO Academy

INFORMATION SYSTEMS AUDITOR

BY ISACA

Duration: 4 days



Overview:

The CISA certification training provides a comprehensive review of the five critical domains necessary for auditing, controlling, and securing information systems. Recognized globally as the "gold standard" in IT/IS audit certification, the CISA prepares professionals to assess and ensure the reliability, confidentiality, and integrity of information assets. This training is ideal for IT auditors and professionals looking to validate their skills in information systems governance and security.

Relevant Audience:

- Security Managers
- IT Auditors and Compliance Officers
- IT Governance Specialists
- Risk and Assurance Managers
- IT and Security Systems Engineers

Prerequisites:

- Three to five years of professional experience in IT, Auditing, or security
- Understanding of IT governance, risk management, and compliance frameworks
- Familiarity with IT audit principles, security controls, and business processes
- Experience with IT systems, infrastructure, and organizational policies

Delivery Method:

Virtual, Live Instructor-Led Training

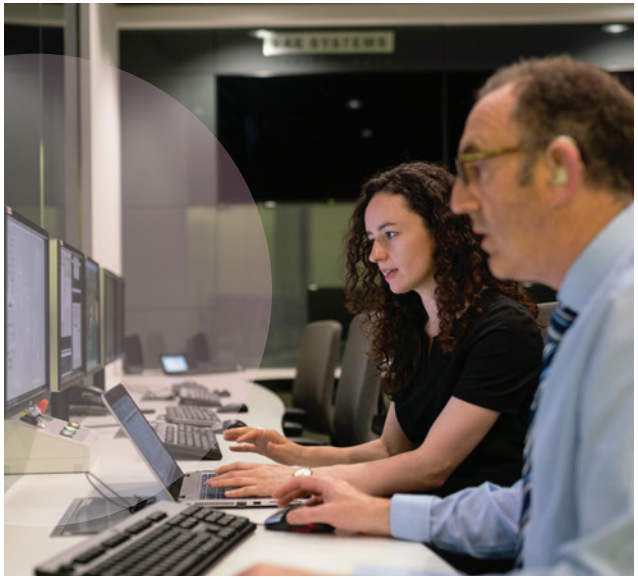
Link to Enroll

INFORMATION SECURITY MANAGER

BY ISACA

CISO Academy

Duration: 4 days



Overview:

The CISM certification training provides a focused overview of essential information security management principles across four domains: Governance, Risk Management, Program Development, and Incident Response. Designed for security managers and professionals in leadership roles, this course prepares participants to manage and align security strategies with organizational objectives, making it ideal for those seeking to advance in information security management.

Relevant Audience:

- Information Security Managers
- Security Consultants or Security Analysts
- IT Directors or Security Directors
- Security Architects
- Risk and Compliance Managers
- Chief Information Security Officers (CISO)

Prerequisites:

- Five years of professional experience in Information Security or IT Management
- Understanding of Information Security Governance, Risk Management, and Compliance
- Experience in Security Program Development, Incident Response, and business continuity
- Familiarity with IT security frameworks, policies, and Access Control Management

Delivery Method:

Virtual, Live Instructor-Led Training

Link to Enroll

CISO Academy

READY, STEADY, HACK

BY NotSoSecure part of claranet cyber security

Duration: 1/2 day

Overview:

A half-day, hands-on course designed for security and IT decision-makers to step into the mindset of real-world threat actors. Participants will engage in lab-based exercises to explore common adversary techniques, helping them develop a more strategic approach to cyber security by understanding how attackers operate and identifying security weaknesses in their environment.

Relevant Audience:

CISOs, Heads of Security, Security Managers, CTOs, Development Team Leads, and Network Managers. It is not suitable for technical practitioners like SOC Analysts or Penetration Testers.

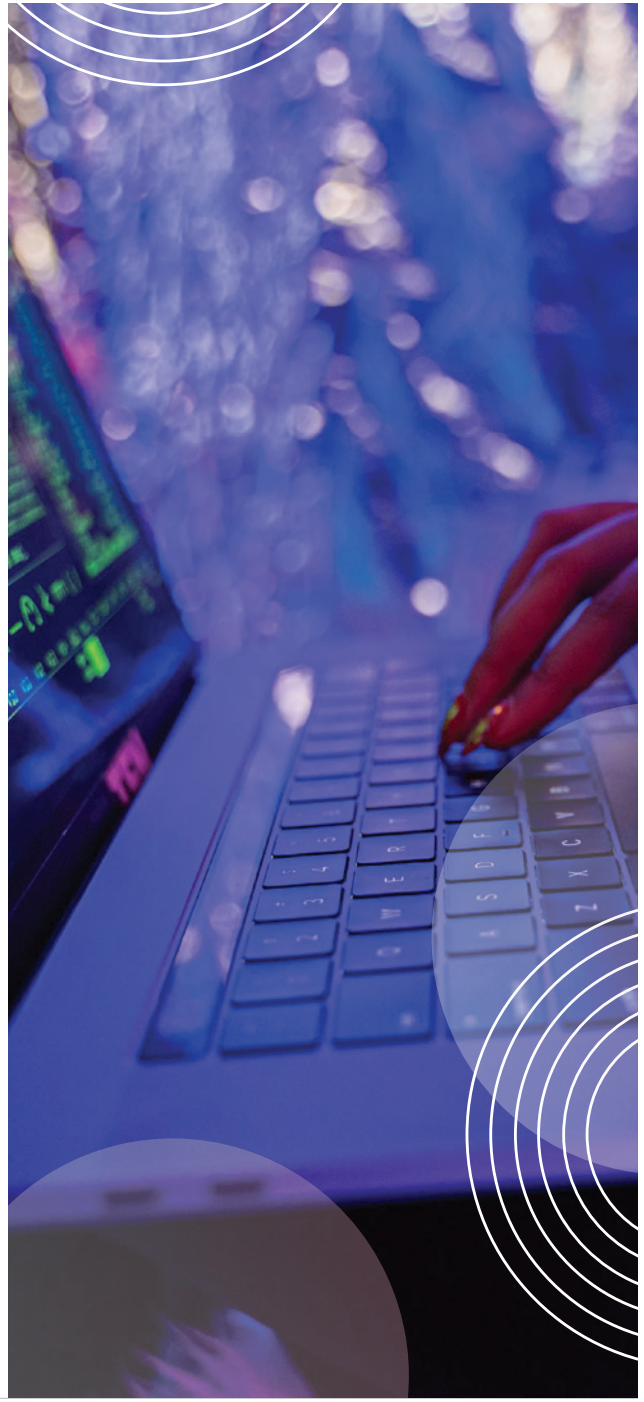
Prerequisites:

- Intermediate to advanced cyber security knowledge
- Basic networking skills
- Confidence with basic computer commands

Delivery Method:

Virtual, Live Instructor-Led Training

Link to Enroll



CISO'S SECRETS PODCAST

The CISO's Secrets podcast offers a rare opportunity for CISOs and CIOs to gain insights from their peers while providing valuable perspectives for those working closely with them. Whether you're a C-level executive, a board member, or simply someone looking to deepen your understanding of the challenges and opportunities in this role, this podcast is for you. Our esteemed guests include industry leaders such as Brian Lozado (HBO MAX), Kurt John (Siemens), Max Garcia (NCR), Ross Young (Caterpillar), and many more. And here's a little (CISO) secret—listening to our podcast also counts toward CPE credits!

Learn More

Listen Now

SMARTAWARENESS

A security awareness platform that provides training and phishing simulations, empowering employees with the knowledge and skills to stay cyber secure.

SMARTAWARENESS

SaaS SOLUTION FOR SECURITY AWARENESS TRAINING AND PHISHING SIMULATIONS

Check Point SmartAwareness is a security awareness training that empowers employees with the knowledge and skills to stay cyber secure at work and home.
With thousands of awareness training resources and phishing simulations, you'll have everything you need to increase cyber security awareness for all employees.

FEATURES AND BENEFITS:

+2,000 Security Awareness Training Modules and Phishing Simulations:
Designed to reinforce secure habits and prepare your employees for the most challenging threats.

Unlimited Usage of Content:
Complete access to phishing campaigns, training modules, and future updates with no extra costs.

Expert Guidance:
Personalized support from a dedicated Customer Success Manager to optimize your security awareness strategy.

HIGH QUALITY TRAINING

Available as a Managed Service:
A trusted team of experts who will manage and conduct your team's awareness training for you.

Supports Over 35 Language:
Enable your employees to gain a deep awareness of security issues in their language.

Program Automation:
Save time and deliver training in the teachable moment by automating training delivery.

Reporting and Assessments:
Pre-built automated reports, training campaign summaries and unlimited custom reporting.

Compatible with All Check Point Products:
Ensuring a unified approach to cyber security training and threat management.

PROUD TO PARTNER WITH:

INFOSEC

Request a Demo

Link to Enroll

CYBER PARK

A gamified hacking environment to solve real-life problems in cyber ranges, escape rooms, and quests.

CYBER PARK

Cyber Park is an immersive, gamified cyber security experience designed to showcase cutting-edge threats and threat prevention through interactive simulations, real-world attack scenarios, and expert-led demonstrations. It serves ad Check Point's "flight simulator" for cyber security professionals, providing participants with hands-on experience tackling the latest cyber threats and using the most advanced mitigation strategies. Whether you're a security professional, executive, or just passionate about cyber security, Cyber Park offers a unique opportunity to explore the future of cyber defense in a dynamic and engaging environment.

Visit Cyber Park

ANATOMY OF ATTACK PART 1 & 2

CYBER RANGE

Gamified Live Attack Simulation

Cyber Park

Duration: 120 Minutes

Red Team Scenario

Part 1 Overview:

Join Javelin, an elite penetration testing team, on a covert assignment to assess the security of Redford's municipal network. As the city strives to become a global leader in smart-city infrastructure, it has implemented an advanced traffic-light control system. Javelin's mission is to infiltrate the network, identify vulnerabilities, and ultimately disable the system to simulate the potential impact of a cyber attack. Through Port Scanning, Privilege Escalation, and Remote Execution, participants will demonstrate the risks and reinforce the importance of strong cyber security measures for Redford's engineers.

Link to Enroll

Part 2 Overview:

In this campaign, participants are members of Javelin, an elite penetration testing team, tasked with testing the security of Universe, a fast-growing credit card company. Starting with access to a standard employee workstation, participants must uncover vulnerabilities and escalate privileges to expose critical weaknesses in the network. From exploiting open ports and brute-forcing passwords to leveraging misconfigured scripts and cracked zip files, this operation will demonstrate Universe's security gaps and prove the value of thorough network testing.

Link to Enroll

Relevant Audience:

Offensive Security Practitioners, Vulnerability Assessment Management

Prerequisites:

Basic offsec knowledge. Need to bring own offensive tools, all TCP/UDP ports available.

Delivery Method:

On-Demand

APPOCALYPSE NOW

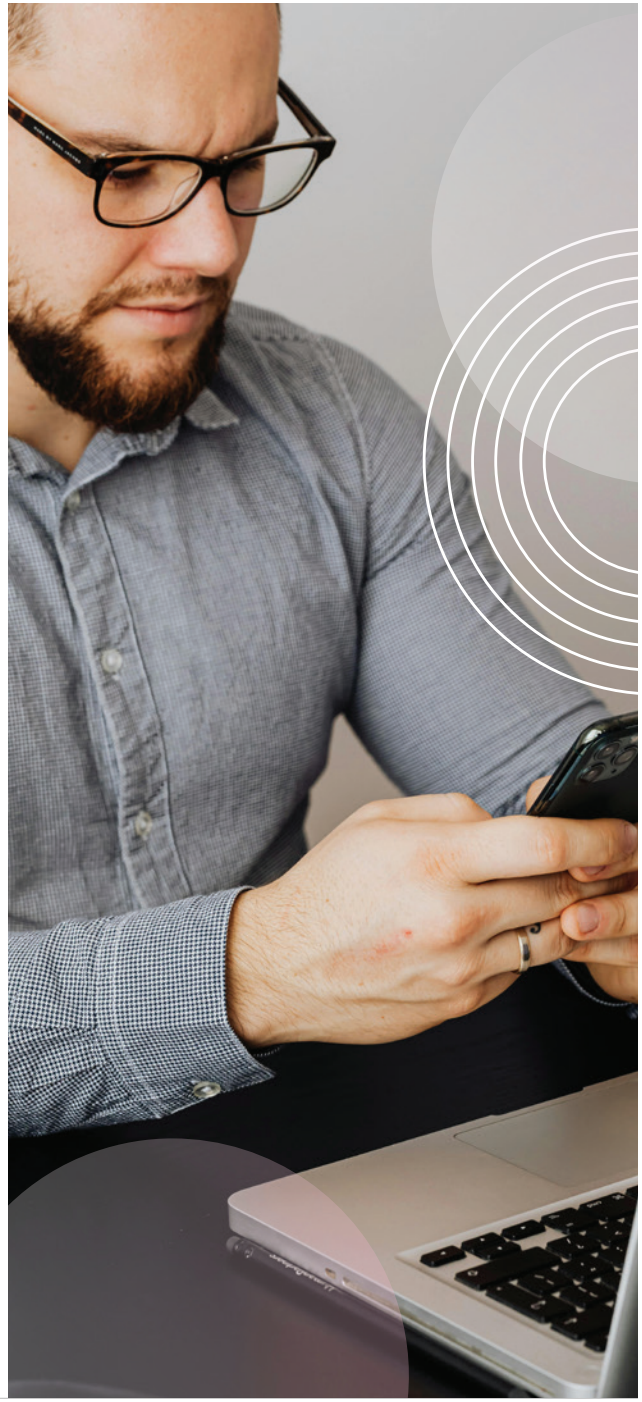
CYBER RANGE

Gamified Live Attack Simulation

Cyber Park

Duration: 240 Minutes

Red Team Scenario



Overview:

In this campaign, participants take on the role of a black-ops cyber agent gathering intelligence on a fictional nuclear program. After breaching a government network, participants are tasked with identifying an entry point into the nuclear program and conducting covert operations to advance the mission. Using reverse engineering, vulnerability exploitation, and brute-force tactics, participants will work to infiltrate key systems, delay personnel, and capture sensitive data.

