ITHUM
it's for human

EC-Council

Approved by

ict academy

Clusit
Associazione Italiana per la Sicurezza Informatica

EUROPEAN CYBER SECURITY MONTH

giovedì 24 ottobre - Ore 17:00

CYBER SECURITY & CERTIFICAZIONI DI MERCATO: LE NOVITÀ DI EC-COUNCIL

DAI NUOVI CORSI ESSENTIALS ALLA CEH CON L'ARTIFICIAL INTELLIGENCE

Relatori:

- **Vincent BARTEZAK** - Responsabile EC-Council Italia
- **Salvatore CRISTOFARO** - Cybersecurity Advisor & CEH Instructor
- **Marco CIAMPI** - Founder & CEO at ITHUM

Agenda

Agenda:

- 17.00 Presentazione
- 17.10 Speech
- 17.45 Feedback / Prossime iniziative
- 17.50 Dibattito - Q&A
- 18:15 (circa) Saluti

Relatori:

Vincent BARTEZAK – (LinkedIn)
Salvatore CRISTOFARO– (LinkedIn)

Presenta e Modera:

Marco CIAMPI – (LinkedIn)

Evento Linkedin: Link

Know your Speaker

Vincent BARTEZAK

Responsabile EC-Council Italia

EC-Council

vbartezak@it-gnosis.eu

LinkedIn: vincent-bartezak/

EC-Council

Oltre **20 anni** di esperienza nella formazione e certificazione in sicurezza informatica
150 paesi si fidano delle nostre certificazioni riconosciute a livello mondiale
380000 professionisti certificati in tutto il mondo

L'ambizione di EC-Council - Essere in grado di aiutare qualsiasi persona interessata dalla cyber security

ANSI 17024

American National Standards Institute

DoD

Department of Defense Directive 8140

NICE

National Initiative for Cybersecurity Education

GCT

GCHQ Certified Training

UK intelligence, cyber and security agency

NSA

National Security Agency USA

E TANTI ALTRI…

Essentials Series

Cyber Security & certificazioni di mercato EC-Council (ITHUM)

