HACKERU

Introduction To Malware Analysis

CR112

02
Days

Introduction To Malware Analysis

Outline

Malware analysis is a field common to both offensive & defensive security. This course introduces the basics of malware analysis and the use of manual & automated tools to analyze malicious activity & files. During this course, students will learn how to identify & analyze various types of malware. The curriculum focuses on static & dynamic malware analysis techniques. Topics include suspicious file analysis, process monitoring & analysis & network traffic monitoring & analysis. Students will also learn how anti-virus applications operate, and how to create custom AV detection rules.

Target Audience

- SoC analysts and incident responders.
- Junior level penetration testers.
- System security personnel who are interested in malware analysis.

Prerequisites

Before attending this course, students must have the following technical knowledge:

- Working knowledge of the Windows OS and information security.
- Basic knowledge of the Linux OS.
- Basic knowledge of a programming language.

Objectives

Upon completing this course, students will be able to:

- Analyze simple and mid-level malware.
- Investigate malware in contained environments.
- Investigate systems and networks for indicators of compromise.

Content

Day 1 **Module 01**
Introduction to Malware Analysis

- What is Malware analysis
- Types of malware
- Malware analysis types
- Structure of PE files & analysis
- Static analysis methodology
- Sysinternals Suite

Day 1 **Module 02**
Understanding Anti Virus's

- VirusTotal
- AV engines
- Yara Rules
- IoC's and finding them
- ClamAV rule-based detection
- File signatures & manually creating file signatures

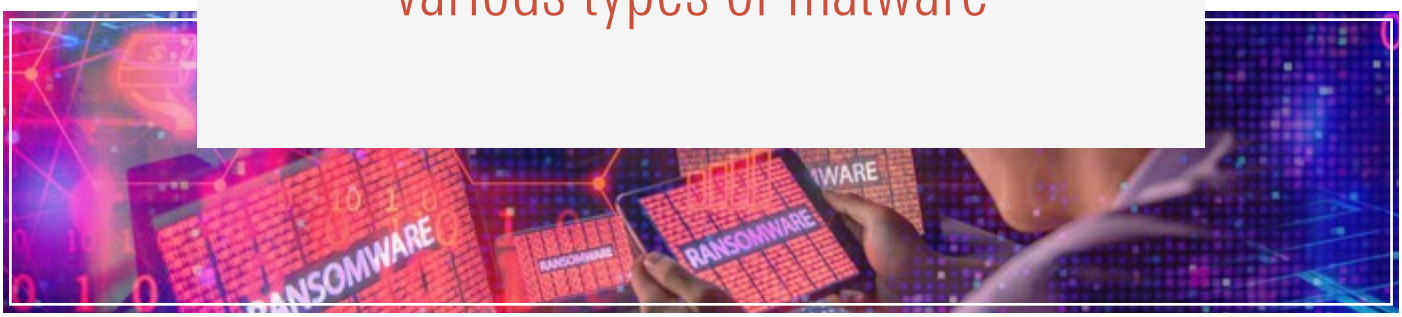
Day 2 **Module 03**
Basic Dynamic Analysis

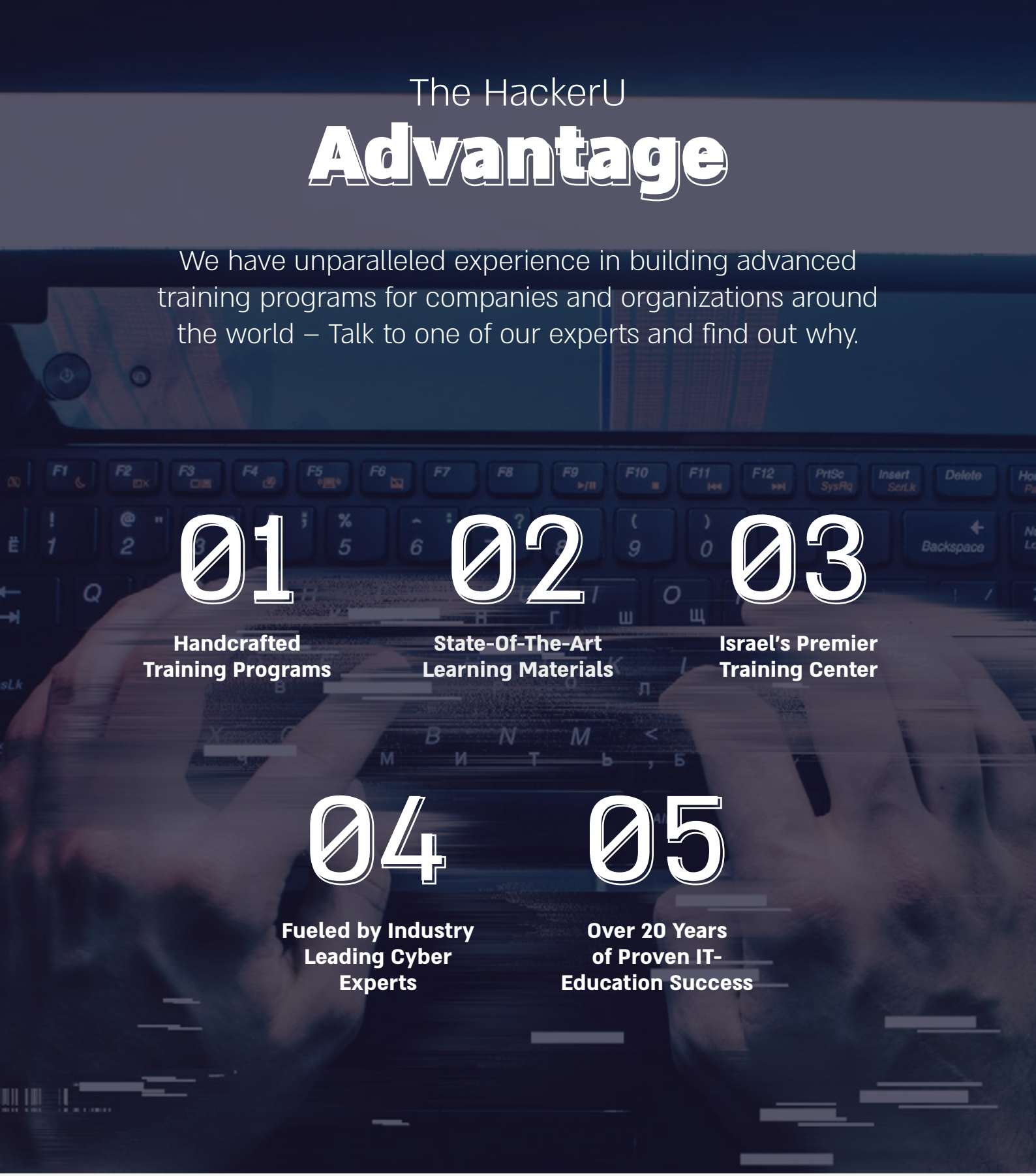
- Dynamic analysis methodology
- Dynamic analysis environments
- DLL files analysis
- Filesystem monitoring
- Registry analysis
- Network monitoring

Day 2 **Module 04**
Sysmon & Sandboxing

- Sysmon installation & Configuration
- Sysmon – Rule-based detection
- Sandbox analysis
- Malware samples

identify and analyze
various types of malware"





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