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.**

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:

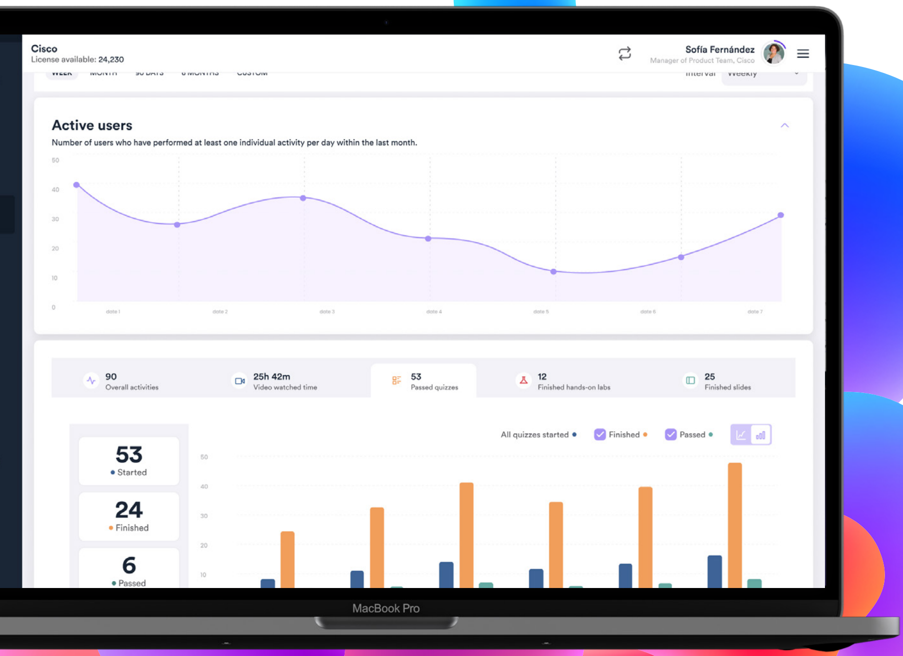
By providing practitioners with more than 3,400 labs (through training and specialized labs) - we know that the learner is equipped to respond to real-workplace scenarios.

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.



Cisco
License available: 24,230

Sofía Fernández
Manager of Product Team, Cisco

Active users

Number of users who have performed at least one individual activity per day within the last month.

