HACKERU

SIEM & SOC

CR107

05
Days

SIEM & SOC

Outline

This course provides students with the knowledge and practical training needed to design and 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:

- This course is designed for IT personnel who want to improve their skills in the areas of network monitoring and protection solutions.
- Students who are looking for employment in SIEM or SOC teams.
- Students who want to join cyber threat incident response teams.
- Students who work in the Cyber Security industry.

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 and how to work with them.
- Understand and access common OS logs.
- Manage Splunk rules and alerts.
- Manage ESET.
- Manage ELK for threat hunting.

Content

Day 1

Module 01
Security Measures

- Network Security Measures
- Endpoint Security Measures
- Additional Security Measures
- SIEM Basics
- SIEM Logs
- SIEM Monitoring

Day 2

Module 02
SIEM Solutions + Log Generation & Collection

- SIEM Operations
- Get to Know Splunk
- Splunk Configuration
- Splunk Logging & Filtering
- Additional Splunk Abilities
- Understanding System Logs

Day 3

Module 03
Log Generation & Collection + Monitoring Attacks

- Windows Event Viewer
- GPO Configuration
- Endpoint Security
- Monitoring Attacks
- Attack Differentiation
- Corelated Rules
- Windows Security Logs

Day 4

Module 04
Security Measures Integration – ESET + SOC Life Cycle

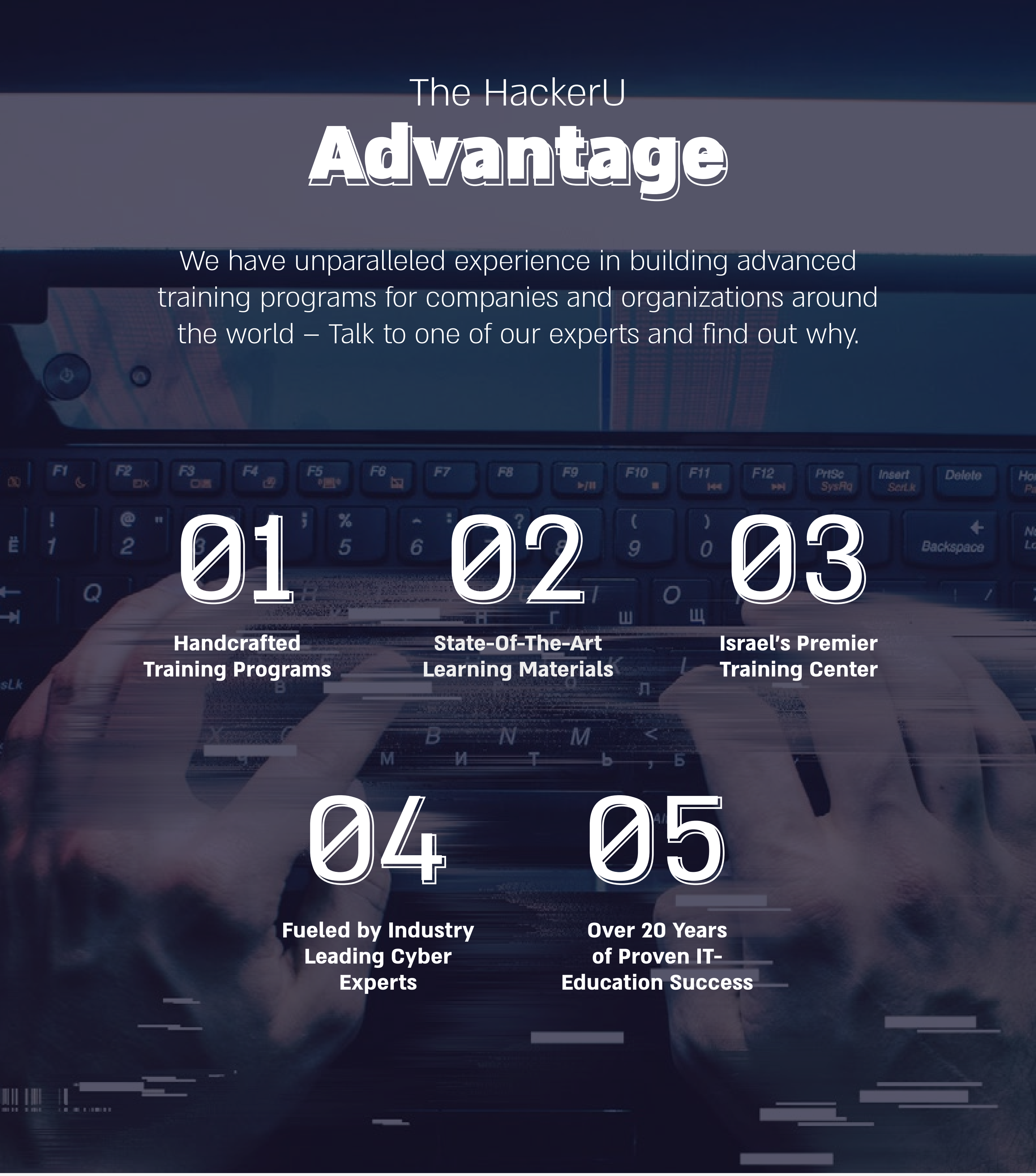
- ESMC & Agent
- Tasks & Group Configuration
- Policy Management
- Mobile Management
- SOC Life Cycle
- Get to Know SOC

Day 5

Module 05
SOC Life Cycle + Threat Haunting Through Logs

- Vulnerability Assessment
- Task Management System
- Policy Management
- Mobile Management
- Threat Hunt Trough Logs
- Get to Know Zeek
- Get to Know ELK

> “**design and maintain**
> secure infrastructures and
> learn how to work with
> Security Information & Event
> Management (SIEM) solutions”



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

hackerupro.com