INE SECURITY

Training and Certifications

Start here to build and mature cybersecurity teams.

Whether you're looking to sharpen red and blue team skills, upskill or retain existing employees, or close skill gaps on your team, **INE has the right training at an affordable cost.**



US: 877.224.8987 | Intl: 984.444.9917 | support@ine.com

INE for Organizational Training

Discover a New Approach to Cybersecurity Training with INE.

Improve your team performance and productivity while closing crucial skill gaps, keeping your organization ahead of the technological curve by using INE's subscription-based training program.

Affordable // Hands-On // Continuous

Choose INE for Its Full-Cycle Training Approach

Immersive Lab-Based Learning:

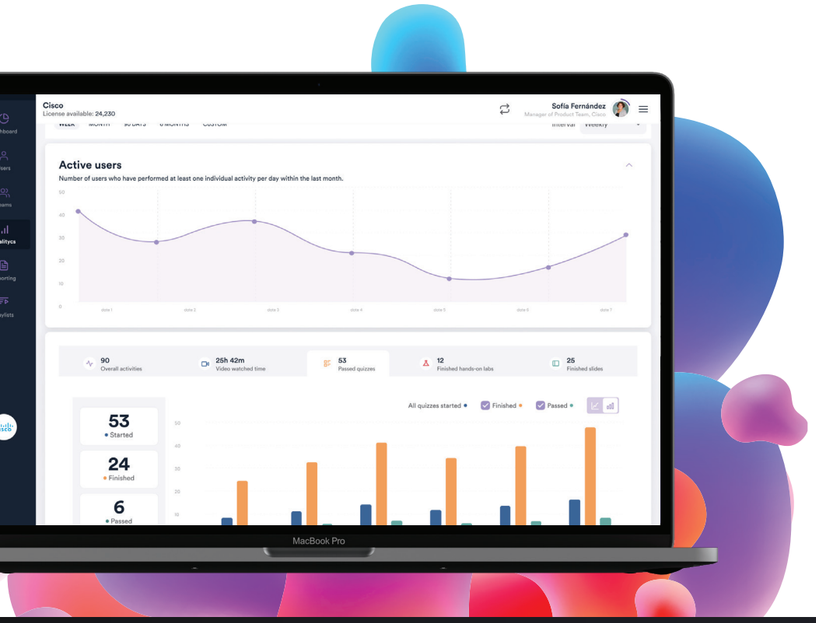
By providing practitioners with more than 3,400 labs (through training and specialized labs) - we know that the learner is equipped to respond to real-workplace scenarios.

Continuous and Adaptable Learning:

INE regularly updates and adds new content to give practitioners what they need to succeed in their roles. We offer training across disciplines and at every proficiency level to help professionals keep learning throughout their career.

Authentic Assessment:

Practitioners are put to the test with our hands-on labs, skills assessments for teams, and certifications, giving accurate, real-time feedback on their ability to translate skills into the real-world.



Business Solutions

Trusted by organizations globally, INE provides solutions to ensure that you're not only training individuals but upskilling teams across the enterprise. Enhance workforce competence and productivity by closing KSA (knowledge, skills, and abilities) gaps.

See our Training For Teams
at https://ine.com/enterprise

Continuous Cycle of Learning

Today's cyber threats demand that your team is constantly at the top of their game.

At INE, we have created a continuous cycle of learning, so your team is always trained on the latest technology and emerging threats.

Assess

INE's Skill Sonar tool measures progress and proficiency. Assess your skills to ensure you're always on the right track.

Train

Our content library and on-demand courses provide learners with the knowledge and skills needed to succeed in Networking, Cybersecurity, and Cloud.

Practice

Dive deep into exclusive Lab Collections, specifically curated to challenge technical skills and reinforce advanced understanding of tasks.

Validate

INE Security's certifications confirm your learning and proficiency, providing recognition of mastery in necessary work role skills.

CONTINUOUS CYCLE OF LEARNING

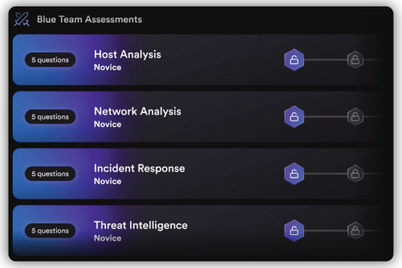
US: 877.224.8987 | Intl: 984.444.9917 | info@ine.com

skillsonar
You have to know to grow.

