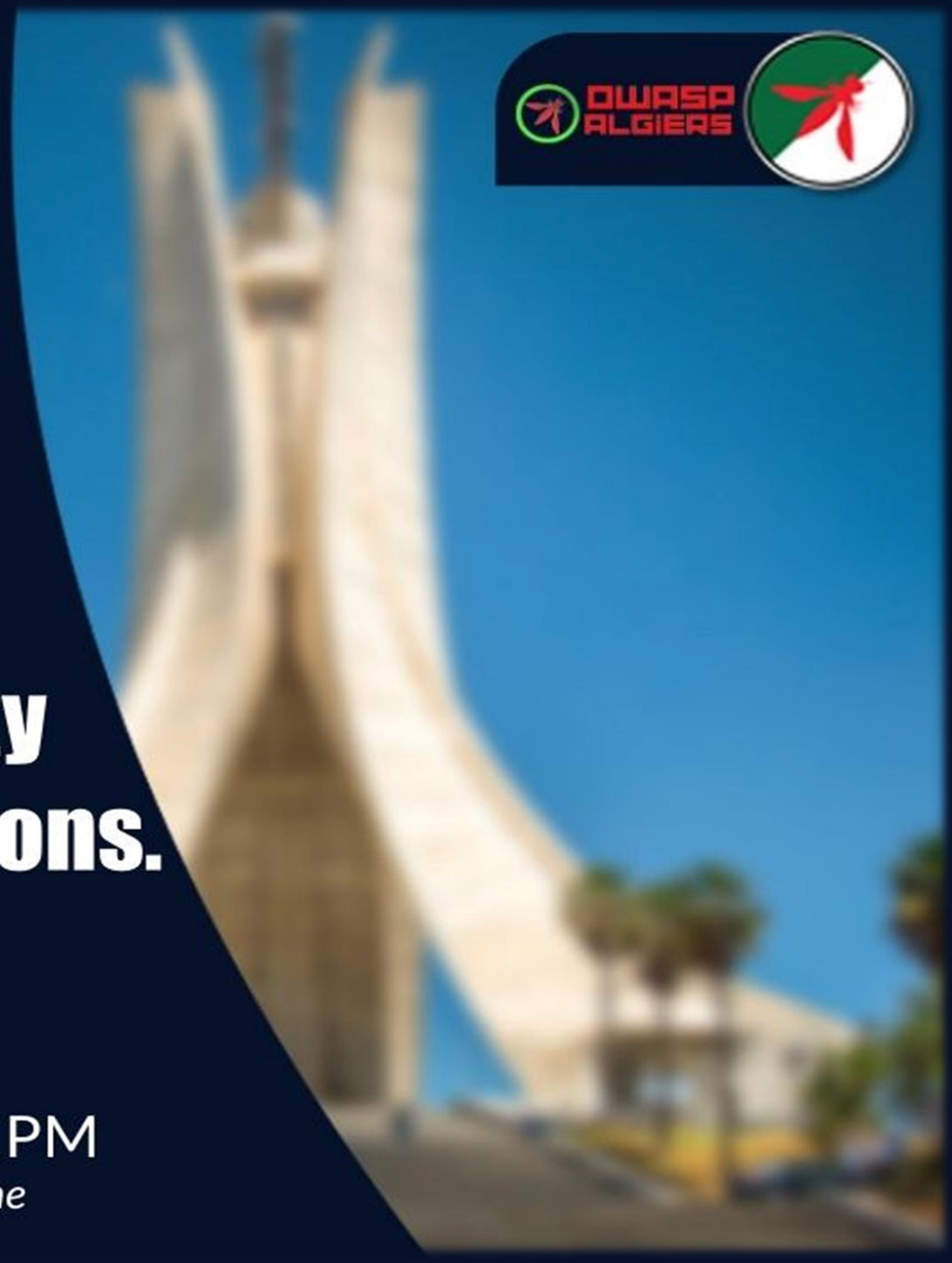
OWASP ALGIERS



OWASP ALGIERS

Webinar

Exploring cybersecurity careers and certifications.

24/02/2024

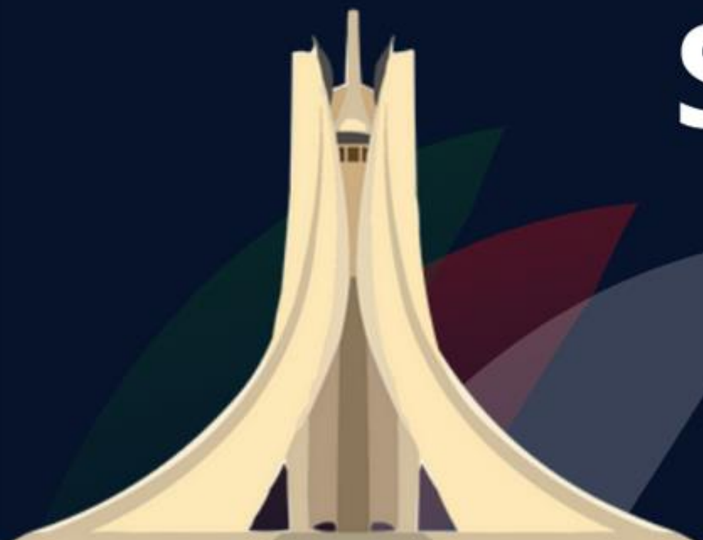
4 PM ~ 7 PM

Algiers Time

Our Speakers

OWASP ALGIERS

SPEAKER



Taher Amine ELHOUARI

CyberSecurity Leader & Global Consultant

- Founder & President @ OWASP Algiers Chapter
- Global Member @ OWASP Foundation
- Founding Board Member @ ISC2 ElDjazair Chapter
- Global Member @ ISC2
- CyberSecurity Instructor @ GoMyCode
- Global CyberSecurity Advisor @ AlphaSights
- CyberSecurity Ambassador @ Cyber Cohesion
- Independent Consultant & Instructor
- CISSP, Mini-MBA, CC, ISO27001, CEHv12, CCSP/AWS, CNPen, CAP, CNSP, CNSS, CPTAv2, C3SA, ACE/MCNA, QCS/VMDR, CCNA..

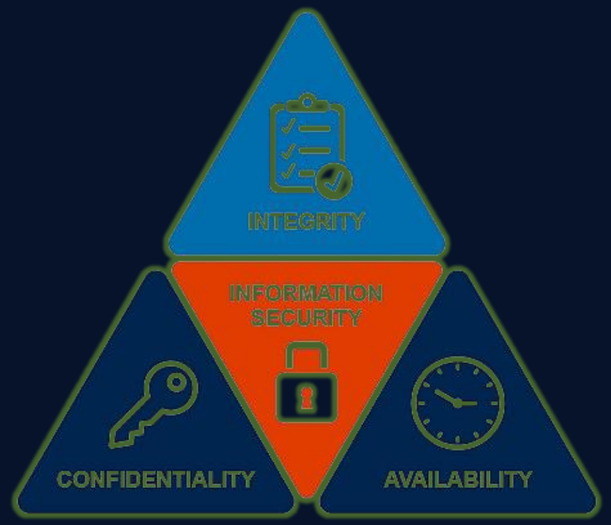
SUMMARY

- Introduction to Information Security & CyberSecurity
- Privacy and Data Protection
- IT Security RoadMap & Careers
- OT Security – ICS, IoT, SCADA
- GRC – Governance, Risk, and Compliance
- Red Teams and Offensive Security
- Blue Teams and Defensive Security
- CyberSecurity Certifications
- Networking in the Industry
- Resources & Platforms to Practice
- Project Ideas
- SURPRISEs!!

Intro to InfoSec & CyberSec

What is Information Security?

- Information Security refers to the practice of protecting information from unauthorized access, use, disclosure, disruption, modification, or destruction.
- It involves implementing measures to ensure the confidentiality, integrity, and availability of information, whether it is stored in digital or physical form.

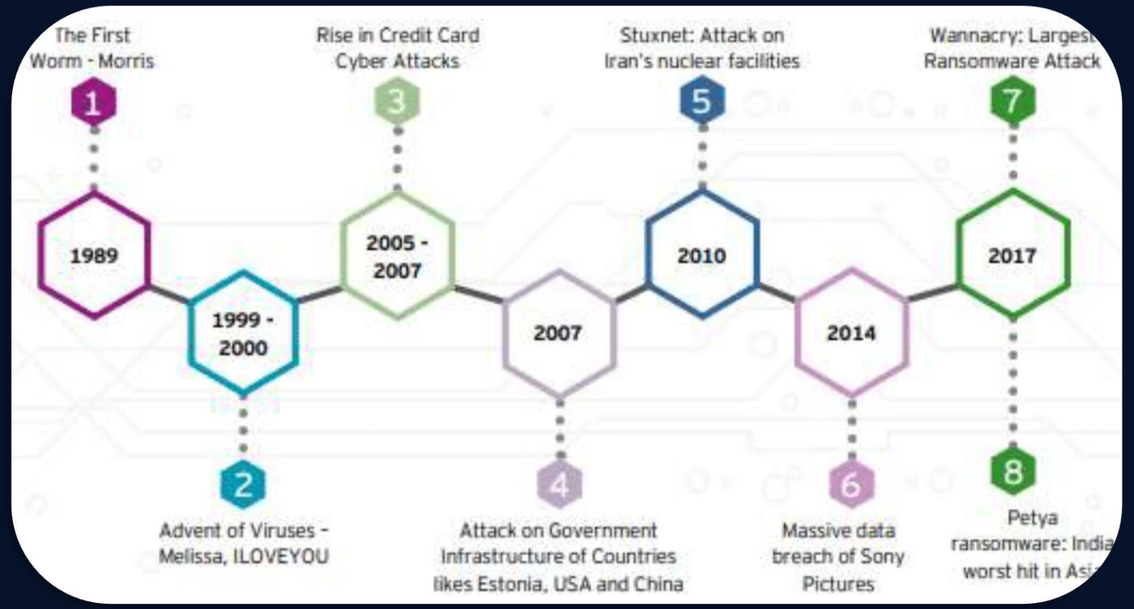


From CIA to CIAAN

- Authenticity
- Non-Repudiation

What is Cyber Security?

- CyberSecurity refers to the practice of protecting computer systems, networks, and data from digital attacks, unauthorized access, and other cyber threats.
- InfoSec focuses on protecting all forms of information, regardless of the medium, while CyberSec specifically deals with securing digital assets such as computer systems, networks, and data from cyber threats.



What about Privacy & Data Protection?

Privacy & Data Protection:

- Privacy and data protection involve safeguarding individuals' personal information from unauthorized access, use, disclosure, alteration, or destruction.

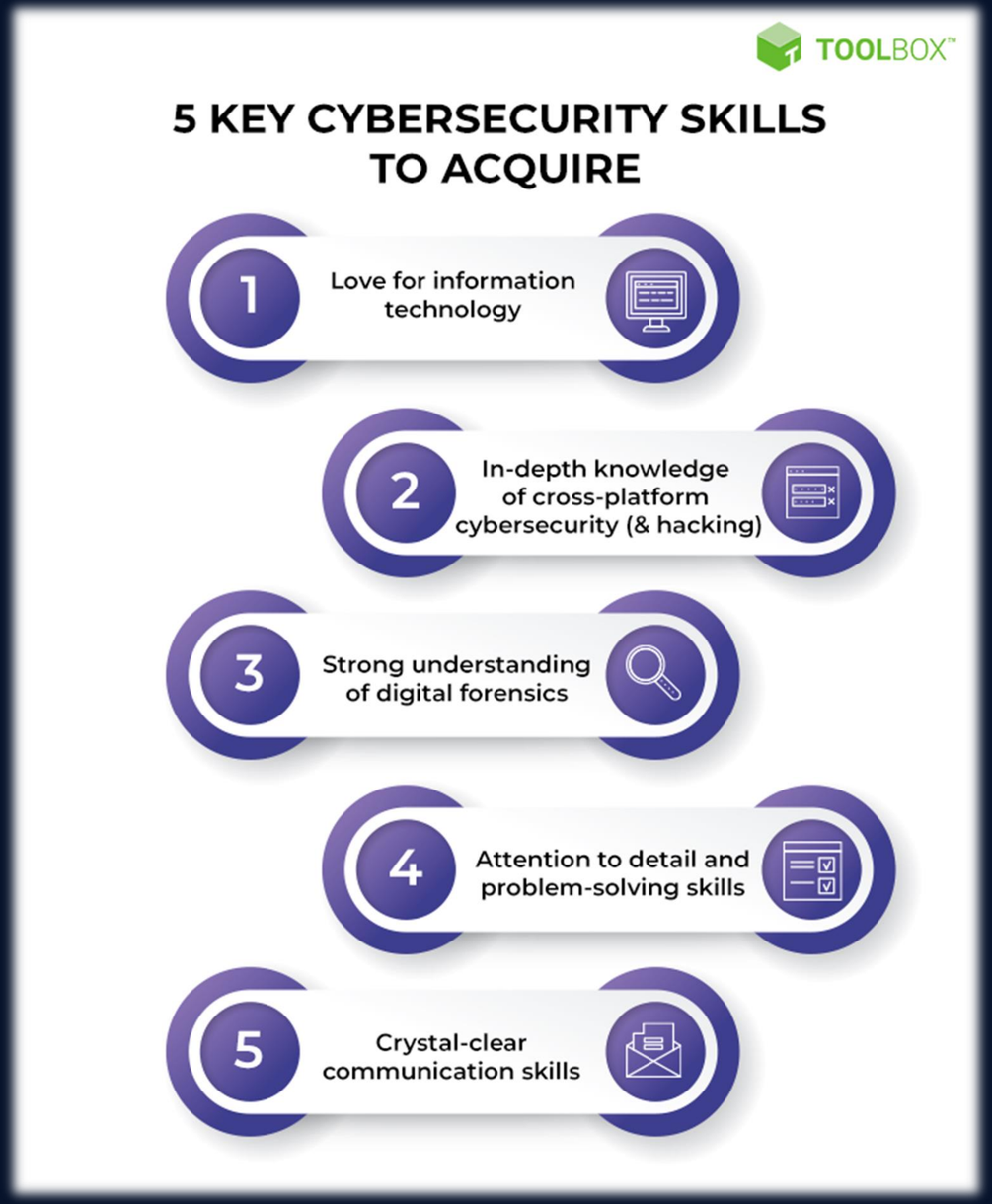
- It includes implementing measures to ensure that personal data is collected, processed, and stored in accordance with applicable laws and regulations, as well as respecting individuals' rights to control their own data.

IT Security
Careers & RoadMap

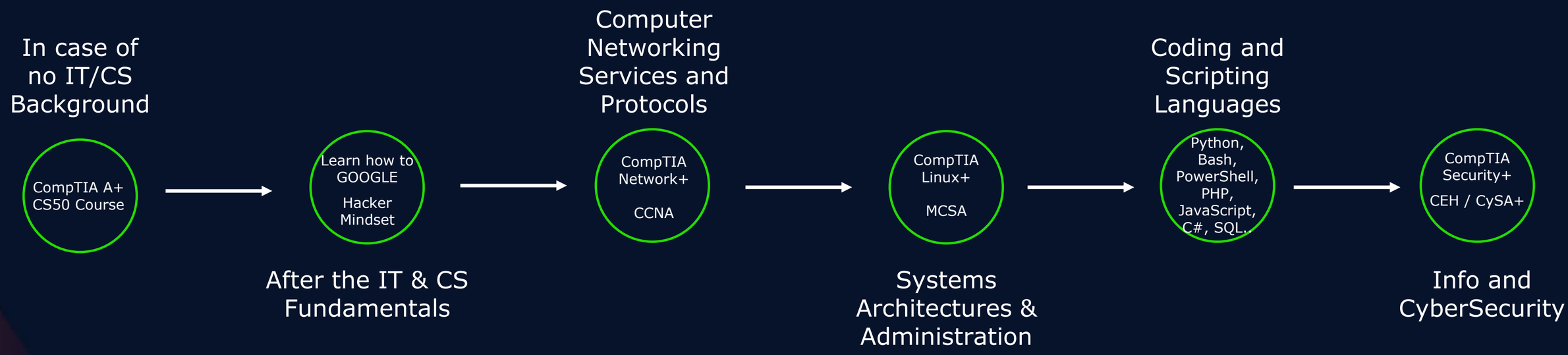
Career Options in IT Security:

Offensive Security	Defensive Security	GRC & Management
Red Team Operator	Threat Hunter	CISO / VP of Security
Offensive Sec Specialist	DFIR Specialist	IT Security Director
Penetration Tester	CERT/CSIRT Operator	IT Security Manager
Vulnerability Assessor	SOC Analyst	IT Security Auditor
Ethical Hacker	IT Security Engineer	IT Security Risk Analyst

Extra:


TOOLBOX
5 KEY CYBERSECURITY SKILLS TO ACQUIRE
1
Love for information technology
2
In-depth knowledge of cross-platform cybersecurity (& hacking)
3
Strong understanding of digital forensics
4
Attention to detail and problem-solving skills
5
Crystal-clear communication skills

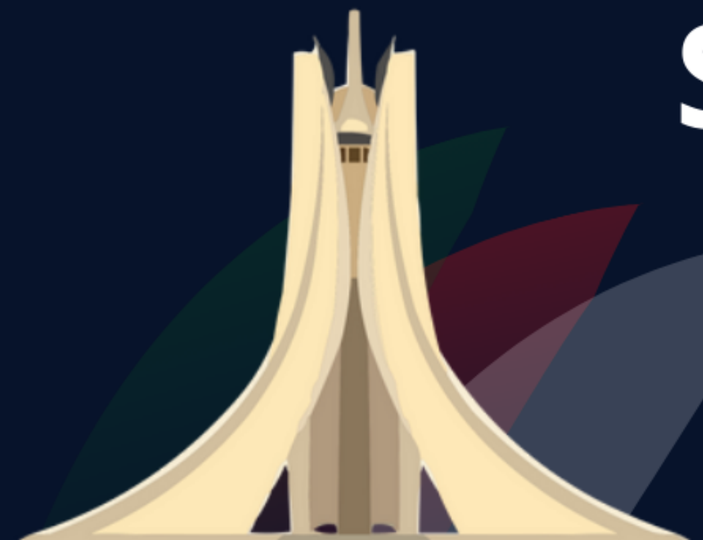
IT Security: Zero to Hero



Intro to OT Security (ICS, IoT, SCADA)

OWASP ALGIERS

SPEAKER

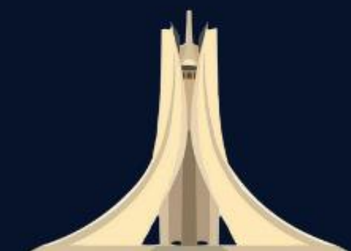


Mehdi Nacer KERKAR

IT/OT Cyber Security Consultant

- Board Member @ OWASP Algiers Chapter
- Member @ ISC2 El Djazair Chapter
- Global Member @ ISC2
- Global Member @ ISA

OT/IACS Subject



What is OT / What is IACS

- Operational Technology is all what is used to control Physical Process
- A mix of Hardware & Software Systems
- Used to Monitor, Control and Supervise Physical Processes

- Including:
  - Sensors & Actuators
  - Programmable Logical Controllers (PLCs),
  - Human-Machine Interfaces (HMIs),
  - Supervisory Control & Data Acquisition (SCADA) Systems.

Industrial Automation & Control Systems

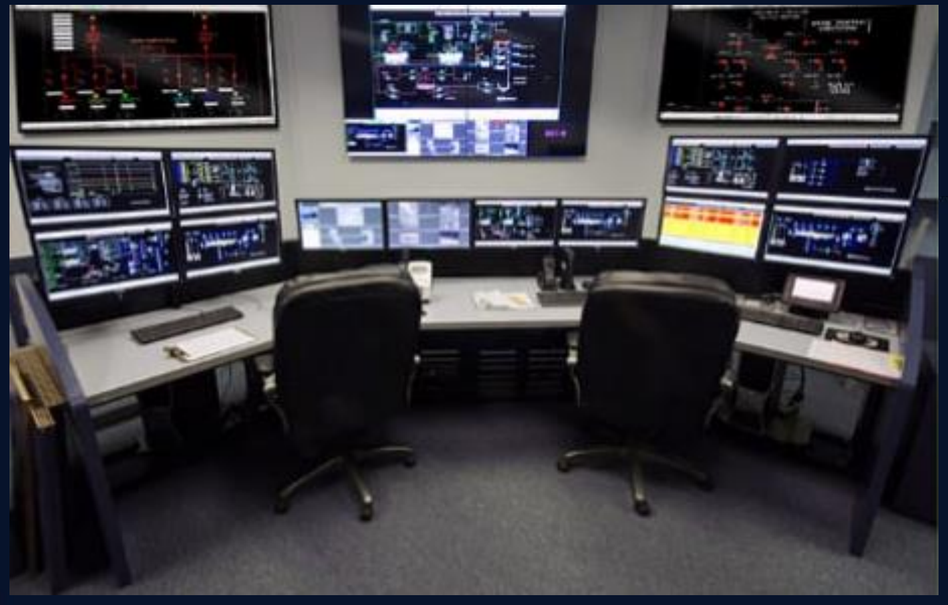




OWASP ALGIERS

OT is used for ?

Monitoring, Control, Operation



Industrial Automation

OWASP ALGIERS

Where is OT ?

Water & Sewage

Electricity

Transportation

Critical manufacturing

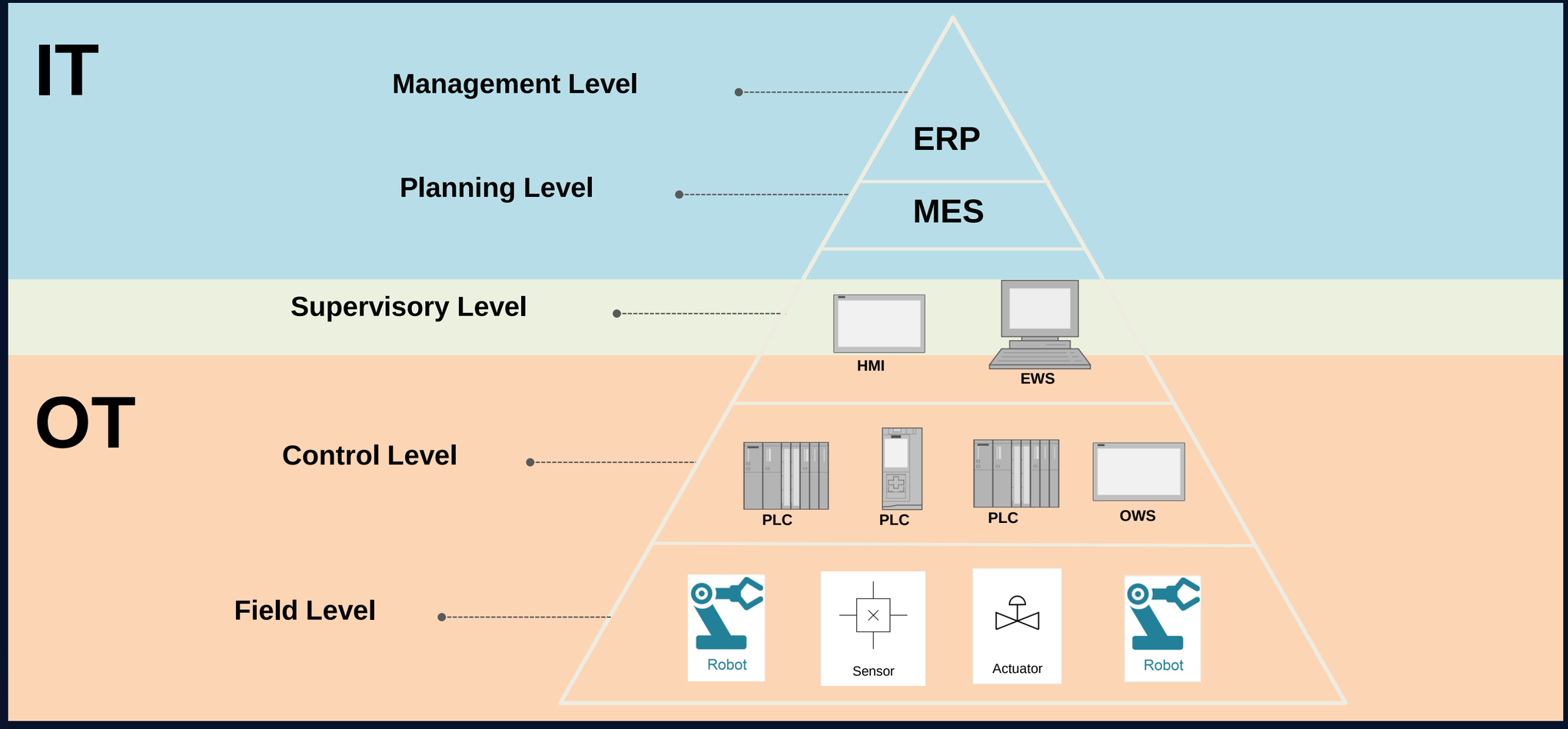
Industrial Automation

Oil & Gas

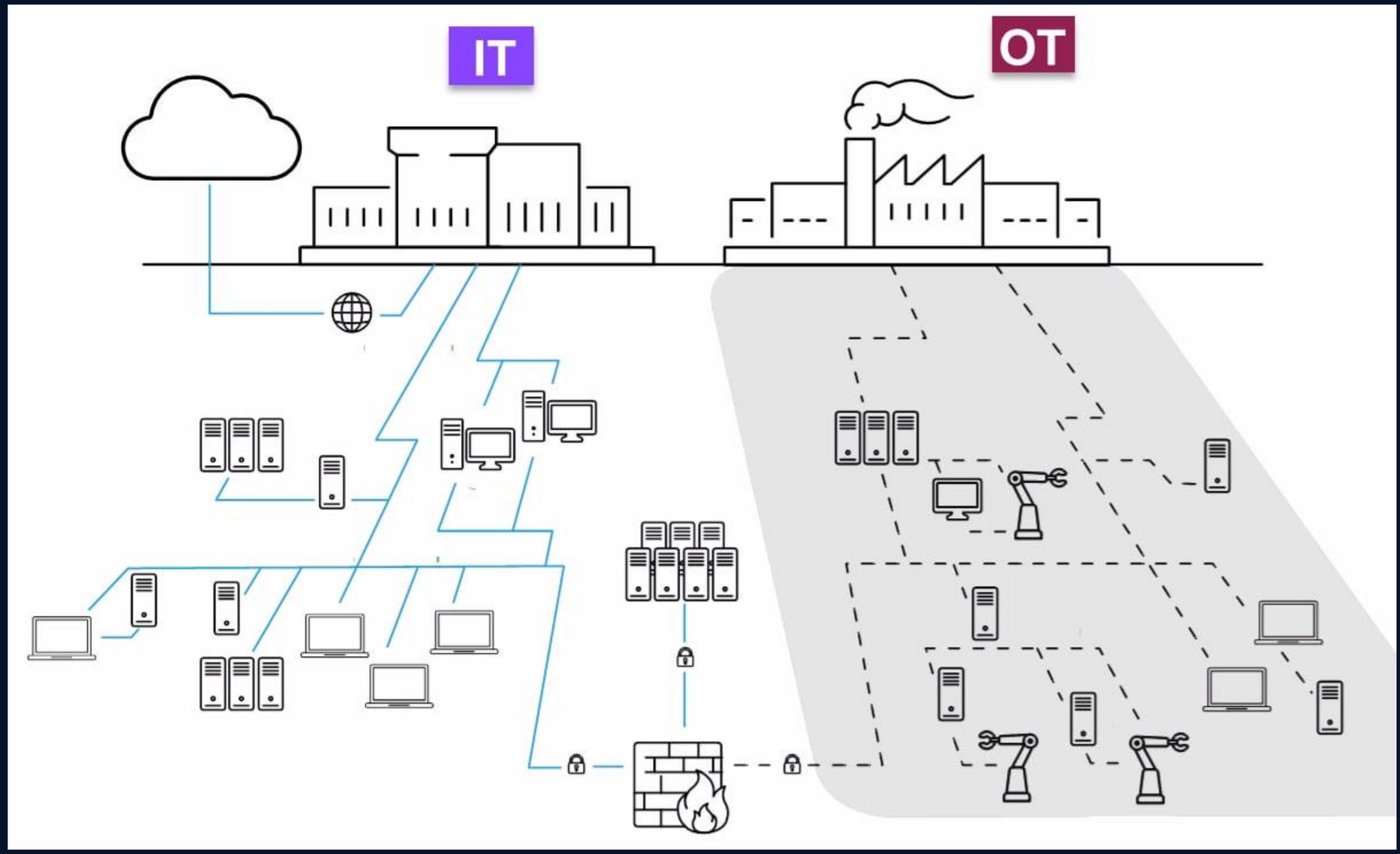
Building Management

All around Us !!

