Deloitte.

Deloitte Advanced Cyber Training:
Cyber Threat Intelligence Analysis

Cyber Threat Intelligence Analysis course (CTIA) guides analysts and defenders through the process of planning, collecting, analyzing, reporting, and integrating cyber threat intelligence into network defense operations.

Course length

CTIA is typically offered in 16-or 40-hour programs, however the duration of the course can be tailored to meet specific client requirements.

Program overview

Module 1: Introduction to Cyber Threat Intelligence (CTI)
Module 2: CTI Lifecycle
Module 3: Data Sources for CTI
Module 4: Tools and Techniques
Module 5: OSINT Data Collection Lab
Module 6: CTI Analysis
Module 7: MITRE ATT&CK® & D3FEND Frameworks
Module 8: Operationalizing CTI
Module 9: Advanced Topics in CTI
Module 10: Real-World Threat Scenario Lab

Value to participants

- CTIA provides an in-depth introduction to intelligence practices and the role of cyber threat intelligence in cybersecurity planning and defensive cyber operations.
- The course also guides participants through leading practices in cyber collection, information processing, exploitation operations, and the production of CTI deliverables.
- CTIA equips participants with strategies for implementing CTI-driven proactive defensive cyber operations and enhancement of the cyber resilience of their organization.

Target audience

CTIA develops the knowledge, skills, and abilities (KSA) for cyber professionals serving in both technical and non-technical roles, including—but not limited to—All-Source Analysts, Cyber Operators, Network Operations Specialists, and Cyber Defense Analysts.

Prerequisites

There are no prerequisite training requirements for CTIA.

Delivery options

CTIA is live, instructor-led and available either virtually via live video conferencing or on-site at the customer's location. Virtual instructor-led training can be presented over consecutive days or in nonconsecutive sessions of four (4) to eight (8) hours.

What makes Deloitte's Advanced Cyber Training different?

Deloitte's advanced cyber training includes 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 KSAs
- **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 the National Institute of Standards and Technology (**NIST**)/National Initiative for Cyber Security Education (**NICE**) job work role frameworks and to the DoD Cyber Workforce Framework

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: