

Deloitte Advanced Cyber Training: Cyber Threat Intelligence Analysis

Deloitte Advanced Cyber Training's 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 Threat Intelligence
Module 2: Bias and Cognition
Module 3: Planning and Direction
Module 4: Collection, Processing, and Exploitation
Module 5: Analysis and Production
Module 6: Dissemination, Integration, Evaluation, and Feedback
Module 7: Intelligence-driven Network Defense Operations and Capstone Exercise



Value to Participants

- CTIA provides a comprehensive introduction to intelligence practices and the role of cyber threat intelligence in cybersecurity planning and operations.
- The course also guides participants through leading practices in cyber collection, information processing, exploitation operations, and the production of intelligence deliverables.
- CTIA equips participants with strategies for implementing intelligence-driven network security operations to enhance 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 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 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 **diverse 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**
- Deloitte's **diverse training team** provides more than content facilitation, including the mindset associated with offensive and defensive operations and real-world operational insight



Trusted

- Deloitte Advanced Cyber 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 National Institute of Standards and Technology (**NIST**)/National Initiative for Cybersecurity Education (**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 KSA
- **Deloitte's evolving content** presents learners with exposure to emerging adversary tactics, techniques, and procedures (TTP) 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

Please contact usadvancedcybertraining@deloitte.com or one of the executives below to learn more about Deloitte Advanced Cyber Training opportunities and capabilities.



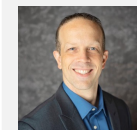
Ryan Roberts

Principal
Cyber and Strategic Risk
Deloitte & Touche LLP
Work: 303 305 3932
Email: rroberts@deloitte.com



Michael Tessier

Specialist Leader
Cyber and Strategic Risk
Deloitte & Touche LLP
Work: 850 521 4846
E-mail: mitessier@deloitte.com



Eric Stride

Specialist Executive
Cyber and Strategic Risk
Deloitte & Touche LLP
Work: 210 390 3278
Email: estride@deloitte.com

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.