Relevant Audience:

Offensive Security Practitioners, Vulnerability Assessment Management

Prerequisites:

Reverse engineering, Buffer Overflow, need to bring own offensive tools, all TCP/UDP ports available.

Delivery Method:

On-Demand

Link to Enroll

BROKEN ACCESS CONTROL

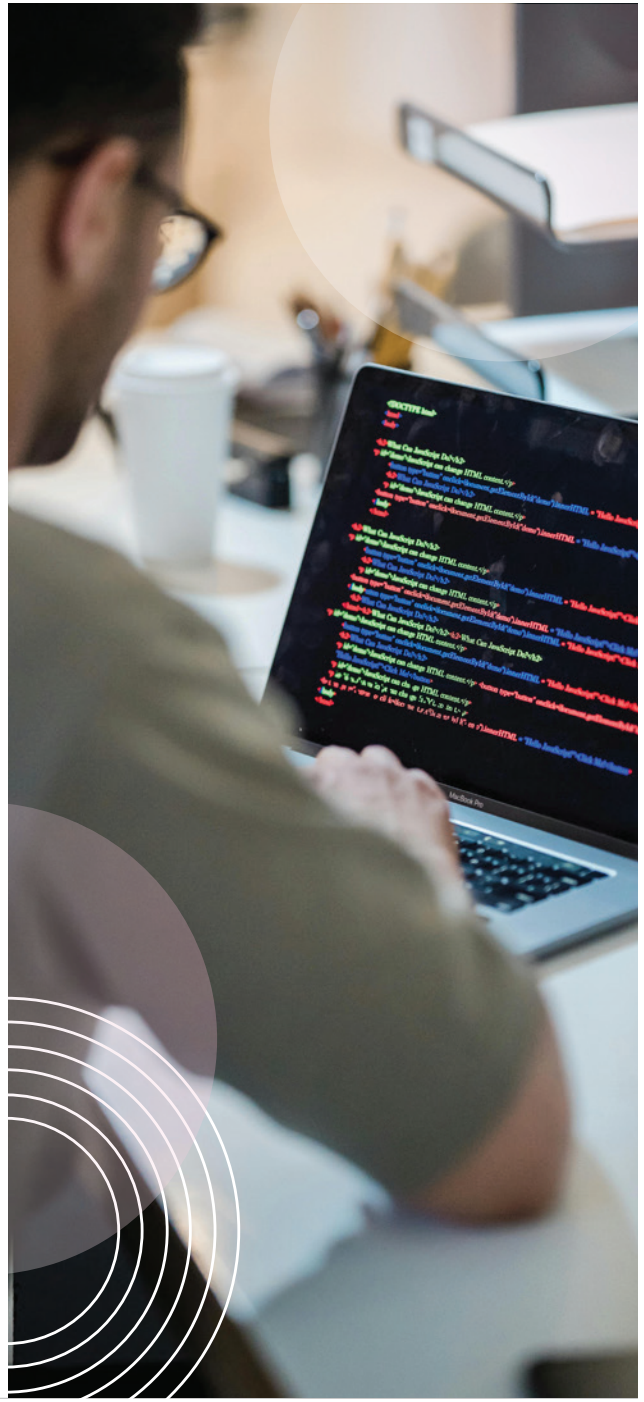
CYBER RANGE

Gamified Live Attack Simulation

Cyber Park

Duration: 240 Minutes

Red Team Scenario



Overview:

In this campaign, participants explore the concept of privilege escalation by exploiting vulnerabilities in a multi-user environment. Through various scenarios, they will attempt to gain unauthorized access to restricted features, manipulate data, and execute actions on behalf of other users. This includes two types of Privilege Escalation: Vertical Privilege Escalation, where a low-privilege user gains unauthorized access to higher-level privileges, and Horizontal Privilege Escalation, where a user accesses functions or data intended for another user at the same privilege level.

The campaign emphasizes the importance of robust access controls and proper permissions to safeguard systems from such threats.

Relevant Audience:
Offensive Security Practitioners, Vulnerability Assessment Management

Prerequisites:
Knowledge of web vulnerabilities. Can bring own tools as needed (recommend Burpsuite or similar); all TCP/UDP ports available