90 Overall activities
25h 42m Video watched time
53 Passed quizzes
12 Finished hands-on labs
25 Finished slides

53 Started
24 Finished
6 Passed

Business Solutions

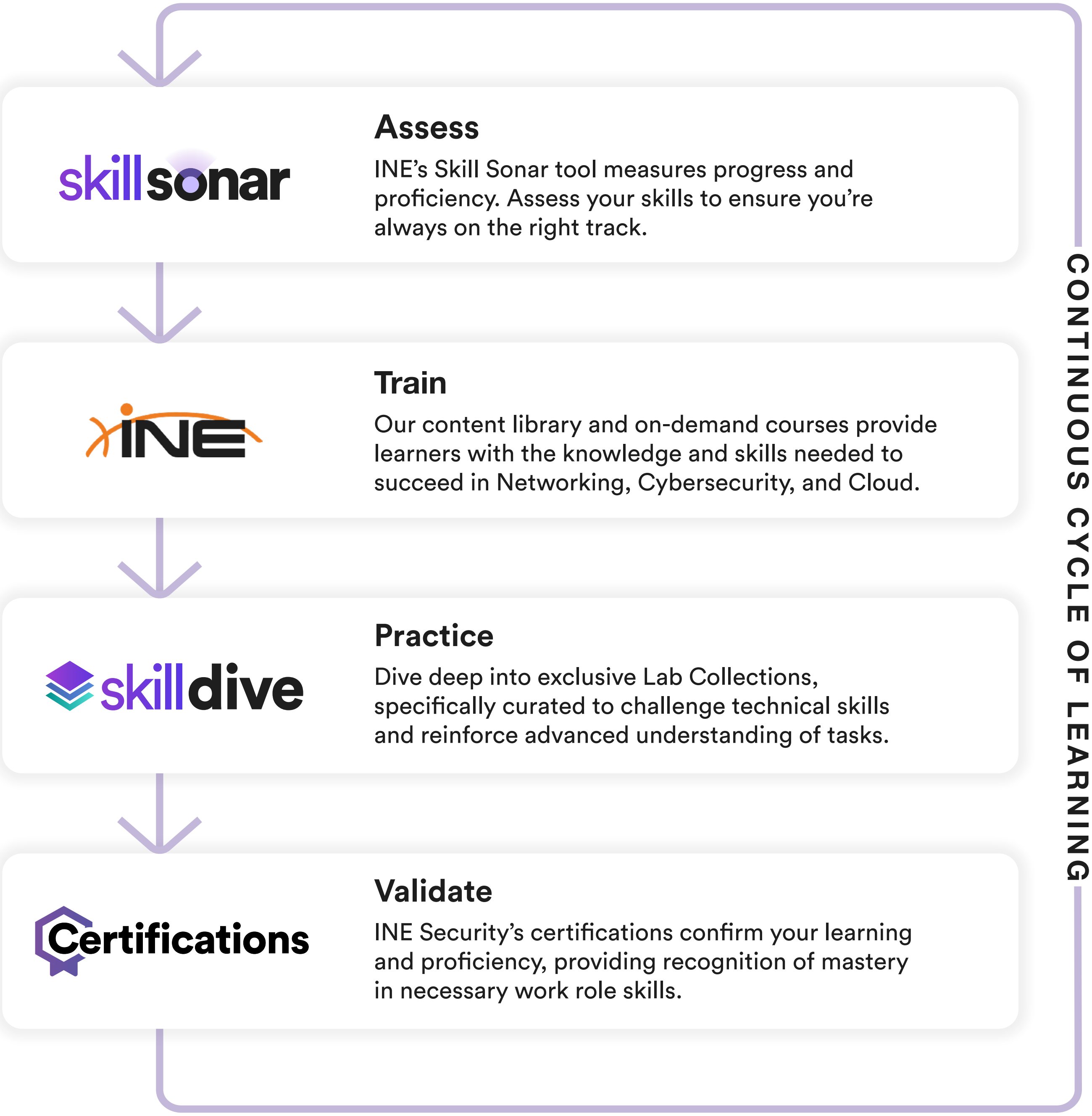
Trusted by organizations globally, INE provides solutions to ensure that you're not only training individuals but upskilling teams across the enterprise. Enhance workforce competence and productivity by closing KSA (knowledge, skills, and abilities) gaps.

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.



skillsonar

Assess

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

INE

Train

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

skilldive

Practice

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

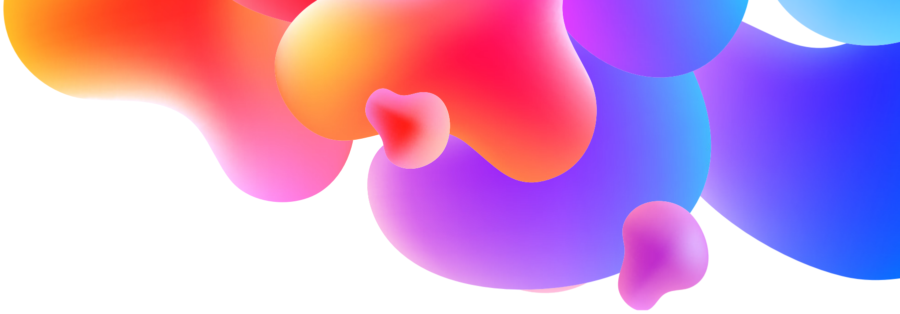
Certifications

Validate

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

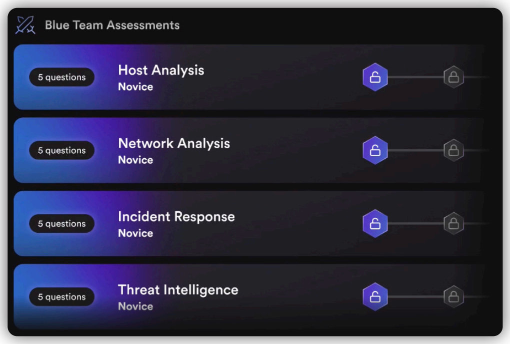
skillsonar

You have to know to grow.



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

How Does It Work?



