SECURITY AND RISK: MANAGEMENT AND CERTIFICATIONS

Antonio **Belli**

M10 Most common Certifications available on the market

Contents

M10.2 Most common Certifications available on the market

- IT security and Ethical hacking certifications (Comptia, SANS-GIAC, ISC, CSA, ISACA and Ec-Council. Offensive security - OSCP)
- Training programs, labs, and penetration testing (TryHackMe, Hack the Box and Infosec)
- Differences between certifications and training programs

IT Security Certification for people

INTRODUCTION

Why certification is important

Job Security
82% of organizations prefer hiring candidates with certifications. The right certification could signal to HR teams and hiring managers that you have the specific job-role skills they need.

[Source: giac.org]

IT Security Certification for people

INTRODUCTION

Why certification is important

A possible *obstacle* that is encountered in the search for professional figures in the field of cybersecurity is that of not having the people who are able to *evaluate* and *measure* the skills that are needed, especially for those organizations that are starting to have to build their own staff because they do not still have one.

IT Security Certification for people

INTRODUCTION

Why certification is important

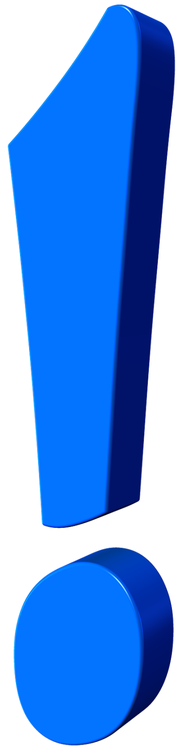
In these cases, but not limited to, certification constitutes a credential that helps people to be recognized as competent by different employers and contexts.
But there are many **certifications** and different **bodies** and **companies** that issue them. It is not always easy to find your way around in this world.

IT Security Certification for people

INTRODUCTION

Why certification is important

The **urgency** to find experts who know how to defend data and IT technologies from possible cyber attacks does not help and can lead to a poor consideration of real needs of the company.



IT Security Certification for people

INTRODUCTION

Why certification is important

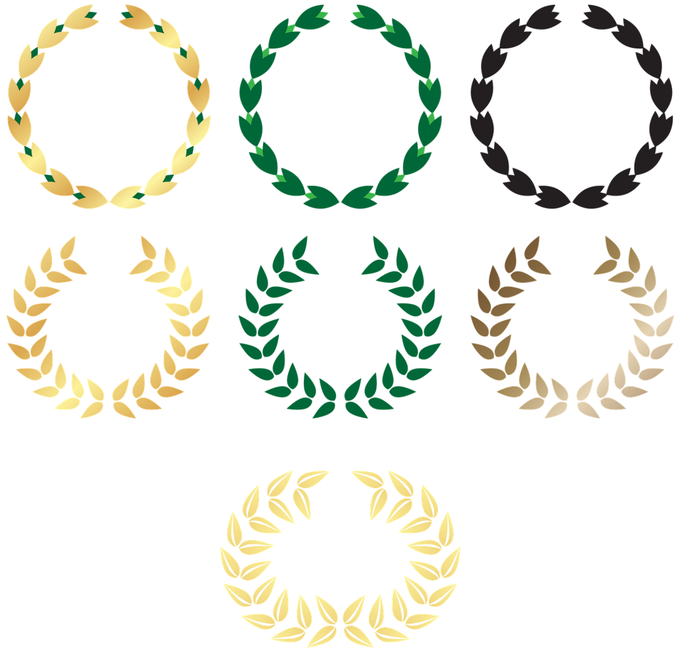
On the one hand, therefore, organizations must clarify, based on the type of data processed, the type of *technologies*, the *size*, the *people* and all the other factors that we have mentioned so far, **which** (and **how many**) are the people to be included. On the other hand, people themselves must build a **path** that possibly *reflects* their inclinations and passions, but also a coherent and realistic set of skills as close to demand as possible.

IT Security Certification for people

INTRODUCTION

Why certification is important

Enterprise Security
Certifications provide confirmation of the skills needed to combat breaches and mitigate threats to the enterprise. 94% of cybersecurity practitioners believe their certs have better prepared them for their current role, allowing them to successfully protect their organization.

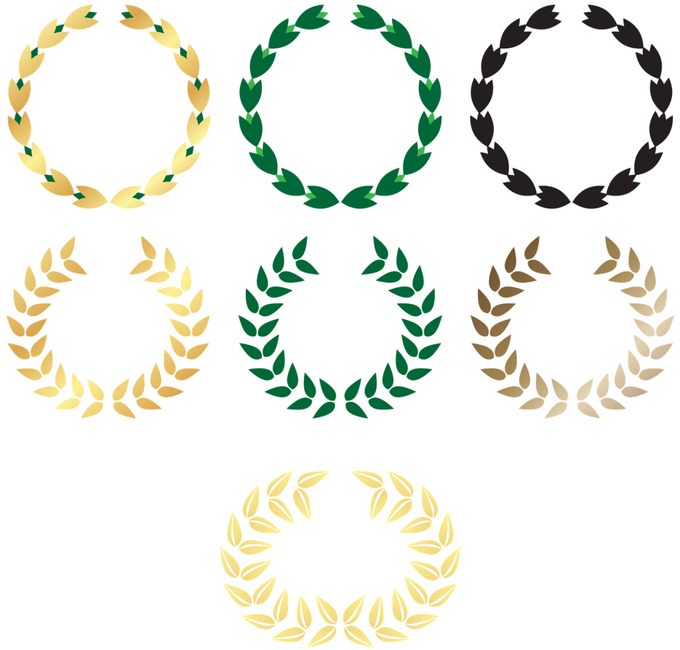


[Source: giac.org]

IT Security Certification for people

Why certification is important

Proven Ability
If you have a certification proving you've mastered a specific skillset, both **employers** and your **industry** peers know that you've got what it takes.