Usable Benchmarks for Your Training Roadmap

Skill Sonar puts authentic, real-time assessment data in the hands of leaders to help them succeed.

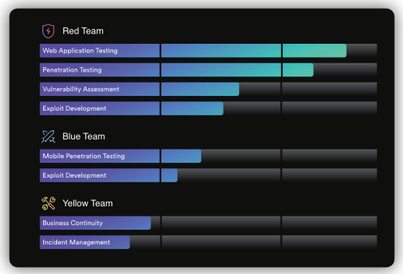
How Does It Work?



01 Assess

Measure current proficiency levels.

Ask your team to take assessments. Skill Sonar offers assessments in cybersecurity and networking, with cloud assessments coming soon.



02 Evaluate

Identify skill gaps.

See the results for each team member, broken down by skill set, so you can determine exactly where they have room to grow.



03 Improve

Create targeted training.

Automated, dynamic training playlists based on individual skill assessment performance can be assigned to offer targeted training that updates according to their most current training needs.

Skill Sonar Playlists

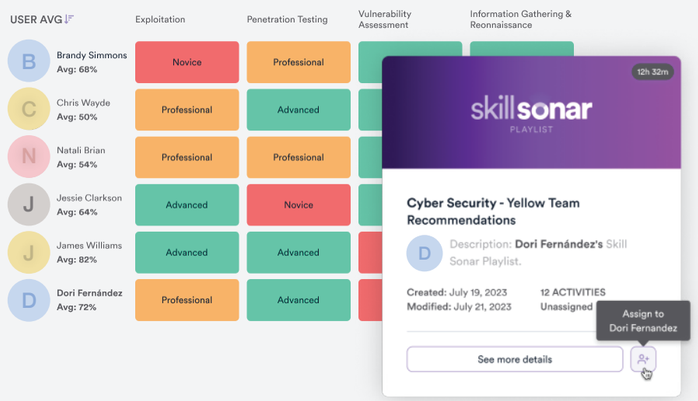
Upskill your team with auto-generated, dynamic playlists based on user performance. INE's playlist system makes it easy to assign relevant training material to individual skill levels - with less manual lift from team managers.

ENHANCE Employee Retention + **RECRUIT** Exceptional Talent + **UPSKILL** Teams

Dynamic, Adaptable Content
Playlists evolve with the user's growth, encouraging users to reassess as they progress through training.

Minimal Team Manager Involvement
Team managers assign auto-curated playlists based on individual assessment performance - no curation required from leaders.

Targeted Learning
Tailored to the specific strengths, weaknesses, and progress of each learner, playlists leverage Skill Sonar assessment data to offer highly targeted learning experiences.



Skill Sonar Playlists

Upskill your team with auto-generated, dynamic playlists based on user performance. INE's playlist system makes it easy to assign relevant training material to individual skill levels - without a manual lift from team managers.

US: 877.224.8987 | Intl: 984.444.9917 | support@ine.com

skilldive

Capture The Flag (CTF) Arena by INE

Go Beyond Theoretical Training



Skill Dive is a collection of labs that grow your skillset by immersing you in a practical learning environment. Put what you've learned in traditional training to practice in a risk-free environment. Take your training to the next level with Skill Dive.

Exclusive Labs & CTFs:

Provide your team access to unique, hands-on content not found within INE's Learning Paths and training, including Capture the Flag and Networking challenges.

Common Vulnerabilities & Exposures (CVE) Labs:

Train your team on real-time threats. From widespread software platforms to niche systems, this collection sheds light on a variety of recent and relevant vulnerabilities.

Lab Collections:

Featuring thousands of immersive labs, lab collections are carefully curated to meet relevant challenges technology teams are facing.

Navigate your team's learning journey with dozens of lab collections, CVEs, and CTFs that align with your organizational objectives and specialties, spanning Networking, Cybersecurity, and Cloud.

Lab Collections

- Vulnerabilities
- Ransomware Fundamentals
- Deploying Cisco Collaboration Solutions
- Android Pentesting
- And many more!

Labs

- Cisco Unity Connection Call Handlers
- Leveraging Azure Virtual Network
- Cracking SHA-3 Digests
- RIPng Default Routing
- And many more!

