HACKERU

Digital Forensics & Incident Response

CB110

05
Days

Digital Forensics & Incident Response

Outline

The 5-day Digital Forensics & Incident Response course introduces participants to DFIR concepts and transfers goal-oriented use techniques. Participants will learn how to investigate an incident, how to gather supportive forensic data, and how to handle it.

Target Audience

This course is designed for learners who already have hands-on technical experience.

Primarily

- IT Teams
- SOC Teams
- Forensics Teams
- Penetration Testers

Prerequisites

Before attending this course, participants must have:

- Hands-on experience with Linux and Windows systems
- A solid understanding of networking infrastructure

Objectives

Upon course completion, participants will be able to:

- Investigate Security Events
- Analyze Network Traffic
- Recover Lost Data
- Recover Traces and Actions Made on PCs

Content

Day 1

Module 01
Introduction to DFIR

- Introduction to DFIR
- DF vs IR vs TH
- Incident Response planning
- Targeted artifacts
- DFIR use-cases
- DFIR Toolset
- SANS & NIST

Day 1

Module 02
Incident Response - Preparation

- Defining assets & values
- CIA
- Risk management
- Roles & Responsibilities
- 4 & 6 stages of IR
- Creating IR Plan
- DRP & BCP
- GRC
- ATT&CK
- Compliances – ISO, GDPR, HIPPA, PCI-DSS

Day 1

Module 03
Incident Response - Response

- SOC Operation & Lifecycle
- Identification & Scoping
- Containment
- Intelligence gathering
- Eradication
- Chain of custody

Day 2

Module 04
Data Acquisition

- Dead System Analysis
- Live System Analysis
- Drive Cloning
- Image Mounting
- Memory Dumping
- Evidence Documentation

Day 2

Module 05
Live Forensics

- Artifacts on a Windows computer
- Browser History
- USB History
- DNS Cache
- Prefetch
- MRU
- Nirsoft

Day 3

Module 06
Windows Forensics

- Windows DF Specifics
- NTFS
- ADS & MFT
- File Carving
- Registry Forensics
- Forensics using powershell

Day 3

Module 07

Memory Analysis

- Memory structure
- Memory analysis tools
- Volatility Breakdown & Usage
- Process exploration
- DLL inspection
- Acquiring memory artifacts

Day 4

Module 08

Linux Forensics

- Linux Filesystems
- Network configuration
- Login information
- Bash history
- Identifying Persistence
- Logfile Analysis

Day 4

Module 09

File Upload

- Windows EventLog
- PowerShell logs
- Timeline analysis
- DF Timeline
- Log2timeline

Day 5

Module 10

Threat Hunting – consider moving after Malware

- Threat Hunting
- Threat intelligence
- Collecting IoCs
- Malware characteristics
- from DF to TH
- Common Hiding Mechanisms

Day 5

Module 11

Network Forensics

- Traffic interception & Network Evidence
- Reverse Proxy
- Wireshark
- DF using Wireshark
- Common Protocol Analysis
- Zeek NSM