Delivery Method:
On-Demand

Link to Enroll

BROKEN AUTHENTICATION

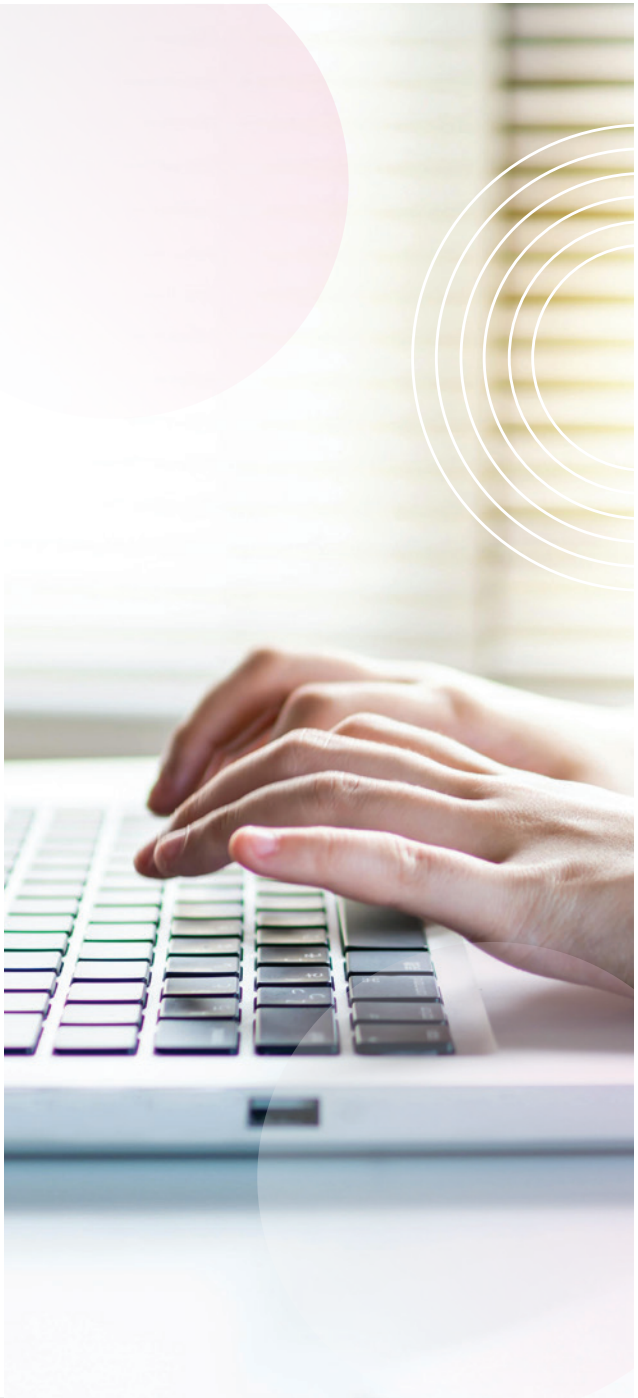
CYBER RANGE

Gamified Live Attack Simulation

Cyber Park

Duration: 180 Minutes

Red Team Scenario



Overview:

In this campaign, participants tackle various authentication vulnerabilities, focusing on broken authentication and flawed session management. The missions simulate real-world scenarios such as exploiting weak password mechanisms, bypassing two-factor authentication, resetting passwords via social engineering, and leveraging OAuth exploits to gain unauthorized access. These challenges reinforce the importance of strong authentication protocols, secure password policies, and careful implementation of OAuth to prevent unauthorized access and data breaches.

Relevant Audience:

Offensive Security Practitioners, Vulnerability Assessment Management

Prerequisites:

Knowledge of web vulnerabilities. Can bring own tools as needed (recommend Burpsuite or similar); all TCP/UDP ports available.

Delivery Method:

On-Demand

Link to Enroll

Cyber Park

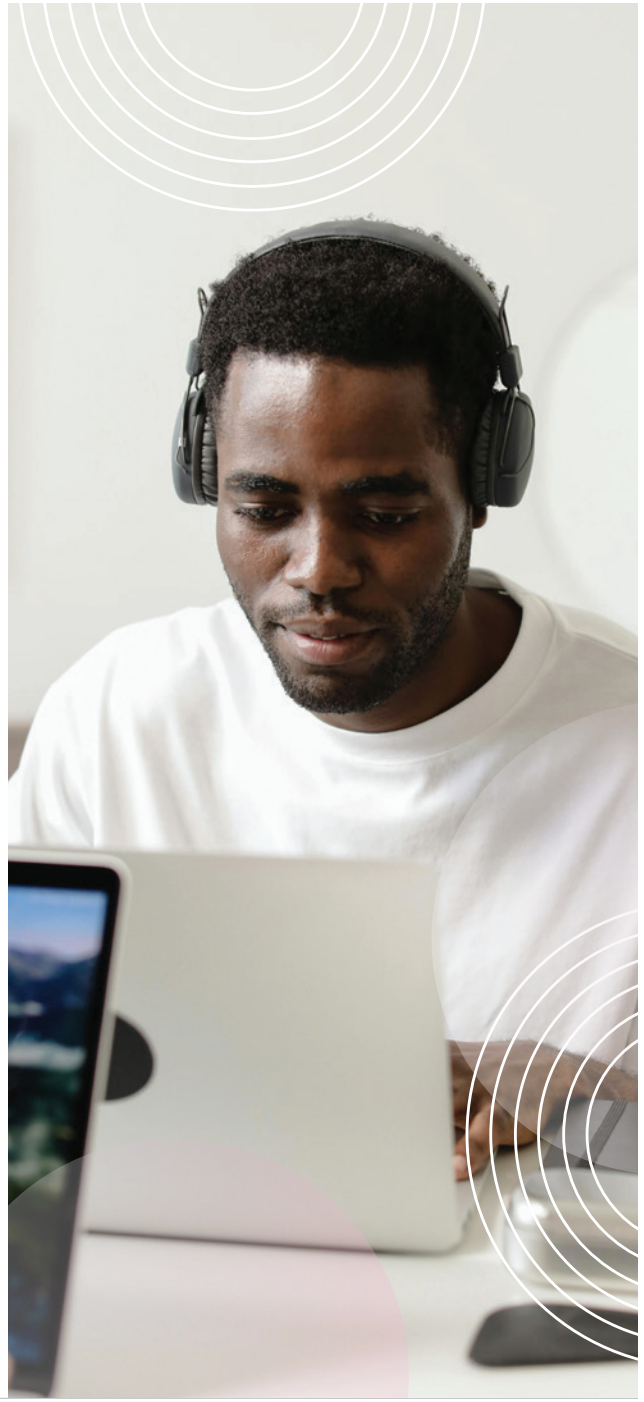
CATCH ME IF YOU CAN PART 1

CYBER RANGE

Gamified Live Attack Simulation

Duration: 240 Minutes

Red Team Scenario



Overview:

In this campaign, participants play the role of the IT security team in a small coastal town facing a coordinated heist. When $25,000 is stolen from a local bank, the robbers create chaos by disabling street cameras, controlling traffic lights, and jamming police radios to ensure a smooth getaway. Participants must re-enable surveillance systems, analyze network traffic, and counteract interference in police communications to aid the pursuit. This high-pressure scenario tests skills in network enumeration, credential access, and real-time response to cyber disruptions.

Relevant Audience:

Offensive Security Practitioners, Vulnerability Assessment Management

Prerequisites:

Reverse engineering

Delivery Method:

On-Demand

Link to Enroll

CLOUDY FOR CXO

CYBER RANGE

Gamified Live Attack Simulation

Cyber Park

Duration: 60 Minutes

Blue Team Scenario

Overview:

In this campaign, participants will step into the role of a Chief Information Security Officer (CISO) for a pharmaceutical company facing the ongoing threat of data breaches and cyber attacks. Participants will investigate a potential phishing attack targeting one of the company's scientists and track down the origin, motive, and methodology behind it. This hands-on exercise emphasizes key skills in email forensics, phishing detection, and understanding data loss prevention (DLP) techniques. Through simulated scenarios, participants will uncover security events and analyze threats using tools available in the Harmony Email & Collaboration platform.

Relevant Audience:

SOC Analysts and IT professionals

Prerequisites:

Fundamental knowledge of cyber security principles, methodologies, and tactical approaches.

