

Cybersecurity Fields

Prepared by: PalCyberSec Team



TABLE OF CONTENTS

01

Guide to Entering the
Cybersecurity Fields

Roadmaps

02

03

Learning
Models/Techniques

Certifying-
Organizations

04

TABLE OF CONTENTS

05

Bug Bounty Platforms

Practice Platforms

06

07

Some of Cybersecurity
Conferences

Lack of Resources!!

08

Guide to Entering the Cybersecurity Fields (1)

Important Points to Consider Before Entering the Cybersecurity Fields

Many Paths to Success	Quality Over Quantity	Connect with Others
Stay Curious	Avoid Negative Vibes	Research First
Check Multiple Sources	Keep Discussions Cool	Free Learning
Degree is Nice, Not Necessary	It's Never Too Late to Start	Career Change is Possible
Avoid Self-Blame	Patience is Key	Share Knowledge
Stay Updated	Start Immediately	Please don't just say "hello"

Guide to Entering the Cybersecurity Fields (2)

Questions and Answers

Q1: Timeframe for Professional Development

There is no standardized timeline for professional development in the field; it largely depends on individual effort. The more time invested in both theoretical and practical learning, the faster significant progress can be achieved.

Q2: Evaluating Certificates from Various Companies

Assessing certificates from different companies requires a comprehensive approach. Conducting a survey, seeking testimonials from past participants, and considering their experiences can provide valuable insights. Additionally, factor in the certificate's cost and regularly check for updates to course content and conditions.

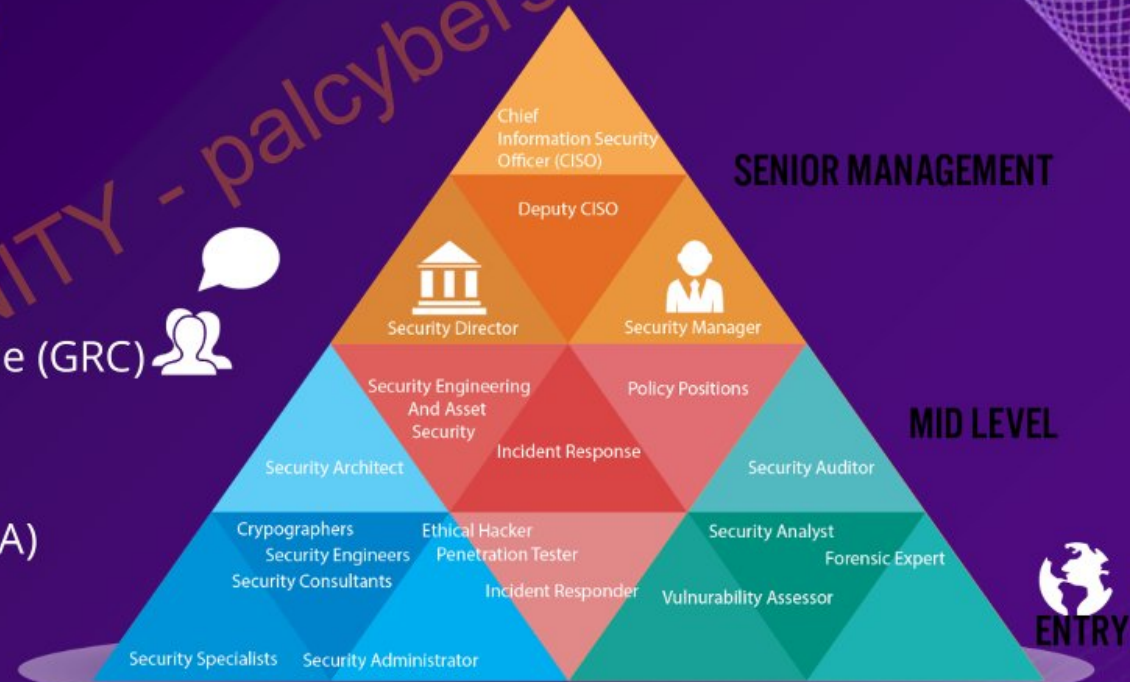
Q3: Overcoming Limited Resources

The absence of a computer or possessing a poorly configured one should not be viewed as a hindrance to progress. Resource constraints should not serve as an excuse. One can make strides by utilizing available resources, even if it means starting on a mobile device. The key is to initiate the learning process and actively work towards personal development.