24 ottobre 2024

3 Corsi Esistenti + 5 NUOVI Corsi

N|DE Network Defense Essentials

E|HE Ethical Hacking Essentials

D|FE Digital Forensics Essentials

Network Defense Essentials

Ethical Hacking Essentials

Digital Forensics Essentials

IoT Security Essentials

I|SE IoT Security Essentials

Threat Intelligence Essentials

T|IE Threat Intelligence Essentials

Cloud Security Essentials

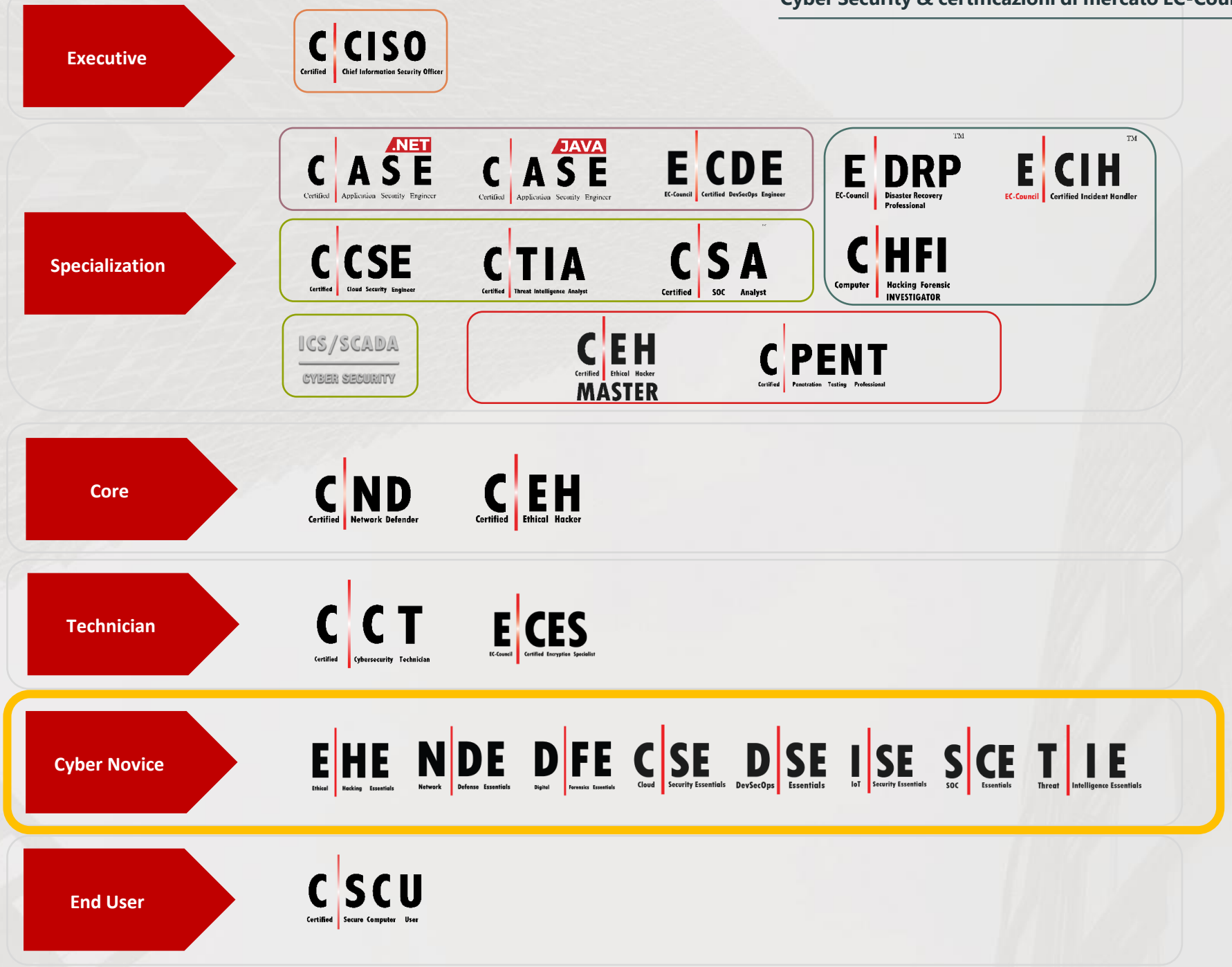
C|SE Cloud Security Essentials

DevSecOps Essentials

D|SE DevSecOps Essentials

Security Operations Essentials

S|CE SOC Essentials


Executive
C|CISO
Certified | Chief Information Security Officer
Specialization
C|ASE .NET
Certified | Application Security Engineer
C|ASE JAVA
Certified | Application Security Engineer
E|CDE
EC-Council | Certified DevSecOps Engineer
E|DRP
EC-Council | Disaster Recovery Professional
E|CIH
EC-Council | Certified Incident Handler
C|HFI
Computer | Hacking Forensic INVESTIGATOR
C|CSE
Certified | Cloud Security Engineer
C|TIA
Certified | Threat Intelligence Analyst
C|SA
Certified | SOC Analyst
ICS/SCADA CYBER SECURITY
C|EH MASTER
Certified | Ethical Hacker
C|PENT
Certified | Penetration Testing Professional
Core
C|ND
Certified | Network Defender
C|EH
Certified | Ethical Hacker
Technician
C|CT
Certified | Cybersecurity Technician
E|CES
EC-Council | Certified Encryption Specialist
Cyber Novice
E|HE
Ethical | Hacking Essentials
N|DE
Network | Defense Essentials
D|FE
Digital | Forensics Essentials
C|SE
Cloud | Security Essentials
D|SE
DevSecOps | Essentials
I|SE
IoT | Security Essentials
S|CE
SOC | Essentials
T|IE
Threat | Intelligence Essentials
End User
C|SCU
Certified | Secure Computer User

I Corsi Essentials

Una serie di corsi di base sulla cybersecurity creata dalle certificazioni EC-Council di livello superiore.

Pubblico target

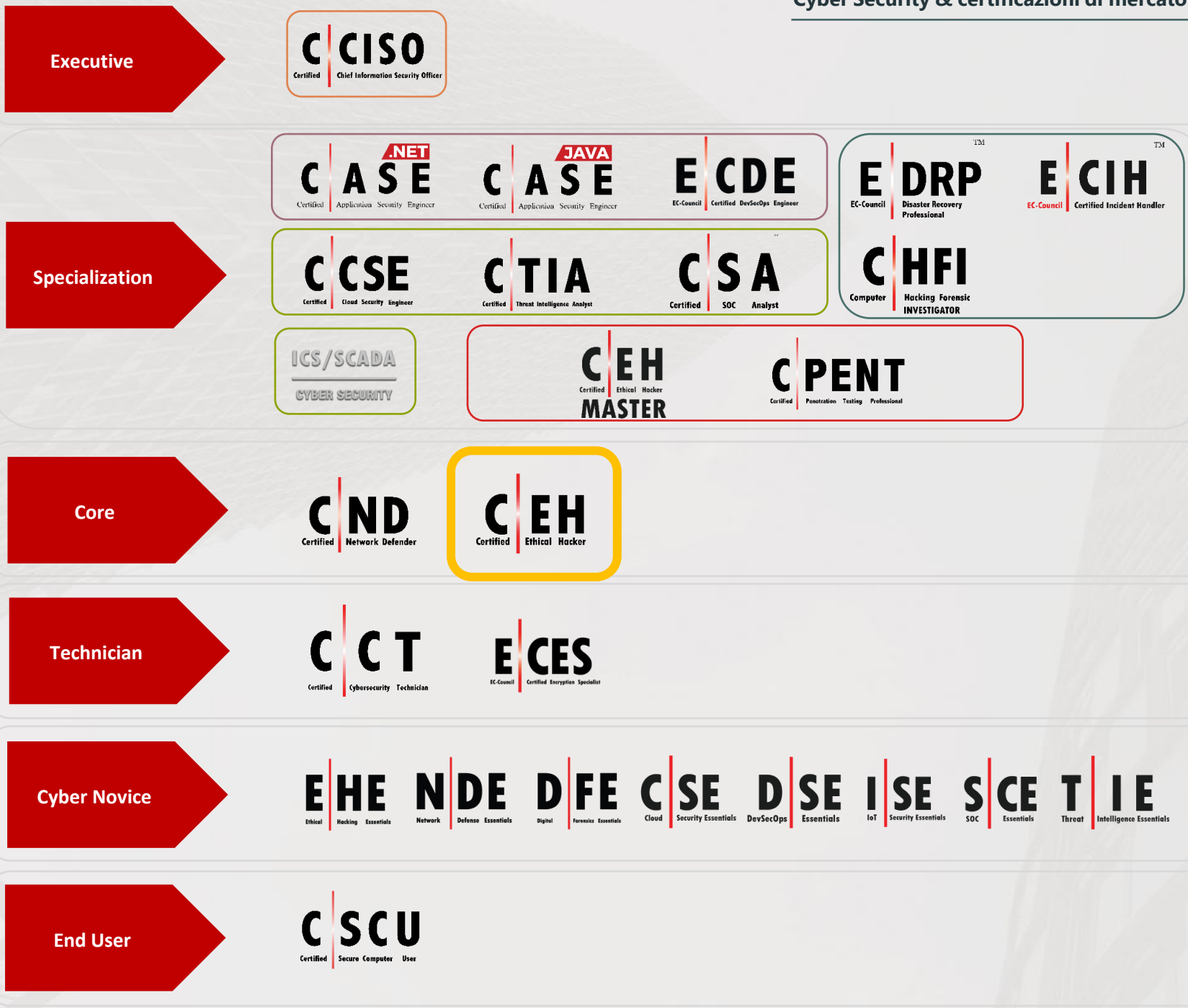
- Studenti
- Professionisti
- Profili Junior
- Appassionati di tecnologia

Risorse a disposizione

- eBook
- Lezioni Video
- Laboratori
- Voucher di esame

BASE	AVANZATO
Network Defense Essentials	C|ND Certified Network Defender
Ethical Hacking Essentials	C|EH Certified Ethical Hacker
Digital Forensics Essentials	C|HFI Computer Hacking Forensic INVESTIGATOR
IoT Security Essentials	Multiple Courses
Threat Intelligence Essentials	C|TIA Certified Threat Intelligence Analyst
Cloud Security Essentials	C|CSE Certified Cloud Security Engineer
DevSecOps Essentials	E|CDE EC-Council Certified DevSecOps Engineer
Security Operations Essentials	C|SA Certified SOC Analyst


EC-Council
Building A Culture Of Security
CERTIFIED
ETHICAL
HACKER v13
C|EH
Certified Ethical Hacker


