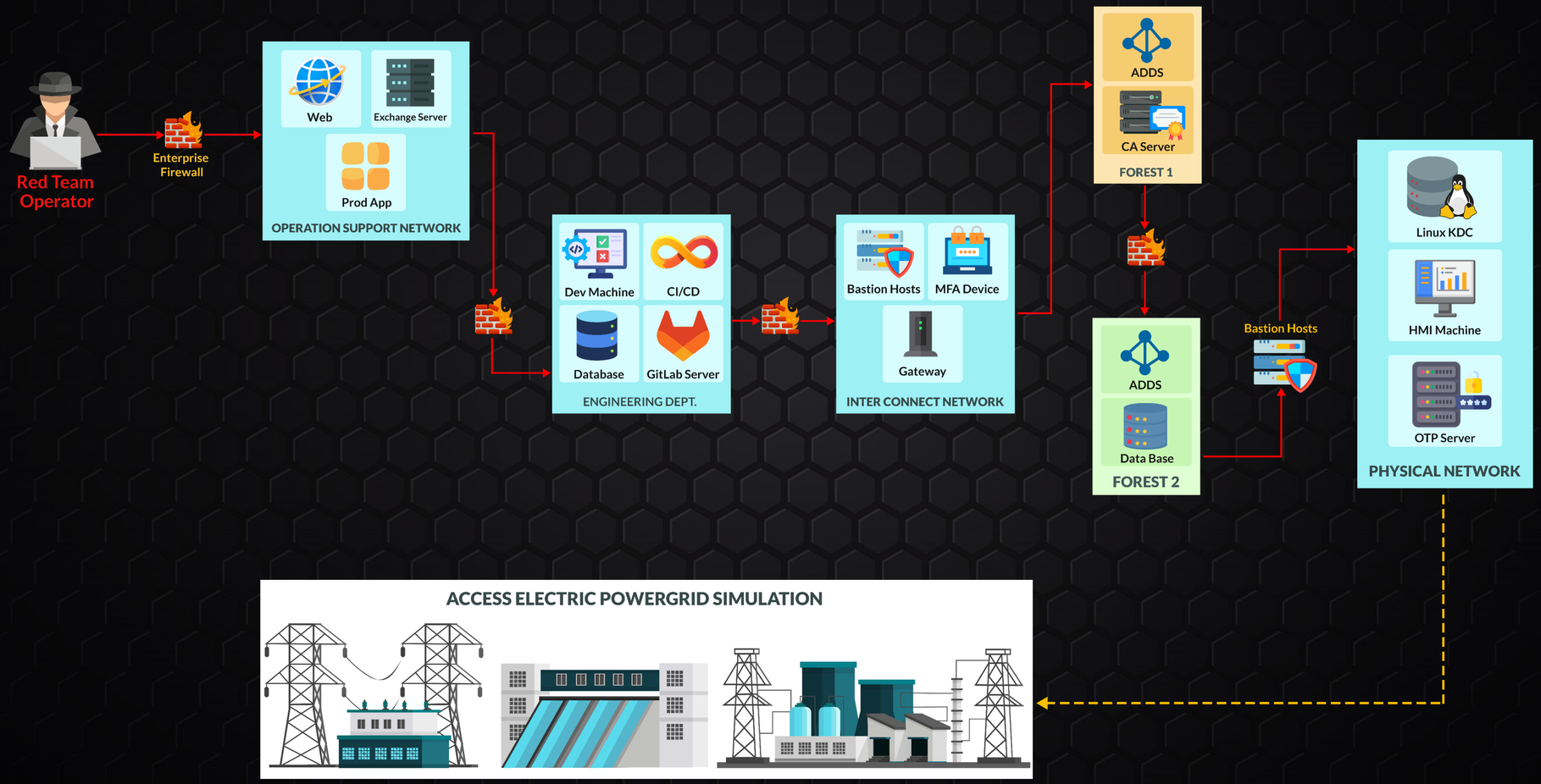
CWL
CyberWarFare Labs

Certified Red Team Specialist V2 [CRTS V2]

@CyberWarFare Labs

Certified Red Team Specialist V2 Architeture



CWL
CyberWarFare Labs

MODULE 1 : INITIAL ACCESS

CWL
CyberWarFare Labs

Module 1
Perform Cyber Kill Chain

1. Case Studies

- **Real Life Case Studies**

  - Abusing Web App based Vulnerabilities
  - Leaked PAT to Self-Hosted GitLab Runner
  - Adversary In the Middle Attack (AiTM)
  - Manipulating Exchange Rules
  - Abusing & Impersonating Enterprise Applications

    - Zoom
    - Visual Studio

MODULE 2 : ADVANCED AD ATTACKS

CWL
CyberWarFare Labs

Module 2
Advanced AD Attacks

1. **Kerberos Delegation**
   - Kerberos Extension
     - S4U2Self
     - U2U
     - S4U2Self + U2U
   - **Attacks**
     - **Diamond Tickets**
     - **Sapphire Tickets**

2. **Linux Active**
   - **Credential Discovery**
   - **Kerberos in Linux**
   - **Credential Extraction**

3. Group Managed Service Account (gMSA)

- Machine Access
- User Access

4. Certificate Services

- Introduction
- Authentication
- ESC Abuse
  - ESC1
  - ESC4
  - ESC6
  - ESC8
- Golden Certificate
- Un-PAC the Hash
- Shadow Credentials

5. Cross-Forest Attacks

- Kerberoasting
- ACL Abuse
- Foreign Security Principal
- Trust Key
- Privileged Access Management (PAM)
- Over-Permissible Certificate Template

CWL
CyberWarFare Labs

Thank You

Cyberwarfare.live