[Source: giac.org]

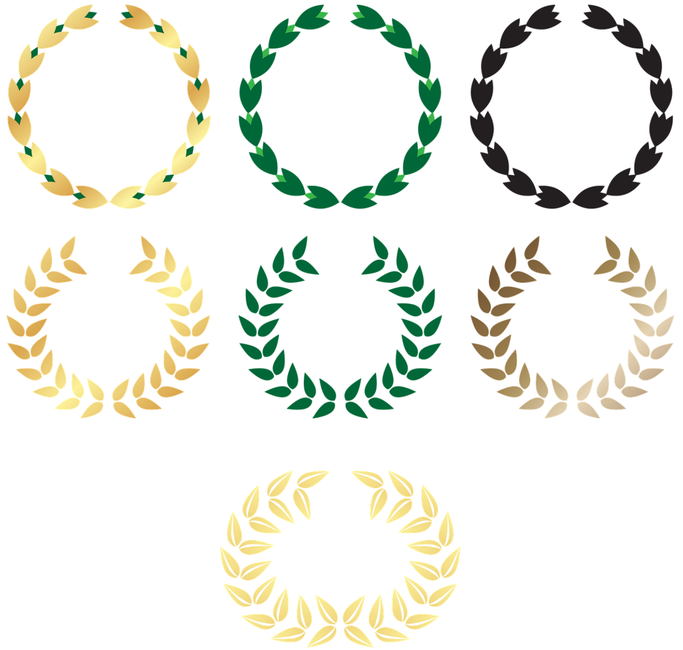
IT Security Certification for people

INTRODUCTION

Why certification is important

Personal Validation
Setting goals to learn new skills and pass a certification exam can be a *challenging* and *rewarding* internal experience. Proving to yourself that you can master skills and conquer the exam creates a sense of purpose and personal satisfaction.

In the following slides we'll see many certifications for people among the most valued in the field.



[Source: giac.org]

IT Security Certification for people

COMPTIA

Comptia is a vendor-neutral, independent source of information on a wide range of technology topics, including cybersecurity; education, training and certification of the global tech workforce; new and emerging technologies; legislation and policies affecting the industry and workforce data, development and trends.

[Source: comptia.org]

IT Security Certification for people

COMPTIA

CompTIA has four IT certification series that test different knowledge standards – from entry-level to expert.

Certifications are divided in different levels:

- Core
- **Cybersecurity**
- Infrastructure
- Data and Analysis
- Additional Professional

[Source: comptia.org]

IT Security Certification for people

COMPTIA - SECURITY+

CompTIA Security+ is a global certification that validates the baseline skills necessary to perform core security functions and pursue an IT security career.

Security+ is compliant with ISO 17024 standards and approved by the US DoD to meet directive 8140/8570.01-M requirements. Regulators and government rely on ANSI accreditation, because it provides confidence and trust in the outputs of an accredited program. Over 2.3 million CompTIA ISO/ANSI-accredited exams have been delivered since January 1, 2011.

[Source: comptia.org]

IT Security Certification for people

COMPTIA - CYBERSECURITY ANALYST (CYSA+)

CompTIA Cybersecurity Analyst (CySA+) is an IT workforce certification that applies behavioral analytics to networks and devices to *prevent*, *detect* and *combat* cybersecurity **threats** through continuous security **monitoring**.

[Source: comptia.org]

IT Security Certification for people

COMPTIA - CYBERSECURITY ANALYST (CYSA+)

CompTIA CySA+ *meets the ISO 17024 standard* and is approved by U.S. Department of Defense to fulfill Directive 8570.01-M requirements. It is compliant with government regulations under the Federal Information Security Management Act (FISMA). Regulators and government rely on ANSI accreditation because it provides confidence and trust in the outputs of an accredited program.

[Source: comptia.org]

IT Security Certification for people

COMPTIA - CYBERSECURITY ANALYST (CYSA+)

CySA+ will verify the successful candidate has the knowledge and skills required to:

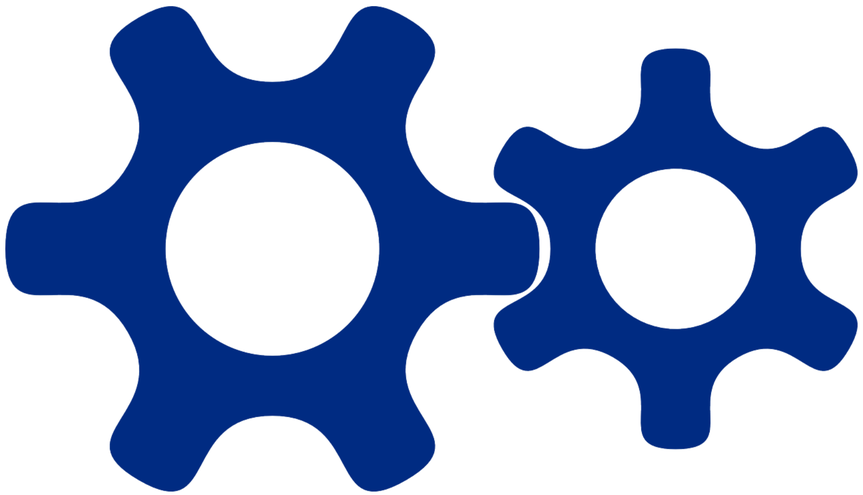
- Leverage *intelligence* and *threat detection* techniques
- Analyze and interpret *data*
- Identify and address *vulnerabilities*
- Suggest preventative *measures*
- Effectively respond to and recover from *incidents*

[Source: comptia.org]

IT Security Certification for people

COMPTIA ADVANCED SECURITY PRACTITIONER (CASP+)

CompTIA Advanced Security Practitioner (CASP+) is an advanced-level cybersecurity certification for **security architects** and **senior security engineers** charged with leading and improving an enterprise's cybersecurity readiness.



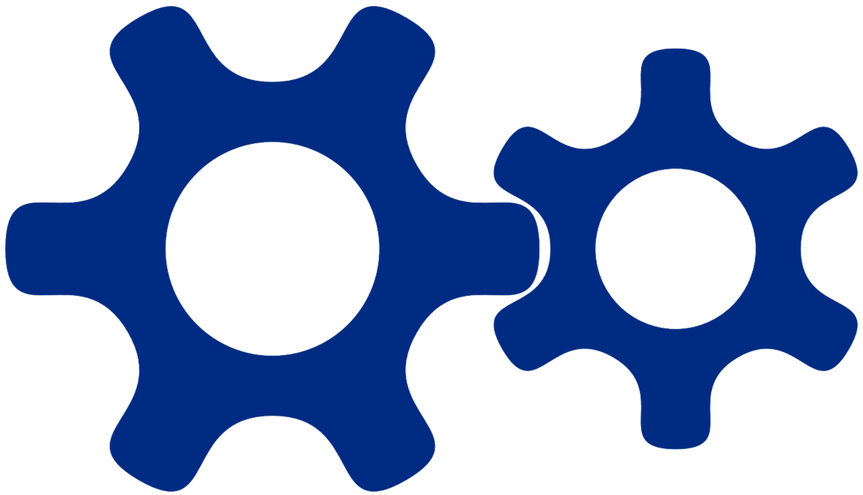
[Source: comptia.org]

IT Security Certification for people

COMPTIA ADVANCED SECURITY PRACTITIONER (CASP+)

Successful candidates will have the knowledge required to:

- Architect, engineer, integrate, and implement secure solutions across *complex environments* to support a resilient enterprise
- Use *monitoring*, *detection*, incident *response*, and *automation* to proactively support *ongoing security* operations in an enterprise environment
- Apply security practices to *cloud*, *on-premises*, *endpoint*, and *mobile infrastructure*, while considering c*ryptographic technologies* and *techniques*
- Consider the impact of *governance*, *risk*, and *compliance* requirements throughout the enterprise

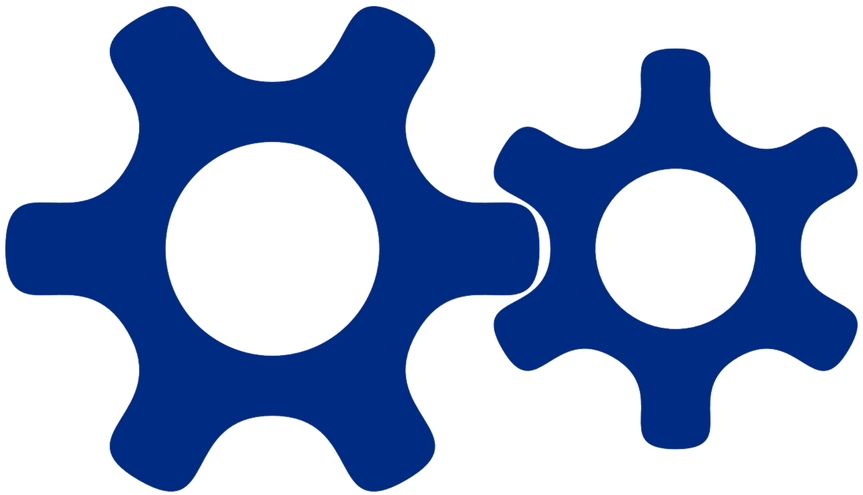


[Source: comptia.org]

IT Security Certification for people

COMPTIA ADVANCED SECURITY PRACTITIONER (CASP+)

CASP+ is compliant with *ISO 17024* standard and approved by the *US DoD* to meet directive 8140/8570.01-M requirements. Regulators and government rely on ANSI accreditation, because it provides confidence and trust in the outputs of an accredited program.