Executive
C|CISO
Certified Chief Information Security Officer
Specialization
C|ASE .NET
Certified Application Security Engineer
C|ASE JAVA
Certified Application Security Engineer
E|CDE
EC-Council Certified DevSecOps Engineer
E|DRP
EC-Council Disaster Recovery Professional
E|CIH
EC-Council Certified Incident Handler
C|CSE
Certified Cloud Security Engineer
C|TIA
Certified Threat Intelligence Analyst
C|SA
Certified SOC Analyst
C|HFI
Computer Hacking Forensic INVESTIGATOR
ICS/SCADA
CYBER SECURITY
C|EH MASTER
Certified Ethical Hacker
C|PENT
Certified Penetration Testing Professional
Core
C|ND
Certified Network Defender
C|EH
Certified Ethical Hacker
Technician
C|CT
Certified Cybersecurity Technician
E|CES
EC-Council Certified Encryption Specialist
Cyber Novice
E|HE
Ethical Hacking Essentials
N|DE
Network Defense Essentials
D|FE
Digital Forensics Essentials
C|SE
Cloud Security Essentials
D|SE
DevSecOps Essentials
I|SE
IoT Security Essentials
S|CE
SOC Essentials
T|IE
Threat Intelligence Essentials
End User
C|SCU
Certified Secure Computer User

[Certified Ethical Hacker]^{AI}

Master Ethical Hacking with Our Exclusive 4-Phase AI-Powered Learning

Learn

- 20 modules
- 2,500+ pages of the student manual
- 2,000 pages of lab manual
- Over 221 hands-on labs to practice attack vectors and hacking tools
- AI-integrated skills in the 5 phases of the ethical hacking framework
- Hacking AI system, based on the Top 10 OWASP vulnerabilities
- Over 4,000 hacking and security tools

Certify

Two exams that lead to a globally recognized certification!

Knowledge exam (ANAB ISO/IEC 17024)

- 4 hours
- 125 multiple choice questions

Or

Practical exam (ANAB ISO/IEC 17024)

- 6-hour practical exam
- 20 scenario-based questions

Engage

- 4,000 hacking tools
- 550 attack techniques
- Conducting a real-world ethical hacking assignment
- Applying the skills in 5 phases of ethical hacking

Compete

- New challenges every month
- 4-hour CTF competition
- Competing with your peers worldwide
- Hack your way to the top of the leaderboard
- Focus on new attack vectors
- Exploit emerging vulnerabilities

[Certified Ethical Hacker] AI

Know your Speaker

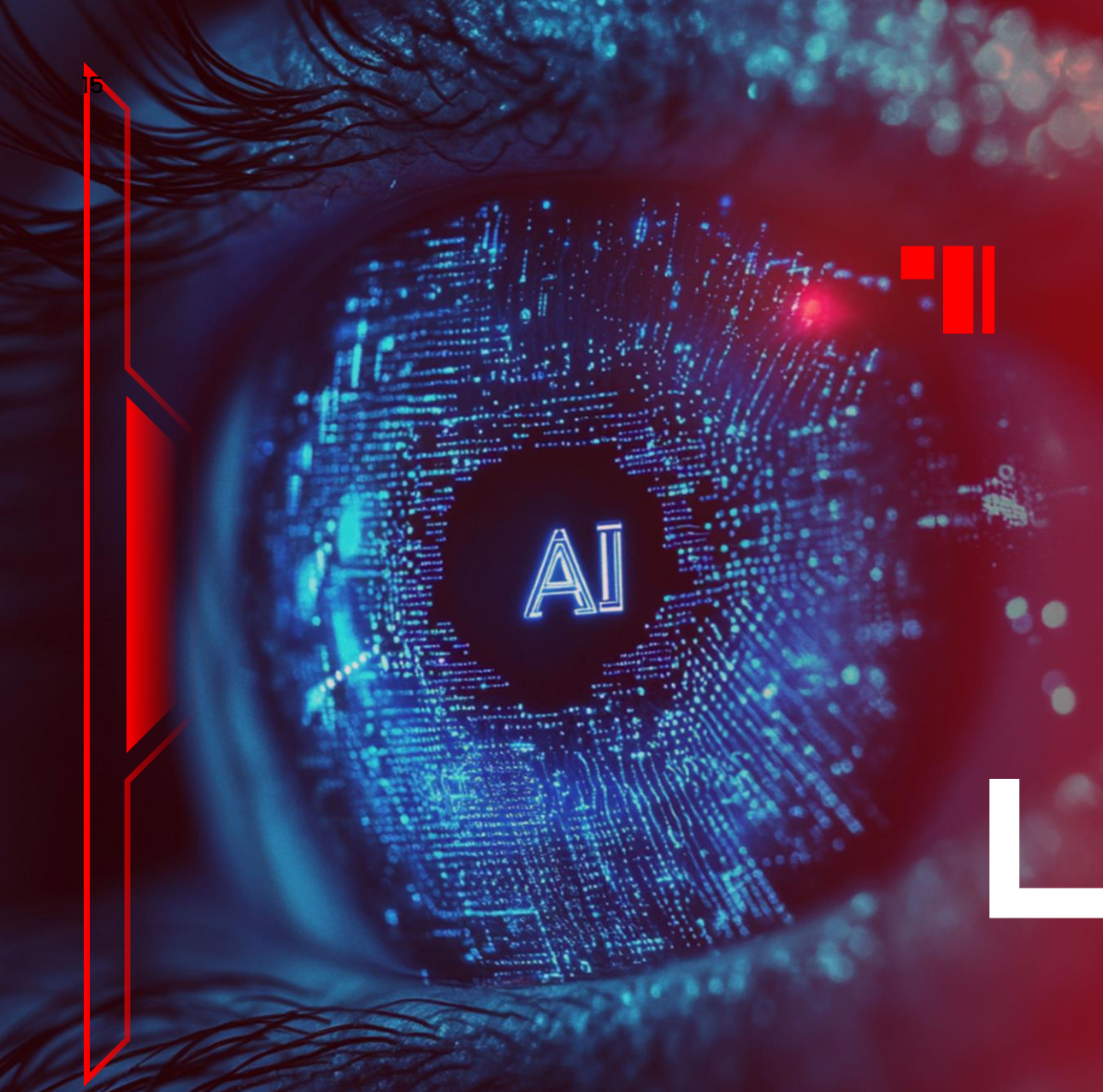
Salvatore CRISTOFARO

Cybersecurity Advisor & Instructor
CEI (Certified EC-Council Instructor) **- CEH, CHFI, ECIH, CSA, CND**
Trainer:

- Master Cybersecurity LUISS – Privacy & IT Security
- Data Protection Officer, Manager, Specialist (UNI 11697 – GDPR)
- Information Security
- Secure Code Review & Software Development Life Cycle, OWASP
- Penetration Test & Vulnerability Assessment
- LPI - Linux Professional Istitute
- Risk Management & Analysis (ISO 31000, ISO/IEC 27005)
- Cisco Academy Instructor

s.cristofaro@ithum.it

LinkedIn: salvatorecristofaro



AI in Cybersecurity

The Outcome: Gain More with (C|EH v13)AI

Ai - Driven Cybersecurity Skills

1. **40%** more efficiency in cyber defense
2. **90%** accuracy in detecting various cybersecurity threats
3. **2X** double employee productivity gains

4. Master How To Use AI Skills
5. Learn To Hack AI Systems
6. Learn Multiple AI And GPT Tools
7. Automate Of Repetitive Tasks
8. Advanced Threat Detection
9. Enhanced Decision-Making
10. Adaptive Learning
11. Enhanced Reporting

Myth: AI will Replace Ethical Hackers

CEH V12 FRAMEWORK

- Reconnaissance
- Vulnerability Scanning
- Gaining Access
- Maintaining Access
- Clearing Tracks

Footprinting and Reconnaissance

↓

Scanning and Enumeration

↓

Vulnerability Analysis

↓

Ethical Hacking Domains

- System Hacking
- Web App Hacking
- Network Hacking
- Mobile Hacking
- Wireless Hacking
- OT/IoT Hacking
- Cloud Hacking