Common Vulnerabilities & Exposures (CVEs)

- Langflow AI RCE (CVE-2025-3248)
- Bento ML RCE (CVE-2025-27520)
- Sudo-Privilege Escalation (CVE-2025-32463)
- Next.js - Middleware Authorization Bypass (CVE-2025-29927)
- And many more!

Equip Your Teams to Tackle Cyber Threats

Your Team's Cybersecurity, Upgraded

INE's Capture The Flag Arena offers cybersecurity challenges designed to engage team members in continuous training with friendly competition in new challenges released monthly.

Test and prove your skills, climb the leaderboards, and emerge victorious in an ongoing series of contests designed to push you to your limits.

Using CTF Arena in Your Organization

01 Team Collaboration:

- Utilize the CTF for your team's bi-weekly tabletop exercise
- Enrich traditional learning through gamified scenarios
- Encourage post-challenge recap to simulate report-out and best practices used in real cyber events

02 Support Individual Learning:

- Encourage team members who get "stuck" to identify their needed areas of training and create playlists to help them succeed
- Work with team members to identify gap areas
- Keep learners engaged by embedding challenges in the training ecosystem

03 Past CTF Arena challenges include:

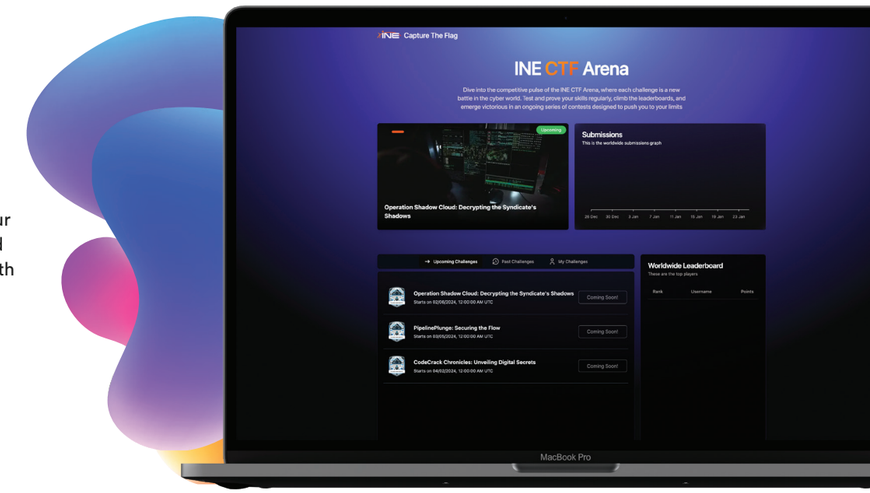
- Operation Shadow Cloud: Decrypting the Syndicate's Shadows
- PipelinePlunge: Securing the Deployment
- CodeCrack Chronicles: Unveiling Digital Secrets

**Retired CTF Arena challenges are available in Skill Dive*

Schedule a demo today!

See how INE can further future-proof your cybersecurity organizational strategy and consistently elevate your team's game with continuous learning.

learn.ine.com/schedule-a-demo



US: 877.224.8987 | Intl: 984.444.9917 | support@ine.com

Learning Paths

INE's learning paths are curated to provide the training cybersecurity professionals need for on-the-job success. Each learning path contains a collection of courses which include hands-on labs, videos, and quizzes.

INE continuously updates courses and learning paths to ensure learners stay ahead of the newest technology, prevention, and mitigation tactics.

Novice	Training Hours
Enterprise Defense Administrator (eEDA)	53h
Penetration Testing Student (eJPT)	156h
Security Operations Certified - Level 1 (eSOC)	--
CompTIA Security+	53h

Professional	
Incident Handling & Response Professional (eCIR)	62h
Mobile Application Penetration Testing Professional (eMAPT)	49h
Penetration Testing Professional (eCPPT)	107h
Threat Hunting Professional (eCTHP)	26h
Web Application Penetration Testing Student (eWPT)	107h
CISSP: Certified Information Systems Security Professional	60h
Malware Analysis Professional	17h
Reverse Engineering Professional	12h
Web Defense Professional	41h

Advanced	
Advanced Web Application Penetration Testing (eWPTX)	77h
Digital Forensics Professional (eCDFP)	24h
Advanced Penetration Testing	9h
Exploit Development Student	22h