[Source: comptia.org]

IT Security Certification for people

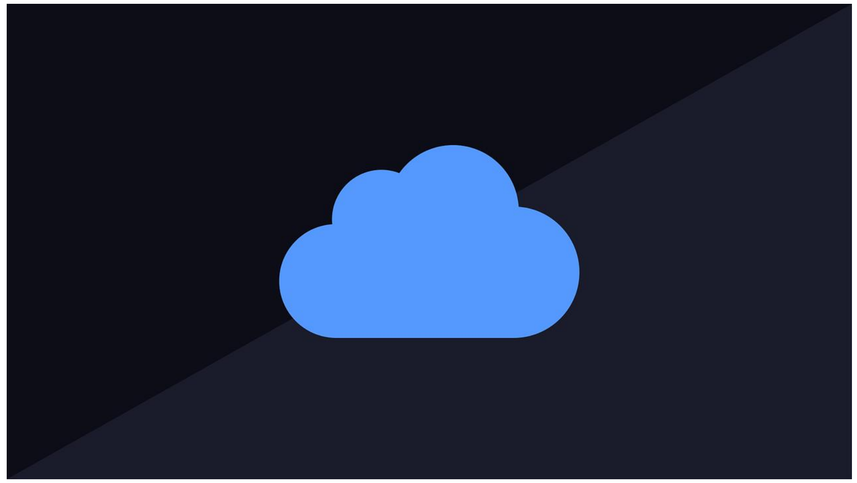
GIAC CLOUD SECURITY ESSENTIALS (GCLD)

The GCLD certification validates a practitioner's ability to implement preventive, detective, and reactionary techniques to defend valuable cloud-based workloads.

Covered areas:

- Evaluation of cloud service provider similarities, differences, challenges, and opportunities
- Planning, deploying, hardening, and securing single and multi-cloud environments
- Basic cloud resource auditing, security assessment, and incident response

[Source: giac.org]



IT Security Certification for people

GIAC PUBLIC CLOUD SECURITY (GPCS)

The GPCS certification validates a practitioner's ability to secure the cloud in both public cloud and multi cloud environments. GPCS-certified professionals are familiar with the nuances of AWS, Azure, and GCP and have the skills needed to defend each of these platforms.

Covered areas:

- Evaluation and comparison of public cloud service providers
- Auditing, hardening, and securing public cloud environments
- Introduction to multi-cloud compliance and integration

[Source: giac.org]

IT Security Certification for people

(ISC)^2

The **International Information Systems Security Certification Consortium** (ISC)^2, is a non-profit organization that provides security training and certificates.

It is worldwide known for issuing, in particular, CISSP, CCSP and CSSLP certifications.

IT Security Certification for people

(ISC)^2 - CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL - CISSP

Who Earns the CISSP?

The CISSP is ideal for experienced security practitioners, managers and executives interested in proving their knowledge across a wide array of security practices and principles, including those in the following positions:

- Chief Information Security Officer
- Chief Information Officer
- Director of Security
- IT Director/Manager
- Security Systems Engineer
- Security Analyst
- Security Manager
- Security Auditor
- Security Architect
- Security Consultant
- Network Architect

The CISSP meets the U.S. Department of Defense (DoD) Directive 8570.1

[source: www.isc2.org]

IT Security Certification for people

(ISC)^2 - CERTIFIED CLOUD SECURITY PROFESSIONAL - CCSP

Who Earns the CCSP?

The CCSP is ideal for IT and information security leaders responsible for applying best practices to cloud security architecture, design, operations and service orchestration, including those in the following positions:

- Cloud Architect
- Cloud Engineer
- Cloud Consultant
- Cloud Administrator
- Cloud Security Analyst
- Cloud Specialist
- Auditor of Cloud Computing Services
- Professional Cloud Developer

the CCSP meets the U.S. Department of Defense (DoD) Directive 8570.1

[source: www.isc2.org]

IT Security Certification for people

(ISC)^2 - CERTIFIED SECURE SOFTWARE LIFECYCLE PROFESSIONAL - CSSLP

Who Earns the CSSLP?

The CSSLP is ideal for software development and security professionals responsible for applying best practices to each phase of the SDLC – from software design and implementation to testing and deployment – including those in the following positions:

- Software Architect
- Software Engineer
- Software Developer
- Application Security Specialist
- Software Program Manager
- Quality Assurance Tester
- Penetration Tester
- Software Procurement Analyst
- Project Manager
- Security Manager
- IT Director/Manager

the CSSLP meets the U.S. Department of Defense (DoD) Directive 8570.1

[source: www.isc2.org]

IT Security Certification for people

CSA AND ISACA - CERTIFICATE OF CLOUD AUDITING KNOWLEDGE (CCAK)

This certification helps professionals learn how to audit **cloud systems**.

CCAK is the first-ever, technical, vendor-neutral credential for cloud auditing. This certificate qualifies competent technical professionals who can help organizations mitigate risks and optimize *Return of Investment* in the cloud.

[source: isaca.org]

IT Security Certification for people

CERTIFICATE OF CLOUD SECURITY KNOWLEDGE (CCSK)

As organizations migrate to the cloud, they need information security professionals who are cloud-savvy.

The CCSK certificate is widely recognized as a standard of expertise for cloud security and gives a cohesive and vendor-neutral understanding of how to secure data in the cloud.