Automation Pyramid



Same challenges of IT Professionals



OT Diversity

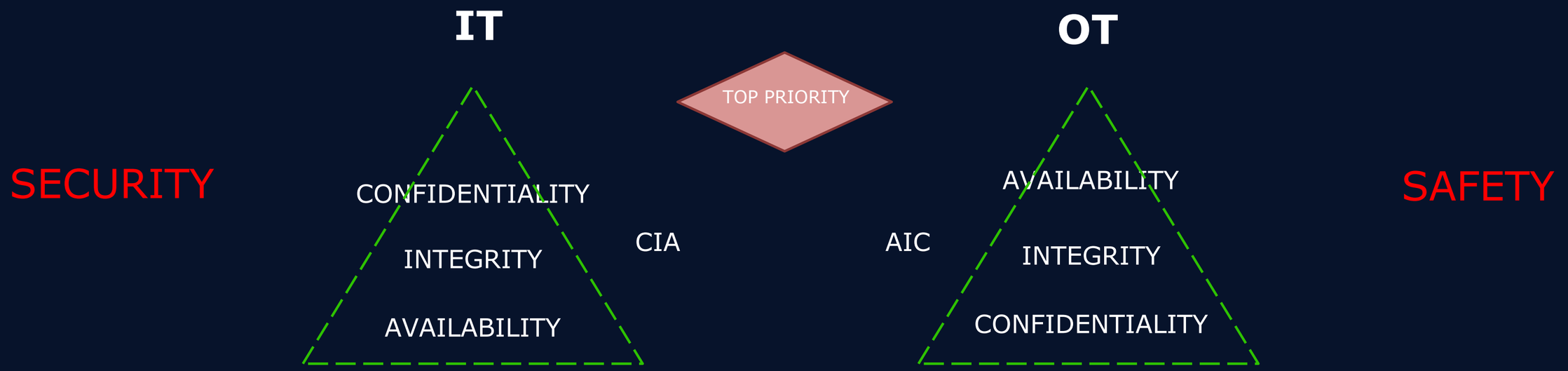
Industry Vendors

Industrial Protocols

ABB PGP2PGP, Aspentech Cim/IO, BACNet, Beckhoff ADS, BSAP IP, CC-LINK IE, CEI 79-5/2-3, COTP, DNP3, Emerson DeltaV, Enron Modbus, EtherCAT, EtherNet/IP - CIP, Foundation Fieldbus, Foxboro IA, Generic MMS, GE EGD, GE iFix2iFix, GE SRTP, GOOSE, Honeywell Experion protocols, Kongsberg Net/IO, IEC 60870-5-7 (IEC 62351-3 + IEC 62351-5), IEC 60870-5-104, IEC-61850 (MMS, GOOSE, SV), IEC DLMS/COSEM, ICCP, Modbus/RTU, Modbus/TCP, Modbus/TCP - Schneider Unity extensions, MQTT, OPC, PCCC, PI-Connect, Profinet/DCP, Profinet/I-O CM, Profinet/RT, ROC, Sercos III, Siemens S7, S7 Plus, Telvent OASyS DNA, Triconex TSAA, Vnet/IP

Standards Development Organization

How are IT and OT different ?



Characteristics
Security objective priorities

Medium, delays accepted	Availability requirement	Very High
Delays accepted	Real-time requirement	Critical
3-5 years	Component lifetime	Up to and 20 years
Regular / Scheduled	Application of patches	Slow / infrequent
Scheduled and mandated	Security testing / Audit	Occasional
High / mature	Security awareness	Increasing

Operation Profile

Asset Owner

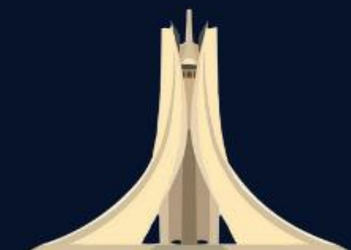
- Responsible on the IACS Environment
- Operate IACS, equipment under control

Product Supplier

- Manufacture, Develop and Support IACS hardware & Software problems

Service Provider

- Integrate, Maintain and Concept
- Analyze, Install, Configure and Test



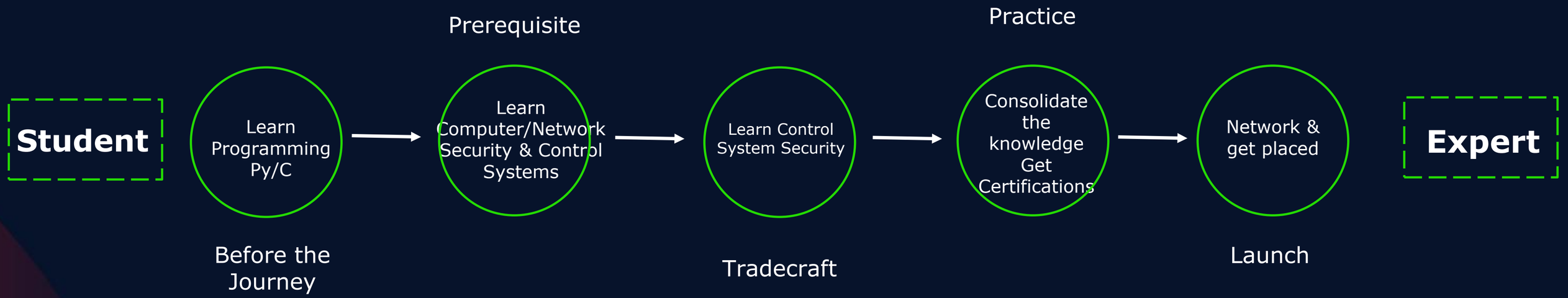
Career option in OT Security

Career Evolution

Manufacturing	Research/Product Development	Advisor/Consulting	OT Certifications
CISO	Head of OT Technology	IT/OT Sr Manager	CISSP CISM / COSM ICS410 GICSP ICS515 GRID ICS610
Head of OT Cybersecurity Operations	Head of OT Research	IT/OT Sr Consultant	
OT Cybersecurity Engineer	OT Architect	OT Risk Specialist	ISA/IEC 62443 Expert COSP ISA/IEC 62443 Maintenance Specialist ISA/IEC 62443 Design specialist ISA/IEC 62443 Risk Assessment Specialist
OT Cybersecurity Maintenance Specialist	OT Architect/Expert	OT Consultant	
OT System Analyst	OT Researcher	OT Analyst	ISA/IEC 62443 Fundamental Specialist

OWASP ALGIERS

OT Security: Zero to **Hero**



Transition to OT Security

From OT (Industrial) Background

OT Security

1. Build a strong foundation in cybersecurity
   - Cybersecurity principles, practices, and technologies
   - Network security, security architecture, Cryptography and risk management
2. Gain hands-on experience OT Security
   - Network security, security architecture and risk management
3. Pursue relevant certifications

From IT Security Background

OT Security

1. Build a strong foundation in Operational Security
   - System Architecture, Network Architecture
   - Communication Protocols (Modbus, DNP3, Profibus Ethernet/IP etc.,)
2. Gain hands-on experience OT Security
   - Network security, security architecture and risk management
3. Pursue relevant certifications

OWASP ALGIERS

Platform to practice

ControlThings.io

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

https://www.cisa.gov/ics-training-available-through-cisa

https://github.com/dark-lbp/isf

https://github.com/nsacyber/ELITEWOLF

CSET®
CYBER SECURITY EVALUATION TOOL

FORTIPHYD LOGIC GRFICSv2

https://github.com/Fortiphyd/GRFICSv2

Training Game
FACILITY CYBERSECURITY

https://facilitycyber.labworks.org/training/trainingGame/landing

IAAE®
International Academy of Automation Engineering®

Low-cost ICS Testbed
https://github.com/thainnos/LICSTER

opendnp3

https://dnp3.github.io/

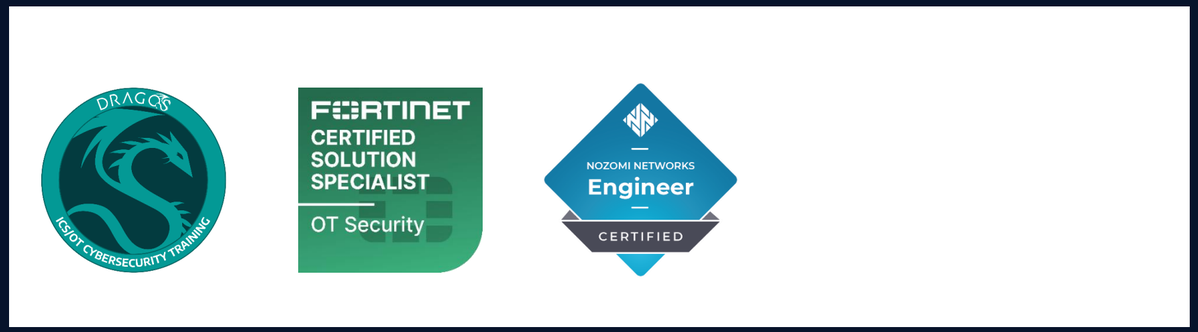
Try Hack Me
Attacking ICS Plant

OWASP ALGIERS

Learning & Certifications

OT Security Certifications

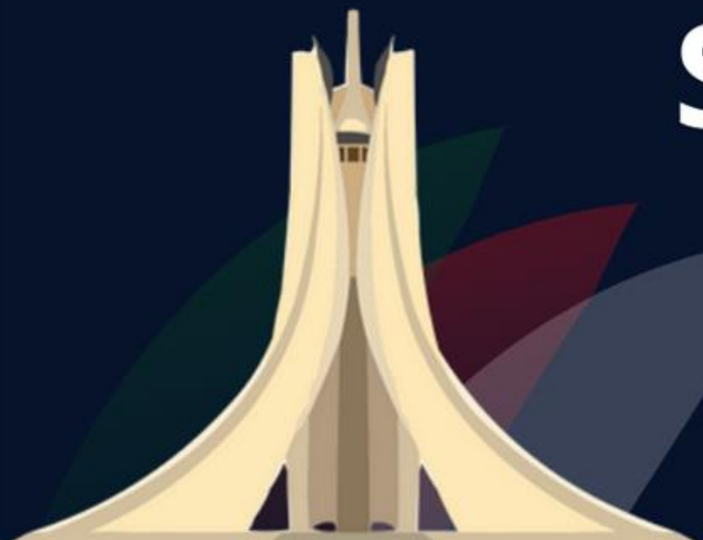
Vendors Trainings



ISA/IEC 62443 Standard Certifications

OWASP ALGIERS

SPEAKER



Taher Amine ELHOUARI

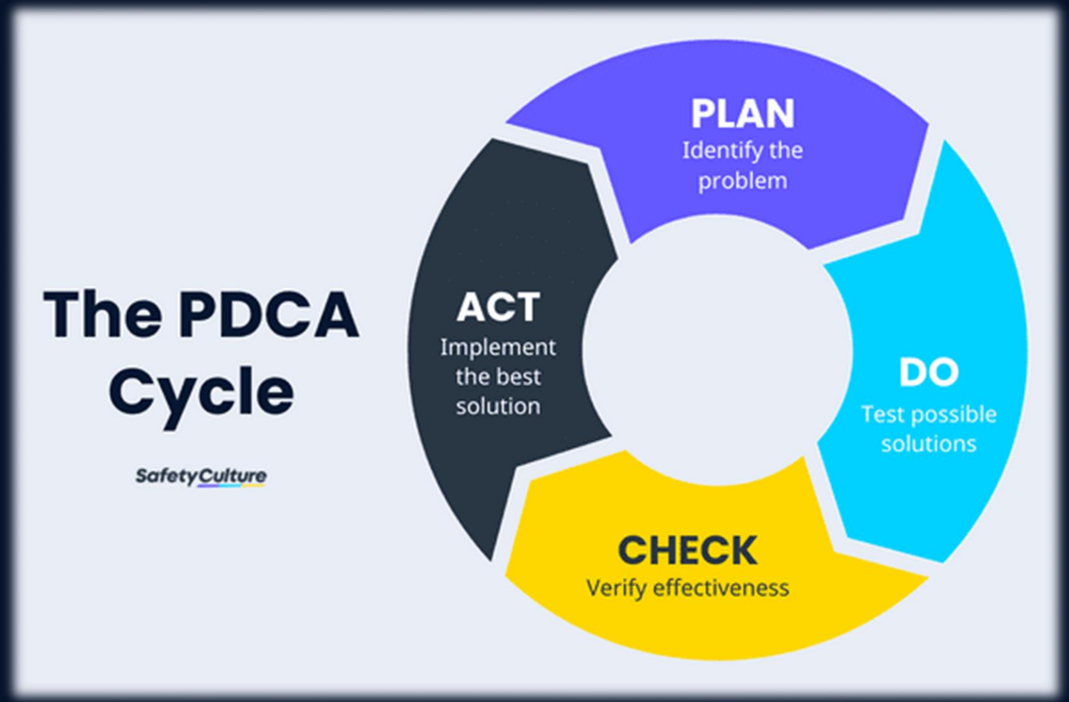
CyberSecurity Leader & Global Consultant

- Founder & President @ OWASP Algiers Chapter
- Global Member @ OWASP Foundation
- Founding Board Member @ ISC2 ElDjazair Chapter
- Global Member @ ISC2
- CyberSecurity Instructor @ GoMyCode
- Global CyberSecurity Advisor @ AlphaSights
- CyberSecurity Ambassador @ Cyber Cohesion
- Independent Consultant & Instructor
- CISSP, Mini-MBA, CC, ISO27001, CEHv12, CCSP/AWS, CNPen, CAP, CNSP, CNSS, CPTAv2, C3SA, ACE/MCNA, QCS/VMDR, CCNA..