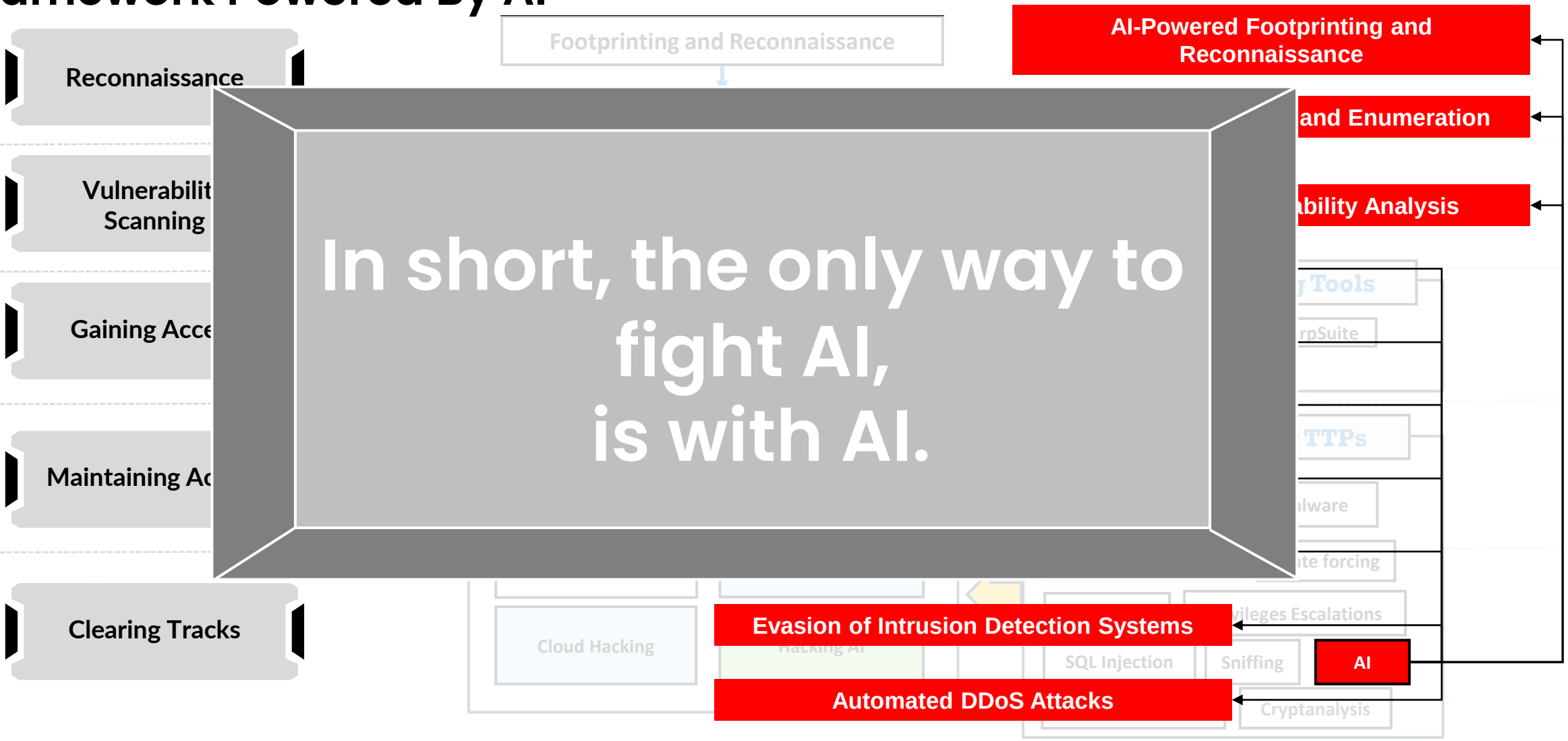
Ethical Hacking Tools

- Nmap
- Wireshark
- Burp Suite
- Metasploit
- SET

Ethical Hacking TTPs

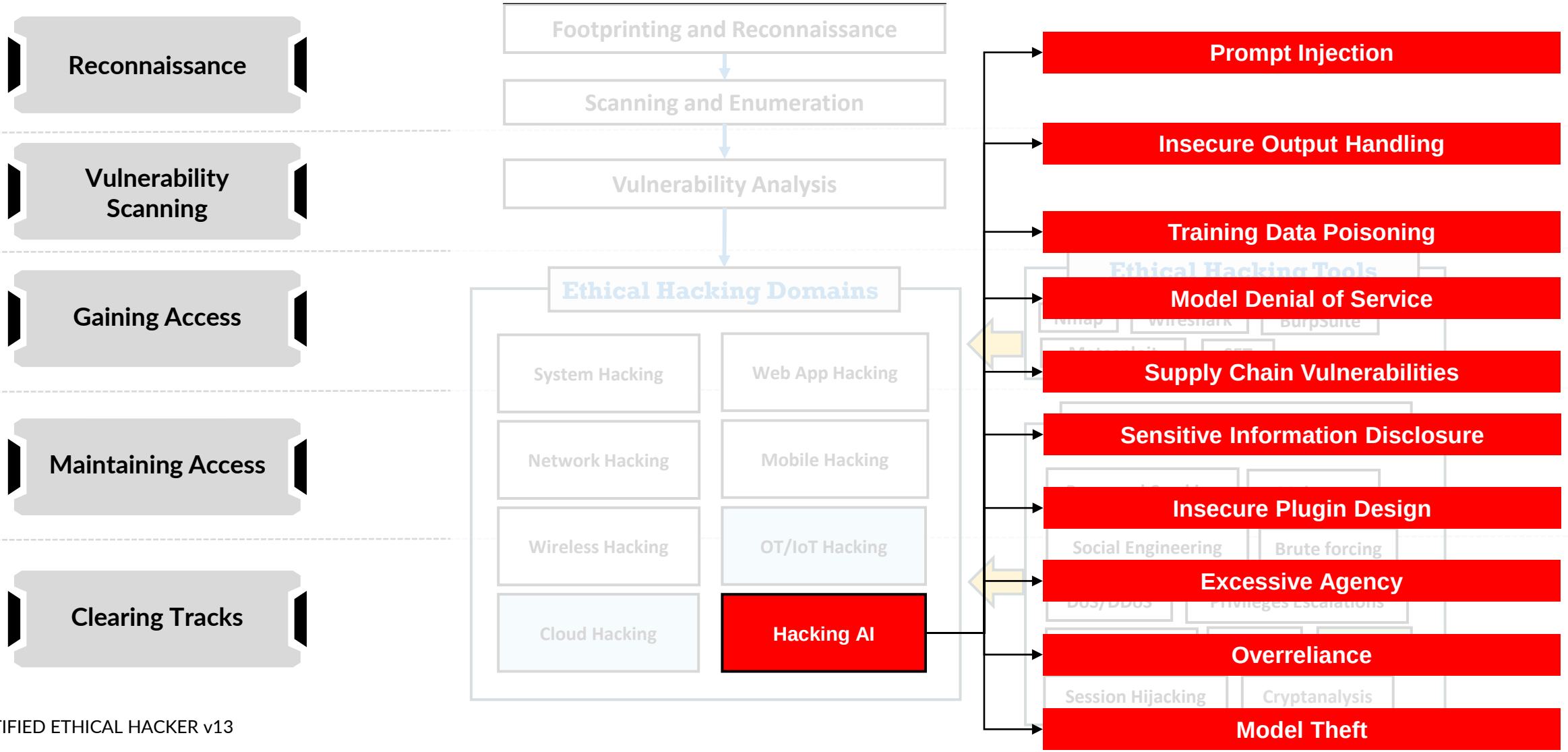
- Password Cracking
- Malware
- Social Engineering
- Brute Forcing
- DoS/DDoS
- Privileges Escalations
- SQL Injection
- Sniffing
- Session Hijacking
- Cryptanalysis

Using AI: Master 5 Phases of the Ethical Hacking Framework Powered By AI



Hacking AI Systems: Based On OWSAP Top 10 Attacks

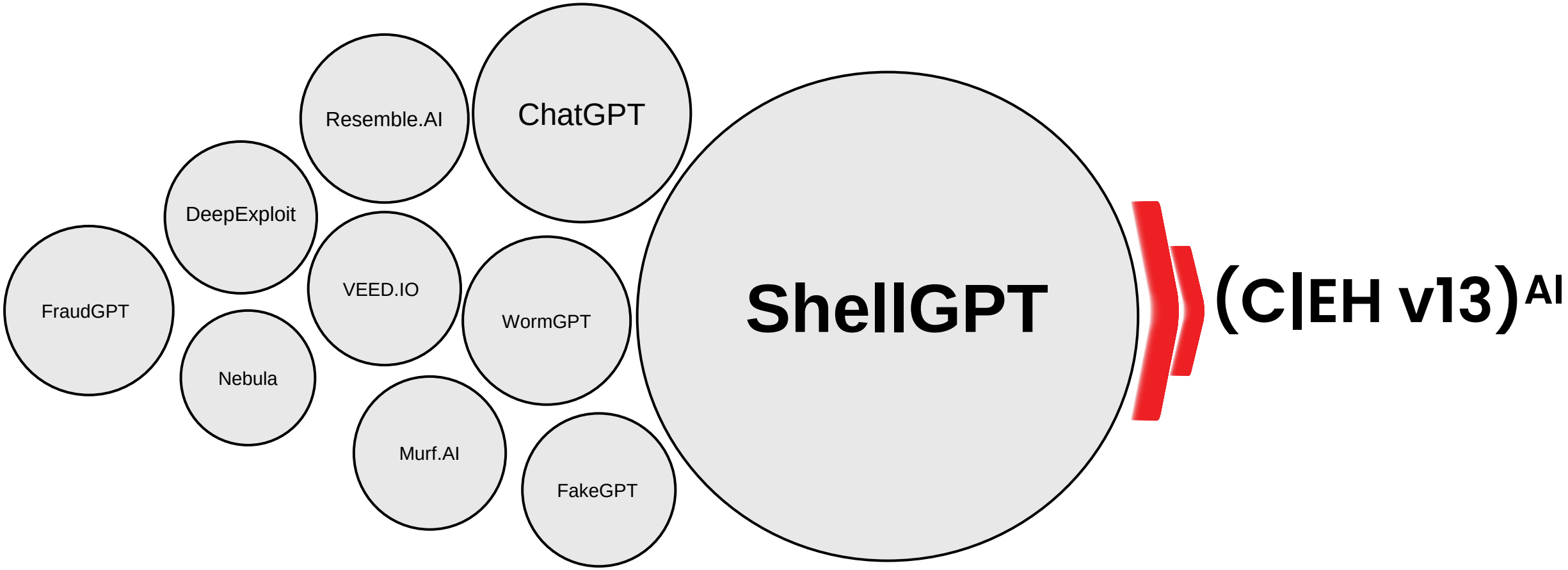
Supplementary / Bonus Module (Not a Part of Core Module: Self Study)