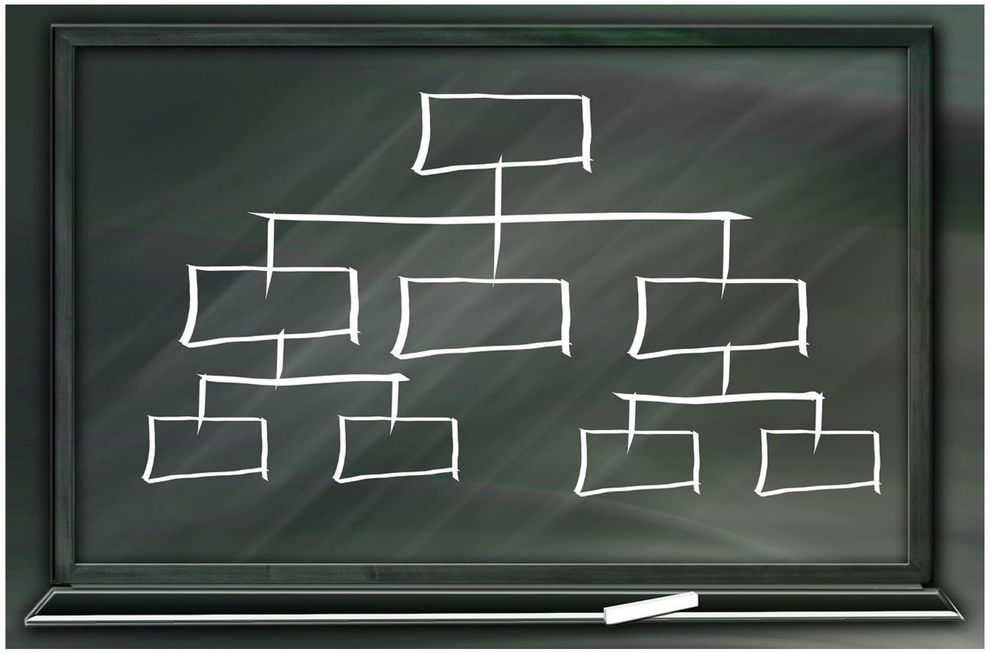
It covers key areas, including best practices for *IAM*, cloud *incident response*, *application* security, data *encryption*, *SecaaS*, securing emerging technologies, and more.

[source: cloudsecurityalliance.org]

IT Security Certification for people

EC COUNCIL - CISO

EC-Council's Certified Chief Information Security Officer Program
The CCISO Certification is a program that recognizes the real-world experience necessary to succeed at the highest executive levels of information security.



[source: eccouncil.org]

IT Security Certification for people

EC COUNCIL - CHFI

EC-Council's Certified Hacking Forensic Investigator (CHFI) is ANSI accredited, **lab-focused** that gives organizations **vendor-neutral training** in digital forensics. CHFI provides its attendees with a firm grasp of digital forensics, presenting a detailed and methodological approach to digital forensics and evidence analysis that also pivots around *Dark Web*, *IoT*, and *Cloud Forensics*. The tools and techniques covered in this program will prepare the learner for conducting digital investigations using ground-breaking digital forensics technologies.

[source: eccouncil.org]

IT Security Certification for people

EC COUNCIL - CHFI

The program is designed for IT professionals involved with information system security, computer **forensics**, and *incident response*. It will help fortify the application knowledge in digital forensics for forensic analysts, cybercrime investigators, cyber defense forensic analysts, incident responders, information technology auditors, malware analysts, security consultants, and chief security officers.

The program equips candidates with the necessary skills to proactively *investigate* complex security threats, allowing them to investigate, record, and report cybercrimes to prevent future attacks.

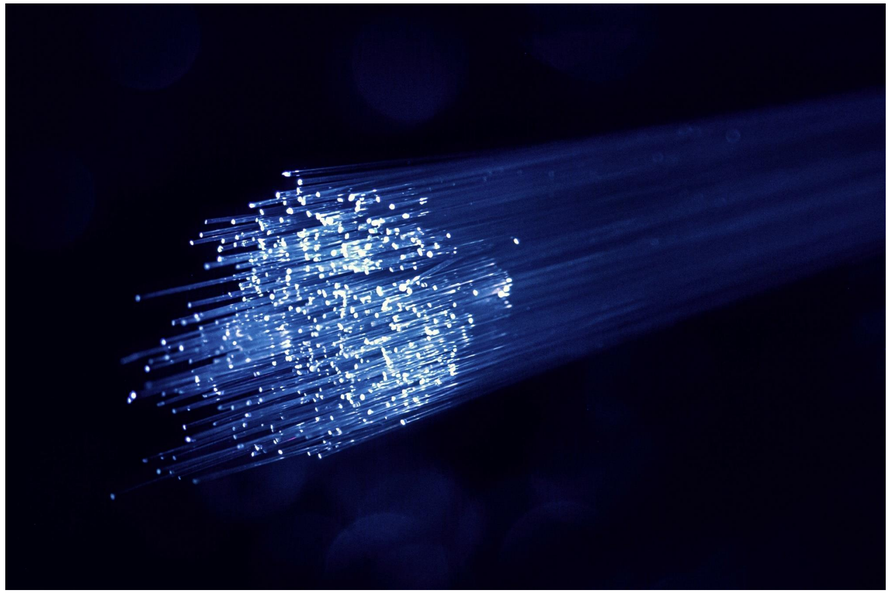
[source: eccouncil.org]

IT Security Certification for people

EC COUNCIL - CND

EC-Council Network Defender certifications are vendor-neutral and provide an approach to learning secure networking practices, as well as how to analyze and harden computing systems prevalent in the current IT infrastructure.

It is completely focused on network *security* and *defense*.

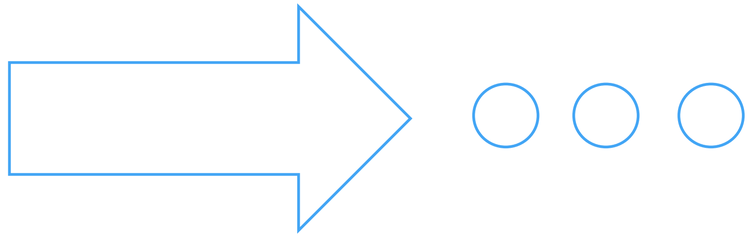


[source: eccouncil.org]

IT Security Certification for people

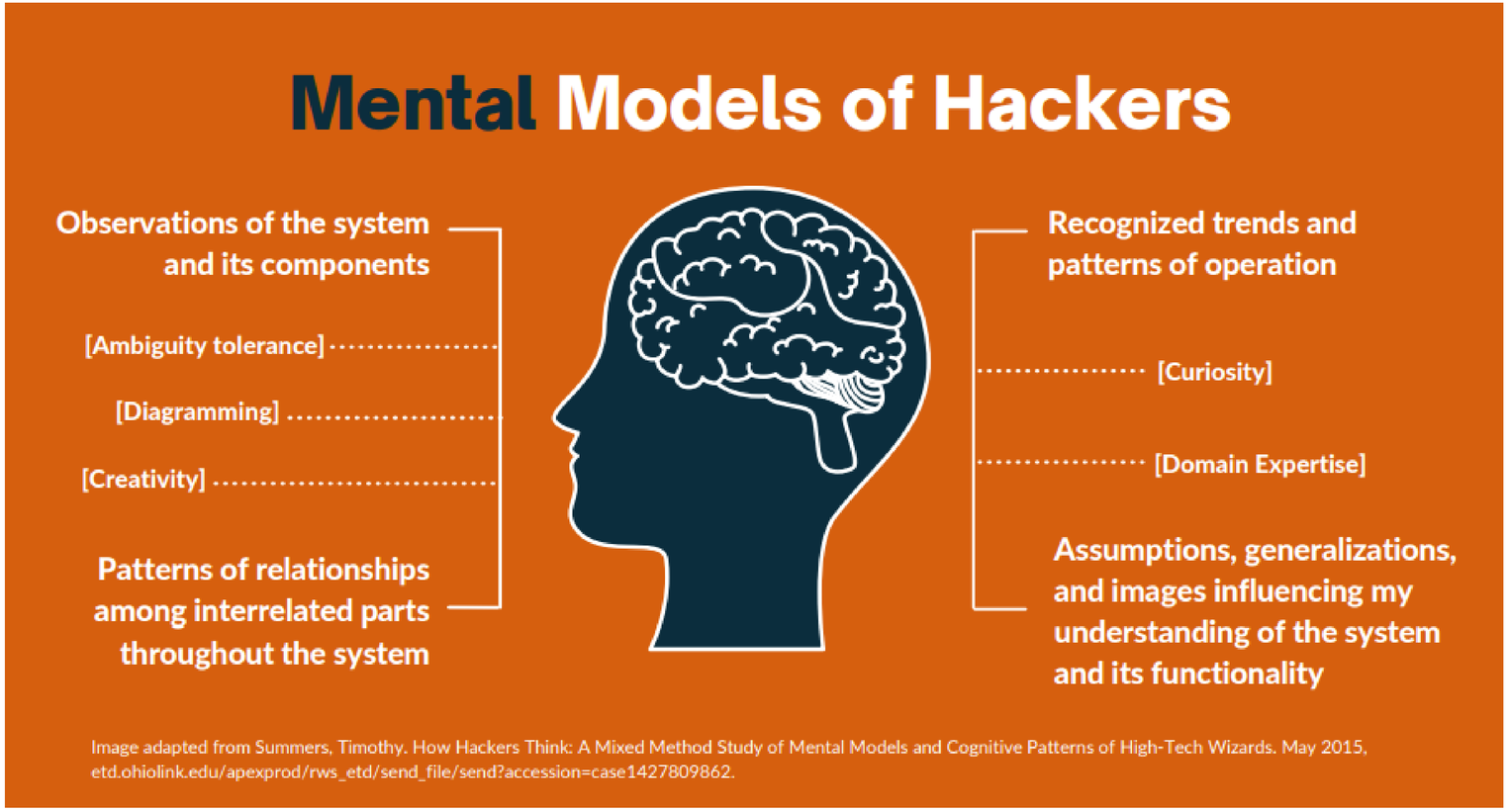
ISACA

Isaca's CISA, CRISC, CGEIT, CISM, CSX-P, CDPSE, ITCA certifications are shown in the specific slides.