Intro to GRC

What is GRC?

- GRC stands for Governance, Risk, and Compliance. It's a program that organizations use to manage and align their strategies, policies, and regulations to achieve business objectives while addressing risks and ensuring compliance with laws, regulations, and standards.



What is Governance?

- Governance refers to the overall management structure and processes within an organization. It involves defining roles, responsibilities, and decision-making processes to ensure that objectives are achieved efficiently and effectively.

- It focuses on establishing oversight mechanisms and accountability structures to ensure that the organization's activities align with its strategic goals and values.

- Governance frameworks often include elements such as corporate governance, IT governance, and data governance to ensure that resources are managed responsibly and ethically.

What is Risk Management?

- Risk management involves identifying, assessing, and mitigating risks that could impact the achievement of organizational objectives. Risks can arise from various sources, including strategic, operational, financial, and compliance-related factors.

- In the GRC framework, risk management aims to proactively identify and evaluate potential threats and vulnerabilities to the organization's assets, including data, systems, and processes.

- Risk management processes typically involve risk assessment, risk treatment, and risk monitoring to ensure that risks are effectively managed and controlled within acceptable levels.

What is Compliance?

- Compliance refers to the adherence to laws, regulations, standards, and internal policies relevant to the organization's operations and industry.
- In the GRC context, compliance activities focus on ensuring that the organization complies with applicable legal and regulatory requirements, as well as internal policies and standards.
- Compliance efforts typically involve conducting regular audits, assessments, and reviews to verify adherence to relevant requirements and to identify areas for improvement.
- Compliance with GRC standards helps organizations mitigate legal and regulatory risks, enhance trust and confidence among stakeholders, and promote a culture of integrity and accountability.

Standards, Laws, and Regulations:

- Standards are established guidelines or frameworks developed by recognized authorities or organizations to define best practices or requirements in specific areas. They provide guidance on how organizations can achieve certain objectives or meet specific criteria related to governance, risk management, and compliance.

- Laws are legal statutes enacted by legislative bodies, such as governments or regulatory agencies, that mandate specific behaviors or actions and may impose penalties for non-compliance. They are legally binding and enforceable, and organizations must comply with them to avoid legal consequences.

- Regulations are rules or requirements issued by government agencies or regulatory bodies to implement and enforce laws within specific industries or sectors. They provide detailed guidance on how organizations must comply with legal requirements and may include specific technical standards, reporting obligations, or procedural requirements.

Standards, Laws, and Regulations:

- Government agencies in different nations take different approaches to cybersecurity laws and regulations. The laws of different nations may be structured to result in very dissimilar styles of regulation.

- No country has the perfect solution to the challenge of how best to regulate cybersecurity—this is an area where learning from the variety of approaches around the world can be instructive.

- The word “standards” actually has multiple meanings in the cybersecurity domain. Besides “best practice” standards (such as ISO/IEC 27000), there are “technical standards,” such as IEEE 802.11, which defines wireless protocols used on Wi-Fi networks. A third meaning for “standards” refers to the rules that an organization might develop and enforce internally. (e.g., how often employees need to change their passwords.) All meanings are correct, and the intended meaning is usually apparent from the context (Harris and Maymi 2016).

Standards, Laws, and Regulations:

- In summary, standards are voluntary guidelines or frameworks, laws are legal statutes enacted by legislative bodies, and regulations are rules issued by regulatory agencies to implement and enforce laws.

- While organizations may voluntarily adopt standards to improve practices, compliance with laws and regulations is mandatory and carries legal implications for non-compliance.

- GRC programs aim to ensure that organizations effectively navigate and comply with relevant standards, laws, and regulations to manage risks and achieve their objectives.

Goals and Importance:

- Laws and regulations provide incentives for utilities to adopt effective cybersecurity measures. This motivation may include incentives for strengthening cybersecurity or repercussions for failing to do so.

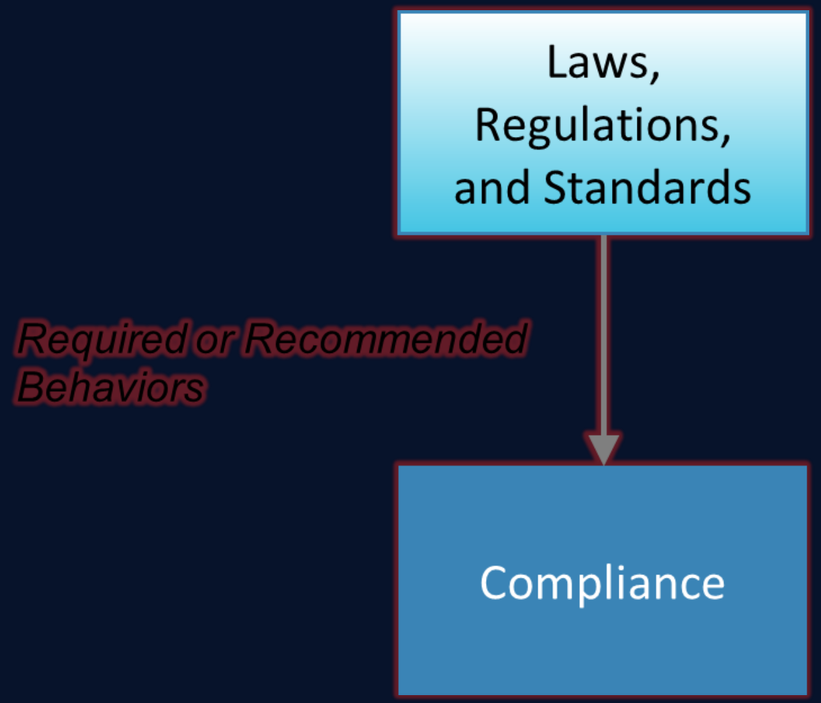
- A well-structured regulation will balance the cybersecurity benefit of compliance against the cost to the utility. However, creating a “well-structured” regulation can be tricky, and the consequence of getting it wrong can be dire. A poorly structured regulation could force utilities to expend their resources on compliance with little actual cybersecurity benefit.

- This could result in an electric grid that is even less secure than if no regulation had been implemented. In other words, the organization might have achieved more effective cybersecurity if it had invested its resources as it saw fit, rather than spending to comply with poorly structured regulations. Internationally recognized standards are valuable because the best practices they embody go through an extensive vetting process. They also provide a “common language” for security professionals.

Compliance:

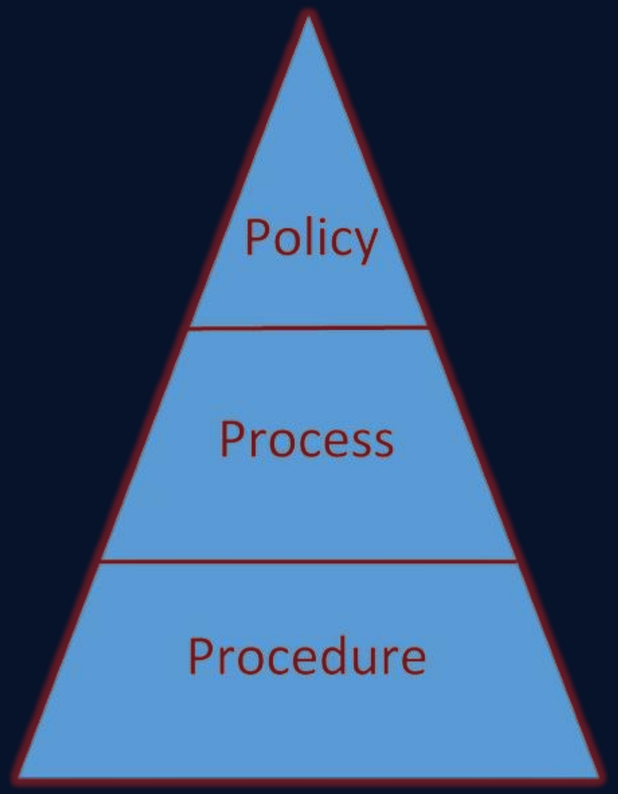
- Laws and regulations are implemented by governments to define required behaviors. Standards may be implemented by many types of organizations (including international standards bodies) and define recommended behaviors.

- The compliance effort within the utility strives to interpret and enact those behaviors, as well as document the utility's adherence to the regulations and standards.

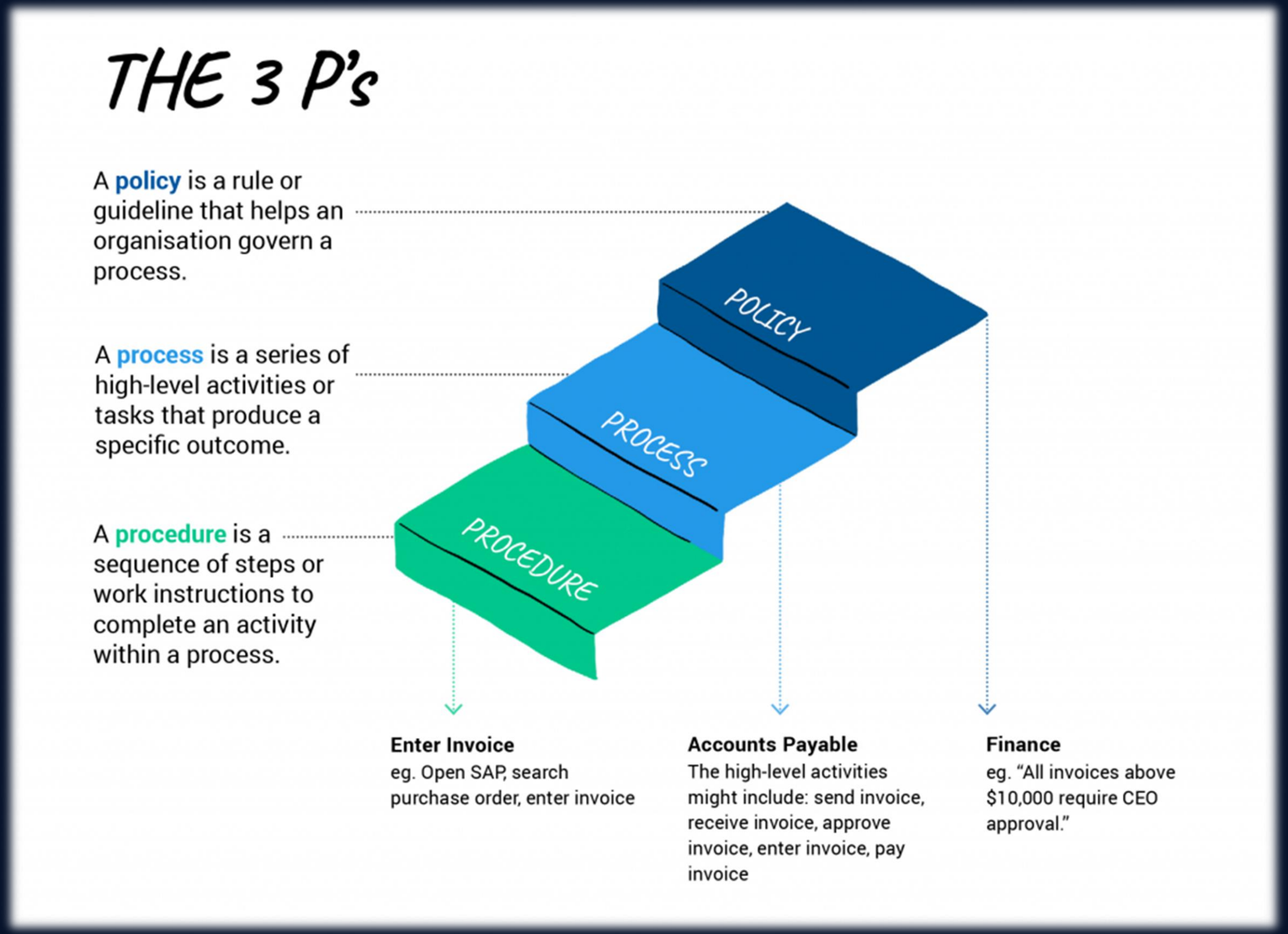


Policy, Process, and Procedure:

- In the context of Governance, Risk, and Compliance (GRC), policies, procedures, and processes are distinct but interconnected components that help organizations establish and maintain effective governance structures, manage risks, and ensure compliance with relevant laws and regulations:



The Triple P / 3Ps:

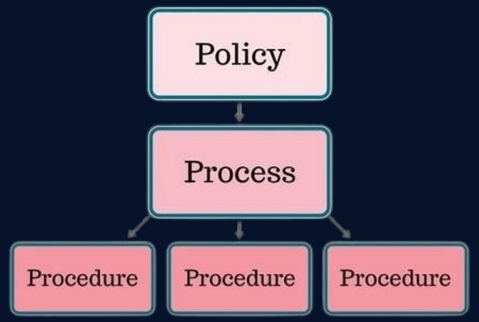


Policy, Process, and Procedure:

- A policy is a high-level statement or directive that outlines the organization's objectives, principles, or rules governing a particular area of activity. Policies set the overall direction and framework for decision-making and behavior within the organization.