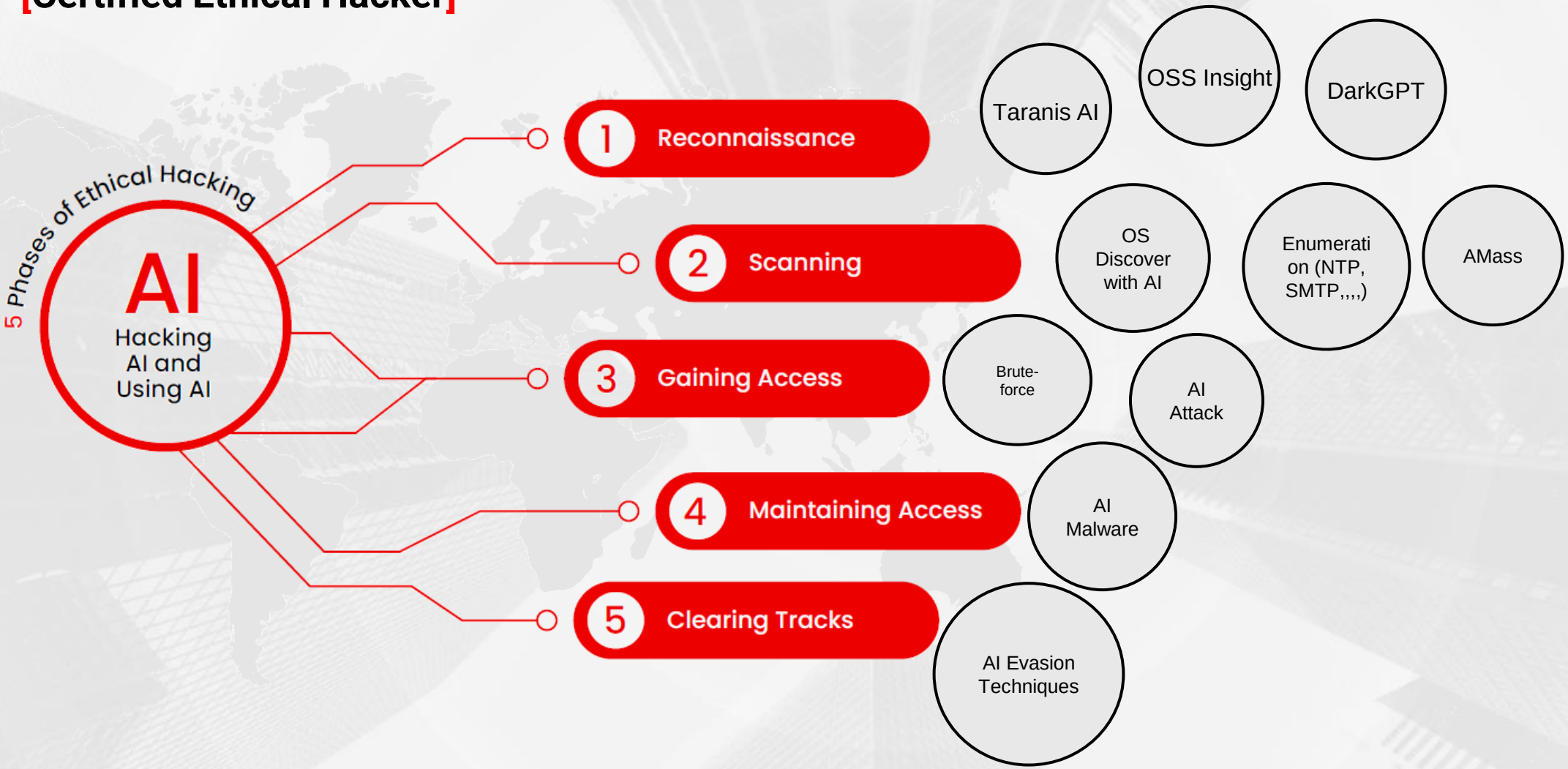
Hacking AI Systems: Based On OWSAP Top 10 Attacks

Prompt Injection	Direct Prompt injections (Jailbreaking) Indirect Prompt Injections (external source controlled by an attacker)
Insecure Output Handling	Insufficient validation, sanitization, and handling of the outputs generated by large language models before they are passed downstream to other components and systems
Training Data Poisoning	The deliberate introduction of misleading or harmful information into a language model's training data, leading to biased or inaccurate outputs
Model Denial of Service	Malicious actor overwhelms a language model with excessive requests, preventing it from serving legitimate users
Supply Chain Vulnerabilities	Security weaknesses in the development, distribution, or maintenance of software, which can be exploited by attackers to compromise systems
Sensitive Information Disclosure	Accidental or intentional release of private or confidential data from a language model, potentially leading to privacy breaches or security risks
Insecure Plugin Design	Creation of plugins for language models that are vulnerable to exploitation, potentially allowing attackers to compromise the model
Excessive Agency	Language model exhibits behavior that goes beyond its intended role or purpose, potentially leading to harmful or unintended consequences
Overreliance	Overreliance refers to the excessive dependence on a language model's outputs without considering their potential limitations or inaccuracies
Model Theft	Unauthorized acquisition or use of a language model's intellectual property, such as its training data or algorithms

AI Tools: Beyond ChatGPT



[Certified Ethical Hacker] AI



ShellGPT working scenarios

ShellGPT, unlike ChatGPT, does not just create commands like writing the NMAP command but performs the scans in a given network.

- **Setup:**
  - You have ShellGPT configured in your cybersecurity toolkit.
  - You have various network scanning tools like Nmap, Masscan, and Angry IP Scanner.

g tool.

s Nmap.

).10.1.0/24 for active hosts.

ting an active host.

devices.

  - ShellGPT creates a detailed report summarizing the scan results, including the number of active hosts and any potential issues.
  - **Example:** The report lists active IP addresses and their corresponding MAC addresses.
- **Ongoing Scanning:**
  - ShellGPT can be scheduled to perform regular network scans and alert you of any changes or new devices.
  - **Example:** It can run scans daily and send you a weekly summary report.

Scenario: Automate
Scanning for Active

Background: Imagine y
administrator responsib
maintaining the security
company's internal netw
to regularly scan the ne
active hosts and ensure
unauthorized devices a

Problem: Manually sele
running network scanni
take time, mainly if you
perform scans. For ease
to automate this proces
and ensure consistent monitoring.