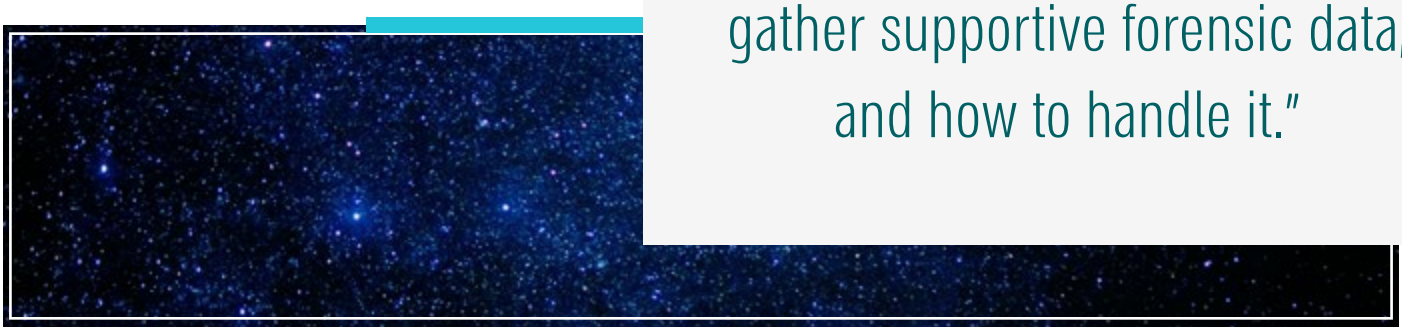
Day 5

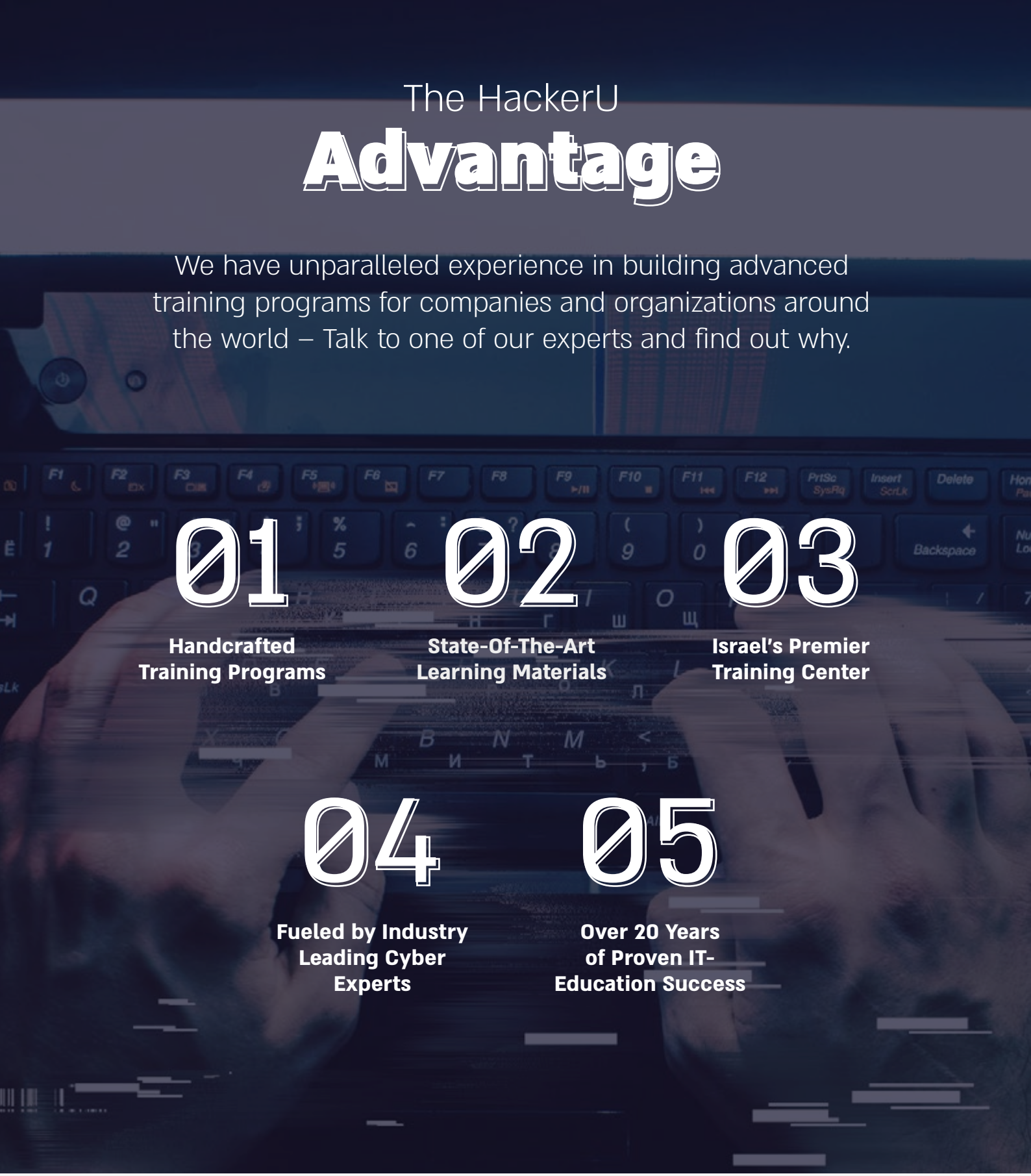
Module 12

DFIR Simulation

- DF lab & Recap

"Participants will learn how to investigate an incident, how to gather supportive forensic data, and how to handle it."





The HackerU Advantage

We have unparalleled experience in building advanced training programs for companies and organizations around the world – Talk to one of our experts and find out why.

01 Handcrafted Training Programs

02 State-Of-The-Art Learning Materials

03 Israel's Premier Training Center

04 Fueled by Industry Leading Cyber Experts

05 Over 20 Years of Proven IT-Education Success

Info@hackerupro.com

www.hackerupro.com