NETRIDERS
الأمن السيبراني يتحدث العربية

eCTHP v3

Introduction

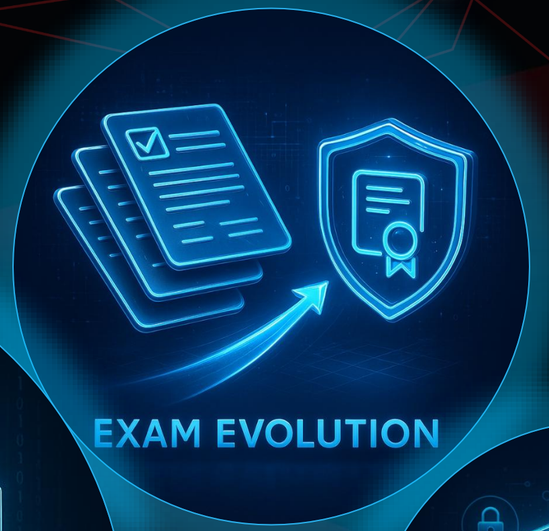
By: **Mohamed Amr**

NETRIDERS
الأمن السيبراني يتحدث العربية

eCTHPv2 vs. eCTHPv3 (2025)

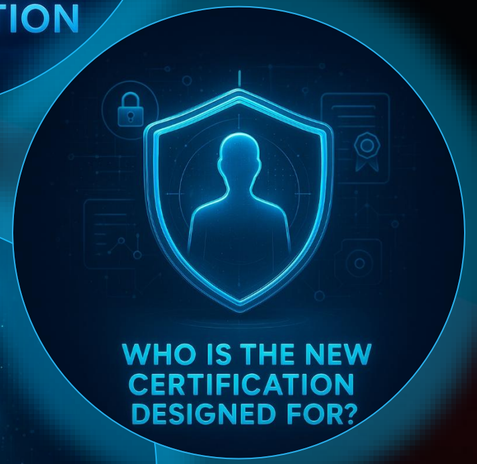
Evolution of Threat Hunting Skills


2025


EXAM EVOLUTION


FRAMEWORKS
& METHODOLOGY


eCTHP


WHO IS THE NEW
CERTIFICATION
DESIGNED FOR?


eCTHP
Hands-On Labs &
Tools Evolution


v2
(Older)
2025 Updates
(Modern)
eCTHP
Version Overview


THE EVOLUTION
CONTINUES

eCTHP Certification Evolution

v1 (2019)

Foundational threat hunting certification introducing basic concepts and methodologies

v2 (2021)

Enhanced Labs with MITRE ATT&CK framework integration

v3 (2025)

Revolutionary update with advanced tooling, real-world scenarios, and streamlined methodology

Version Comparison Overview

v2 Features		v3 2025
26 hands-on labs MITRE ATT&CK framework focus		10 advanced labs till now Enhanced ATT&CK integration
3 Chapters Traditional exam format Incident response workflows		5 Chapters MCQ exam format Real-world hunt simulations
Standard tools		Modern SIEM & Network tools

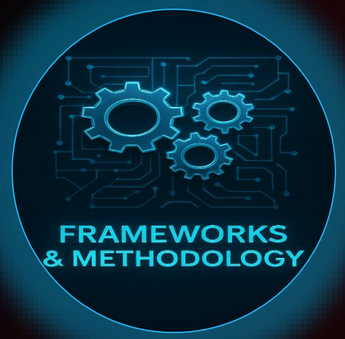
Hands-on Labs & Tools Evolution

v2 Labs

- 26 Labs covering fundamentals
- Basic ELK/Splunk usage
- Basic incident response scenarios
- Threat intelligence & Log analysis

