HACKERU

# Cyber Security for IT & SOC

CB111

04
Days

# Cyber Security for IT & SOC

## Outline

Organizations & companies face a critical stage; cyber-attacks have transformed dramatically over the past few years. Unfortunately, banks, corporates & financial services are still being breached too often, most frequently by those with insider access, and as a result, these companies are under more pressure than ever to secure their financial systems. In this course the students will introduce with the different ways to perform manipulation & bypass security measures in order to gain access to a sensitive service/information.

## Target Audience

IT/Security teams oversee the cyber challenges experienced on the technical layer of the organization. HackerU's training programs will help security teams build & maintain a secure network & system, protect data, maintain a vulnerability management program & implement strong access control measures, as well as regularly monitor & test networks and maintain a consistent information security policy.

## Prerequisites

This course is designed for people with an IT background skill and Experience with both Linux and Windows operation system.

## Objectives

On completing this course, delegates will be able to:

- Understand the flow of a cyber-attack cycle.
- Review the different approaches to address past and future cyber threat.
- Discover best practices and innovative techniques to help combat cyber-attacks.
- Learn how to work with SIEM technologies and automate detection and response.
- Perform static & dynamic analysis of malware samples to understand how they work.
- reverse engineer and understand how the underlings of a program work.
- Explore how building windows tools can be utilized in attacks.
- Review persistence techniques and typical backdoors using hidden users.
- Learn the different methods used to bypass SIEM and Security measures' detection.
- Explore the modern platforms used to share and collect threat related information
- Learn how to utilize the ELK stack in thread hunting and investigation.

# Content

Day 1

## Module 01
## Cyber Kill Chain

- What is Information Security
- Terminology
- Types of Hackers
- Hacker State of Mind
- World of Security
- Operation systems

Day 1

## Module 02
## DFIR Fundamentals

- DFIR Fundamentals
- Image Capture
- Memory Capture
- Forensics Tools
- Forensic Methodologies

Day 1

## Module 03
## SOC Life Cycle

- SOC Fundamentals
- SOC Team Responsibilities
- Incident Prioritization
- Vulnerability Assessment

Day 1

## Module 04
## Utilizing SOAR in a SIEM Environment

- SOAR
- Automation Objectives
- Successful Defense
- Effective Usage
- Demisto

Day 2

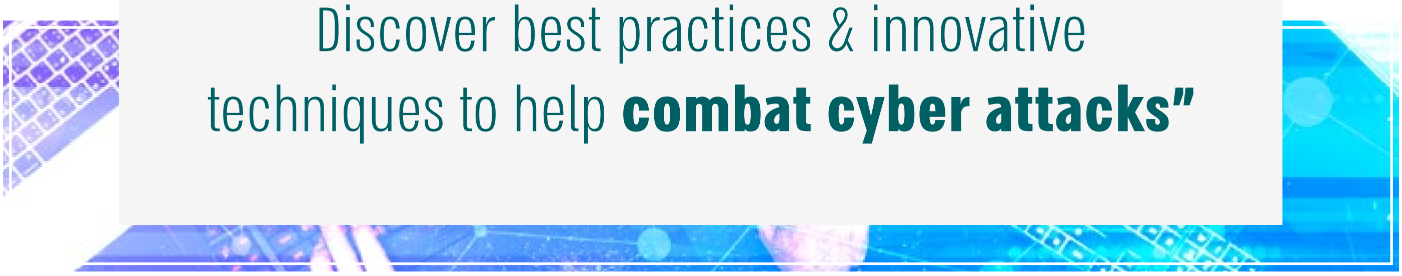
## Module 05
## Malware Analysis & Reverse Engineering - Static Analysis

- Malware Analysis Introduction
- Enumeration Techniques & Common Scanners
- Portable Executable
- Dynamic Link Library

Day 2

## Module 06
## Malware Analysis & Reverse Engineering - Dynamic Analysis

- Dynamic Analysis Introduction
- System Monitoring
- Networking Monitoring
- Malware Samples



"Discover best practices & innovative techniques to help **combat cyber attacks"**

Day 2

**Module 07**

## Reversing with IDA

- Introduction to IDA
- IDA Code Flow
- Documentation Options
- Patching with IDA

Day 2

**Module 08**

## PowerShell

- PowerShell Fundamentals
- PowerShell ISE
- PowerShell Modules
- PowerCat & Nishang
- PowerShell to EXE

Day 3

**Module 09**

## Privilege Escalation

- Windows Privileges
- Domain Privileges
- Windows Boot Process
- Exploitation
- Windows Defender ATP
- Means of Protection

Day 3

**Module 10**

## Bypass SIEM Detection

- Detection Fundamentals
- Detection Bypass methodologies & Tools
- External Bypass
- Internal Bypass

Day 3

**Module 11**

## Obfuscation

- What is Obfuscation?
- Types of Obfuscation
- Packing
- Various Tools
- Tools Comparison
- Multi-Layered Obfuscation

Day 3

**Module 12**

## Threat Hunting Vs Threat Intelligence

- Threat Hunting
- Threat Intelligence
- Hunts and Cycles
- Manual Threat Hunting
- Threat Hunting Automation
- Threat Hunting with Zeek

Day 4

**Module 13**

## ELK

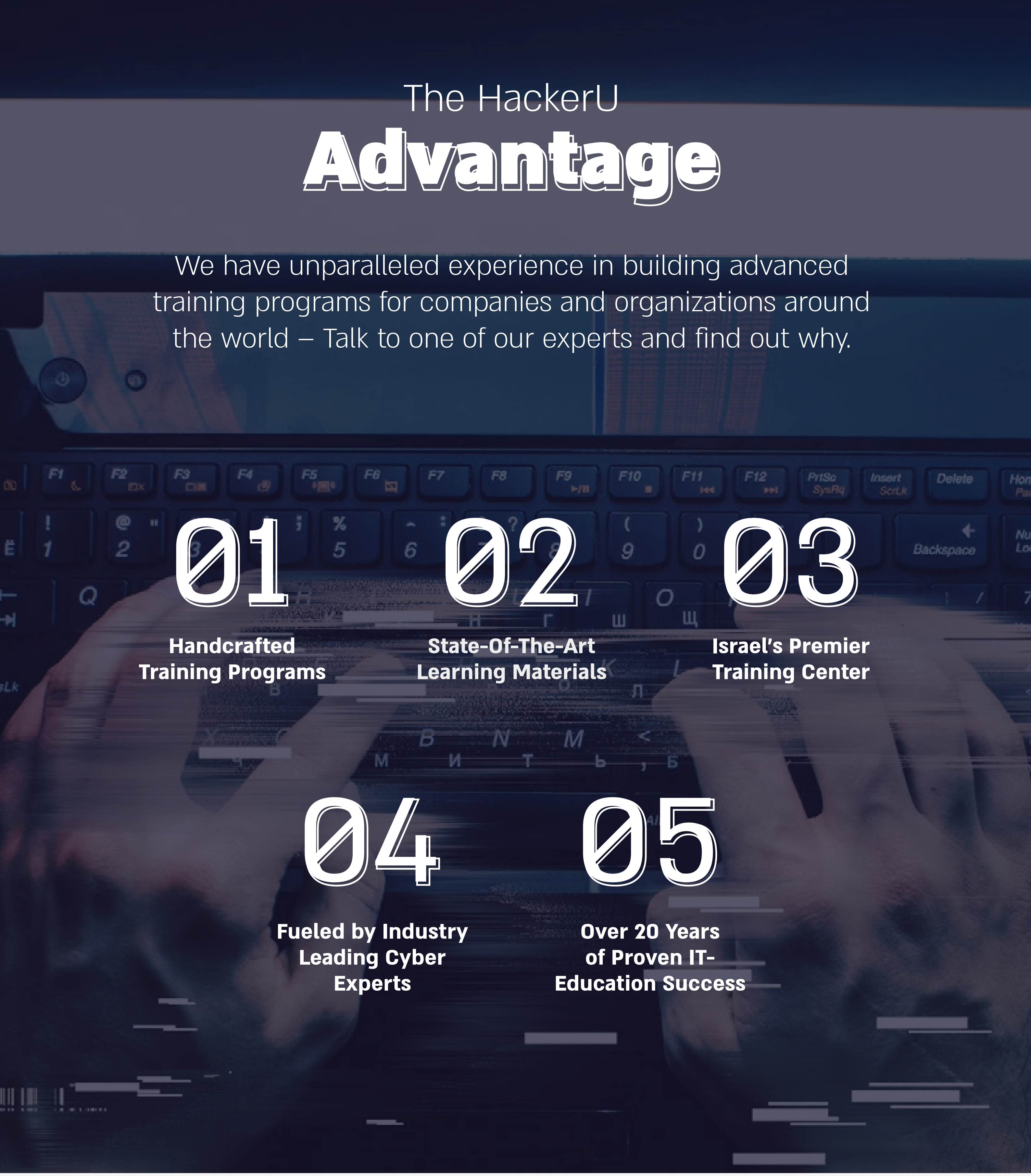
- ELK Components
- ELK installation & Configuration
- ELK Functions
- Threat Hunting with ELK

Day 4

**Module 14**

## Office Exploitation

- VBA & Macro Injection
- DDEAUTO Word Exploitation
- CSV Injection
- PowerPoint Exploitation
- Social Engineering with SFX
- Full Review over all the modules.



## 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