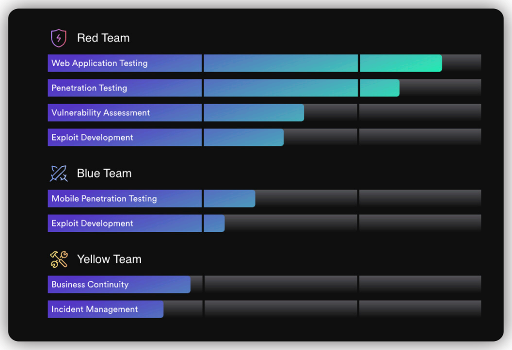
Blue Team Assessments

- 5 questions — Host Analysis — Novice
- 5 questions — Network Analysis — Novice
- 5 questions — Incident Response — Novice
- 5 questions — Threat Intelligence — Novice

01 Assess

Measure current proficiency levels.

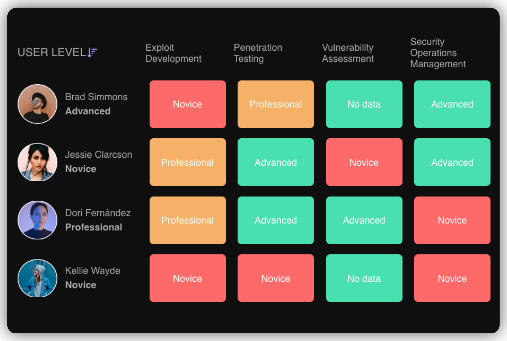
Ask your team to take assessments. Skill Sonar offers assessments in cybersecurity and networking, with cloud assessments coming soon.



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.



USER LEVEL	Exploit Development	Penetration Testing	Vulnerability Assessment	Security Operations Management
Brad Simmons **Advanced**	Novice	Professional	No data	Advanced
Jessie Clarcson **Novice**	Professional	Advanced	Novice	Advanced
Dori Fernández **Professional**	Professional	Advanced	Advanced	Novice
Kellie Wayde **Novice**	Novice	Novice	No data	Novice

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.

Usable Benchmarks for Your Training Roadmap

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

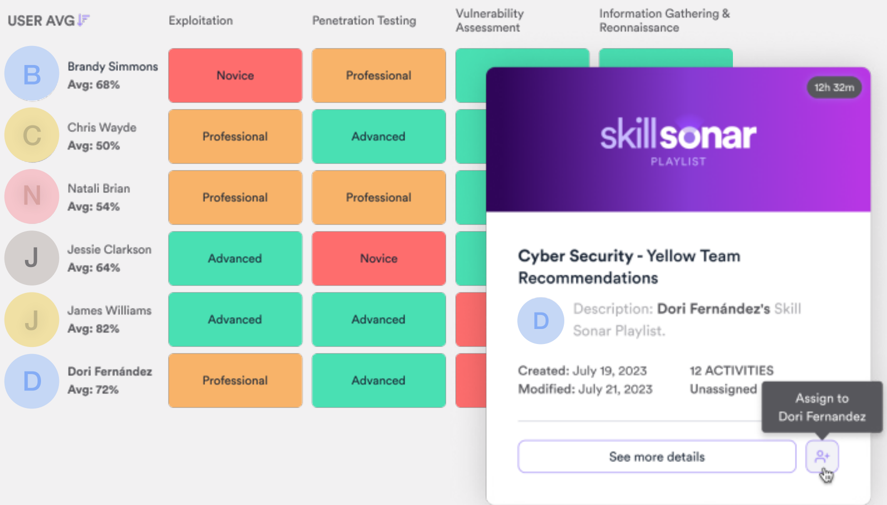
Playlists evolve with the user’s growth, encouraging users to reassess as they progress through training.

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.



USER AVG	Exploitation	Penetration Testing	Vulnerability Assessment	Information Gathering & Reconnaissance
B Brandy Simmons Avg: 68%	Novice	Professional		
C Chris Wayde Avg: 50%	Professional	Advanced		
N Natali Brian Avg: 54%	Professional	Professional		
J Jessie Clarkson Avg: 64%	Advanced	Novice		
J James Williams Avg: 82%	Advanced	Advanced		
D Dori Fernández Avg: 72%	Professional	Advanced		

Cyber Security - Yellow Team Recommendations

D Description: Dori Fernández's Skill Sonar Playlist.

