CWL
CyberWarFare Labs

Purple Team Analyst V2 [CPTA V2] Premium Edition Launch Webinar

© 2023 CyberWarFare Labs

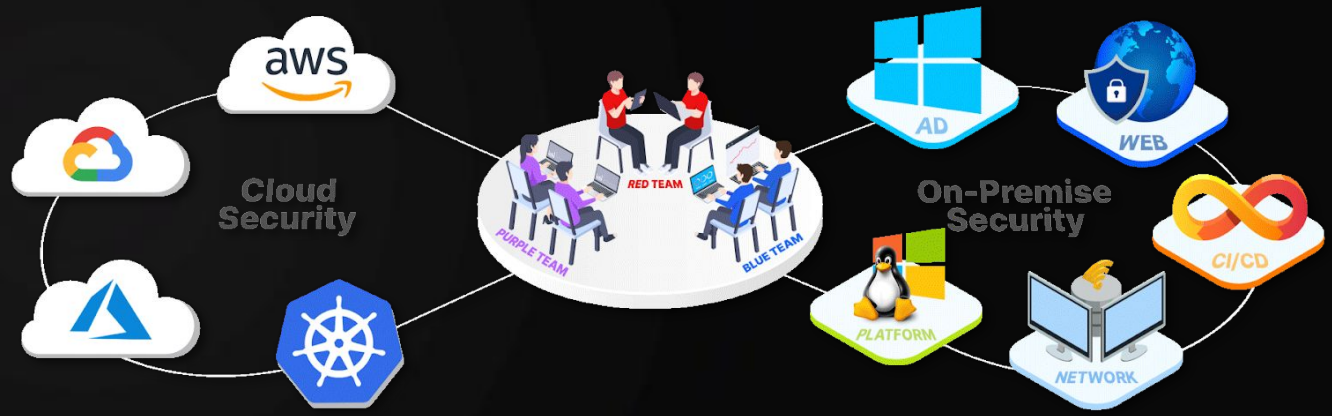
CWL
CyberWarFare Labs

About CyberWarFare Labs :

CW Labs is a renowned UK based Ed-tech company specializing in cybersecurity cyber range labs. They provide on-demand educational services and recognize the need for continuous adaptation to evolving threats and client requirements. The company has two primary divisions :

1. Cyber Range Labs

2. Up-Skilling Platform



© 2023 CyberWarFare Labs

About Speaker :

Harisuthan S

(Senior Security Engineer)

Cyber Security Aspirant with lots of passion and interest towards Cyber Defence

© 2023 CyberWarFare Labs

CWL
CyberWarFare Labs

Understanding the concept of Purple Teaming

Generally **Purple Teaming** is a collaborative operation between two traditionally separate teams: the "**Offensive Team**" and the "**Defensive Team**"

This strategy is designed to enhance the overall security of an organization's ability to detect, prevent, and respond to security threats effectively and efficiently.

© 2023 CyberWarFare Labs

CWL
CyberWarFare Labs

The Red Teaming !

Red teaming aims to **identify weaknesses, vulnerabilities**, and blind spots in an organization's security, processes, systems, and infrastructure.

By simulating real-world attacks and adversarial tactics, it helps organizations understand where they are most susceptible to threats.

© 2023 CyberWarFare Labs

CyberWarFare Labs

The Blue Teaming !