Delivery Method:

On-Demand

Link to Enroll

Cyber Park

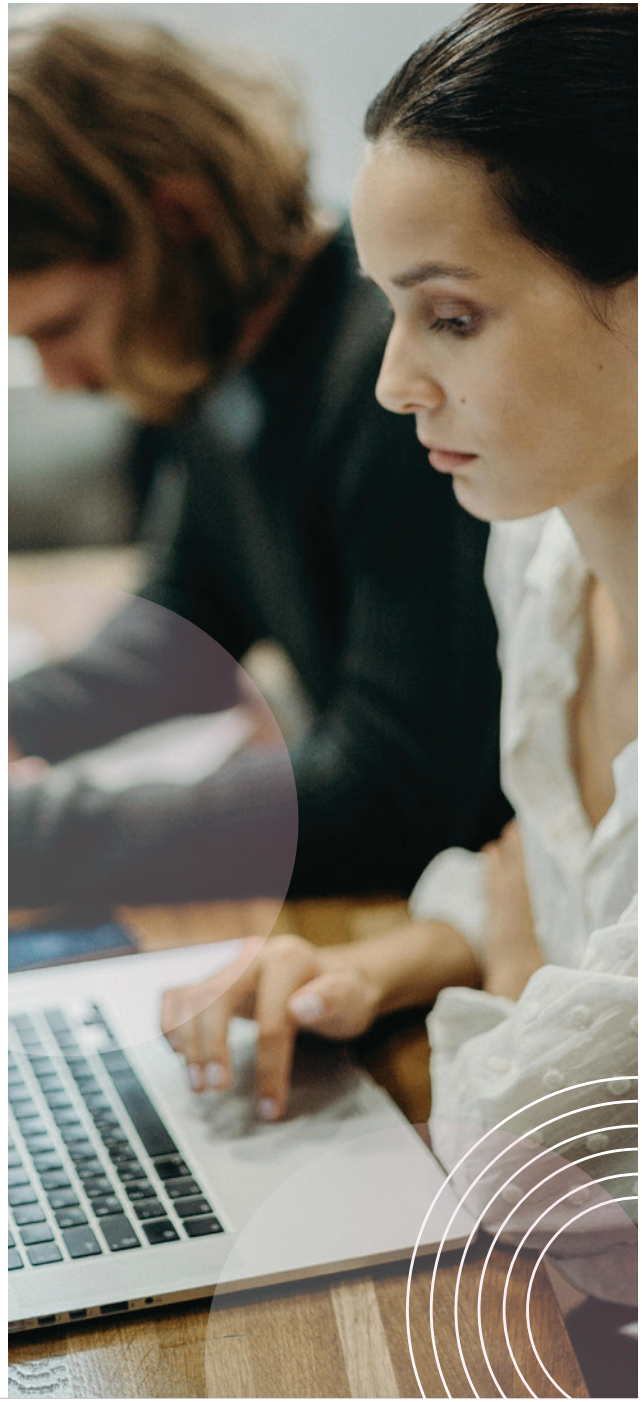
CRYPTOGRAPHIC ISSUES

CYBER RANGE

Gamified Live Attack Simulation

Duration: 180 Minutes

Red Team Scenario



Overview:

In this campaign, participants address cryptographic flaws that can lead to serious data security vulnerabilities. The mission challenges users to identify weak encryption implementations, decipher poorly encrypted data, and explore cryptographic techniques used incorrectly in applications. From spotting outdated algorithms to manipulating encrypted coupon codes, this exercise reinforces the importance of using strong encryption practices and adhering to industry standards for protecting sensitive information.

Relevant Audience:

Offensive Security Practitioners, Vulnerability Assessment Management.

Prerequisites:

Encryption, decoding. Can bring own tools as needed (recommend Burpsuite or similar); all TCP/UDP ports available.

Delivery Method:

On-Demand

Link to Enroll

Cyber Park

GAME OF CLOUDS

CYBER RANGE

Gamified Live Attack Simulation

Duration: 50 Minutes

Blue Team Scenario

Overview:

In this campaign, participants are tasked with uncovering the security breach in a massively popular game, which has seen unauthorized access to user credentials and in-game purchases. Acting as a security investigator, they work closely with Yelloworks' cloud infrastructure on AWS to trace how attackers gained access and exploited the system. Using Check Point CloudGuard and forensic tools, participants will identify the vulnerabilities, analyze suspicious traffic and SSRF attacks, secure the backend, and close gaps in the cloud configuration. By resolving these critical security issues, they help restore trust and ensure the game's continued success.

Relevant Audience:

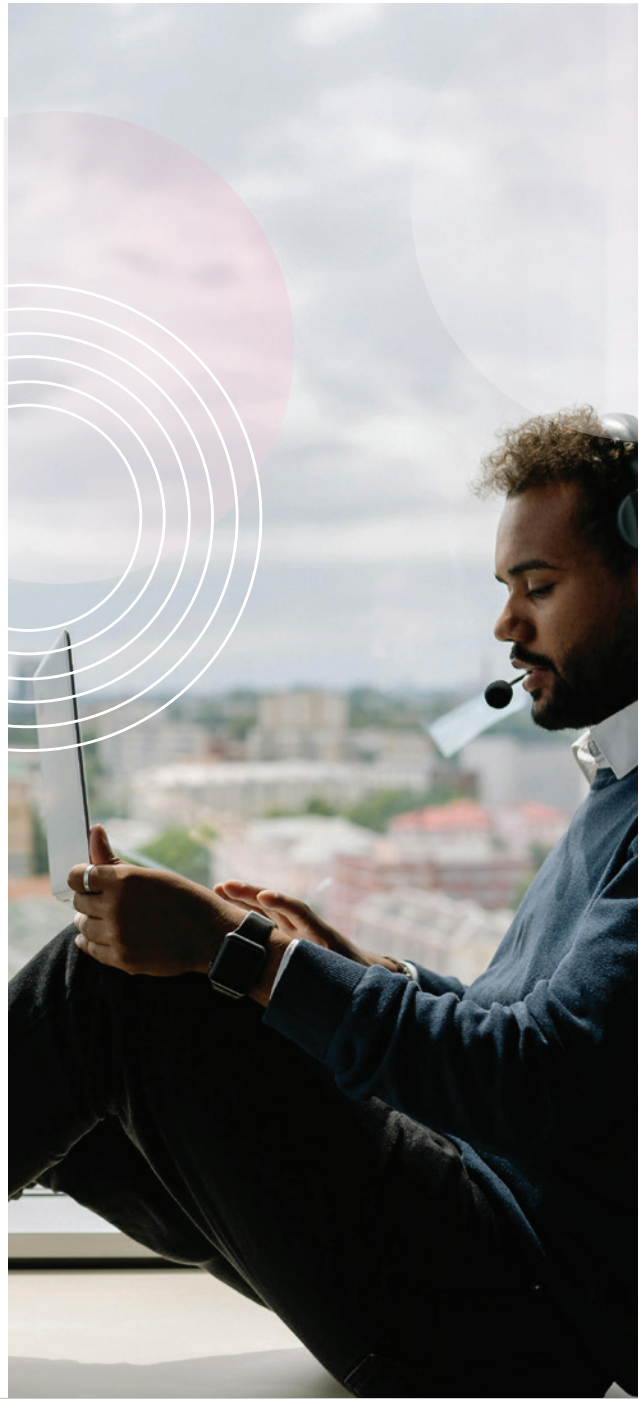
SOC Analysts and IT Professionals

Prerequisites:

Fundamental knowledge of cyber security principles, methodologies, and tactical approaches.