Solution: ShellGPT Automating Network Scanning

Tremendous value to businesses today in focusing their cyber teams on what matters!

Modules

Module 01: Introduction to Ethical Hacking
Module 02: Footprinting and Reconnaissance
Module 03: Scanning Networks
Module 04: Enumeration
Module 05: Vulnerability Analysis
Module 06: System Hacking
Module 07: Malware Threats
Module 08: Sniffing
Module 09: Social Engineering
Module 10: Denial-of-Service

Module 11: Session Hijacking
Module 12: Evading IDS, Firewalls, and Honeypots
Module 13: Hacking Web Servers
Module 14: Hacking Web Applications
Module 15: SQL Injection
Module 16: Hacking Wireless Networks
Module 17: Hacking Mobile Platforms
Module 18: IoT Hacking
Module 19: Cloud Computing
Module 20: Cryptography

C|EH v13 **Technology Updates**

Active Directory Attacks	Zero Trust Architecture	Ransomware Attacks and Mitigation
Deepfake Threats	IoT Security Challenges	Critical Infrastructure Vulnerabilities
Cloud Security	Extended Detection and Response (XDR)	Quantum Computing Risks and Threats
Post-Quantum Cryptography	AI and Machine Learning in Cybersecurity	

Active Directory Attacks

95 million accounts attacked daily
Microsoft says that 95 million of the 500 million AD accounts are attacked every day, but most of these attacks go unnoticed until they disrupt an organization's workflow.

Via Stolen credentials
According to semperis.com, most attackers gain access to AD through stolen credentials, which can be compromised in many ways.

Zero Trust Architecture

Zero Trust Segmentation (ZTS) in 2023:
61% of organizations found ZTS critical for their cloud security strategy, while nearly 60% considered it important for business continuity (Statista, 2023).

ZTS Adoption Forecast:
By 2025, 60% of organizations will embrace Zero Trust as a starting point for security (Gartner, 2022).

Network Analytics Adoption in the US:
43% of US organizations practice network analytics as part of a zero-trust framework (Statista, 2023).

Ransomware Attacks and Mitigation

Increased Ransomware Payments:
The average ransom payment has increased 500% in the last year. Organizations that paid the ransom reported an average payment of $2 million, up from $400,000 in 2023 (Sophos, 2024).

Ransomware Targets:
Healthcare is the most affected critical infrastructure sector, with 249 reported cases in 2023. Other frequently targeted sectors include critical manufacturing, government facilities, and other essential services (FBI, 2024).

Global Impact:
Ransomware is projected to cost victims approximately $265 billion (USD) annually by 2031, with a new attack occurring every 2 seconds as cybercriminals continuously enhance their malware tactics (Cybersecurity Ventures, 2021).

Deepfake Threats

Deepfake Identity Theft Surge:
There was a tenfold (10x) rise in the global detection of deepfakes from 2022 to 2023 (Sumsub Identity Fraud Report 2023).

Exponential Growth of Deepfakes:
In 2023, deep fake phishing and fraud incidents increased by 3,000% (Onfido Identity Fraud Report).

Difficulty In Detecting Deepfake Audio:
A survey of 529 people found that nearly one-quarter of the participants were unable to distinguish deepfake audio from actual voice recordings (PLOS ONE).

Government Agencies Taking Action:
In September 2023, the NSA, CISA, and FBI released a Cybersecurity Information Sheet on deepfake threats (Cybersecurity and Infrastructure Security Agency, 2023).

IoT Security Challenges

1. Global spending on industrial IoT solutions is projected to reach $500 billion by 2025, with over 70% of new deployments using wireless sensors. These solutions enable remote monitoring, reducing the need for on-site inspections by 60%, and companies report a 25% increase in operational efficiency and a 50% reduction in unplanned downtime.

2. Increased Attack Surface:
Forecasts indicate that by 2025, over 75 billion devices will be connected to the Internet of Things (IoT). (Statista)

3. Approximately 500 publicly disclosed data breaches involving IoT devices in 2023. (bytebeam)

4. Roughly 100,000 IoT tracking devices are attached to UPS transportation assets. And these devices generate 60 million messages every week. (UPS)

Critical Infrastructure Vulnerabilities

1. Increase in Attacks:
The number of cyberattacks targeting critical infrastructure has grown significantly, now accounting for 40% of all government attacks (20% in 2021) (Microsoft, 2022).

2. Vulnerability to Ransomware:
The FBI reported that 870 critical infrastructure organizations were victims of ransomware in 2022, affecting 14 of the 16 critical infrastructure sectors (GAO, 2022).

3. Operational Impact:
89% of electricity, oil & gas, and manufacturing firms experienced cyber-attacks impacting production and energy supply over the past 12 months (Trend Micro, 2022).

Cloud Security

1. Rising Cloud Incidents
80% of organizations experienced at least one severe cloud security incident in the past year, including data breaches, data leaks, and intrusions into their environments (Snyk, 2022).

2. Cloud Security Threats:
80% of security exposures are found in cloud environments versus on-premises due to factors such as frequent misconfigurations and shared responsibilities (Palo Alto Networks, 2023).

3. Cloud Security Risk Analysis
An analysis identifies the cloud as the dominant attack surface, with 80% of medium, high, and critical exposures found in cloud-hosted assets (Palo Alto Networks, 2024).

Extended Detection and Response (XDR)

1. XDR Market Growth:
The global Extended Detection and Response (XDR) market size is expected to increase at a CAGR of 38.4%, from USD 1.7 billion in 2023 to USD 8.8 billion by 2028 (MarketsandMarkets, 2024).

2. Post XDR adoption it will take
another 24 months for SIEM coverage to cross the 80% penetration rate, SP Global marketing intel

Quantum Computing Risks and Attacks

1. Growth of Quantum Computing Industry:
Quantum computing could account for nearly $1.3 trillion in value by 2035 (McKinsey & Company, 2024).

2. High Impact
95% of respondents believe quantum computing's relevance and potential impact on today's cryptographic security systems is 'very high or high, (KPMG)

3. Quantum Computing High Risks
60% of respondents in Canada and 73% in the US believe 'it's only a matter of time' before cybercriminals are using the power of quantum to decrypt and disrupt today's cyber security protocols (KPMG).