- A procedure is a detailed set of steps or instructions that outline how a specific task or activity should be performed to achieve a desired outcome. Procedures provide a systematic approach for carrying out tasks consistently and efficiently.

- A process is a series of interrelated activities or tasks that work together to achieve a specific objective or deliver a particular outcome. Processes represent the end-to-end flow of activities within an organization, from initiation to completion.



Examples:

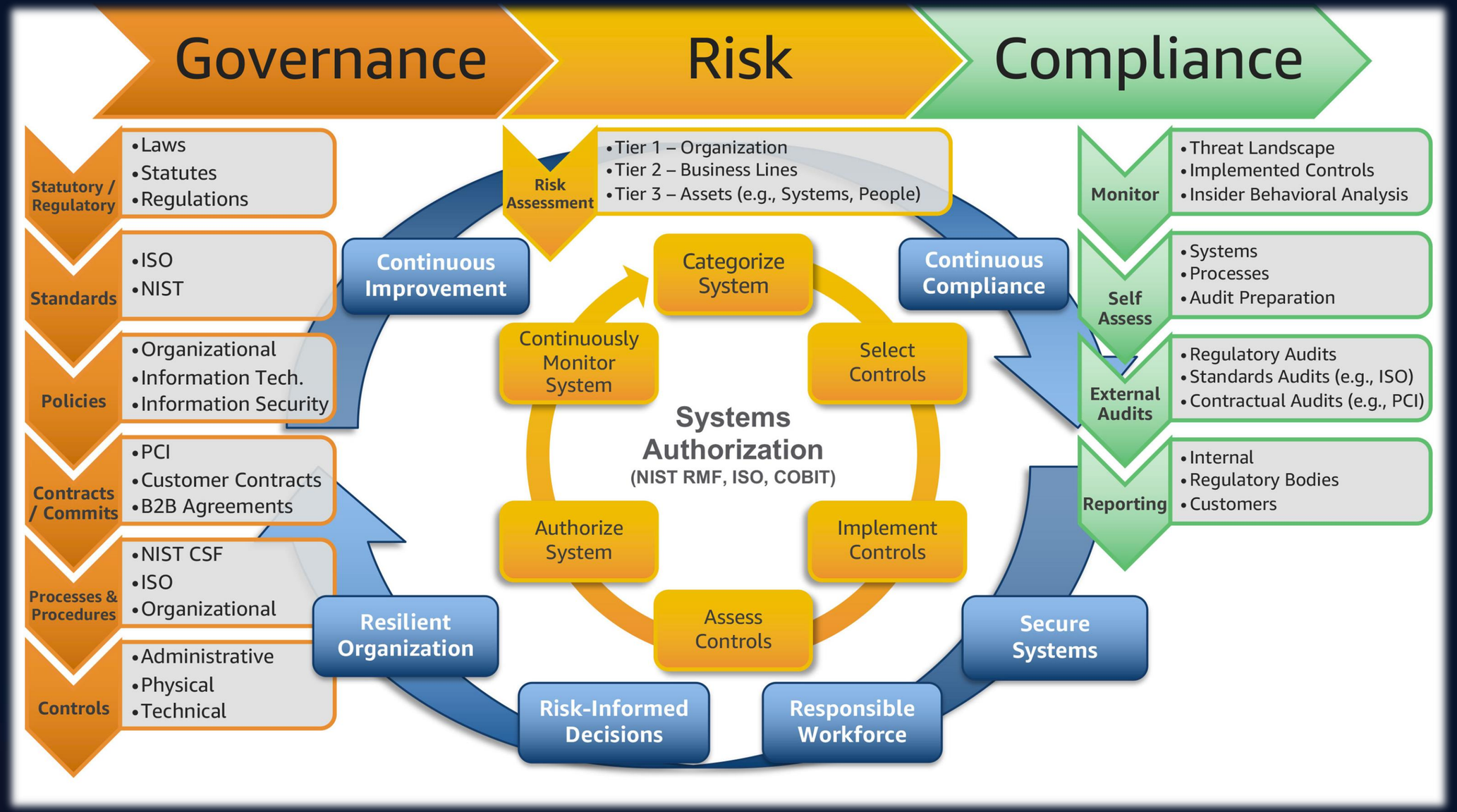
- Information Security Policy: outlining the organization's commitment to protecting sensitive information and defining responsibilities for information security management.
- Risk Management Process: outlining the systematic approach for identifying, assessing, mitigating, and monitoring risks across the organization.
- Incident Response Procedure: detailing the steps to be followed in the event of a security incident, including reporting, assessment, containment, and remediation.

Information Security Policy

Policy, Process, and Procedure:

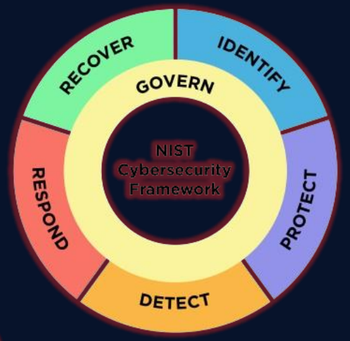
- In summary, policies provide high-level guidance and principles, procedures offer detailed instructions for performing specific tasks, and processes define the overall flow of activities to achieve organizational objectives.
- While policies set the direction, procedures provide the "how-to" guidance, and processes outline the sequence and coordination of activities to accomplish desired outcomes.
- Together, they form the foundation of effective GRC programs, ensuring that organizations establish clear expectations, implement consistent practices, and achieve compliance with relevant standards, laws, and regulations.

Governance, Risk, and Compliance:



Most Common Standards & Regulations:

- Several standards, laws, and regulations are prominent in the realm of Governance, Risk, and Compliance (GRC). Here are some of the most famous ones:



Intro to Blue Teams & Defensive Security (SOC)

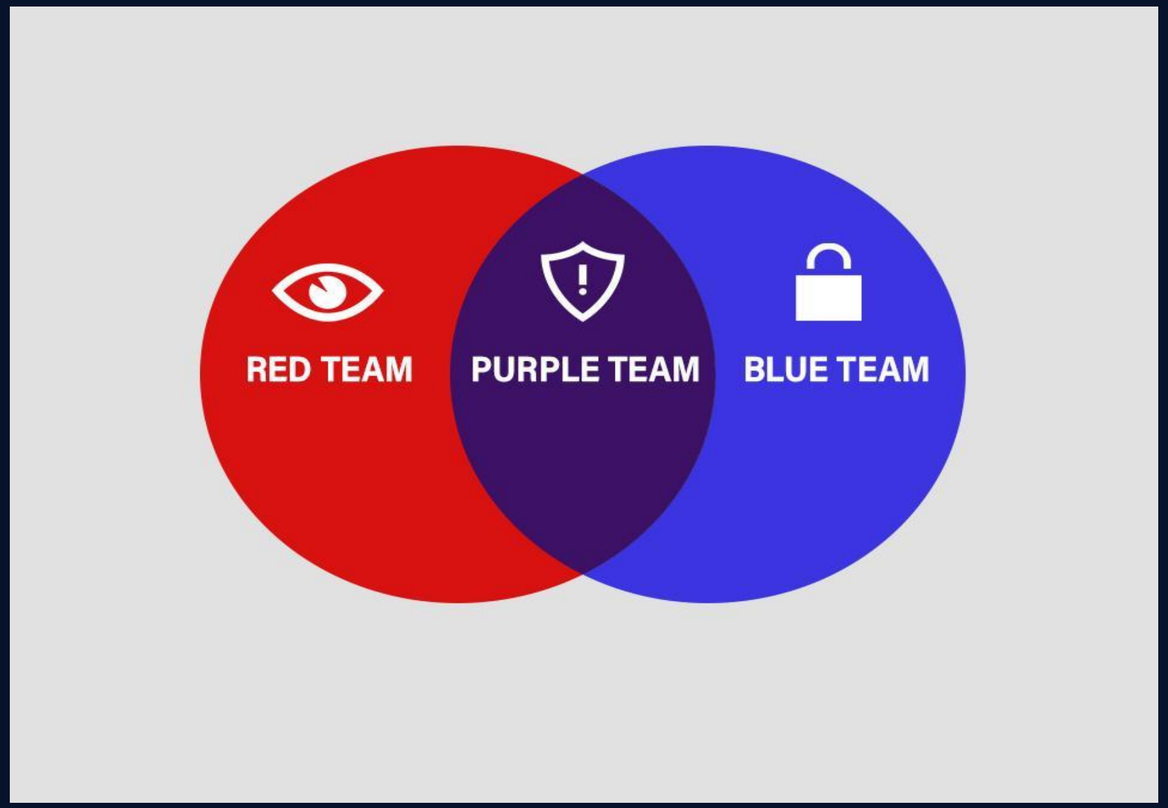
Blue Team and Cyber Defense

1. Blue Team
2. Security Engineering
3. Security operations center
4. SOC Manager
5. SOC Analysts
6. Most Famous Blue Team specialities
6.1. Digital Forensics and Incident Response (DFIR)
6.2. Threat Hunting
6.3. Malware Analysis and Reverse Engineering
6.4. Threat Intelligence
7. Blue Team training platforms

Blue Team and Cyber Defense

1. Blue Team

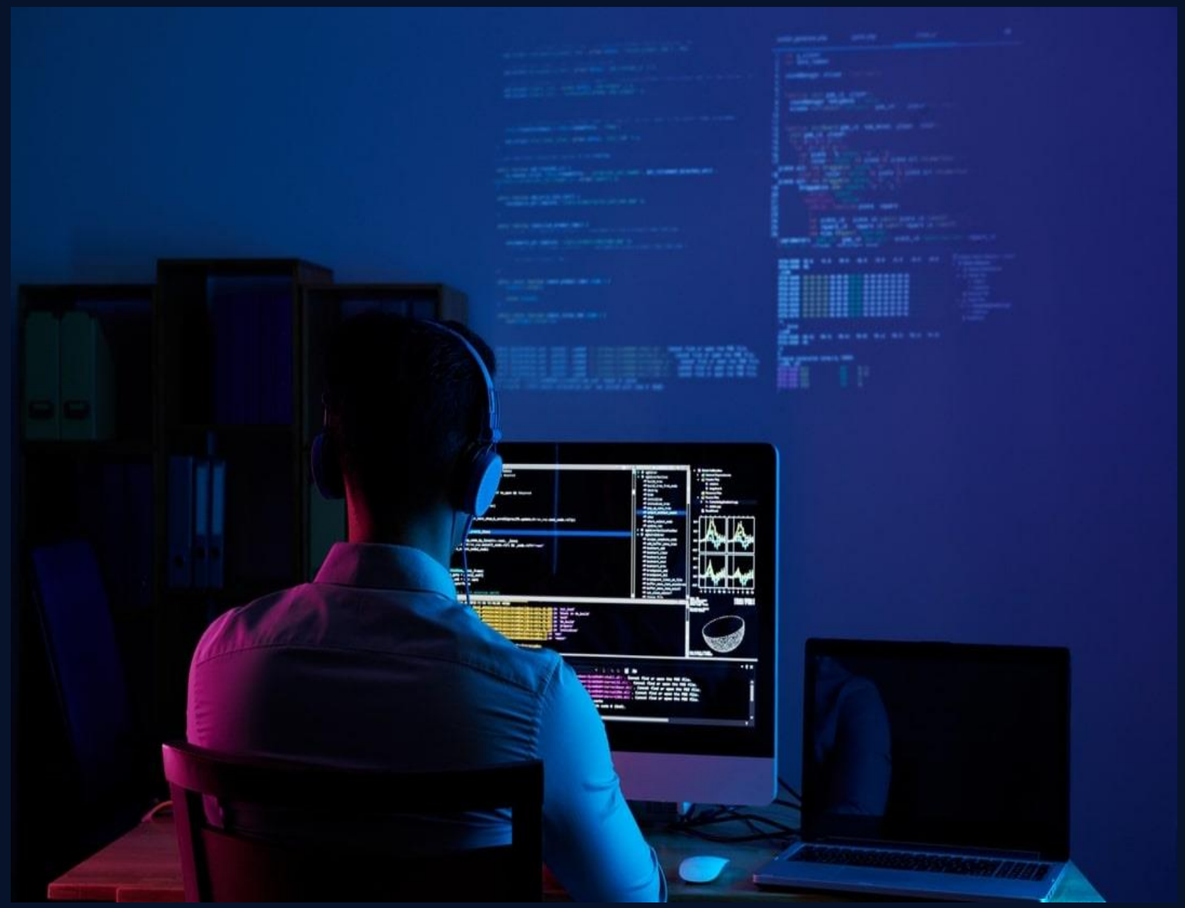
The group responsible for defending an enterprise's use of information systems by maintaining its security posture against a group of mock attackers.