Delivery Method:

On-Demand



Link to Enroll

Cyber Park

LORD OF THE PINGS

CYBER RANGE

Gamified Live Attack Simulation

Duration: 240 Minutes

Red Team Scenario

Overview:

In this high-stakes cyber operation, participants work to infiltrate and disable critical infrastructure within a fictional nation's nuclear program. Beginning with network access and progressing through SQL injection, directory traversal, and code injection, they will uncover sensitive data, disable air defenses, and simulate a system malfunction in the nuclear plant. Using Check Point CloudGuard and advanced security tools, participants will play a crucial role in a covert mission aimed at preventing a global crisis.

Relevant Audience:

Offensive Security Practitioners, Vulnerability Assessment Management.

Prerequisites:

Knowledge of web and Linux vulnerabilities. Need to bring own offensive tools, all TCP/UDP ports available

Delivery Method:

On-Demand

Link to Enroll

Cyber Park

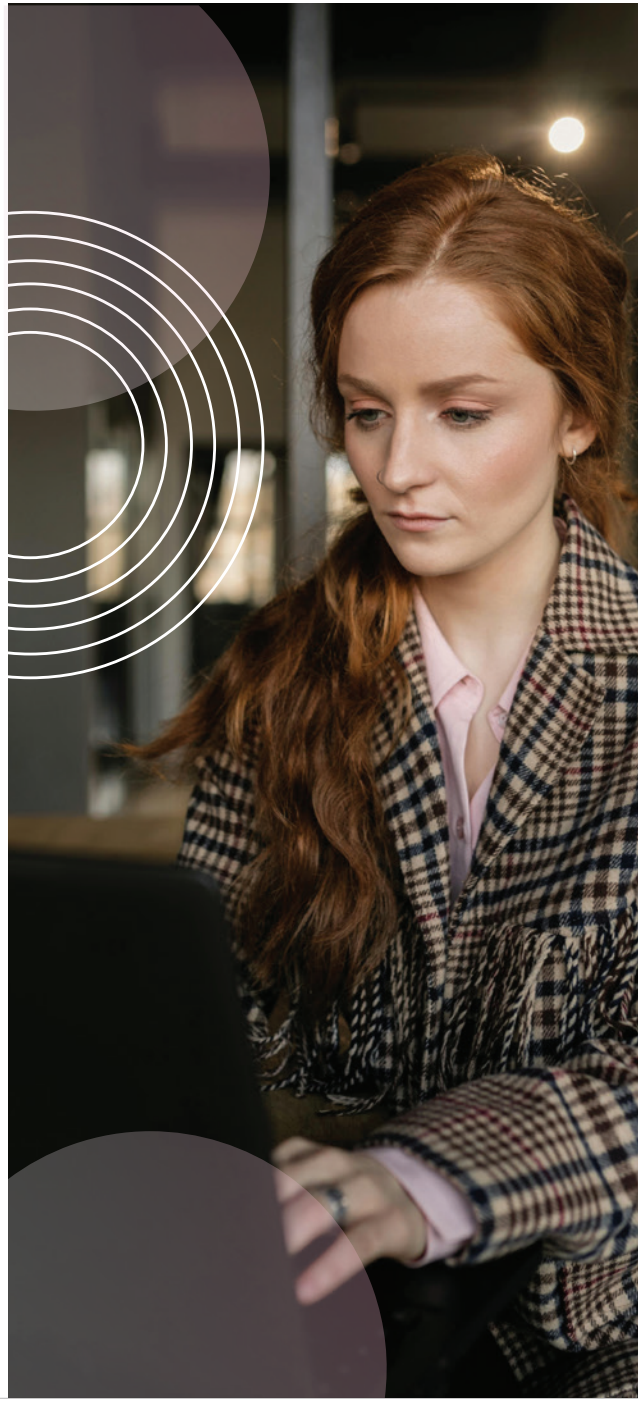
RECORDING CRUCIAL ERROR (RCE)

CYBER RANGE

Gamified Live Attack Simulation

Duration: 180 Minutes

Red Team Scenario



Overview:

In this campaign, participants act as BlueSec analysts tasked with assessing the security of a global gaming company's internal network. Due to a critical, recently discovered vulnerability, the company has requested immediate penetration testing. Starting with access through an employee's endpoint, participants will map the network, identify vulnerable services, exploit weaknesses, and confirm access to restricted areas. By uncovering and demonstrating vulnerabilities, participants help the company secure its systems against potential exploitation.

Relevant Audience:

Offensive Security Practitioners, Vulnerability Assessment Management.

Prerequisites:

Offsec knowledge; Linux internals. Need to bring own offensive tools, all TCP/UDP ports available

Delivery Method:

On-Demand

Link to Enroll

SENSITIVE DATA EXPOSURE 1

CYBER RANGE

Gamified Live Attack Simulation

Cyber Park

Duration: 120 Minutes

Red Team Scenario

Overview:

In this campaign, participants act as cyber security professionals investigating the security of a niche online juice venture set up by a relative of their boss. Despite using "super secure technologies," human error and misconfigurations have left the business vulnerable. The campaign guides participants through weaknesses in user credentials, social engineering, and exposed sensitive data, demonstrating how even secure systems can be undermined by overlooked vulnerabilities. The goal is to gather evidence of these weaknesses to protect the company and prevent potential costly breaches.