Guide to Entering the Cybersecurity Fields (3)

List of Some Cybersecurity Fields

- Penetration Tester (PT)
- Security Operation Center (SOC)
- Governance, Risk Management, and Compliance (GRC)
- Digital Forensic and Incident Response (DFIR)
- Reverse Engineering (RE) & Malware Analyst (MA)
- Cyber Threat Intelligence (CTI)



Roadmaps (1)

1. BASELINE SKILLS

Core Techniques
Prevent, Defend, Maintain

4 COURSES

Security Management

Managing Technical Security Operations

4 COURSES

2. FOCUS JOB ROLES

Monitoring & Detection

Intrusion Detection, Monitoring Over Time

2 COURSES

Offensive Operations

Penetration Testing, Offensive Security

2 COURSES

Incident Response & Threat Hunting

Host & Network Forensics

6 COURSES

3. CRUCIAL SKILLS, SPECIALIZED ROLES

Cyber Defense Operations

Harden Specific Defenses

10 COURSES

Specialized Offensive Operations

Focused Offensive Techniques

12 COURSES

Threat Intel & Forensics

Specialized Investigative Skills

7 COURSES

Advanced Leadership

Leadership Specializations

8 COURSES

Cloud Security

Design, Develop, Build & Deploy

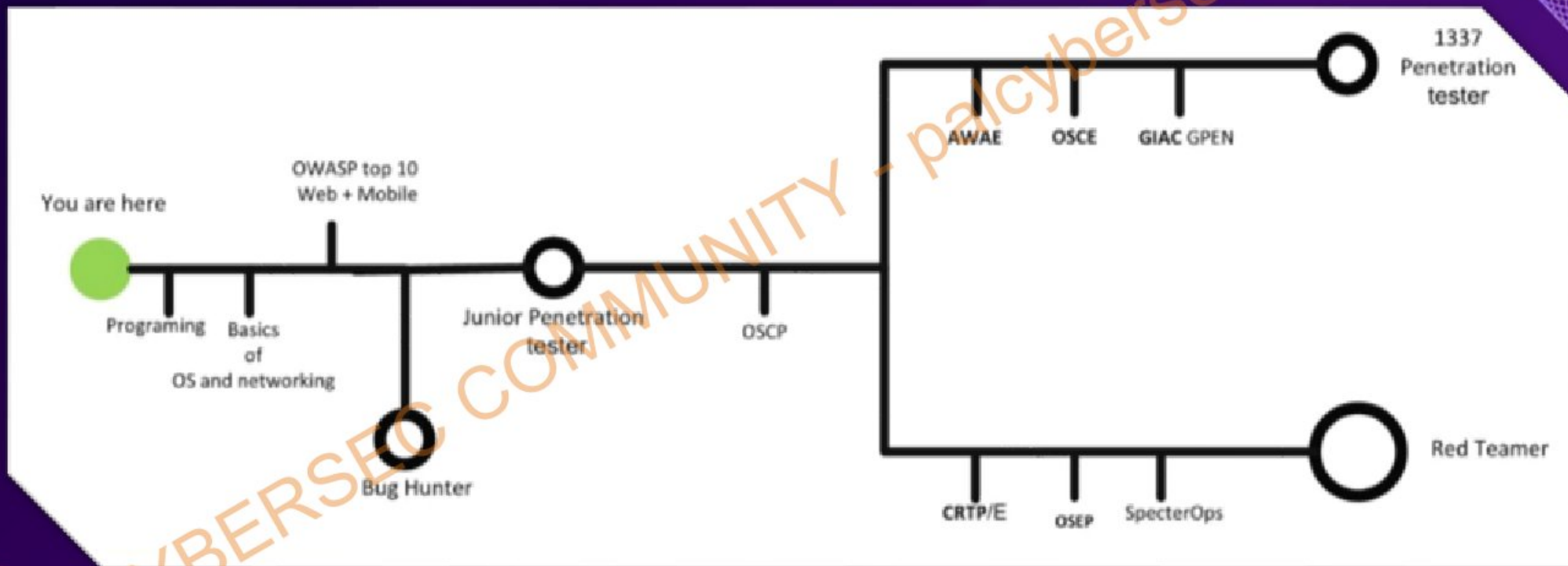
9 COURSES

Industrial Control Systems

Defend Critical Infrastructure

6 COURSES

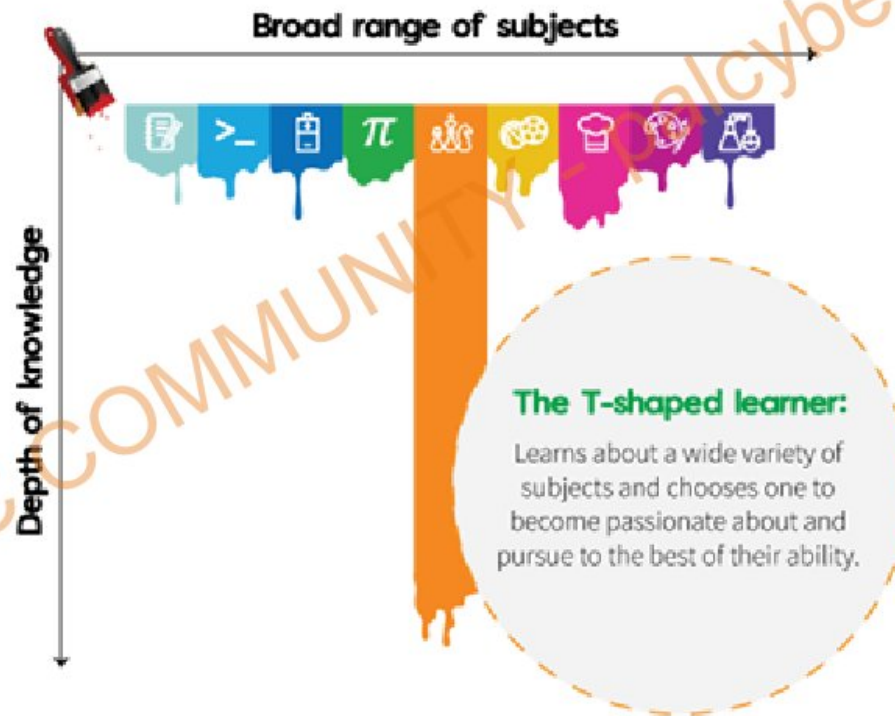
Roadmaps (2)



Roadmaps (3)