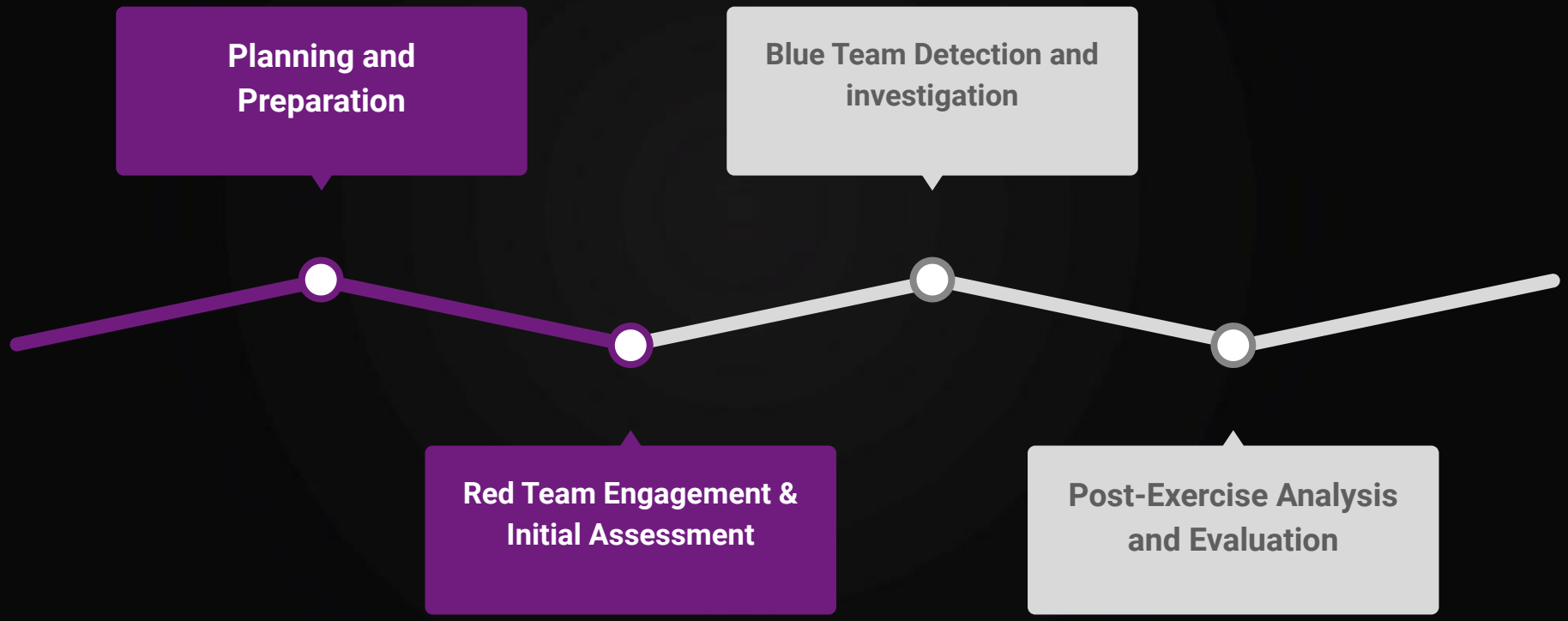
Blue teams generally continuously **monitor** the organization's network, systems, and infrastructure for signs of unauthorized or malicious activities.

They use security tools, such as intrusion detection systems (**IDS**), intrusion prevention systems (**IPS**), security information and event management (**SIEM**) systems, and endpoint detection and response (**EDR**) solutions to detect anomalies and potential security incidents.

© 2023 CyberWarFare Labs

CWL
CyberWarFare Labs

Purple Teaming life Cycle



© 2023 CyberWarFare Labs

CyberWarFare Labs

Traditional On Premise Purple Teaming

Traditional On Premise Purple Teaming methodologies are the systematic approaches used to assess the security of Web, Host, Network and AD Infrastructure of an organisation. Regular security testing and assessments are crucial for maintaining a strong security posture in an ever-evolving threat landscape.

© 2023 CyberWarFare Labs

Purple Team Analyst V2 [CPTA V2] Premium Edition

Certified Purple Team Analyst V2 [**CPTA V2**] provides a Unified Approach to Purple Teaming, This training is designed to equip the participants with the knowledge and skills to become an effective **Purple Team practitioner**

- Investigation & Detection
- Multiple Defensive tools Integration
- Hunting Cyber Threats
- DFIR Investigation
- Perform BAS
- Custom Rule creation

