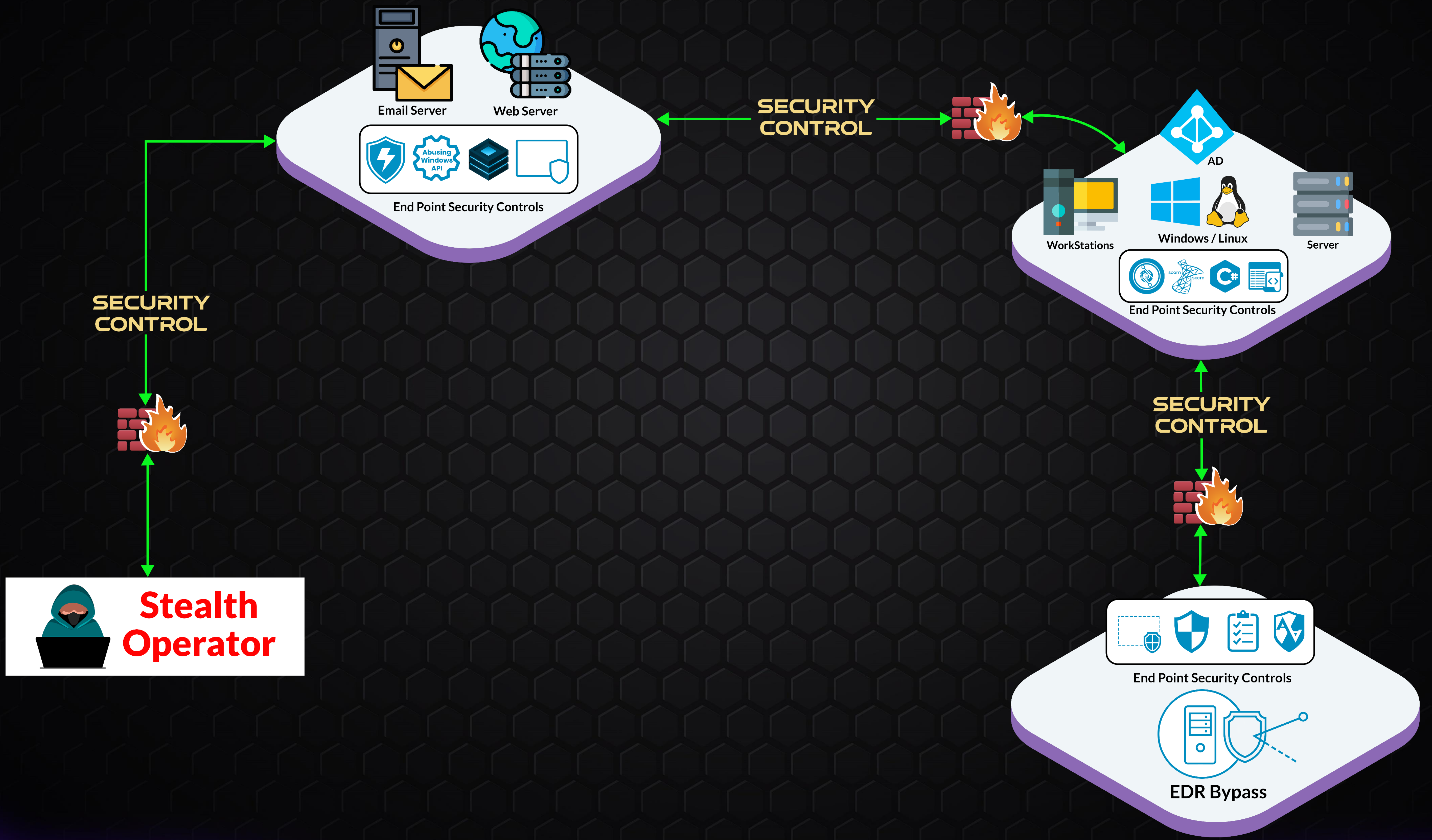
CWL

CyberWarFare Labs

Certified Stealth Cyber Operator [CSCO]

@CyberWarFare Labs

Stealth Cyber Operator Architeture



CWL
CyberWarFare Labs

MODULE 1

Red Team Resource Development

Enterprise Security Controls Architecture

- Initial Access Defenses
- HTML Smuggling
- Anti-Virus & End-Point Detection and Response (EDR)
- End-Point Defender Features (AMSI, CLM, UAC, Applocker, WDAC, WDAG, WDEG (ASR))
- Directory-Level Controls (JEA, JIT, PAW, PAM, Credential Guard, LAPS, Delegation etc)
- Linux Environment (AppArmor)

Red Team Infrastructure Development

- OPSEC Safe C2 Server Implementation
- Payload Server
- Re-director
  - Server-less
  - With Server
- Phishing Infra Setup
- Initial Access Vector
  - MOTW Evasion
- Phish to persist exercise (APT29 Initial Access Simulation)