Post-Quantum and Cryptography

1**. Urgency for Adoption:**
The NSA has set a 2035 deadline for the adoption of post-quantum cryptography across national security systems. This timeline highlights the critical nature of preparing for quantum computing threats well in advance (Inside Quantum Technology, 2023).

Grazie per l'attenzione!

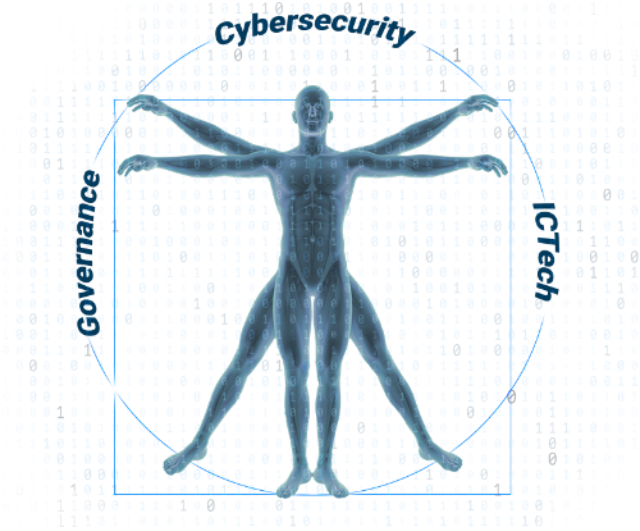
QUESTIONARIO

- ❑ Gradimento
- ❑ Privacy
- ❑ Newsletter

Scrivere a eventi@ithum.it per:

- ✓ Attestato di partecipazione
- ✓ Slide proiettate
- ✓ Informazioni varie

ITHUM
it's for human



Fields of interest:
Training & **Certifications**
Specialized **Consultancy**

Founded in **2005**
by ICT professionals

HQ located **in Rome**
Active in Italy & Europe

Collaborative & strategic approach
to build Value

Cyber Security

- IT Security
  - Attacks & Warfare
  - Defence & Analysis
  - Secure Coding
  - Operation Technology Security
- Governance & Management
- Intelligence & Social
- Investigation & Forensic
- Regulatory Compliance
- Artificial Intelligence

Governance

- National & International Standards
  - Information Security
  - Artificial Intelligence
  - Business Continuity
  - Quality
  - IT Services
  - Anti-Bribery
  - Environment Social Government
  - Privacy GDPR
  - Professional Profiles UNI/EN (ICT & HR)
- Project Management & Framework
- Job Safety & Security
- Management & Soft skills

ICTech

- IT & Operative Systems
- Networking & DevNet
- Cloud & Virtualization
- Containers
  - Docker
  - Kubernetes
- Blockchain
- Development & Programming
- Industry 4.0 (IoT, Big Data, AR)
- Artificial Intelligence, Deep & Machine Learning

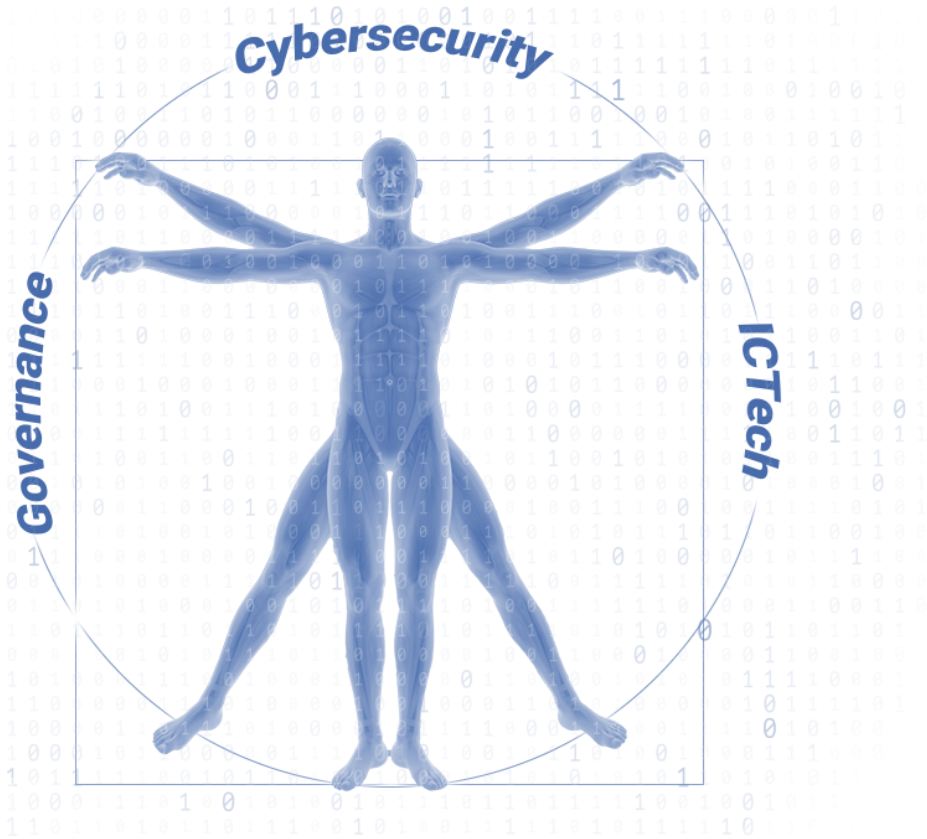
ITHUM
it's for human

(+39) 06 2158915
(+39) 06 86726329

Via Cristoforo Colombo, 149
00147 Roma (RM) Italy

informazioni@ithum.it

www.ithum.it



Corsi correlati

CEH
Certified Ethical Hacker

Inizio corso: mercoledì 13 novembre

CND
Certified Network Defender

Inizio corso: lunedì 11 novembre

CSA
Certified SOC Analyst

Inizio corso: mercoledì 13 novembre

CHFI
Certified Hacking Forensic Investigator

Inizio corso: lunedì 18 novembre

CCISO
Certified Chief Information Security Officer

Inizio corso: venerdì 13 dicembre

CTIA
Certified Threat Intelligence Analyst

Inizio corso: giovedì 21 novembre

CPENT
Certified Penetration Testing Professional

Inizio corso: venerdì 13 dicembre

ECIH
Certified Incident Handler

Inizio corso: giovedì 21 novembre

I nostri Webinar

2 ottobre

[Normative europee in ambito OT e Cyber Security]

29 ottobre (ore 12:30-13:15)

Clicca **qui** per iscriverti!

Q&A