Created: July 19, 2023
Modified: July 21, 2023

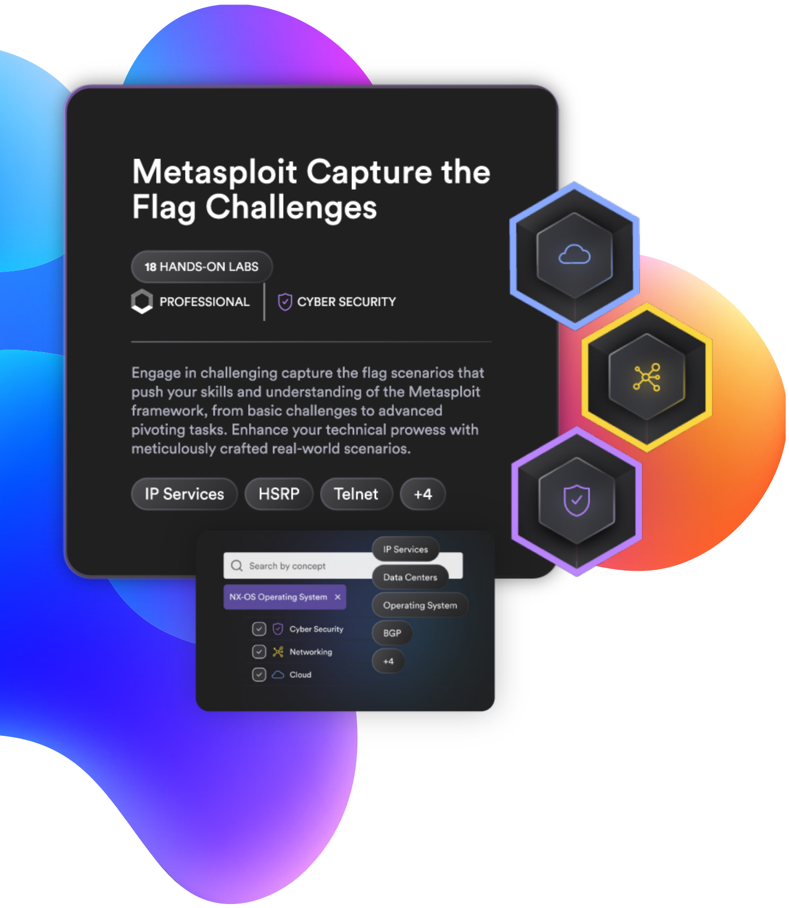
12 ACTIVITIES
Unassigned

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.

skilldive

Go Beyond Theoretical Training



Metasploit Capture the Flag Challenges

Engage in challenging capture the flag scenarios that push your skills and understanding of the Metasploit framework, from basic challenges to advanced pivoting tasks. Enhance your technical prowess with meticulously crafted real-world scenarios.

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

- CTF Arena Challenges
- Deploying Cisco Collaboration Solutions
- Car Hacking
- Mastering IPv6 Routes & Protocols
- And many more!

Labs

- Kubernetes Exposed API
- Exploiting Targets with Metasploit
- DNS Wildcard Entries
- AD MSSQL Impersonation & Role Abuse
- And many more!

Common Vulnerabilities & Exposures (CVEs)

- FastAPI ReDoS (CVE-2024-24762)
- Jenkins Arbitrary File Read (CVE-2024-23897)
- Bludit PE (CVE-2023-31572)
- Flatpress Path Traversal (CVE-2023-0947)
- Froxlor CSRF (CVE-2023-1033)
- And many more!

Capture The Flag (CTF) Arena by INE

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:

