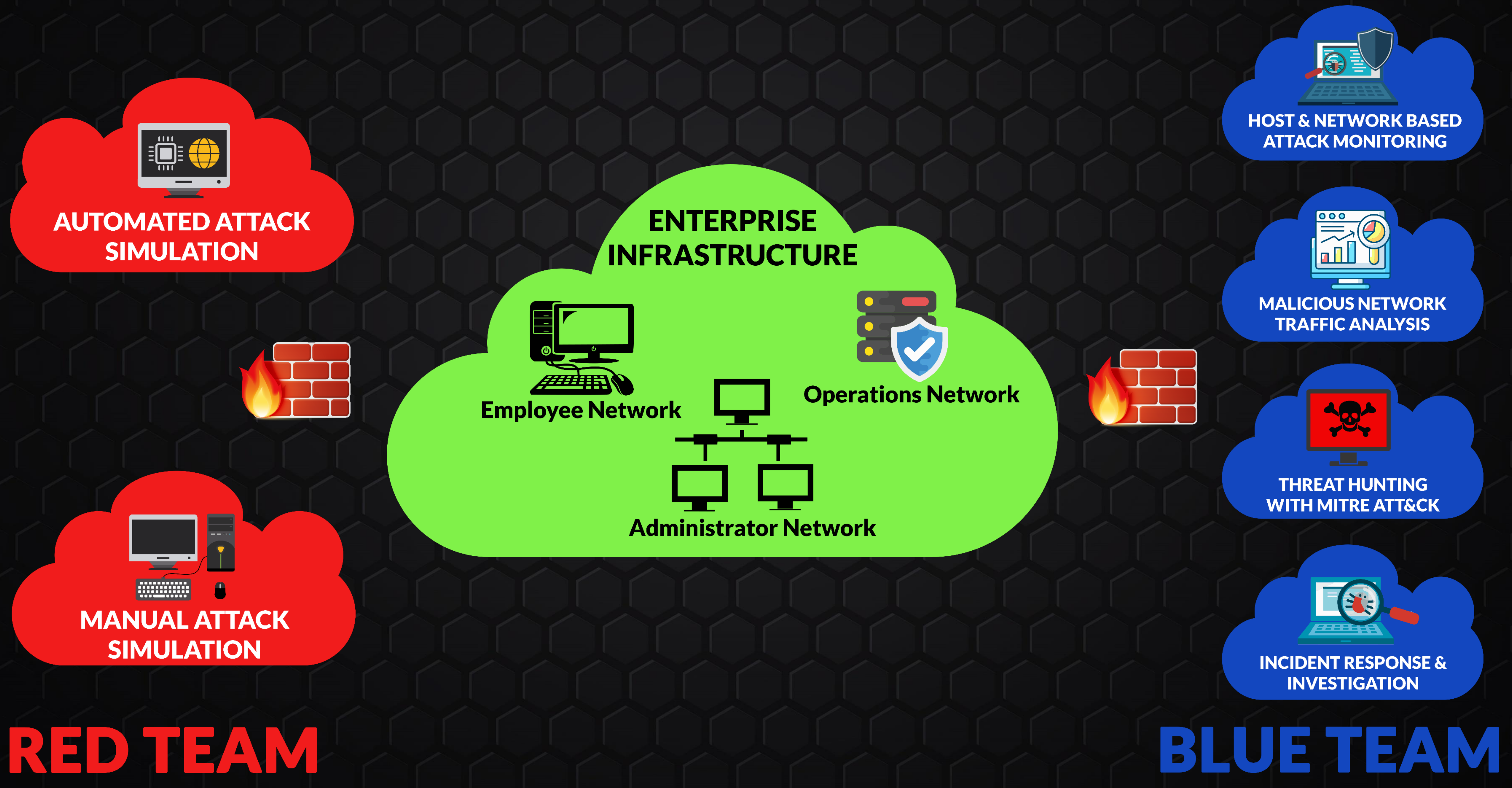
CWL

CyberWarFare Labs

Certified Purple Team Analyst [CPTA]

@CyberWarFare Labs

Certified Certified Purple Team Analyst Architecture


AUTOMATED ATTACK SIMULATION
MANUAL ATTACK SIMULATION
RED TEAM
ENTERPRISE INFRASTRUCTURE
Employee Network
Operations Network
Administrator Network
HOST & NETWORK BASED ATTACK MONITORING
MALICIOUS NETWORK TRAFFIC ANALYSIS
THREAT HUNTING WITH MITRE ATT&CK
INCIDENT RESPONSE & INVESTIGATION
BLUE TEAM

CWL
CyberWarFare Labs

Introduction To Purple Team Analyst

CWL

CyberWarFare Labs

Module 1

Introduction to Purple Teaming:

1.1 About Red Teaming
1.2 About Blue Teaming
1.3 About Purple Teaming

Module 2

Purple Team Adversary Simulation Lab Overview:

2.1 Lab Overview 2.2 Lab Architecture
2.3 Lab Access
2.4 About Enterprise Simulated Environment
2.5 Adversary Simulation
2.6 Adversary Detection
2.7 About Red vs Blue Team Joint Operations

Module 3

Red Team Operations in Simulated Lab

3.1 Automated Adversary Simulation

- Framework Overview
- Setting profile & selecting platform
- Initializing operations

3.2 Manual Adversary Simulation

- Required Tools, Tactics & Techniques
- Mapping defences with our tradecraft

Module 4

Blue Teaming in Simulated Lab

4.1 Host based attack detection

4.2 Network Based attack detection

4.3 AD Based attack detection

4.4 Network Traffic Analysing

4.5 Digital forensic and Incident Response

Module 5

Purple Teaming Exercise (APT attack simulation and detection)

5.1 Adversary Simulation Using MITRE ATT&CK Framework
5.2 Adversary Detection using MITRE Shield Framework
5.3 Tactics, Techniques and Procedures (TTPs) Simulation and Detection

- 5.3.1 Windows Environment
  - Initial Access
  - Execution
  - Persistence
  - Privilege Escalation
  - Defensive Evasion
  - Credential Access
  - Discovery
  - Lateral Movement
  - Collection
  - Command & Control
  - Exfiltration

5.3.2 Linux Environment

CWL
CyberWarFare Labs

5.4 Tactics, Techniques and Procedures (TTPs) Simulation and Detection (contd.)

5.4.1 Linux Environment

- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defensive Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Command & Control
- Exfiltration

CWL
CyberWarFare Labs

Thank You

Cyberwarfare.live