MODULE 2

Offensive C# Tradecraft

CWL
CyberWarFare Labs

CSharp Essentials

- Why Learn C# from a Red Team Perspective ?
- Common Language Runtime (CLR)
- Managed VS Un-Managed Code
- Setting Up Environment

CSharp Beginner

- Utilizing .NET class for stdin / stdout operations
- Identifying the process architecture (32-bit or 64-bit)
- Identifying the state of a process (Hard-Coded Process Name)
- Identifying all Processes Status
- Hidden command prompt
- Domain Environment SID Enumeration
- Utilizing Platform Invoke to call Un-managed Function Calls
- Create & Instantiate a class from a separate library
- Calling our own .NET Assembly (Externally)
- Hijacking AppDomain Manager

Offensive C# Trade-Craft [6 Hands-on Labs]

- Custom Meterpreter Magic
- Invoking PowerShell without Powershell.exe Binary
- Writing Custom Obfuscated C# Reverse Shell
- Weaponizing AppDomain Manager
- Case Study of an Initial Access TTP (Utilizing C# Trade Craft)

MODULE 3

Abusing Windows API

CWL
CyberWarFare Labs

- Introduction
- Windows API Essentials
- Utilizing Windows API for Red Team Profit

Process Injection Basics

- Listing DLLs loaded by a Process
- Writing Data to a Process in Memory
- DLL Injection

Alternative Code Execution Techniques

- Alternative Shellcode Execution Techniques
  - Via EnumSystemGeoID() Function API
  - Shell Back via CreateThreadPoolWait() Function API

Process Injection Techniques

- Process Hollowing
- Process DoppleGanging
- Process Herpaderping
- Process Ghosting

Bullet-Proof AV Evasion

- Loading Shellcode from a project file
- 2 Exercises

MODULE 4

Abusing / Evading Security Controls

Exploiting Host-Level Security Controls

- **Bypassing Host-Level Defenses**
  - Numerous ways of Bypassing / Disarming AMSI [Custom Ways]
  - Bypassing CLM
  - Evading Script Block Logging
- **Bypassing ASR Rules**
  - Impede JavaScript and VBS to launch executable
  - Block execution of potentially obfuscated scripts
  - Block Office Applications from Creating Child Process
  - Block Win32 API Calls from Office Macro
  - Block Process Creation Originating from WMI / PSEXEC

- **Bypassing Windows Application Whitelisting**
  - Mis-Configured WDAC
  - Mis-Configured AppLocker
    - Abusing LOLBINS
    - Bypass Applocker in an Advanced Initial Access TTP
    - Via installed 3rd Party Applications
    - Via Alternate Data Streams (ADS)
- **Abusing Windows Features (or bug?)**
  - PowerShell
  - Interesting Payload Deliver Techniques
  - Windows Subsystem for Linux (WSL & WSLv2)
  - UAC (You see me?)
    - Custom File-less UAC Bypass (Macro)

- **Credential Access**
  - PowerShell PS-ReadLine Module
  - Credential Guard Bypass
    - Via Custom SSP
    - WDigest.dll Memory Patching
  - LSASS Dumping
    - Via comsvcs.dll
    - Via WerFault.exe
    - Custom C# LSASS Dumper
  - Linux Credential Extraction
    - Discovery
    - Kerberos in Linux
    - Various ways of credential extraction

Exploiting Network-Level Security Controls [13 Hands-on Lab]

- Abusing Resource Based Constrained Delegation (RBCD)
  - With & without adding computer account

Abusing Microsoft Monitoring & Patching Solutions

- Leveraging SCCM
  - Leveraging SCOM
  - Local Administration Password Solution (LAPS)

Cross Forest Abuse Techniques

- Kerberoasting
- Cross-Forest ACL Abuse
- Foreign Security Principal Abuse
- Trust Key
- Abusing PAM Trust

Linux Environment Abuse (AppArmor)

ETW Basics

- ETW Evasion [Exercise]
- ETW + AMSI Evasion [Exercise]

EDR Internals

- Working
- Components
- EDR Case Studies
- General Evasion Areas [4 Exercises] (16:15)
  - NT Calls
  - Syscalls
  - Unhooking (2 Exercises)
- EDR Evasion Challenges (2 Exercises)

MODULE 5

Enterprise Grade Lab Environment [30 Days Lab Access]

- Instructions To Access The Enterprise Simulated Lab With Updated & Patched Security Controls [For Practice]
- Scope Of Engagement [SOE]
- Lab Solution / Walkthrough In Video + Pdf Format
- Technical Support

CWL
CyberWarFare Labs

Thank You

Cyberwarfare.live