IT Security Certification for people

ETICAL HACKING CERTIFICATIONS



[Source: offensive-security.org]

IT Security Certification for people

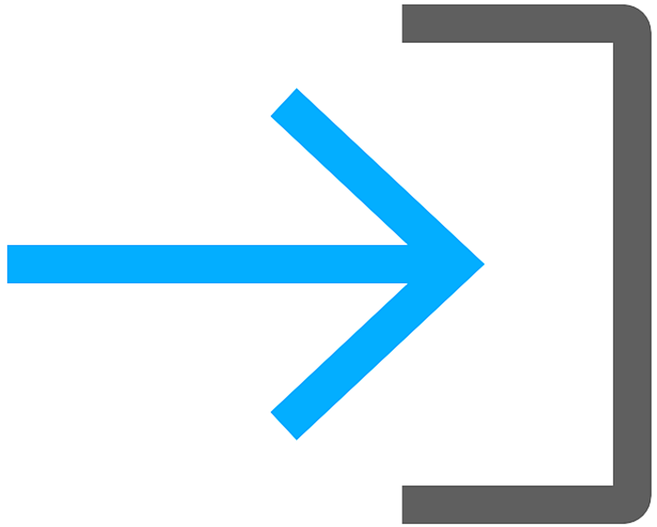
COMPTIA PENTEST+

CompTIA PenTest+ is for cybersecurity professionals tasked with **penetration testing** and **vulnerability management**.

The CompTIA PenTest+ certification exam will verify successful candidates have the knowledge and skills required to:

- Plan and scope a *penetration testing* engagement
- Understand legal and compliance requirements
- Perform *vulnerability scanning* and *penetration testing* using appropriate tools and
- techniques, and then analyze the results
- Produce a *written report* containing proposed remediation techniques, effectively
- *communicate results* to the management team, and provide practical recommendations

[Source: comptia.org]



IT Security Certification for people

SANS INSTITUTE – GIAC - GIAC PENETRATION TESTER (GPEN)

The Giac (Global Information Assurance Certification) program program is run by the SANS Institute, one of the oldest organizations that provide cybersecurity education.

GIAC Penetration Tester (GPEN)
The GIAC Penetration Tester certification validates a practitioner's ability to properly conduct a penetration test, using best practice techniques and methodologies. GPEN certification holders have the knowledge and skills to conduct *exploits* and engage in detailed reconnaissance, as well as utilize a *process-oriented approach* to penetration testing projects.

[Source: giac.org]

IT Security Certification for people

SANS INSTITUTE – GIAC - GIAC PENETRATION TESTER (GPEN)

Covered areas:

- Comprehensive Pen Test Planning, Scoping, and Recon
- In-Depth Scanning and Exploitation, Post-Exploitation, and Pivoting
- In-Depth Password Attacks and Web App Pen Testing

[Source: giac.org]

IT Security Certification for people

EC COUNCIL - CEH

Certified Ethical Hacker CEH v11 is about commercial-grade hacking tools, techniques, and methodologies used by hackers and information security professionals to lawfully hack an organization.

[Source: eccouncil.org]

IT Security Certification for people

EC COUNCIL - CEH

In 2003, CEH introduced the five phases of ethical hacking, the blueprint for approaching target and succeeding at breaking in. CEH has continued to hone these 5 **phases**, updating and refining them to match the skillset ethical hackers need today:

- Reconnaissance
- Gaining Access
- Enumeration
- Maintaining Access
- Covering Your Tracks

[Source: eccouncil.org]

IT Security Certification for people

EC COUNCIL - CEH

CEH v11 covers many *new* threats and vulnerability scenarios, like APT, Fileless Malware, Web API Threats, Webhooks, Web Shell, OT Attacks, Cloud Attacks, AI, ML, and more.

But also emerging technologies such as OT Technology and Container Technology.

CEH v11 includes Malware *Analysis* tactics for ransomware, banking and financial malware, IoT botnets, OT Malware Analysis, Android Malware, and more.

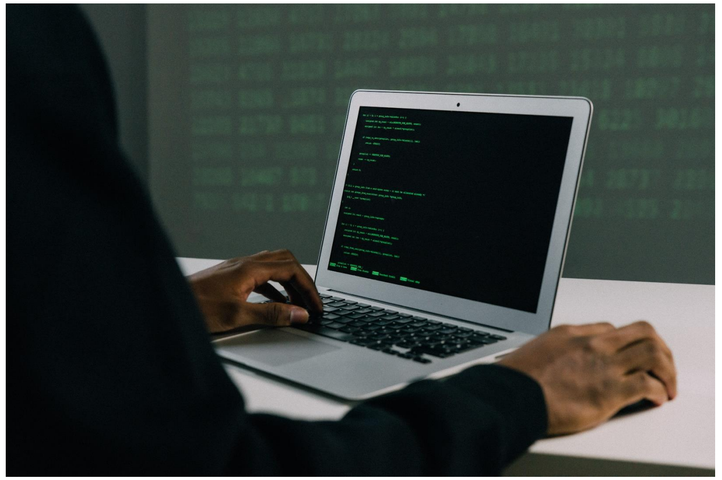
[Source: eccouncil.org]

IT Security Certification for people

OFFENSIVE SECURITY - OSCP

Penetration Testing with Kali Linux (PWK/PEN-200) online ethical hacking course is self-paced. It introduces penetration testing tools and techniques via hands-on experience. PEN-200 trains not only the skills, but also the *mindset* required to be a successful penetration tester.

Students who complete the course and pass the exam earn the Offensive Security Certified Professional (**OSCP**) certification.



[Source: offensive-security.org]

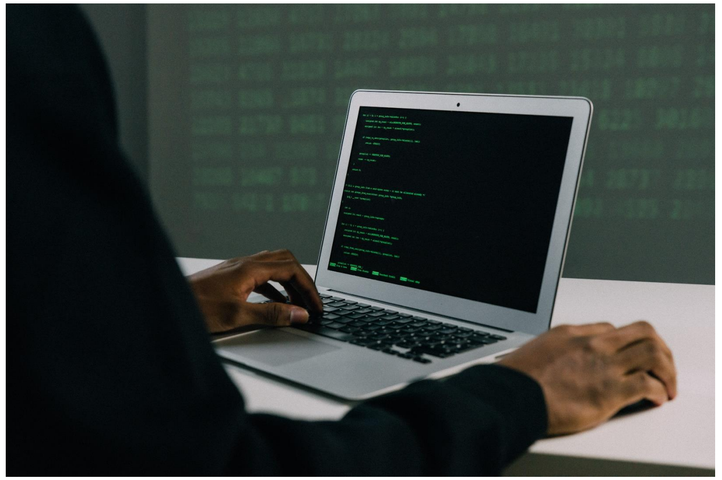
IT Security Certification for people

OFFENSIVE SECURITY - OSCP

All students are required to have:

- Solid understanding of TCP/IP networking
- Reasonable Windows and Linux administration experience
- Familiarity with basic Bash and/or Python scripting

Tips for preparing for the OSCP exam



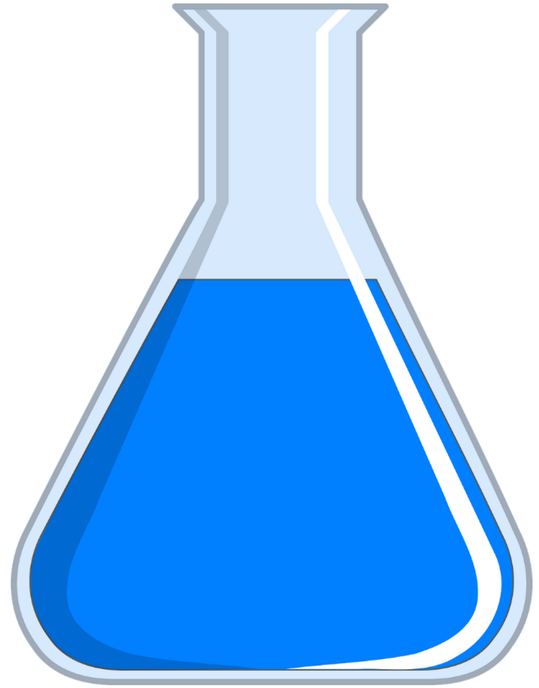
[Source: offensive-security.org]

IT Security laboratories

FEATURES

Gamification, gradual *paths* and *playground* / *community* are some **different** (or somehow additional) powerful tools to guide the *improvement of competence*, even without certifying them.
But are we sure these tools do not *assess* the competence of people and don’t they have a value, in some cases, almost comparable to certifications?

Those who train challenge themselves and other apprentices, improving their own and others' knowledge and skills, obtaining **measurable** results within a *community*, so the usefulness of these workshops is *evident*.

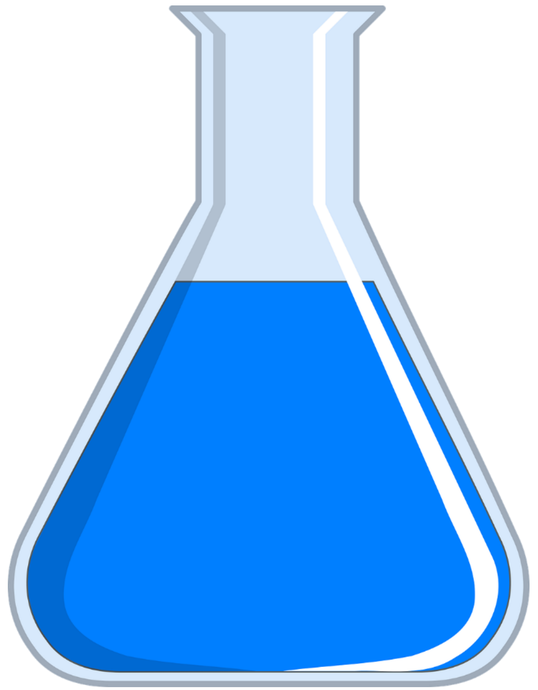


IT Security laboratories

TRYHACKME

Here are some known resources to improve (mostly) …by **doing**

- hackthebox.com
- infoseclearning.com
- tryhackme.com



Certifications and laboratories

KEY ASPECTS AND DIFFERENCES

Certification: has the undisputed advantage of reliably certifying someone's competence, thanks to a system of trust that is built through the consensus that forms around them. Certifications may provide for a necessary level of abstraction (which removes some dimensions in the real world) which varies according to the examination methods, which may be greater if the examination does not include practical tests, and vice versa. The more organizations accept certifications, the more they take on value.

Laboratory: participating in laboratories recognized for the level of difficulty, even in the absence of certification, can actually improve people's skills, especially in those sectors where lateral thinking and the development of concrete working methods are strongly required (such as for those who will carry out an ethical hacking activity).
In this case, competence tends to assert itself in practice, with mechanisms that reward results similar to those expected in *real* scenarios.
The quality and realism of the laboratories are the key to their success (preparing people).

SECURITY AND RISK: MANAGEMENT AND CERTIFICATIONS

Antonio **Belli**
Simone **Soderi**
antonio.belli@unipd.it
simone.soderi@unipd.it

Thanks for your attention!

M10 Most common Certifications available on the market