Blue Team and Cyber Defense

2. Security Engineer

A security engineer is responsible for safeguarding an organization's information technology infrastructure and data from potential threats, vulnerabilities, and cyberattacks. These engineers play an important role in the design, implementation, and maintenance of security measures to protect sensitive information and ensure the integrity, confidentiality, and availability of systems.



Blue Team and Cyber Defense

3. Security operations center (SOC)

A security operations center (SOC) is a command center facility in which a team of information technology (IT) professionals with expertise in information security (infosec) monitors, analyzes and protects an organization from cyber attacks.

Blue Team and Cyber Defense

4. SOC Manager

A SOC manager leads the security operations team and reports to the chief information security officer (CISO).

Blue Team and Cyber Defense

They supervise the team, provide technical guidance and manage activities in the following ways:

- Oversees hiring, training and evaluating SOC staff
- Creates processes
- Assesses incident reports
- Develops and implements crisis communication plans
- Creates compliance reports
- Supports audits
- Measures SOC performance metrics
- Reports on security operations to executive management

Blue Team and Cyber Defense

5. SOC Analyst

An SOC analyst is a person who works on a team to monitor, analyze, and respond to security issues. The main goal of SOC analysts is to prevent attacks on a network. They monitor the network for signs of an attack. Once an attack has been detected, they investigate it with other team members.

Blue Team and Cyber Defense

5. SOC Analysts Levels

5.1 SOC L1: The Level 1 analysts within a SOC are typically entry-level staff responsible for handling the initial triage and response to security alerts and incidents. Their main duties may include: Monitoring, Alert Triage, Initial Investigation, Escalation, Documentation, Adherence to Procedures.

Blue Team and Cyber Defense

5. SOC Analysts Levels

5.2 SOC L2: SOC Level 2 analysts are responsible for conducting in-depth analysis and investigation of security incidents escalated from Level 1 analysts. This involves: Incident Analysis and Investigation, Advanced Threat Hunting, Incident Response Coordination, Tool and Process Improvement, Training and Mentorship.

Blue Team and Cyber Defense

5. SOC Analysts Levels

5.3 SOC L3: SOC Level 3 analysts are responsible for leading and coordinating the response to the most complex and critical security incidents. This includes: Advanced Incident Response, Threat Intelligence Analysis, Security Architecture and Design, Incident Forensics and Analysis, Research and Innovation.

Blue Team and Cyber Defense

6. Most Famous Blue Team specialities

6.1. Digital Forensics and Incident Response (DFIR)

Digital Forensics and Incident Response (DFIR) is a field within cybersecurity that focuses on the identification,
investigation, and remediation of cyberattacks. **CROWDSTRIKE**

Blue Team and Cyber Defense

6.1. Digital Forensics and Incident Response (DFIR)

DFIR has two main components:

Digital Forensics: A subset of forensic science that examines system data, user activity, and other pieces of digital evidence to determine if an attack is in progress and who may be behind the activity.

Incident Response: The overarching process that an organization will follow in order to prepare for, detect, contain, and recover from a data breach. **CROWDSTRIKE**

Blue Team and Cyber Defense

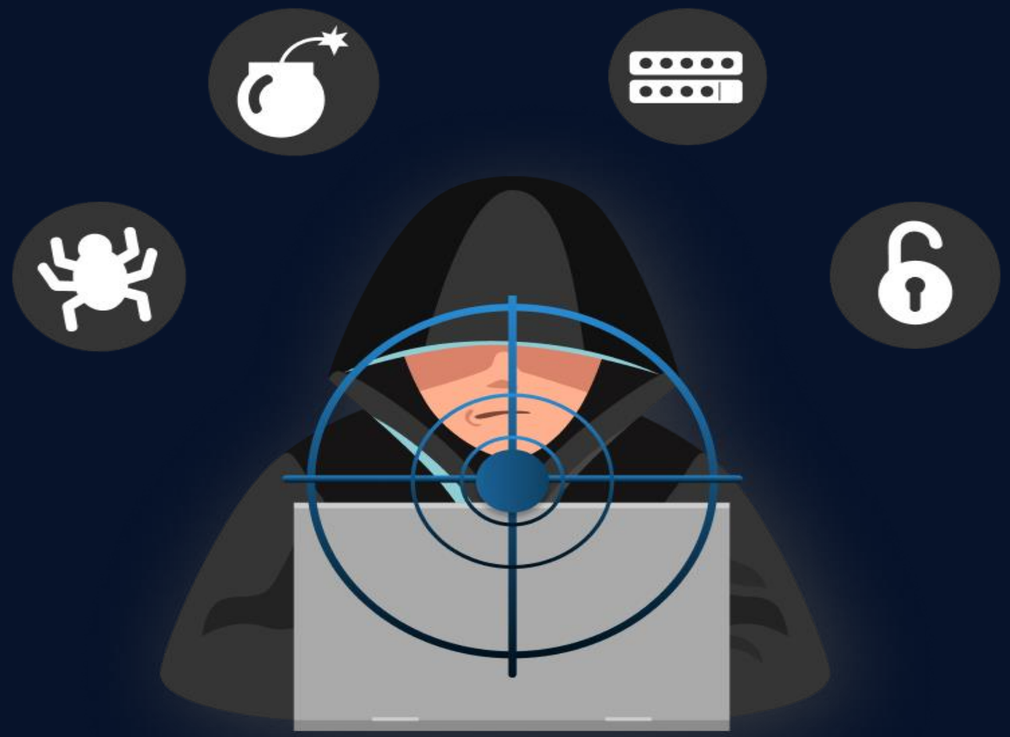
6.1. Digital Forensics and Incident Response (DFIR) Certifications

- CFHI Certified Forensic Hacking Investigator **EC-Council**
- GCFA Certified Forensic Analyst **GIAC**
- GCIH Certified Incident Handler **GIAC**
- ECIH Certified Incident Handler **EC-Council**
- eCIR Incident Responder **INE eLearnSecurity**

Blue Team and Cyber Defense

6.2. Threat Hunting

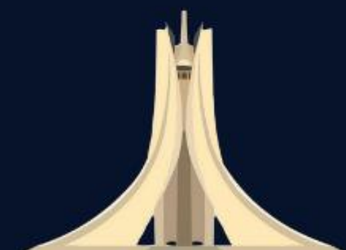
Threat hunting is the practice of proactively searching for cyber threats that are lurking undetected in a network. Cyber threat hunting digs deep to find malicious actors in your environment that have slipped past your initial endpoint security defenses. **CROWDSTRIKE**



Blue Team and Cyber Defense

6.2. Threat Hunting Certifications

- eCTHP Threat Hunting Professional **INE**
- Practical Threat Hunting **MANDIANT**



Blue Team and Cyber Defense

6.3. Malware Analysis and Reverse Engineering

Malware analysis is the study of the unique features, objectives, sources, and potential effects of harmful software and code, such as spyware, viruses, malvertising, and ransomware. It analyzes malware code to understand how it varies from other kinds. **FORTINET**

Blue Team and Cyber Defense

6.3. Malware Analysis and Reverse Engineering Certifications

- GREM Reverse Engineering Malware Certification **GIAC**
- Malware Analysis Professional **INE**

Blue Team and Cyber Defense

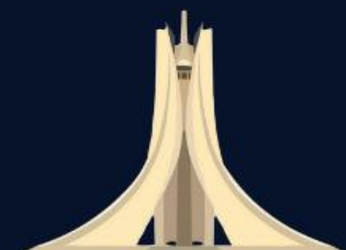
6.4. Threat Intelligence

“Threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications, and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject’s response to that menace or hazard.” **Gartner**

Blue Team and Cyber Defense

6.4. Threat Intelligence Certifications

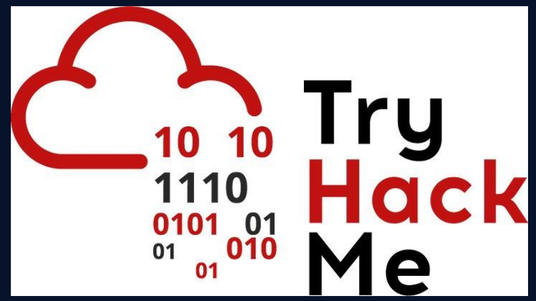
- CTIA Threat Intelligence Analyst **EC-Council**
- GCTI Cyber Threat Intelligence **GIAC**



Blue Team and Cyber Defense

7. Blue Team training platforms

- TryHackMe
- Hack The Box
- Cyberdefenders
- Letsdefend



Intro to Red Teams & Offensive Security (VAPT)

OWASP ALGIERS

SPEAKER

Hichem Belguendouz

Cyber Security Enthusiast

- Board Member @ OWASP Algiers Chapter
- Network Security Professional

Red Team

Agenda :

1- Intro to Vulnerability Assessment, Penetration Testing, Red Teaming, Bug Bounty

2- VA vs VAPT and VAPT vs Bug Bounty

3- Difference Between Red Teaming and Penetration testing

4- Learning Approach and Certifications

5- Platform to Practice and other Resources

What is Offensive Security or Red Team

- **Red Team** consist of Security Professionals Who act as adversaries to overcome Security Controls
- The Red Team in general are **Offensive Security Team** their role is doing **ProActive** Assessement on the People Process and Technology
- They Utilize all the available Techniques to find Weaknesses in PEOPLE, Process and Technology
- As a result of these Simulated Attacks they make recommendations and plans on how to strenghten and **organisation Security Posture**

What is Vulnerability Assessor

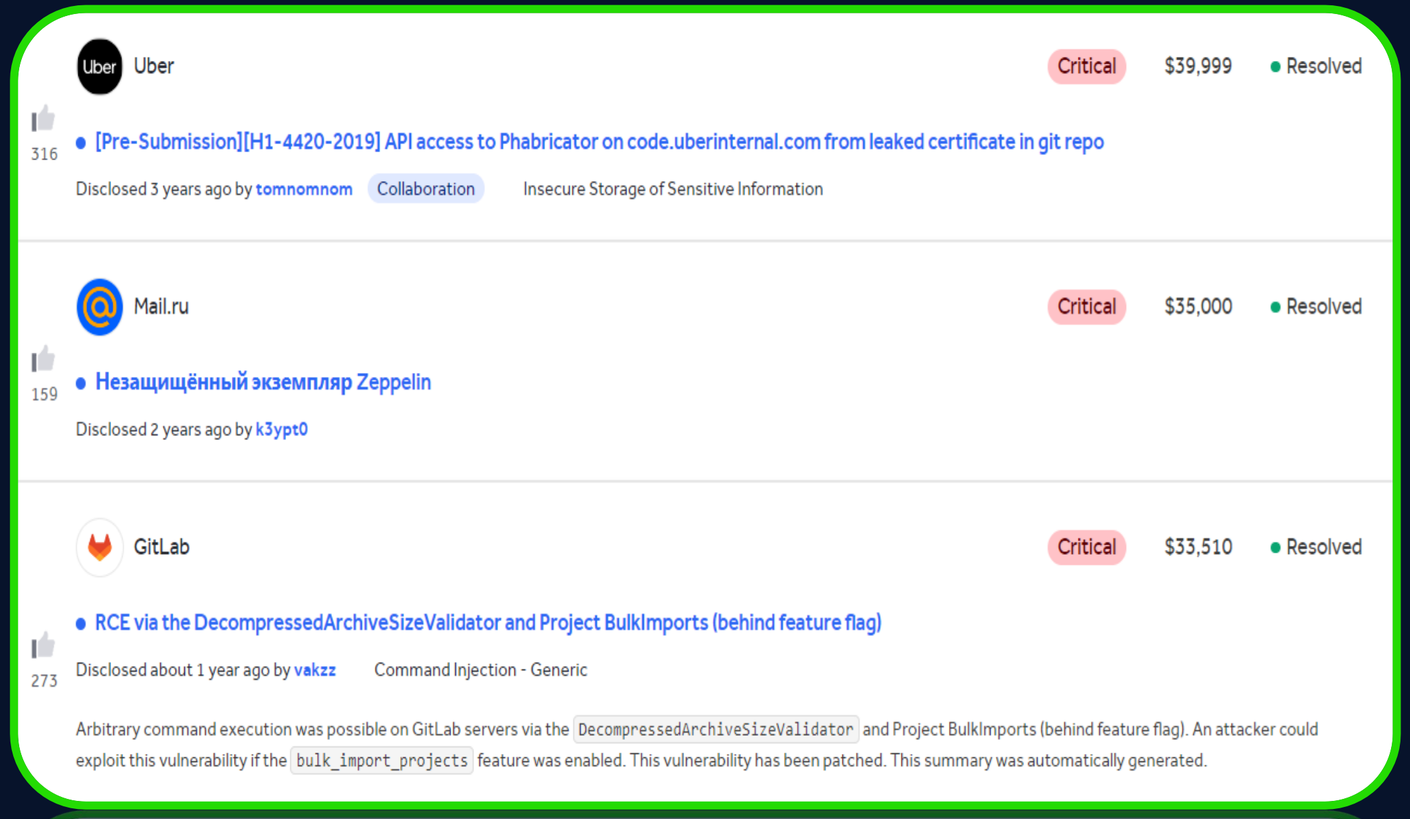
- **Vulnerability assessors** test for security flaws in systems before attackers do.
- They generally perform tasks on computers and networks to determine if they have any **exploitable weaknesses**.
- Vulnerability assessors work with IT Team and other cybersecurity professionals to help maintain data safety.
- They analyze the organization’s cyber defense policies and configurations to evaluate compliance with these **Regulations and Best Practices**.