INE Security Certifications



eJPT

The Jr. Penetration Tester exam (eJPT) validates that the individual has the knowledge and skills required to fulfill a role as an entry-level penetration tester.



eMAPT

The Mobile Application Penetration Tester (eMAPT) exam is ideal for cybersecurity experts to display advanced mobile application security knowledge through a scenario-based exam.



eCIR

The Certified Incident Responder (eCIR) exam is ideal for blue team security professionals.



eWPT

The Web Application Penetration Tester (eWPT) certification assesses a cybersecurity professional's web application penetration testing skills.



eSOC

The Security Operations Certified – Level 1 (eSOC) exam is designed for individuals beginning their career in security operations and validates core skills needed for Tier 1 SOC analyst roles.



eCTHP

The Certified Threat Hunting Professional (eCTHP) is an expert-level certification that proves your threat hunting and threat identification capabilities.



eWPTX

The Web Application Penetration Tester eXtreme (eWPTX) is our most advanced web application pentesting certification. The exam requires students to perform an expert-level penetration test that is then assessed by INE's cybersecurity instructors.



eEDA

The Enterprise Defense Administrator (eEDA) exam is designed for professionals that are just starting their defensive cybersecurity or security engineering journey.



eCDFP

The Certified Digital Forensics Professional (eCDFP) is an advanced digital forensics exam meant for senior-level cybersecurity professionals.



eCPPT

The Certified Professional Penetration Tester (eCPPT) exam is ideal for individuals with a highly technical understanding of networks, systems and web applications attacks.

Together, we can help you build a stronger, more resilient team and organization.

Connect with us to discuss your organization's unique needs and **book a demo today**.

SCHEDULE A DEMO
learn.ine.com/schedule-a-demo

Red Team Training

Junior Penetration Tester (eJPT) Learning Path + Certification

The Junior Penetration Tester (eJPT) Learning Path is designed to be the first milestone curriculum for someone with little to no experience in cybersecurity - **simulating the skills utilized during a real-world engagement.** Upskill and cross-skill your security teams to ensure base-level understanding across your organization.

What You'll Learn:

01 Assessment Methodologies

02 Host & Network Auditing

03 Host & Network Penetration Testing

04 Web Application Penetration Testing

DIFFICULTY	Novice
DURATION	155h 54m
COURSES	12
VIDEOS	242
QUIZZES	200
LABS	112
skillcheck	15 Labs
CERTIFICATION	eJPT

Who It's For:

- IT professionals who are new to cybersecurity
- InfoSec professionals looking to advance their careers in penetration testing
- Red or Blue Team members wanting to validate their knowledge of penetration testing fundamentals



At a Glance

eJPT Certification Exam

Question Format
35 Total (Lab-Dependent)

Time Limit
48 hours

Red Team for Professionals

Certified Professional Penetration Tester (eCPPT) Learning Path + Certification

The eCPPT Learning Path offers a deeper dive into penetration testing tactics, strategies, and best practices against Windows and Linux targets. By studying real-world scenarios, employees can apply new knowledge directly to their roles.

What You'll Learn:

01 Active Directory Pentesting

02 Exploitation & Post-Exploitation

03 Web Application Pentesting

04 Initial Access

DIFFICULTY	Professional
DURATION	107h 21m
COURSES	10
VIDEOS	174
QUIZZES	124
LABS	77
skillcheck	10 Labs
CERTIFICATION	eCPPT

Who It's For:

- InfoSec professionals with deep understanding of networks, systems, and web applications attacks
- eJPT certification holders looking for their next step in pentesting
- Red or Blue Team members wanting to validate their knowledge of advanced penetration testing concepts



At a Glance

eCPPT Certification Exam

Question Format
63 Total (Lab-Dependent)

Time Limit
24 hours

US: 877.224.8987 | Intl: 984.444.9917 | support@ine.com

Red Team for Professionals

Web Application Penetration Testing Professional (eWPT) Learning Path + Certification

The eWPT Learning Path prepares learners for the challenges of assessing and mitigating web application risks and manual exploitation of common web application vulnerabilities. Practical training methods and hands-on labs decrease the time to proficiency for new pentesting technologies, keeping your organization on the cutting edge.