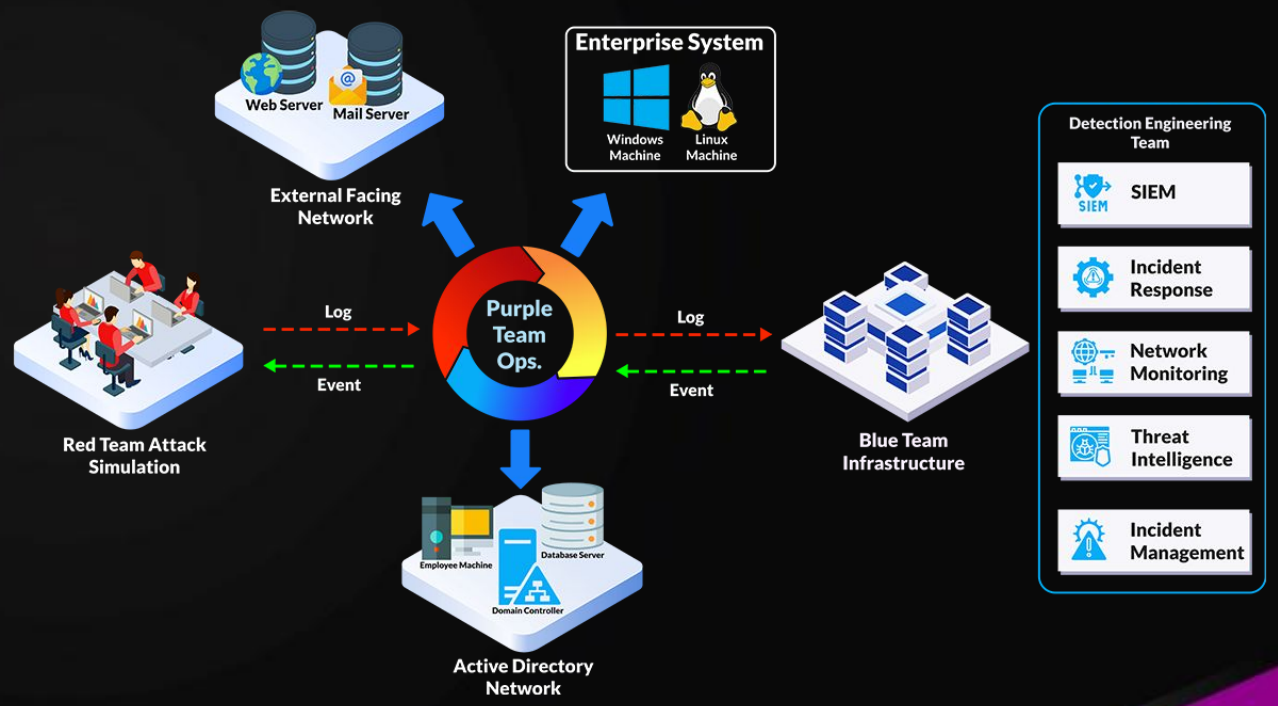
© 2023 CyberWarFare Labs

CWL
CyberWarFare Labs

CPTA V2 lab Overview

Our Purple Team Infrastructure will provides an collaborative and iterative process of both offensive and defensive operations.

Where The **Red Team** identifies vulnerabilities and weaknesses, and the **Blue Team** uses this information to enhance the security of the infrastructure by creating the base line detection rules across multiple defensive solutions.



© 2023 CyberWarFare Labs

CyberWarFare Labs

CPTA V2 lab Highlights

Red Team Highlights	Blue Team Highlights
Perform Breach and attack simulation	Hands-on investigations on various Security solutions [SIEM | IR | Network Monitoring | Threat Intel]
Understand the working behaviour of Security Solutions and detection engineers to bypass it	Understand the working behaviour of various offensive operations to perform better defend against real threats
Enhance Stealth Red Team skills by analysing Blue Team activities	Enhance the real time investigation skills
Simulate Attacks on various environments [Network, Web, Host And Active Directory]	Develop and refine their cybersecurity skills, including network monitoring, intrusion detection, incident response, and security configuration management.

© 2023 CyberWarFare Labs

CyberWarFare Labs

Adversary simulation

Adversary simulation, often referred to as "red teaming," is a cybersecurity practice in which a team of experts (the red team) simulates the tactics, techniques, and procedures (TTPs) of potential adversaries to assess an organization's security posture. The primary goal of adversary simulation is to identify vulnerabilities, weaknesses, and security gaps that could be exploited by malicious actors.

© 2023 CyberWarFare Labs

CWL
CyberWarFare Labs

Importance Defensive Solutions !

The importance of **Defensive Solutions** cannot be overstated, as they play a crucial role in safeguarding against a wide range of threats and vulnerabilities.

Defensive solutions, such as **firewalls**, **intrusion detection** and **prevention systems (IDPS)**, and **antivirus software,** are designed to detect and block malicious activities and cyberattacks. They provide a critical layer of defense against threats like malware, phishing, ransomware, and other malicious activities

© 2023 CyberWarFare Labs

CWL
CyberWarFare Labs

The Blue Teaming Infrastructure !

CPTA V2 infra has been integrated with Security solutions to Monitor, Detect, Identify & Respond during assessments.

SIEM: ELK + WAZUH

Incident Response: Velociraptor

Threat Intelligence: MISP

Incident Management: The HIVE

IDS/IPS: Suricata + IDS Tower

Network Monitoring: Akrime Moloch

Real Time Investigation: OSQuery

© 2023 CyberWarFare Labs

CWL
CyberWarFare Labs

CWL Labs Portal

Introducing our custom **CWL web portal** for purple teaming training is a specialized online platform designed to facilitate collaborative training and knowledge sharing between cybersecurity red team and blue team members.

This portal serves as a central hub for various training modules, resources, and interactive exercises aimed at enhancing the skills, knowledge, and collaboration between offensive (red team) and defensive (blue team) security experts.

© 2023 CyberWarFare Labs

CWL
CyberWarFare Labs

Key features of CWL Labs Portal

- User authentication and access control
- Module Based Badges
- Training modules and materials covering purple teaming concepts, assessments and evaluations
- progress tracking
- realistic scenarios

© 2023 CyberWarFare Labs

Thank You

For Professional Red Team / Blue Team / Purple Team/
Cloud Cyber Range labs / Trainings, please contact :

support@cyberwarfare.live

To know more about our offerings, please visit: https://cyberwarfare.live

© 2023 CyberWarFare Labs