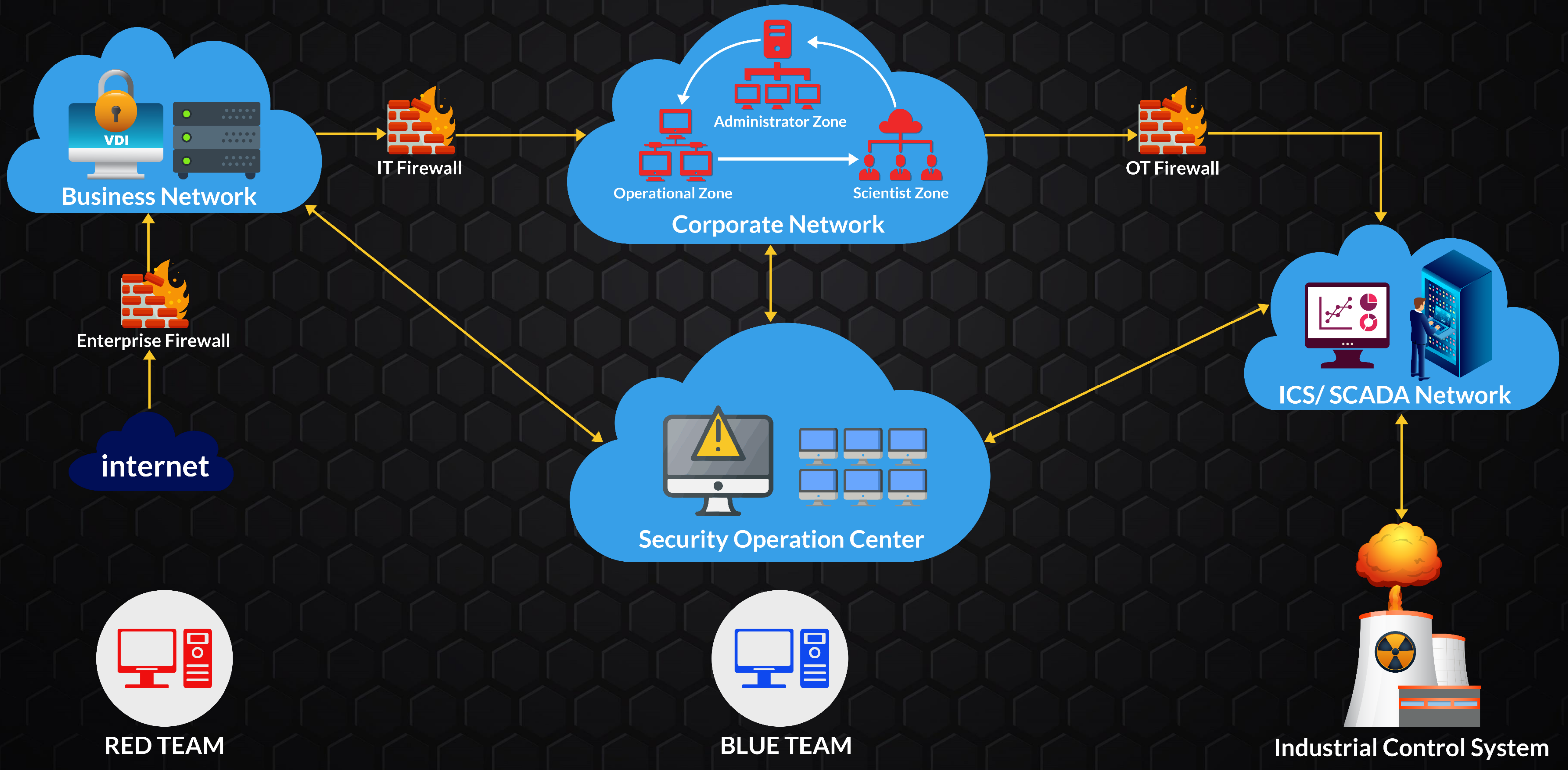
CWL

CyberWarFare Labs

Certified Red Team Specialist [CRTS]

@CyberWarFare Labs

Certified Red Team Specialist Architeture



CWL
CyberWarFare Labs

INTRODUCTION TO RED TEAM SPECIALIST

CWL
CyberWarFare Labs

Module 1

Perform Cyber Kill Chain

- Extensive OSINT Enumeration
- Exploit Remote Access Services (VDI, RDS etc)
- User Enumeration & Phishing
- Various User Simulation in Enterprise Environment
- Custom Privilege Escalation (Windows & Linux)
- Custom Web Exploitation
- Abuse LOLABS to stealthily exfiltrate data
- Follow MITRE ATT&CK Framework

Module 2

Abuse Enterprise Active Directory Environment:

- Enumerate & Identify Mis-Configurations
- Kerberoasting and AS-REP Roasting
- Kerberos Session Hijacking
- Credential Replay Attacks
  - Credential Discovery
  - Pass the Hash (PTH) & Over-Pass the Hash (OPTH)
  - Pass the Ticket (PTT)
- Multiple Cross Forest Abuse Scenarios
  - Abuse Foreign Security Principal (FSPs)
  - Normal & targeted Kerberoasting
  - Delegation Scenarios
- Token Manipulation attacks
- Abusing SQL Server Links from Linux Machines
- Enumerate & Abuse Linux Machines in AD Environment &so much more .....

CWL
CyberWarFare Labs

Module 3

Escape Containerized Environment

- Multiple methods to escape containers
- Multi-Level Container Breakouts
- Simulated Environment

Module 4

Enterprise grade automation software:

- Abuse Automation Software
- Abuse Secret Servers
- Understand & Exploit CI/CD Pipeline
- Custom attack vector development
- Abuse bastion host and so much more ….

CWL
CyberWarFare Labs

Module 5

Lateral Movement and Network Pivoting

- From Linux to Windows, Windows to Windows, Windows to Linux etc.
- File-Less Lateral Movement Methodologies
- Abuse Internal Remote Services in Multi-OS environment
- Alternative authentication methodologies
- Understand Local, Remote Port Forwarding, various proxies etc.
- Multi-level in-depth network pivoting in Windows & Linux OS

CWL

CyberWarFare Labs

Thank You

Cyberwarfare.live