What You'll Learn:

01 Web Application Security Testing

02 Manual Exploitation of Common Web App Vulnerabilities

03 Web Application Vlunerability Assessment

04 Web Service Security Testing

Who It's For:

- IT Professionals with 1-2 years of cybersecurity experience
- eJPT certification holders looking for their next step in pentesting
- Red or Blue Team members wanting to validate their knowledge of advanced penetration testing concepts

DIFFICULTY	Professional
DURATION	106h 48m
COURSES	10
VIDEOS	175
QUIZZES	126
LABS	58
CERTIFICATION	eWPT



At a Glance

eWPT Certification Exam

Question Format
45 Total (All Lab-Related)

Time Limit
18 hours

Red Team for Professionals

Web Application Penetration Testing eXtreme (eWPTX) Learning Path + Certification

Assess and mitigate advanced web application risks to minimize threat risk. The eWPTX Learning Path trains learners on the advanced skills necessary to carry out a thorough and advanced penetration test against modern web applications. The corresponding certification validates that knowledge, giving IT leaders the confidence their team is prepared to keep the organization secure.

What You'll Learn:

01 API Penetration Testing

02 Injection Vulnerabilities

03 Web Application Reconnaissance

04 Authentication Attacks

Who It's For:

- IT professionals with a highly technical understanding of web application security
- Penetration testers looking to upskill into web application penetration testing
- Web Application Testers, Professionals, and Developers

DIFFICULTY	Advanced
DURATION	76h 41m
COURSES	6
VIDEOS	122
QUIZZES	90
LABS	39
CERTIFICATION	eWPTX



At a Glance

eWPTX Certification Exam

Question Format
45 Total (All Lab-Dependent)

Time Limit
18 hours

Red Team for Professionals

Mobile Application Penetration Testing Professional (eMAPT) Learning Path + Certification

The eMAPT certification demonstrates your professional expertise in conducting thorough security assessments of mobile applications, with hands-on evaluation of vulnerabilities across both major mobile platforms. The certification exam tests your ability to perform comprehensive mobile security assessments, requiring candidates to identify and exploit vulnerabilities in authentic Android and iOS applications.

What You'll Learn:

01 Reconnaissance and Static Analysis

02 Dynamic Testing and Runtime Manipulation

03 API and Backend Security Foundations

04 Mobile Application Security Foundations

Who It's For:

- Individuals with a foundational knowledge in cybersecurity and application development
- Penetration Testers, Mobile App Developers, Security Analysts
- IT professionals who are driven to uncover vulnerabilities within mobile applications and fortify them against potential threats.

DIFFICULTY	Professional
DURATION	47h 59m
COURSES	3
VIDEOS	89
QUIZZES	80
LABS	21
CERTIFICATION	eMAPT



At a Glance

eMAPT Certification Exam

Question Format

45 Total (19 Lab-Independent, 26 Lab-Dependent)

Time Limit

12 hours

Blue Team Training

Security Operation Certified - Level 1 (eSOC) Learning Path + Certification

Advance your security operations career with a credential that validates your ability to triage alerts, analyze logs, and escalate incidents effectively in real-world SOC environments. Designed for Tier 1 readiness, eSOC aligns to modern SOC workflows, tools, and decision-making processes used by enterprise security teams. You'll build the practical skills and confidence needed to contribute meaningfully in a SOC from day one.

What You'll Learn:

01 SOC Fundamentals, AI, & Core Analyst Skills

02 Threat Detection, Logging, and Analysis

03 Incident Response & Invsestigation

04 SOC Tools, Reporting, and Emerging Technologies

Who It's For:

- SOC Analysts (Tier 1)
- Cybersecurity Analysts (Generalists and Early Career)
- IT Support, Help Desk, and System Administrators Transitioning into Security
- Students and Career-Changers Entering Cybersecurity



At a Glance

eSOC Certification Exam

Question Format

50 Total (All Lab-Dependent)

Time Limit

18 hours

Incident Handling and Response Professional (eCIR) Learning Path + Certification

The Incident Handling & Response Professional Learning Path will help you understand the mechanics of modern cyber-attacks and how to detect them. The Incident Handling & Response Professional Learning Path also prepares you for the eCIR exam and certification.

