HACKERU

Cyber Infrastructure & Technology

CB107

05
Days

Cyber Infrastructure & Technology

Outline

This course provides students with the knowledge & practical training needed to design & maintain secure infrastructures. Students will also learn to implement various security countermeasures and build their knowledge base in anticipation of taking the CompTIA Security+ certification exam.

The course provides an in-depth examination of the different methods of defensive infrastructure. The curriculum focuses on how to design a secure architecture and will familiarize students with various security measures that can be used to harden networks, devices, and cloud infrastructure. Students will also learn how to work with Security Information & Event Management (SIEM) solutions, with an emphasis on Splunk, a popular open-source solution currently available on the market.

Target Audience

This course is designed for IT personnel who want to improve their skills in the areas of network monitoring and protection solutions.

Prerequisites

The course is designed for people who are already familiar with client-server communication models, networking concepts, and basic computer operations. They should also be familiar with the topic of potential cyber threats and security awareness.

Objectives

Upon completing this course, graduates will be able to:

- Understand security measures.
- Understand and access common OS logs.
- Harden enterprise services using security solutions.
- Install, manage, and configure SIEM solutions.

Content

Day 1

Module 01
Endpoint Security Measures

- Network & Endpoint Security Introduction
- Problems and Risks
- Endpoint Security Components
- Endpoint Detection & Response
- ClamAV Introduction
- Yara Rules & Signatures
- Whitelist Databases

Day 1

Module 02
Honeypots

- Introduction to Honeypots
- Honeypot Strategy
- Honeytokens
- Honeypot Products
- Valhala Honeypot
- Evasion

Day 2

Module 03
Data Loss Prevention

- Sensitive Data
- Data Leak Channels
- Regular Expressions
- DLP Introduction
- OpenDLP
- Risk
- DLP Bypass Techniques

Day 3

Module 04
Mail Security

- DNS Intro
- Mail Protocols
- DNS Mail Protection
- Mail Headers
- Mail Relay Introduction
- Mail relay Concepts
- Mail Relay Features

Learn how to **design secure architecture** and to work with Security Information & Event Management (SIEM) solutions"

Day 4

Module 05
SIEM Introduction

- Security Measures
- Introduction to SIEM
- SIEM Installation
- Log Collection & Types

Day 5

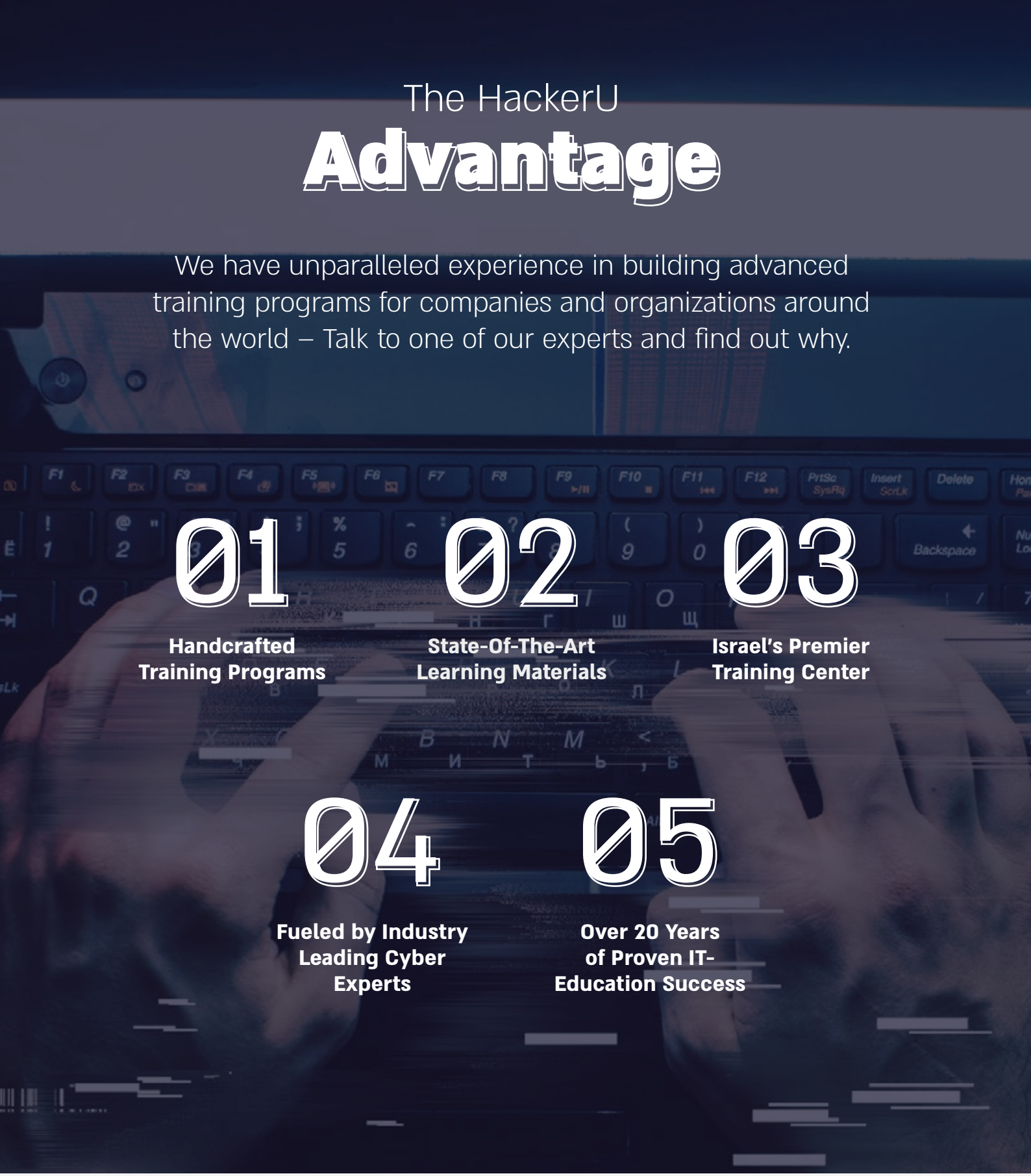
Module 06
Advanced SIEM

- Log Queries
- Log Parsing
- Operators
- Advanced Queries

Day 5

Module 07
SIEM & SOAR

- Alerts
- Trends and Dashboards
- SOAR Introduction
- SOAR Capabilities
- Automation



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