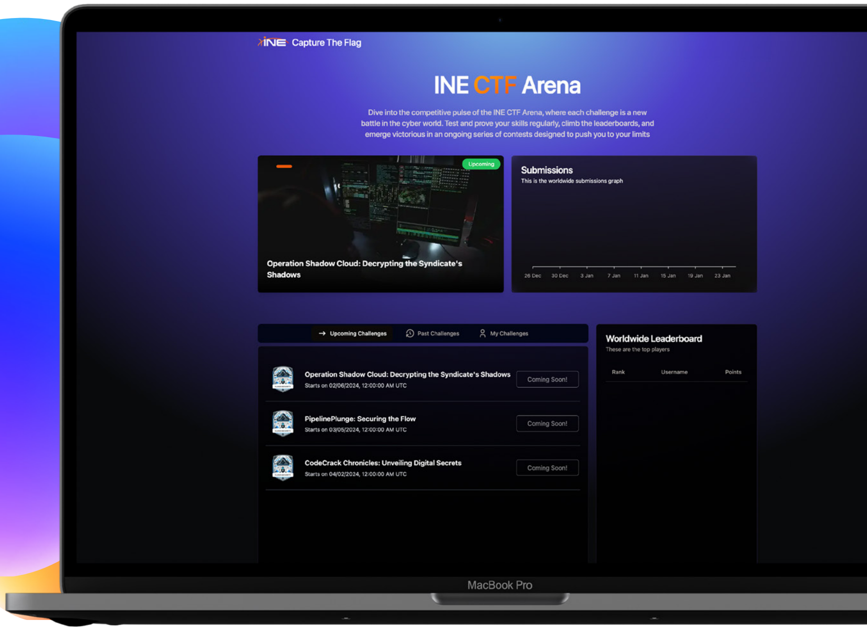
- Operation Shadow Cloud: Decrypting the Syndicate’s Shadows
- PipelinePlunge: Securing the Deployment
- CodeCrack Chronicles: Unveiling Digital Secrets

**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.

info.ine.com/schedule-a-meeting



INE Capture The Flag

INE CTF Arena

Dive into the competitive pulse of the INE CTF Arena, where each challenge is a new battle in the cyber world. Test and prove your skills regularly, climb the leaderboards, and emerge victorious in an ongoing series of contests designed to push you to your limits

Upcoming

Operation Shadow Cloud: Decrypting the Syndicate's Shadows

Submissions

This is the worldwide submissions graph

Operation Shadow Cloud: Decrypting the Syndicate's Shadows
Starts on 02/06/2024, 12:00:00 AM UTC
Coming Soon!

PipelinePlunge: Securing the Flow
Starts on 03/05/2024, 12:00:00 AM UTC
Coming Soon!

CodeCrack Chronicles: Unveiling Digital Secrets
Starts on 04/02/2024, 12:00:00 AM UTC
Coming Soon!

Worldwide Leaderboard

These are the top players

Rank	Username	Points

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)	51h
Penetration Testing Student (eJPT)	156h
CompTIA Security+	36h

Professional

Incident Handling & Response Professional (eCIR)	8h
Mobile Application Penetration Testing Professional (eMAPT)	11h
Penetration Testing Professional (eCPPT)	84h
Threat Hunting Professional (eCTHP)	22h
Web Application Penetration Testing Student (eWPT)	106h
CISSP: Certified Information Systems Security Professional	13h
Malware Analysis Professional	17h
Reverse Engineering Professional	12h
Web Defense Professional	41h

Advanced

Advanced Web Application Penetration Testing (eWPTX)	18h
Digital Forensics Professional (eCDFP)	30h
Advanced Penetration Testing	10h
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.

eCPPT

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

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.

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.

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.

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
info.ine.com/schedule-a-meeting

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

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

DIFFICULTY	Novice
DURATION	153h 38m
COURSES	12
VIDEOS	240
QUIZZES	200
LABS	108
CERTIFICATION	eJPT

At a Glance

eJPT Certification Exam

Question Format

Multiple Choice & Hands-On Labs, Open Book

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 Vulnerability Assessment of Networks & Web Applications

02 Advance Reporting and Remediation

03 Information Gathering and Reconnaissance

04 Exploit Development

DIFFICULTY	Professional
DURATION	107h 3m
COURSES	10
VIDEOS	174
QUIZZES	124
LABS	67
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

Lab-based multiple choice questions, Dynamic exam, open book

Time Limit

24 hours

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 Foundational to Advanced Post-Exploitation Activities

02 OWASP's Top 10

03 Common Web Application Vulnerabilities

04 Master Burp Suite

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 52m
COURSES	10
VIDEOS	175
QUIZZES	126
LABS	58
CERTIFICATION	eWPT

At a Glance

eWPT Certification Exam

Question Format

Lab-based multiple choice questions, Dynamic exam, Open book

Time Limit

10 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 In-depth Web Application Vulnerabilities analysis