What You'll Learn:

01 Endpoint & Network Analysis

02 Threat Detection & SIEM Operations

03 Digital Forensics & Evidence-Based Analysis

04 Reporting & Communication

Who It's For:

- IT professionals aiming to specialize in cybersecurity incident management
- Security Analysts, Incident Responders, Network Administrators, Security Architects
- Individuals seeking to elevate their cybersecurity expertise to navigate and mitigate complex security incidents

DIFFICULTY	Professional
DURATION	61h 45m
COURSES	6
VIDEOS	116
QUIZZES	102
LABS	16
CERTIFICATION	eCIR



At a Glance

eCIR Certification Exam

Question Format

60 Total (All Lab-Dependent)

Time Limit

10hrs

Blue Team Training

Threat Hunting Professional (eCTHP) Learning Path + Certification

The Threat Hunting Professional Learning Path will help you establish a proactive defense mentality, as well as proactively hunt for threats in an organization's network, endpoints, or perimeter and be several steps ahead of forthcoming adversaries. During the learning process, you will leverage tactical threat intelligence, memory forensics, endpoint/IDS/IPS events, uncommon data sources, and SIEM solutions, among others. The Threat Hunting Professional Learning Path also prepares you for the eCTHP exam and certification.

What You'll Learn:

01 Endpoint Threat Hunting

02 Network Threat Hunting

03 Cyber Threat Intelligence

04 Threat Hunting Strategies

DIFFICULTY	Professional
DURATION	25h 26m
COURSES	6
VIDEOS	71
QUIZZES	54
LABS	10
CERTIFICATION	eCTHP

Who It's For:

- Individuals with a highly technical understanding of networks, systems, and cyber attacks
- Security Operations Center (SOC) Analysts, Cybersecurity Consultants, Security Engineers
- Individuals interested in learning to actively hunt and mitigate potential threats before they escalate



At a Glance

eCTHP Certification Exam

Question Format

60 Total (40 Lab-Independent, 20 Lab-Dependent)

Time Limit

10 hours

Digital Forensics Training

Digital Forensics Professional (eCDFP) Learning Path + Certification

The Digital Forensics Professional Learning Path will teach you how to identify and gather digital evidence, as well as retrieve and analyze data from both the wire and endpoints. The Digital Forensics Professional Learning Path also prepares you for the eCDFP exam and certification.

What You'll Learn:

01 Fundamentals of Digital Forensics

02 Digital Forensics Tools & Techniques

03 Storage Device Fundamentals

04 Preservation of Evidence

Who It's For:

- Individuals who are looking to be part of a high-performing forensics investigation team
- Digital Forensic Analysts, Cybersecurity Investigators, IT Auditors, Law Enforcement Personnel, Digital Forensics Professionals
- Individuals with a solid foundation in cybersecurity principles looking to delve into advanced collecting, preserving, analyzing, and reporting techniques

DIFFICULTY	Advanced
DURATION	23h 52m
COURSES	4
VIDEOS	28
QUIZZES	20
LABS	24
CERTIFICATION	eCDFP



At a Glance

eCDFP Certification Exam

Question Format

30 Total (15 Lab-Independent, 15 Lab-Dependent)

Time Limit

24 hours

Blue Team Training

Enterprise Defense Administrator (eEDA) Learning Path + Certification

Blue Team training with zero-risk hands-on training, focused on the practical skills needed for front-line network defense. This learning path establishes a strong foundation for theories, best practices, standards, and frameworks defensive security professionals need to protect their organizations.

What You'll Learn:

01 Security Administration

02 Identity and Access Management

03 Governance Risk and Compliance

04 Secure Engineering Fundamentals

Who It's For:

- IT professionals beginning in defensive cybersecurity or security engineering
- Learners that completed the eEDA Learning Path and want to demonstrate mastery
- Cybersecurity professionals interested in upskilling for blue team work

DIFFICULTY	Novice
DURATION	52h 15m
COURSES	9
VIDEOS	125
QUIZZES	86
LABS	9
CERTIFICATION	eEDA



At a Glance

eEDA Certification Exam

Question Format

50 Total (35 Lab-Independent, 15 Lab-Dependent)

Time Limit

8 hours

Digital Forensics Training

INE offers learning paths for two of cybersecurity's most sought after certifications, CompTIA Security+ (Sec+) and Certified Information Systems Security Professional (CISSP).

INE's CompTIA Security+* Learning Path is one of the only online training options that provides extensive hands-on labs to help prepare learners for the certification exam. The curriculum breaks down topics according to the published Domains and Objectives from CompTIA.

What You'll Learn:

01 General cybersecurity topics, terms, and fundamental concepts
02 How to architect a typical security infrastructure
03 Risk management and compliance topics

AT A GLANCE
Learning Path:

Difficulty: Novice
Duration: 52h 53m
Videos: 109
Quizzes: 79
Labs: 30
Courses: 6

INE's CISSP** Learning Path prepares learners to pass the most globally recognized certification in the information security market by reviewing security concepts and industry best practices included in the CISSP Common Body of Knowledge.

What You'll Learn:

01 Security & risk management
02 Asset security
03 Security Architecture and Engineering
04 Other concepts and best practices in the CISSP Common Body of Knowledge

AT A GLANCE
Learning Path:

Difficulty: Professional
Duration: 59h 53m
Courses: 8
Videos: 210
Quizzes: 178

*CompTIA Security+ certification vouchers must be purchased from CompTIA

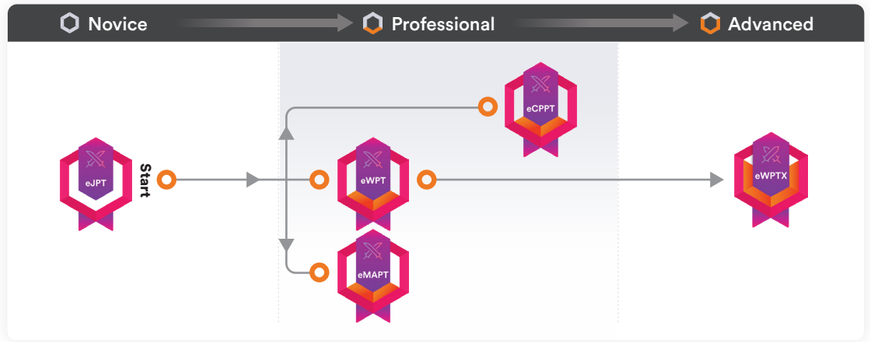
**CISSP certification vouchers must be purchased from ISC2

Certification Pathways

Our cybersecurity certification pathways are designed to support both individual practitioners and security teams. With clearly defined Red Team and Blue Team tracks, organizations can develop targeted offensive and defensive capabilities while ensuring consistent, role-aligned skill progression.

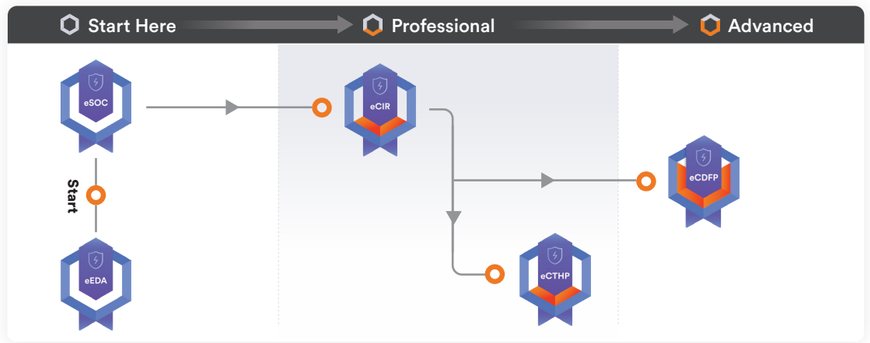
Red Team Certification Pathway

Our Red Team certification pathway is designed to take practitioners from foundational offensive security skills to advanced, real-world attack simulation expertise. Each certification builds progressively, emphasizing hands-on performance and practical application.