OWASP ALGIERS

What is Bug Bounty Hunter

Bug Bounty Hunting is the Process of Indentifying and Reporting Vulnerabilities in a company defined Scope of Assets, for which you get **Rewarded**

Vulnerability Responsible Disclosure Program is a proactive approach taken by organizations to encourage security researchers, report potential vulnerabilities they discover in the organization's systems .



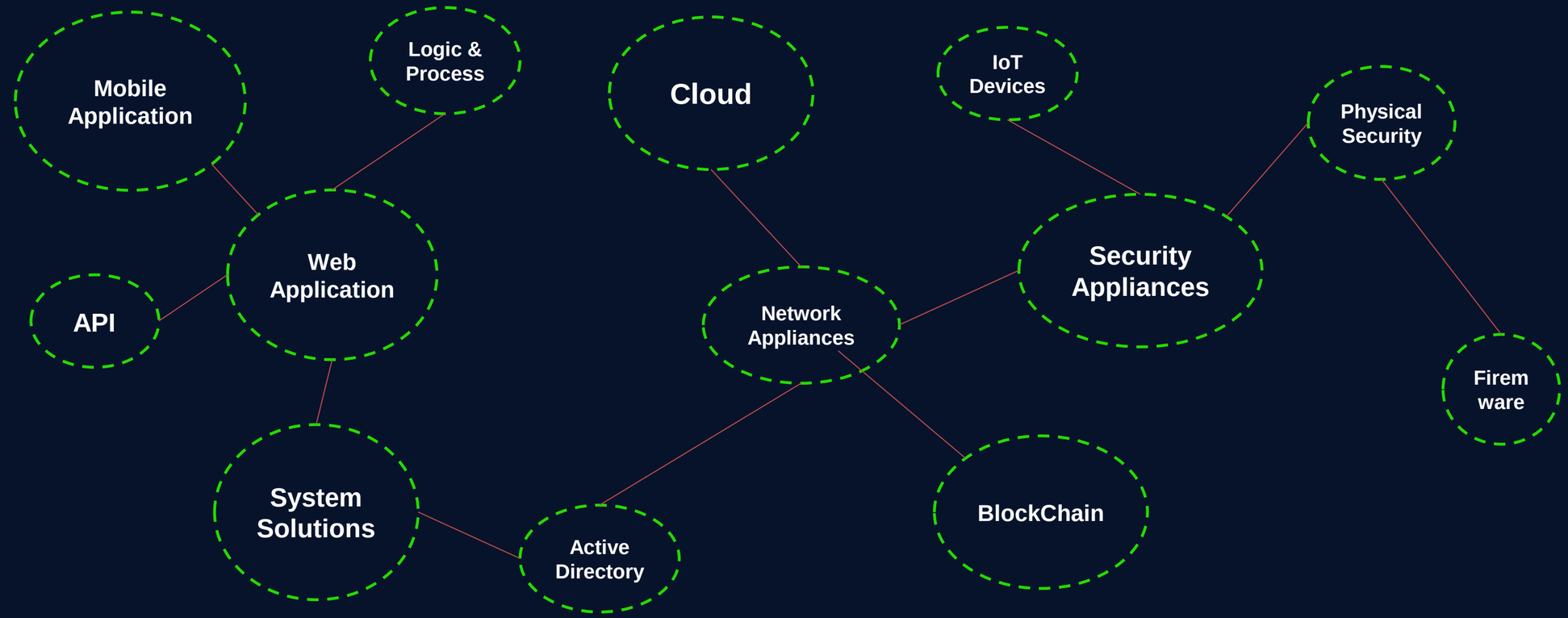
OWASP ALGIERS

What is Pentration testing

- **Penetration testing** is a Security Exercise where a Cyber-Security Expert Attempt to find and Exploit Vulnerabilitities is defined Scope of System
- Penetration testing provides **valuable insights** into an organization's overall security posture.
- Penetration testing helps ensure that organizations meet these **regulatory requirements** and avoid potential penalties for non-compliance

OWASP ALGIERS

What Should Be Tested?



VAPT vs VA

Aspect	Vulnerability Assessent	Penetration testing
Scope	Wide	Deep Focus
Goal	Find as many vulnerabilities as possible	Exploit discovered Vulnerabilities to reach Highest Privileges
Duration	Quick to Complete, Automated	Time Consuming, Manual Work
False Positive	Are Produced, Especially when Automated	Are Manually Filtered out
Impact	Will not impact business processes	Might Disrupt Business Processes
Test Methods	Authenticated and Unauthenticated	Black/White/Grey/Crystal
Frequency	Organizational Attack Surface	Critical Assets
Costs	Cost-effective	Costly, cause of duration and skilled personnes
Report	Partial Details on the fails	Full details of vulnerability exploitation and how to mitigate

VAPT vs Bug Bounty Hunting

Aspect	Penetration Testing	Bug Bounty Hunting
Approach	Formal, contracted assessment	Informal, crowd-sourced vulnerability hunting
Scope	Typically predefined scope	Broader scope often covering entire systems
Engagement duration	Usually conducted over a fixed timeframe	Ongoing, with no set end date
Reporting	Detailed report provided at the end of testing	Continuous reporting as vulnerabilities found
Testing environment	Controlled and simulated	Real-world environment
Expertise required	Requires skilled security professionals	Open to anyone, including non-professionals
Cost	Fixed cost based on scope and duration	Bounty payouts based on severity of vulnerabilities
Confidentiality	Often involves signing NDAs	Publicly accessible platform
Ownership of findings	Owned by the contracting organization	Owned by the finder

What is Red Teaming and Adversary Emulation

- **Red Team** consist of Security Professionals Who act as adversaries to overcome Security Controls
- The Red Team are **Offensive Security Team** their role is doing **ProActive** Assessement on the People Process and Technology
- Red Teaming is a **full-scope**, Multi-Layered Attack Simulation

What is Red Teaming and Adversary Emulation(cont.)

- Red Team has a different **Philisophy** from Penetesting

- The **Most Important Challenges** for Organizations:

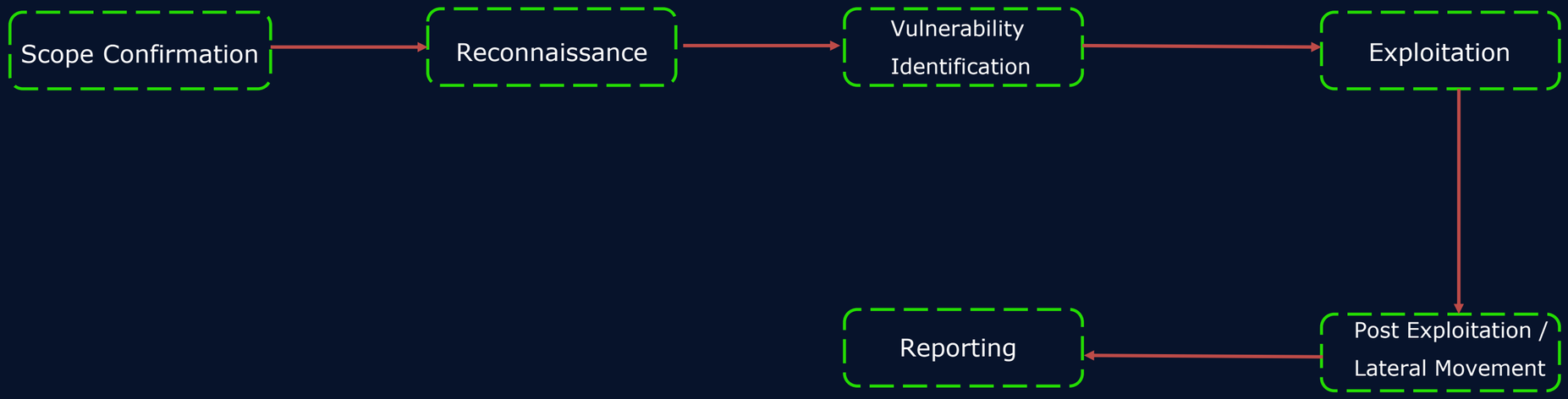
  1- How much time it takes between the Initial Compromise and Detection

  2- How long it takes from detection to Containment

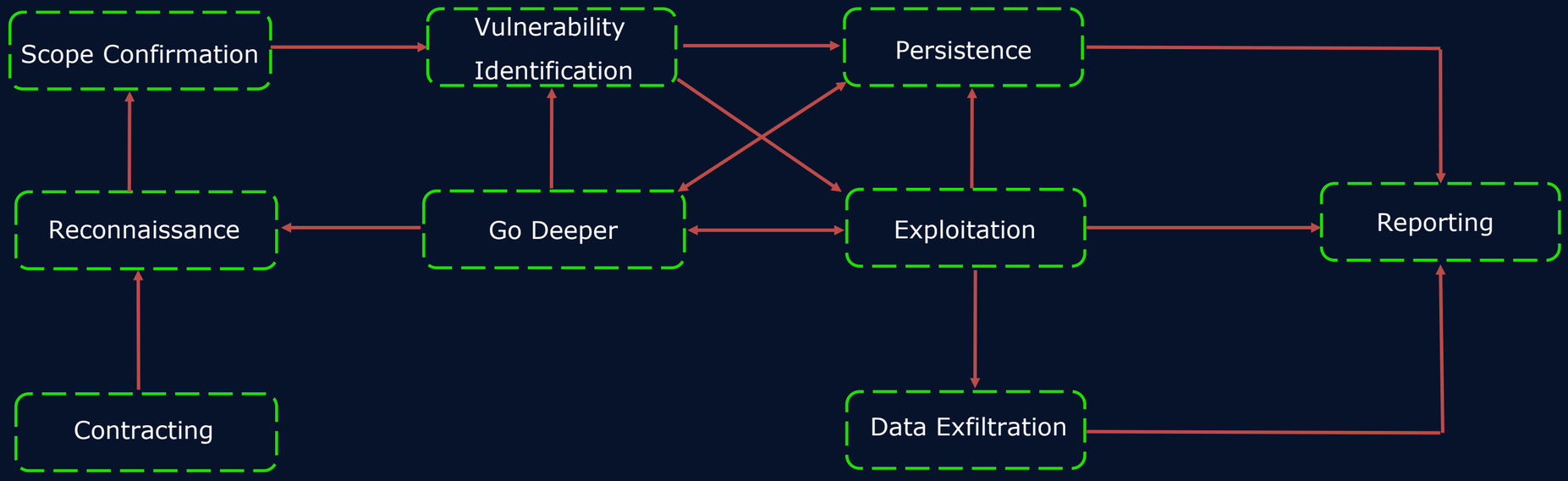
  3- How long it takes from detection to Containment

- The red Team Cover **Technology**, **People**, **Process**

Penetration testing Methodology?



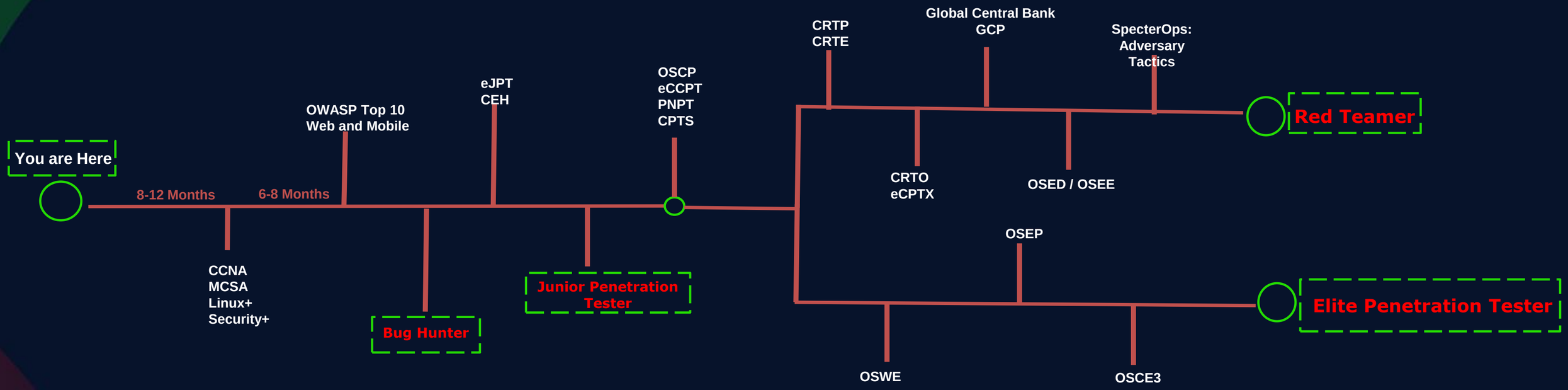
Red Team Exercices?



VAPT vs RedTeam

Actions	Pentest	RedTeam
❖ Check the ability of an organization security systems to defend againts an attack.	✅	✅
❖ Check if the entire company and its networks are prepared to withstand an advanced persistent threat (APT).	❌	✅
❖ Train the Company’s Security Team and Employees to defend against APTs.	❌	✅
❖ The Main Objective is to compromise as many systems and identify as many vulnerabilities as possible.	✅	❌
❖ Attack More than one target, Access Critical Systems, take over admin accounts, exfiltrate Document…etc.	❌	✅
❖ The Company and Security Units know about the test and do not defent againts it.	✅	❌

Offensive Security Careers ROADMAP ?