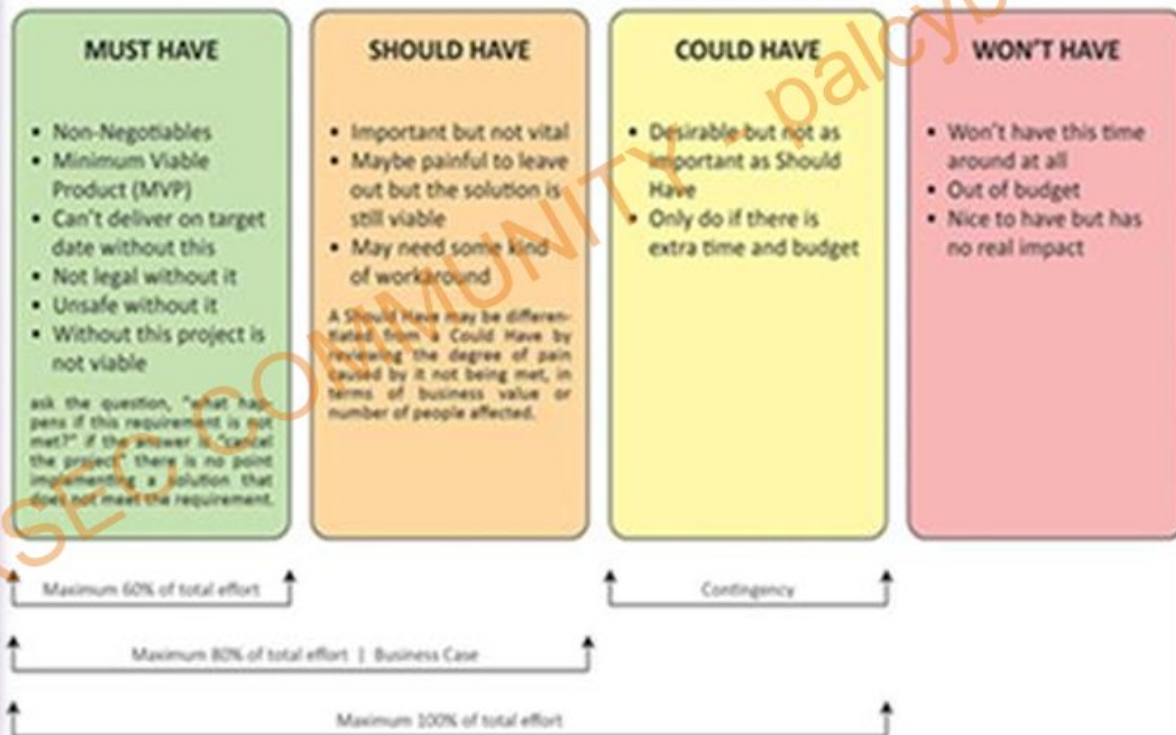


Learning Models/Techniques (1)



Learning Models/Techniques (2)

MoSCoW PRIORITISATION



Certifying-Organizations



EC-Council

SANS



CompTIA

Bug Bounty Platforms

hackerone

bugcrowd



Practice Platforms



Hack The Box
PEN-TESTING LABS



PentesterLab

Root Me



PortSwigger



Try
Hack
Me

ATTACK DEFENSE

1800+ Labs!

<https://start.me/p/KMqznE/it-cyber-security>



CYBER TALENTS

Some of Cybersecurity Conferences

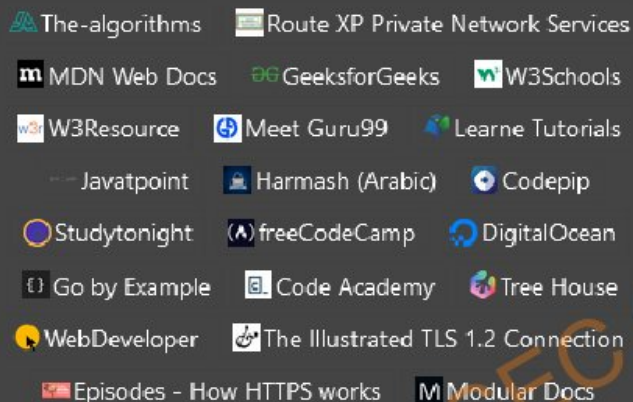


#OSDFCon

https://github.com/MrM8BRH/CyberSecurity_Conferences

Lack of Resources!!

Tutorials Shared



Courses Shared



Cybersecurity Podcasts Shared



<https://start.me/p/KMqznE/it-cyber-security>



THANKS

PALCYBERSEC COMMUNITY - palcybersec@outlook.com