CounterTack®

CounterTack Training

Introduction to Malware Reverse Engineering

In this course CounterTack will show you the basics of how to capture and analyze memory images and reverse engineer malware found in physical memory. This hands-on virtual class will teach repeatable techniques for acquiring and analyzing live Windows memory using the wide range of functionality of Responder® PRO with Digital DNA® has to offer.

Duration:	4 Hours (CPE Credits: 4 Units)
Prerequisites:	An active Responder PRO license seat is required. Knowledge of Basic Windows OS and computer memory architecture also required. Assembly language preferred. A computer investigations background is helpful.
Who Should Attend:	Tier 1 - 3 Reverse Engineers who are interested in becoming more proficient in capturing and analyzing physical memory images and reverse engineering discovered malware. • Forensic Investigators • IT Security Professionals • Security Analysts • Incident Responders
Course Objectives:	By the end of the course, students will be able to: • Properly acquire a memory image using FastDumpPro • Understand the component of Windows memory • Quickly determine the most malicious code using Responder PRO • Decipher common malware behaviors and techniques
Materials:	Each student is provided the following: • Class student guide • Student lab exercise guide • Student lab solution guide • Certificate of completion
Delivery Format:	Online Virtual Instructor-led Training.
More Info:	See *www.countertack.com/training* or email *marketing@countertack.com*.

CounterTack®

100 5th Ave, First Floor
Waltham, MA 02451-1208
855.893.5428
www.countertack.com