02 Advanced PHP, Java, Deserialization, LDAP, Server Side, Authentication/SSO attacks

03 XSS, SQL Injection, HTML5

04 Master API & Cloud-powered Application penetration testing

DIFFICULTY	Advanced
DURATION	76h 29m
COURSES	6
VIDEOS	122
QUIZZES	90
LABS	39
CERTIFICATION	eWPTX

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

At a Glance

eWPTX Certification Exam

Question Format

Lab-based multiple choice questions, Dynamic exam, open book

Time Limit

18 hours

Red Team for Professionals

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

The Mobile Application Security and Penetration Testing Learning Path gives penetration testers and IT security professionals the practical skills to understand the technical threats and attack vectors targeting mobile devices. This learning path covers the process of identifying security issues on Android and iOS applications, using a wide variety of techniques including Reverse Engineering, Static/Dynamic/Runtime, and Network Analysis, as well as prepares you for the eMAPT exam and certification.

What You'll Learn:

01 Identify security issues on Android and iOS applications

02 How to use techniques such as Reverse Engineering, Static/Dynamic/Runtime, and Network Analysis

03 Encryption and cryptography

04 Identify vulnerable implementations

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	11h 7m
COURSES	2
VIDEOS	17
QUIZZES	0
LABS	0
CERTIFICATION	eMAPT

At a Glance

eMAPT Certification Exam

Question Format

Report-based exam

Time Limit

7 days to submit after starting exam

Blue Team Training

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 How to effectively use and fine-tune open source IDS, log management, and SEIM solutions

02 Analyze traffic, flows, and endpoints

03 How to utilize analytics and tactical threat intel

DIFFICULTY	Professional
DURATION	8h 22m
COURSES	3
VIDEOS	1
QUIZZES	0
LABS	7
CERTIFICATION	eCIR

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

At a Glance

eCIR Certification Exam

Question Format

Report-based exam

Time Limit

4 days to submit report after starting exam

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 Use threat intelligence or hypotheses to hunt for known and unknown threats

02 Inspect network traffic and identify abnormal activity

03 Perform memory forensics using Redline, Volatility, and other tools to identify in-memory malware

04 Use alternative data sources such as Sysmon and EilkET to collect event logs

05 Detect advanced hacking techniques such as AMSI bypasses, COM Hijacking, and sophisticated/evasive malware

06 Use PowerShell, ELK, and Splunk to analyze Windows events and detect attacks such as DCSync, Kerberoasting, and obfuscated PowerShell commands

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

DIFFICULTY	Professional
DURATION	21h 28m
COURSES	3
VIDEOS	24
QUIZZES	4
LABS	26
CERTIFICATION	eCTHP

At a Glance

eCTHP Certification Exam

Question Format

Report-based exam

Time Limit

2 days in lab environment, then 4 days from starting the exam to submit report

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 How to acquire volatile and non-volatile data, using various techniques

02 How files are structured and how to analyze file headers, malicious documents, and file metadata

03 Become familiar with walking through partitions, recovering corrupted disks, and locating hidden data

04 How to analyze both FAT & NTFS file system

05 File carving and creating your own custom carving signatures

06 Analyze the Windows registry, LNK files, prefetch files, and previously mounted USB devices

07 Perform thorough investigations, against Skype, explorer's shellbags, and Windows recycle bin

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

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

At a Glance

eCDFP Certification Exam

Question Format

30 Multiple Choice Independent and Lab-Based Questions

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 Basic Defensive Engineering Strategies

02 Network Device and Server Hardening

03 Vulnerability Management

04 Log Gathering and Analysis

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	50h 41m
COURSES	9
VIDEOS	123
QUIZZES	86
LABS	6
CERTIFICATION	eEDA

At a Glance

eEDA Certification Exam

Question Format

Multiple Choice and Hands-On Labs, Open Book

Time Limit

8 hours

The Certification Prep You Need

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.

CompTIA Security+

AT A GLANCE
Learning Path:

Difficulty: Novice
Duration: 53h 10m
Videos: 109
Quizzes: 79
Labs: 30
Courses: 6

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

CISSP®

AT A GLANCE
Learning Path:

Difficulty: Professional
Duration: 46h 56m
Courses: 8
Videos: 150
Quizzes: 138

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

*CompTIA Security+ certification vouchers must be purchased from CompTIA

**CISSP certification vouchers must be purchased from ISC2

INE SECURITY

CYBERSECURITY TRAINING & CERTIFICATIONS

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