Tracks	Cloud PenTesting	BlockChain pentesting	Mobile Apps Pentesting	Web Pentesting
Certifications	**AlteredSecurity:** ○ Certified Azure Red Team Professional (CARTP) ○ Certified Azure Web Application Security Professional (CAWASP)	**Blockchain Council:** ○ Certified Blockchain Security Professional (CBSP) **SANS:** ○ SEC554: Blockchain and Smart Contract Security	**eLearnSecurity:** ○ eMAPT **SANS:** ○ SEC575: Mobile Applications Penetration testing	**eLearnSecurity:** ○ eWAPT ○ eWAPTX ○ eWDP **SANS:** ○ SEC542: Web App PT ○ SEC642: Advanced Web App PT

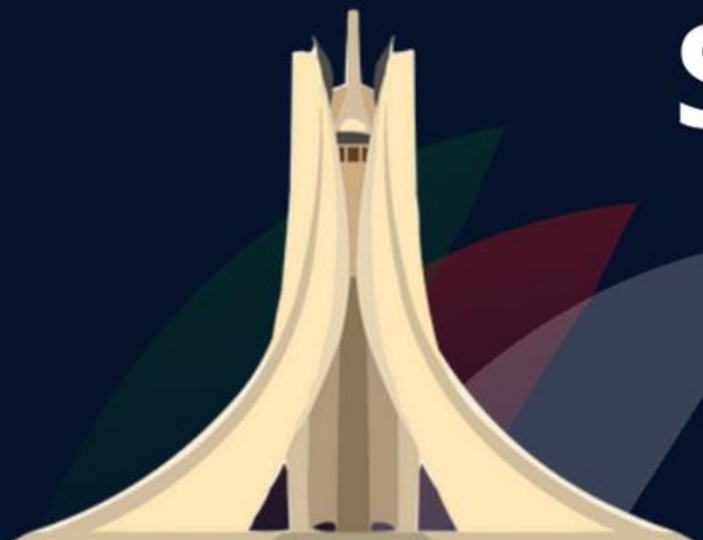
OWASP ALGIERS

Platform to Practice :

- TryHackme
- HackThebox
- Vulnhub
- Portswigger
- PentesterLab

OWASP ALGIERS

SPEAKER



Taher Amine ELHOUARI

CyberSecurity Leader & Global Consultant

- Founder & President @ OWASP Algiers Chapter
- Global Member @ OWASP Foundation
- Founding Board Member @ ISC2 ElDjazair Chapter
- Global Member @ ISC2
- CyberSecurity Instructor @ GoMyCode
- Global CyberSecurity Advisor @ AlphaSights
- CyberSecurity Ambassador @ Cyber Cohesion
- Independent Consultant & Instructor
- CISSP, Mini-MBA, CC, ISO27001, CEHv12, CCSP/AWS, CNPen, CAP, CNSP, CNSS, CPTAv2, C3SA, ACE/MCNA, QCS/VMDR, CCNA..

Cyber Security
Certifications

Most Common Certifications:

ISC2 - CISSP	• Certified Information Systems Security Professional	
ISACA - CISM	• Certified Information Security Manager	
ISACA - CISA	• Certified Information Systems Auditor	
ECCouncil - CEH	• Certified Ethical Hacker	
OffSec - OSCP	• Offensive Security Certified Professional	
CompTIA – S+	• Security+	

Other Certifications?

TCM Security Certified
Practical Network Penetration Tester
PNPT

ISC2
CC SM

CCSP
Certified Cloud Security Professional
ISC2 Certification

CGEIT
Certified in the Governance of Enterprise IT.
An ISACA® Certification

GIAC Penetration Tester
GPEN

OFFENSIVE security
OSEP

OFFENSIVE security
OSCE³

C|PENT
Certified Penetration Testing Professional

eCPPT
V2

Red Team Specialist V2 [CRTS V2]

CCD
CERTIFIED CYBERDEFENDER

Certified CyberDefender (CCD)

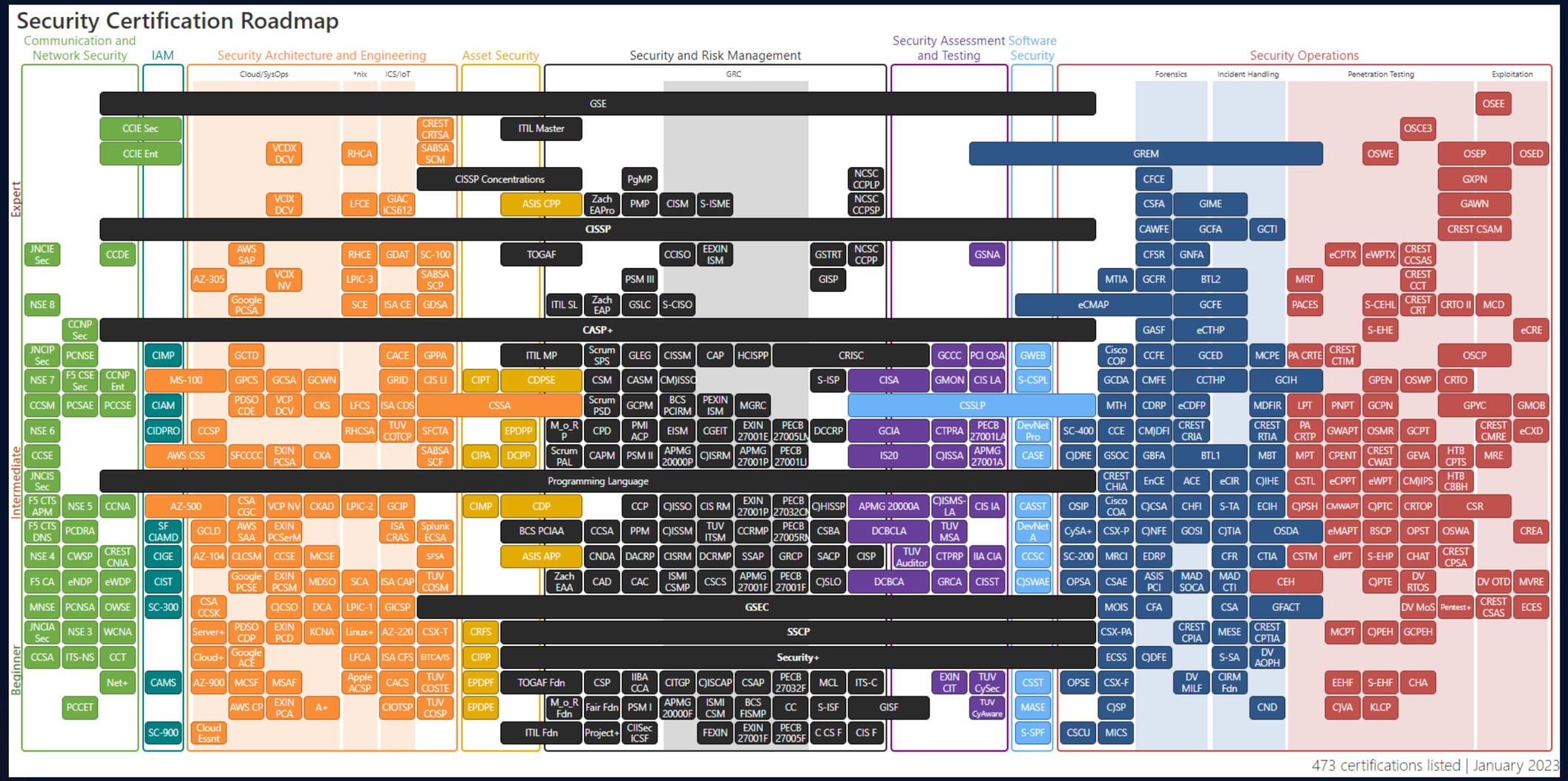
A vendor-neutral, all-practical blue team training and certification for SOC analysts, DFIR, and threat hunters.

CERTIFIED RED TEAM PROFESSIONAL

Certified Red Team Operator
Zero-Point Security
Awarded Jan 14, 2021

OWASP ALGIERS

Other Certifications?



https://pauljerimy.com/security-certification-roadmap/

Networking in the Industry

Networking:

- Networking in the cybersecurity industry is crucial for career advancement, staying updated with industry trends, and building professional relationships.
- Here are some tips on how to network effectively in the cybersecurity industry and the benefits it can bring:

Resources and Platforms to Practice

Practice:

WEBGOAT

DVWA

GOAD
GAME OF ACTIVE DIRECTORY

OverTheWire
We're hackers, and we are good-looking. We are the 1%.

HACKTHEBOX

TryHackMe

VULNHUB
VULNERABLE BY DESIGN

PentesterLab

RootMe

HACKTHISSITE.ORG

CTFTIME

CyberDefenders
Defend Smarter, Not Harder

LetsDefend

PROXMOX

KALI LINUX

PARROT

Project Ideas

Examples:

- **Open Source Security Tool Development:** Contribute to the development of open-source security tools aimed at improving cybersecurity defenses, such as IDS, vulnerability scanners, CTI platforms, or secure coding frameworks.
- **Bug Bounty Program Participation or CVE Hunting:** Participate in bug bounty programs offered by companies and organizations to identify and responsibly disclose security vulnerabilities in their software, websites, or infrastructure.
- **Security Research Projects:** Conduct original research projects on emerging cybersecurity topics, threat trends, or innovative security solutions, and publish findings in academic journals, industry reports, or online platforms.
- **Community Security Events and Workshops:** Organize and host community security events, workshops, or conferences aimed at fostering collaboration, knowledge sharing, and skills development.

S U R P R I S Es!!

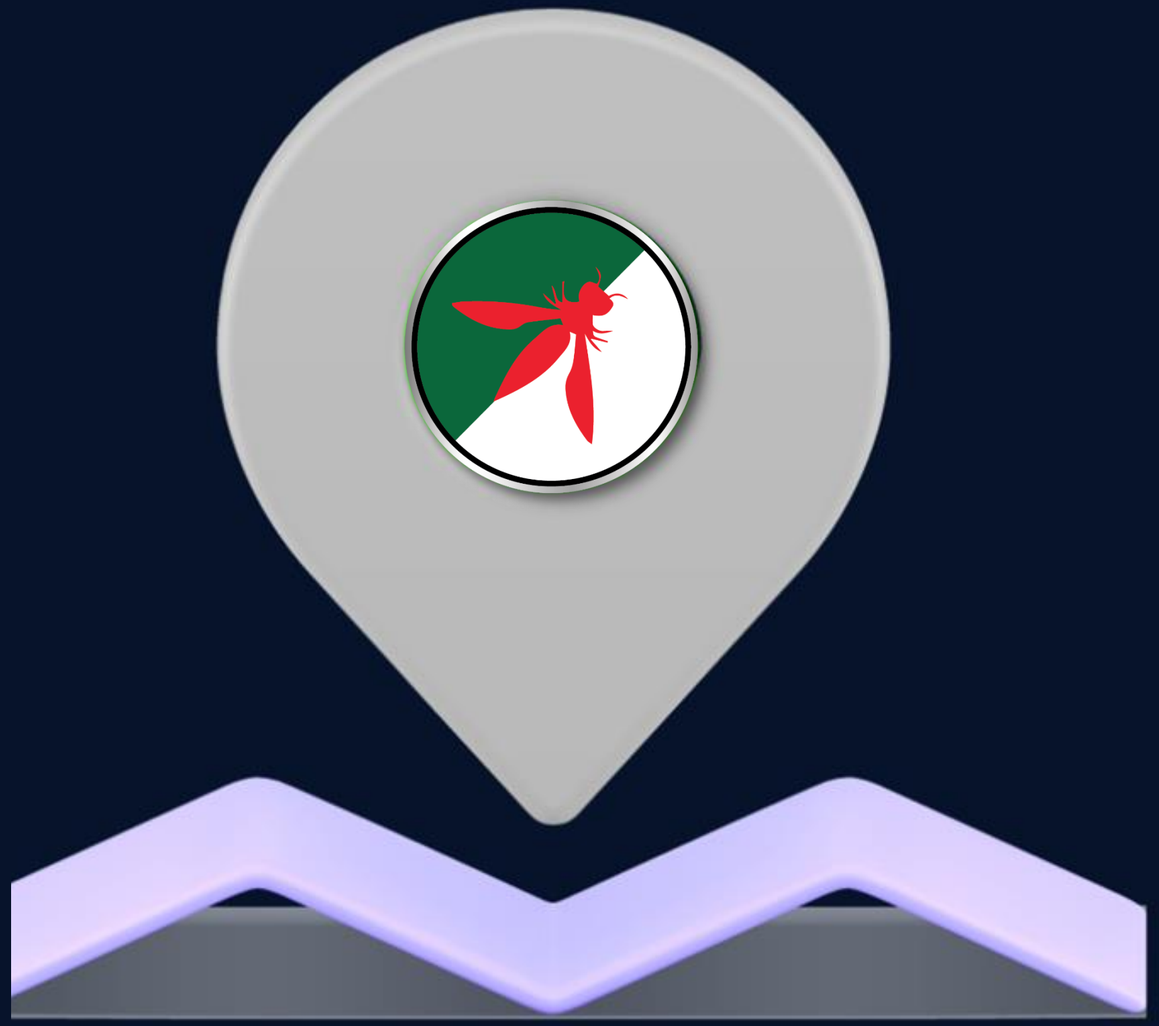
FREEBIES - Free Cyber Security Certifications**:**

- EC-Council - CodeRed: EHE – DFE – NDE
- Qualys: QCS
- ArcX: CTI 101
- SkillFront: ISO 27001:2022 ISMS
- Coursera: IBM, Microsoft, Google
- Fortinet: NSE 1, 2, 3
- Cisco: NetAcad & SkillsForAll
- ISC2: CC

- OWASP ALGIERS CHAPTER!!

OWASP ALGIERS

Contact us



ALGIERS-LEADERS@OWASP.ORG

https://owasp.org/www-chapter-algiers/