Relevant Audience:

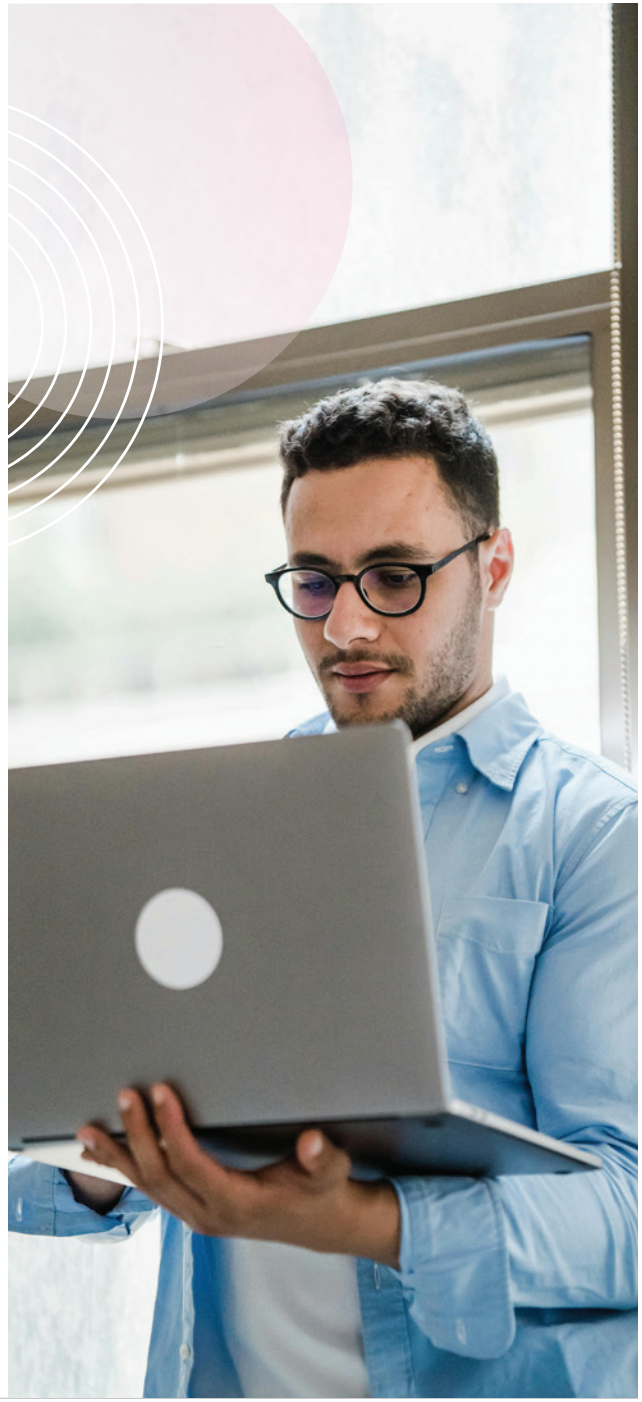
Offensive Security Practitioners, Vulnerability Assessment Management.

Prerequisites:

Knowledge of web vulnerabilities. Can bring own tools as needed (recommend Burpsuite or similar); all TCP/UDP ports available.

Delivery Method:

On-Demand



Link to Enroll

SERVERLESS WORLD

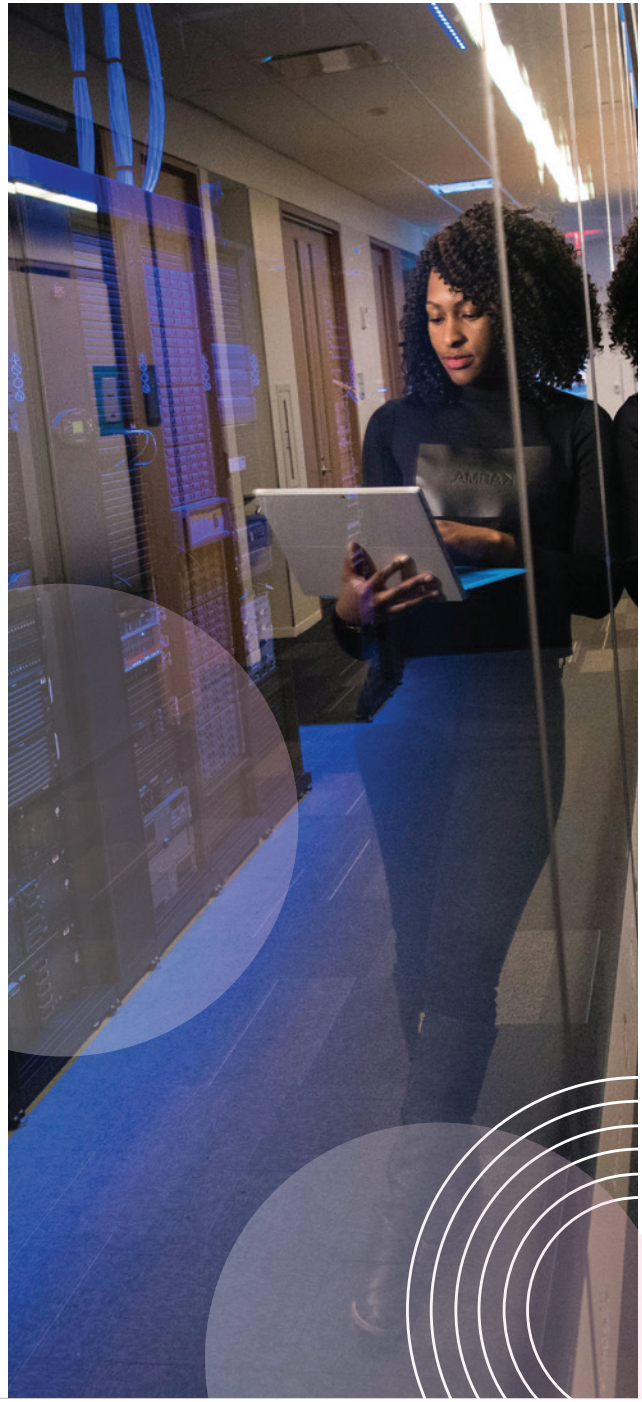
CYBER RANGE

Gamified Live Attack Simulation

Cyber Park

Duration: 60 Minutes

Blue Team Scenario



Overview:

This campaign guides participants through securing an application by embedding security early in the development lifecycle. Participants will use Check Point's CloudGuard and ShiftLeft tools to identify and remediate security vulnerabilities in code, configuration, and permissions, ensuring the application is safe for deployment on cloud infrastructure.

Relevant Audience:

SOC Analysts and IT Professionals.

Prerequisites:

Basic coding understanding.

Delivery Method:

On-Demand

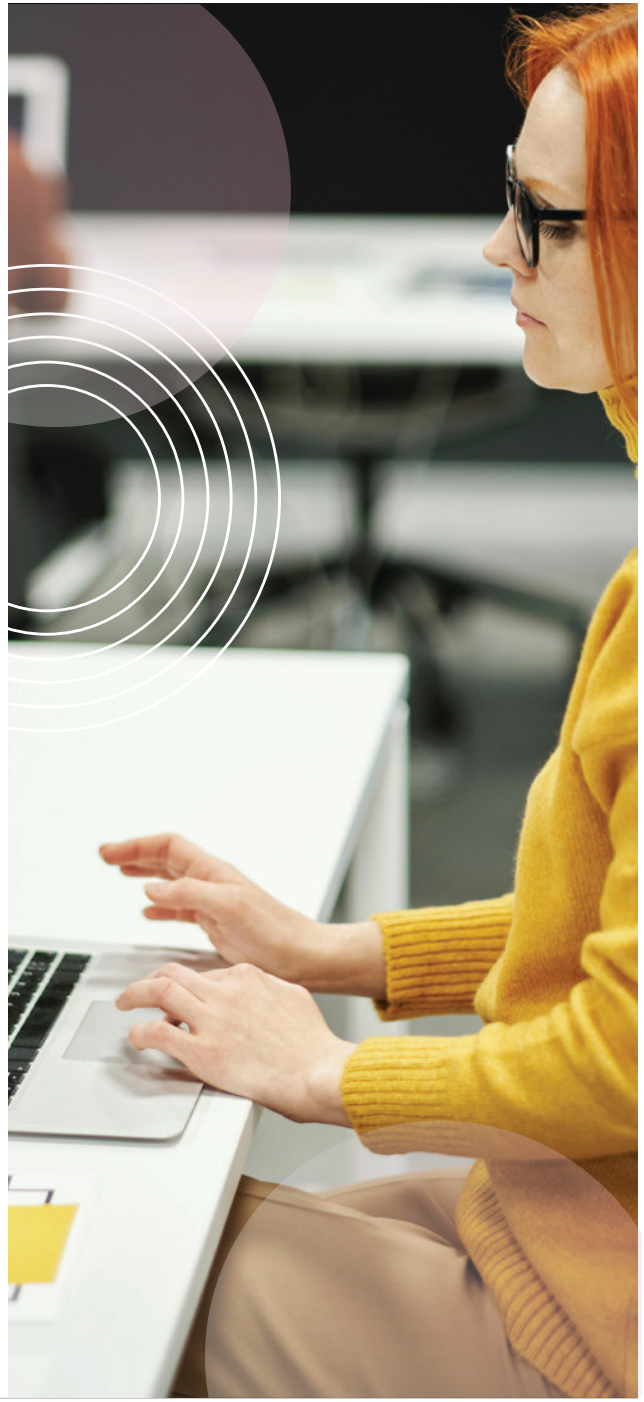
Link to Enroll

Cyber Park

SOUR LEMON
CYBER RANGE
Gamified Live Attack Simulation

Duration: 90 Minutes

Blue Team Scenario



Overview:

In this scenario, SOC Analysts and Threat Hunters will utilize tools to analyze network activity on Windows OS. Your objective is to detect execution, lateral movement, and command and control operations within the network.

Relevant Audience:

SOC Analysts and Threat Hunters

Prerequisites:

Encryption, decoding. Can bring own tools as needed (recommend Burpsuite or similar); all TCP/UDP ports available

Delivery Method:

On-Demand

Link to Enroll

THE WIZARD OF OS

CYBER RANGE

Gamified Live Attack Simulation

Cyber Park

Duration: 240 Minutes

Red Team Scenario

Overview:

In this campaign, participants are part of an elite international cyber team tasked with infiltrating South Rajuan's highly controlled government network. Their mission begins with obtaining an academic credential for an MI6 mole to place her in a key position within the Ministry of Transportation. Once inside, they will work to gather intelligence on the nation's nuclear ambitions, access encrypted data, and establish lateral movement across the network. This operation is a critical first step in a larger mission to dismantle South Rajuan's nuclear capabilities.

Relevant Audience:

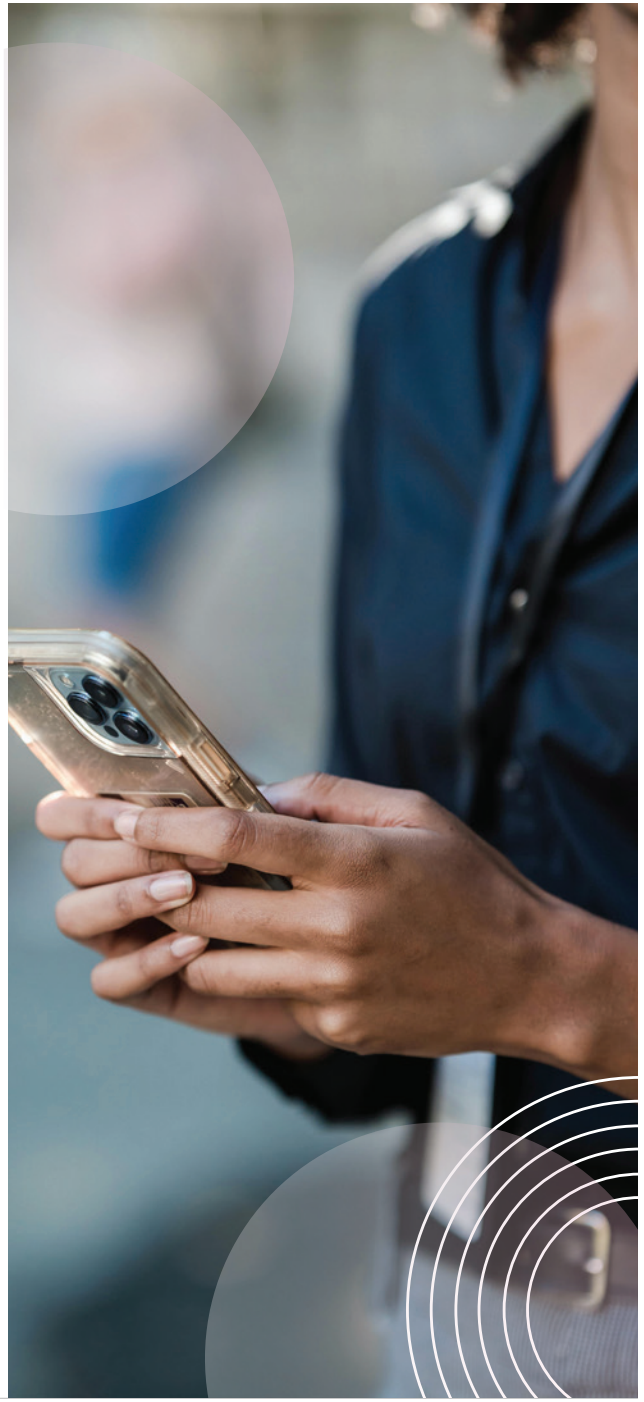
Offensive Security Practitioners, Vulnerability Assessment Management.

Prerequisites:

Basic Offsec knowledge. Need to bring own offensive tools, all TCP/UDP ports available

Delivery Method:

On-Demand



Link to Enroll

QUICK LINKS

IGS Training Website

IGS Training Portal

ATC Locator

CONTACT US

HAVE ANY QUESTIONS?
NEED EXPERT ASSISTANCE TO GET STARTED?

Contact us at services@checkpoint.com