Deloitte.

Deloitte Advanced Cyber Training:
Hunt Malware

The Hunt Malware course provides an in-depth exploration of malware detection and analysis techniques. Participants will learn how to apply hunt methodologies to identify suspicious processes, uncover malware, detect persistence, and analyze malware using both static and dynamic techniques. This course provides cybersecurity professionals with a fundamental understanding of cyber threat hunting, incident response, malware analysis and covers current trends like system and network artifacts and malware hunting in an evolving threat landscape.

Course length

Forty (40) hours of course work, ideally delivered over five (5) consecutive business days.

Program overview

Module 1: Introduction to Hunt Methodology
Module 2: Windows processes
Module 3: Malware persistence
Module 4: Static and dynamic analysis
Module 5: Basics of debugging
Module 6: Living off the Land binaries (LOLBins)
Module 7: Proof of execution
Module 8: Memory forensics and analysis
Module 9: Network artifacts
Module 10: Ransomware and data recovery
Module 11: Current trends
Module 12: Capstone

Value to participants

Deloitte's Advanced Cyber Training courses are designed to be interactive, realistic, and to emphasize hands-on application of presented concepts and material. Additionally, all courses align with the National Institute of Standards and Technology (NIST)/National Initiative for Cyber Security Education (NICE) Workforce frameworks.

Target audience

Cyber professionals involved in or preparing to enter positions including penetration testing, red teaming, incident response, malware analysis, managed detection and response, information security, or hunt operations.

Prerequisites

There are no pre-requisites for attending; however, to ensure maximum participation and training value, Deloitte recommends that attendees have a basic understanding of computer networks and exploitation techniques as well as basic scripting experience.

Delivery options

This course is live/instructor-led and available either virtually or on-site. The course blends multiple instructional methods including lecture, discussion, and extensive hands-on practical lab exercises.

What makes Deloitte's Advanced Cyber Training different?

Deloitte's advanced cyber training includes validated courseware facilitated by accomplished instructors and backed by Deloitte's reputation serving US commercial, defense, and intelligence communities. Whether in-person or virtual, Deloitte's Advanced Cyber Training courses are designed to help participants and organizations develop and mature their defensive cyber capabilities.

Approach

- Deloitte's mission is to help participants to attain an **advanced** level of cybersecurity knowledge, skill and ability (KSA)
- **Delivery methods** are based on US Department of Defense (DoD) and Intelligence Community (IC) training protocols
- Operations and **real-world scenario** directed training
- KSAs are developed via **lecture, discussion, and various hands-on exercises**

Talent

- Deloitte's **experienced training team** provides more than content facilitation; instructors present the mindset associated with offensive and defensive cyber operations and provide real-world mission insight and experience
- Instructors have participated in and developed national-level **offensive and/or defensive cyber operations**

Trusted

- Deloitte's Advanced Cyber Training combines **root9B's (R9B**) training catalog and experience with Deloitte's high-quality reputation and resources
- Prior to acquisition by Deloitte in 2021, R9B was a **trusted training provider** for the DoD for more than (7) years providing training and mission qualification evaluations to DoD cyber operations organizations
- Mature and well-defined training program providing learning objectives that map to **NIST/NICE** job work role frameworks

Accessible

- Training fees are **competitive** with industry peers
- All courses are live, instructor-led and delivered either **in-person** or **virtually** via live video conferencing
- **Flexible** course schedule designed to meet client demands
- Diverse catalog of offerings that can be **tailored to custom requirements**
- Training is operations focused, but caters to professionals serving **multiple security roles and specialties**

Multifaceted

- **Modular content design** that allows for clients to define training requirements based upon need and known gaps in learner KSAs
- **Deloitte's evolving content** presents learners with exposure to emerging adversary tactics, techniques, and procedures (TTPs) and industry leading practices
- Current course catalog includes **Cyber Threat Intelligence Analysis**, **Adversary Tactics and Techniques**, **Hunt Methodology**, **Threat Methodology, Active Cyber Analytics,** and more

Contact usadvancedcybertraining@deloitte.com or one of the professionals below to learn more about Deloitte's Advanced Cyber Training opportunities and capabilities.

Michelle Stele
Managing Director
Cyber Strategy & Transformation
Deloitte & Touche LLP
Work: 719 313 0750
Email: mstele@deloitte.com

Michael Tessier
Specialist Leader
Cyber Defense & Resilience
Deloitte & Touche LLP
Work: 850 521 4846
E-mail: mitessier@deloitte.com

Kiley Weigle
Specialist Master
Cyber Strategy & Transformation
Deloitte & Touche LLP
Work: 443 819 8965
E-mail: kweigle@deloitte.com

Deloitte's Advanced Cyber Training Website: