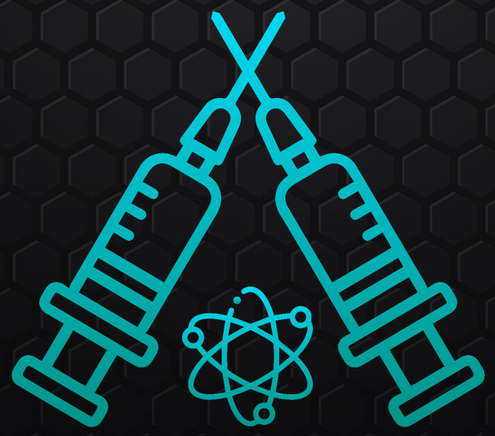
CWL

CyberWarFare Labs

Certified Process Injection Analyst [CPIA]



@CyberWarFare Labs

Certified Process Injection Analyst

1. Process Injection Mindset
2. Classic Process Injection
3. APC Code Injection
4. Section Mapping
5. Module Stomping
6. Process Hollowing
7. Process Doppelganging
8. Transacted Hollowing
9. Process Herpaderping
10. Process Ghosting
11. Understanding Telemetry
12. Event Analysis Using Microsoft Defender for Endpoint (MDE) for all techniques

CWL
CyberWarFare Labs

Red Team	BLUE Team
Advanced Process Injection Techniques used by Threat Actors / Red Teams	Analyse Telemetry data
Identify Telemetry generated from techniques	Event Analysis of Collected Footprints
Lower your footprints during post-exploitation operations	Hands-on Exercises on Microsoft Defender for Endpoint (MDE)
Emphasis on Custom Tooling	Get deeper visibility into the windows hosts machines

CWL
CyberWarFare Labs

CWL
CyberWarFare Labs

Thank You

Cyberwarfare.live