Blue Team Certification Pathway

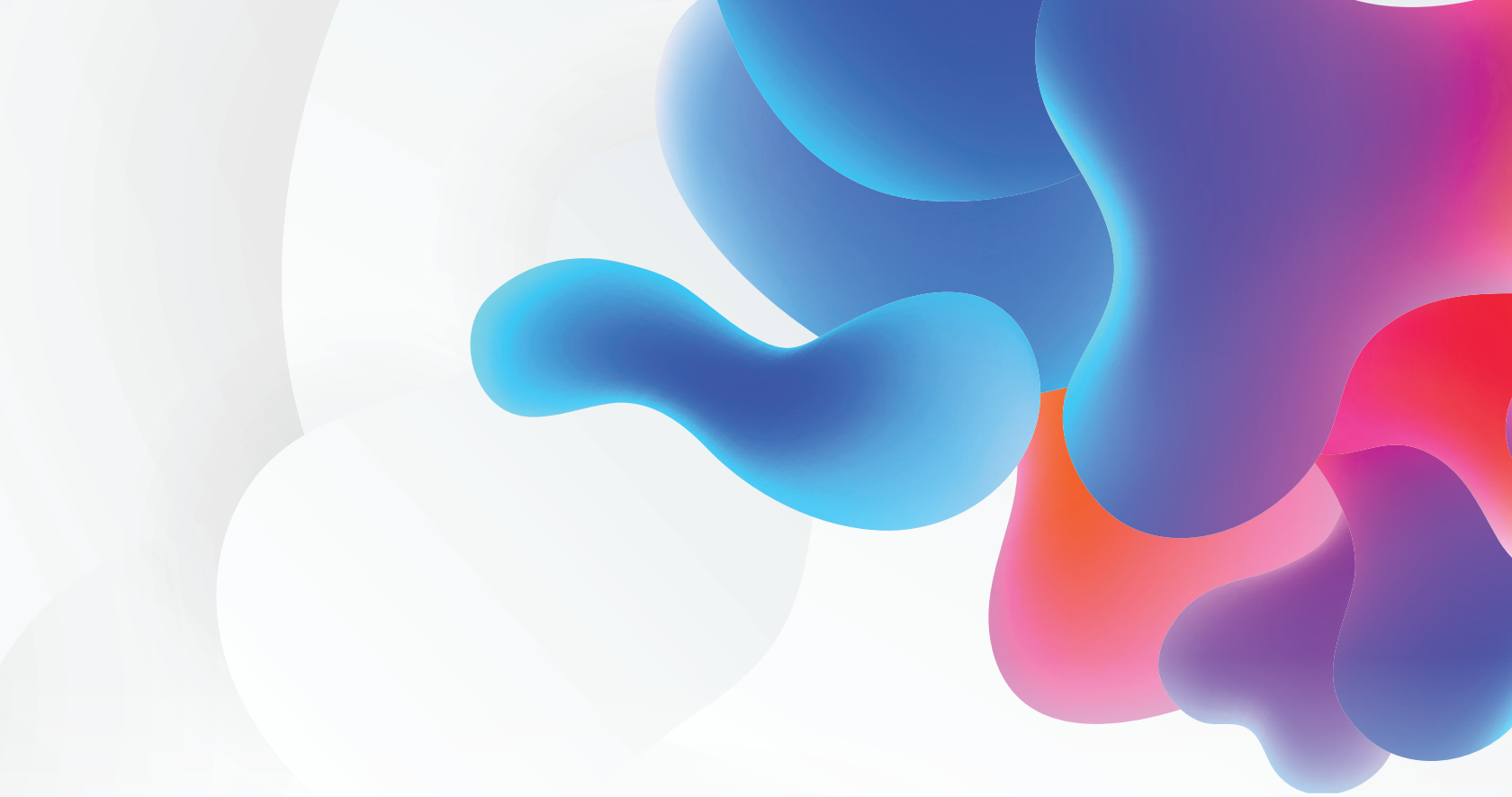
Our Blue Team certification pathway equips defenders with the skills needed to detect, investigate, and respond to modern cyber threats. The pathway emphasizes operational readiness, analytical thinking, and real-world defensive workflows.



Designed for Real-World Impact

Both pathways are built around hands-on, performance-based assessments that reflect real job roles and security challenges. Whether learners are focused on offensive security, defensive operations, or building a well-rounded security team, these certification pathways provide a clear, structured roadmap for skill development and career progression.

US: 877.224.8987 | Intl: 984.444.9917 | support@ine.com



About INE Security

INE Security is a leading provider of online cybersecurity education, offering a comprehensive suite of hands-on courses and certification programs designed to meet the needs of professionals at all levels. INE Security is the top training choice for Fortune 500 companies worldwide for cybersecurity training in business and for IS/IT professionals looking to advance their careers. With a global community of learners, INE Security equips individuals and organizations with the skills necessary to defend against and combat modern cyber threats, offering a wide range of security certifications to build and elevate cybersecurity careers.

US: 877.224.8987 | Intl: 984.444.9917 | support@ine.com