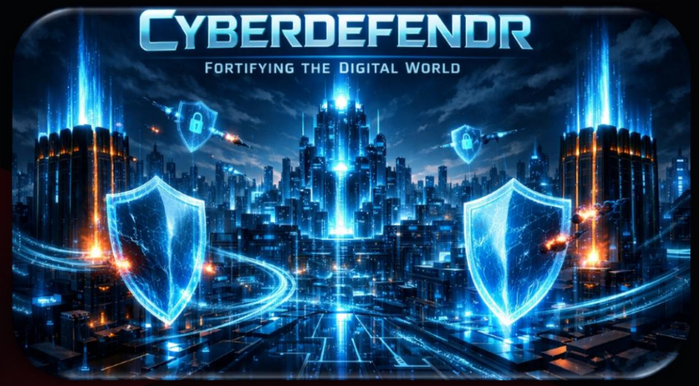
v3 Labs

- 10 labs with advanced SIEM (Splunk, Elasticsearch), Wireshark
- real-world scenarios & Multi-stage attack simulations
- Cyber Defender & TryHackMe Labs. (Instructor Bonus)



INE Labs (Live Sessions)

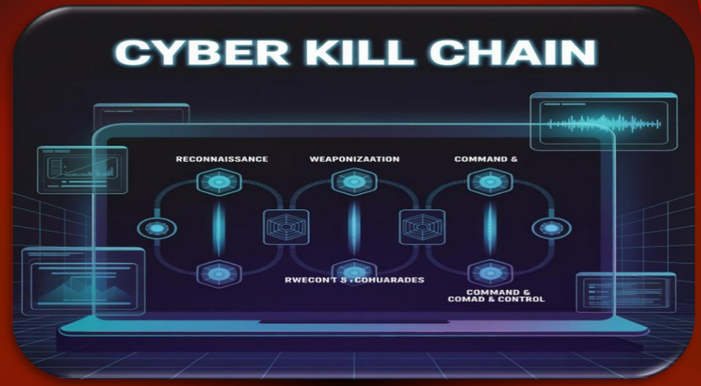
- Labs will Coverage in the Course via **CyberDefender** & **TryHackMe**
- INE's Core Labs Available in a **Separate Course** with **Separate Subscription**
- Live Sessions for Interactive Delivery of INE Labs
- Continuous Updates for New INE Labs
- Recorded Courses Not available Due to Constant Lab Updates



Frameworks & Methodology

v2 Framework

- Basic MITRE ATT&CK mapping
- Linear kill chain approach
- Limited technique coverage



v3 Framework

- Enhanced ATT&CK integration
- Dynamic kill chain variants
- Complete technique matrix

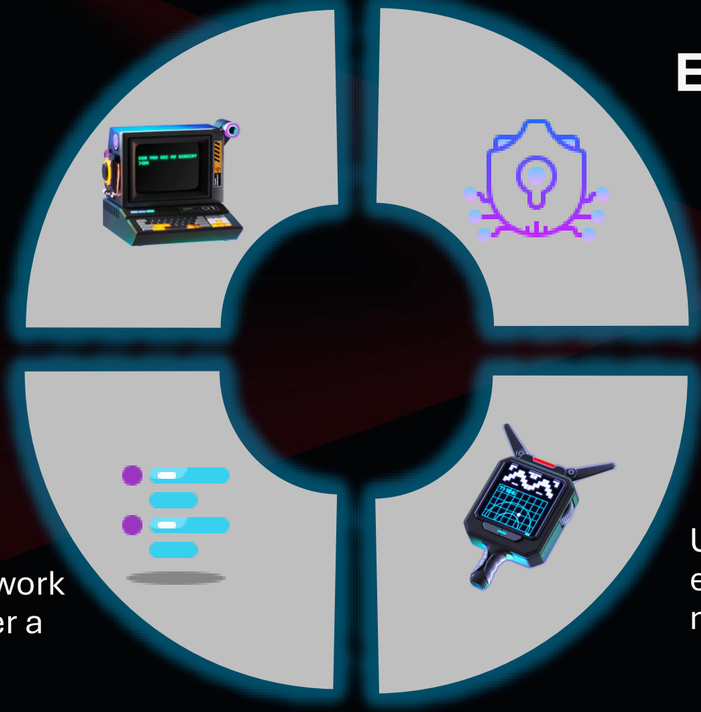
Key Improvements in v3 Updates

Modern Tool Coverage

Full integration with contemporary SIEM, and network security platforms used in enterprise SOCs.

Investigation & Analysis

Capable of investigating endpoints and analyzing network traffic with Wireshark to cover a new techniques.



Enhanced Lab Depth

labs provide realistic multi-layer attack scenarios with persistent threats and lateral movement.

Current Threat Intelligence

Updated with latest adversary TTPs, emerging threats, and recent attack methodologies from 2024-2025.

Exam Evolution

Exam Formats & Style

v2 (The "Classic")

The exam tested two skills: finding the threats and *extensively documenting* it in a formal, multi-page report. This was time-consuming and manual. It tested documentation as much as hunting.

v3 (The "Modern")

The new format is a pure, hands-on simulation. Your actions, findings, and ability to propose defense strategies *within the lab environment* are what matter. It tests pure practical skill.

Exam Evolution

Exam Duration & Structure

v2

(Phase 1)

48 Hours for the practical threat hunt in the lab.

(Phase 2)

A separate 48 Hours dedicated *only* to writing the formal report.

Exam Evolution

Exam Duration & Structure

v3

Key Takeaway

The new format removes the separate, lengthy reporting phase entirely.

Updated Exam

10 Hours, A single, streamlined, time-limited engagement. All tasks are in one session.

Exam Evolution

Grading & Results: From Weeks to Hours

<24hrs

Updated Exam Time

v2: Relied on **manual grading** of a large report, often leading to wait times of several **weeks**.

v3: Uses an **auto-graded system**. This provides fast, consistent results, **immediately** after completing the exam.

Exam Evolution

The Final Deliverable

v2: The Formal Report

A comprehensive PDF detailing every step, finding, and remediation. Graded on clarity, thoroughness, and professionalism.

v3: The Defense Strategy

Answering questions and proposing defense strategies *within the exam platform*. Graded on accuracy and practical application.

Exam Evolution

Voucher / retirement

v2 (The "Classic")

Old vouchers valid until Jan 2026 for the old exam

v3 (The "Modern")

New exam uses new vouchers; switch options available for old ones

Exam Evolution

Certification Validity

Both of V2 & V3 expire after 3 years, requiring recertification to ensure skills remain current.

Exam Evolution

(At-a-Glance Comparison)

Feature	v2 (Older)	v3 (Current)
Main Deliverable	Formal PDF Report	In-platform Answers Q&A
Grading	Manual (Slow)	Auto-Graded (Fast)
Result Time	Weeks (or 1 Month+)	Immediately after Submission
Duration	48h Lab + 48h Report	10h, Single, Streamlined Lab
Validity	3-Year Expiry	3-Year Expiry

Who is the New Certification Designed For?

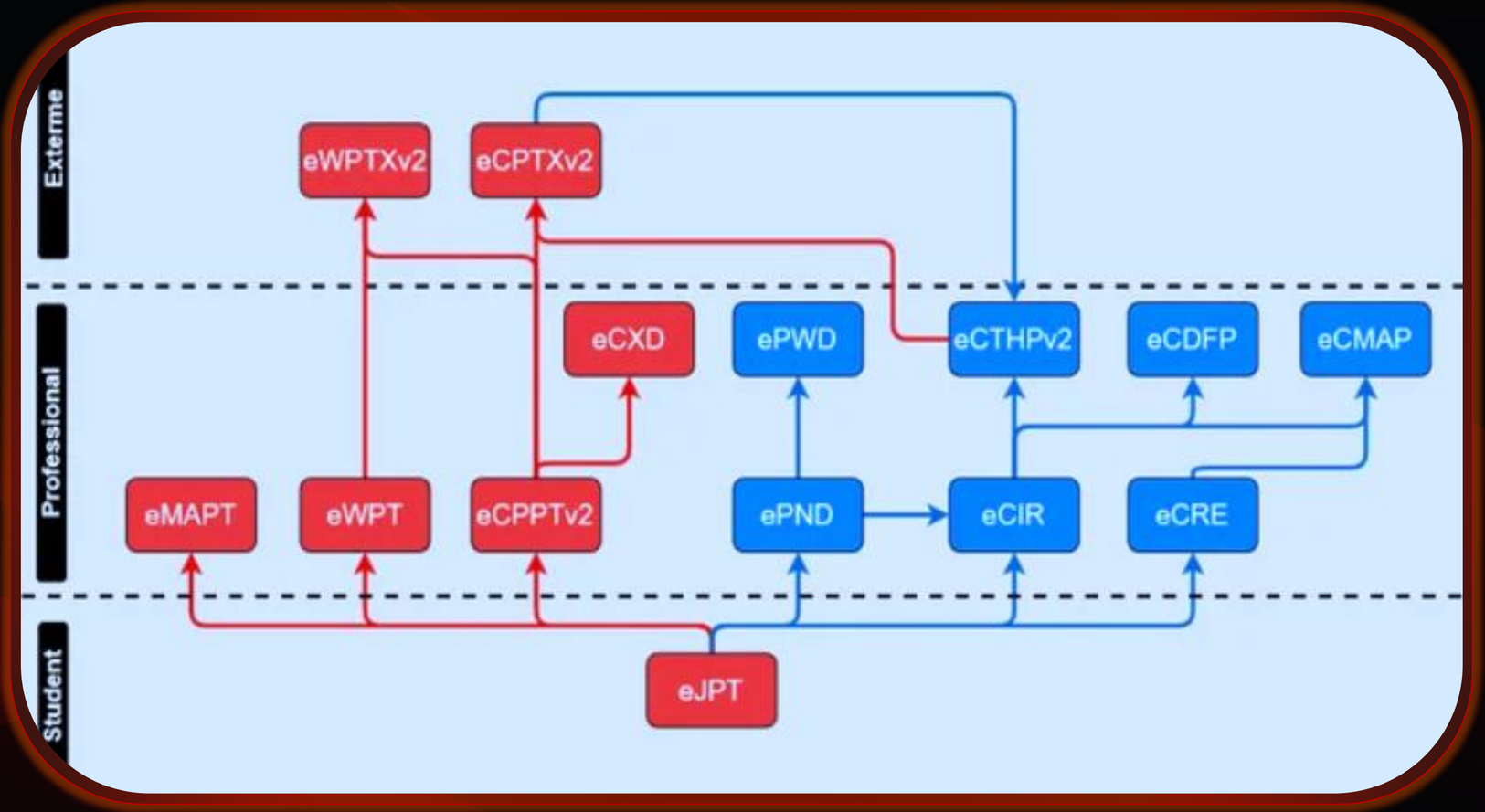
- ❑ The current eCTHP is designed for professionals who already have some experience in defensive security, including:
  - ➢ Security Analysts/SOC Analysts
  - ➢ Cybersecurity Administrators
  - ➢ Cybersecurity Engineers
  - ➢ Cybersecurity Incident Responders
  - ➢ Detection Engineers
- ❑ For who wants cutting-edge skills, real-world experience, and industry-leading certification
- ❑ Career Focus:
  - ➢ Advanced threat hunting roles, senior SOC positions, specialized threat intelligence


WHO IS THE NEW
CERTIFICATION
DESIGNED FOR?


iNE


THE EVOLUTION
CONTINUES

INE Roadmap


Exterme
Professional
Student
eWPTXv2
eCPTXv2
eCXD
ePWD
eCTHPv2
eCDFP
eCMAP
eMAPT
eWPT
eCPPTv2
ePND
eCIR
eCRE
eJPT

The Evolution Continues → *Hunt Smarter, Not Harder*

Both v2 and v3 certification represent commitment to threat hunting excellence.

Get Certified

INE's eCTHP certification validates your threat hunting proficiency with industry recognized credentials.

Build Skills

Hands-on labs and real-world scenarios develop practical capabilities in active threat detection.

Advance Career

Threat hunting expertise opens opportunities in SOC operations, incident response, and security leadership.

Questions?

Feal free to ask 🤍