

Deloitte Advanced Cyber Training:

Active Cyber Analytics Course

Deloitte's Active Cyber Analytics Course (ACAC) provides cyber defenders with a new set of tools to successfully analyze large collections of mission data. Collection, refinement, scripting, descriptive statistics, and visualizations come together to help the operator find "useful patterns" left behind by a potentially malicious actor.



Course length

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



Program overview

Module 1: Introduction to Data Analytics
Module 2: Data Basics
Module 3: Scripting
Module 4: Data Wrangling
Module 5: Tests & Statistics
Module 6: Visualizations and Analysis
Module 7: Report Writing & Capstone Exercise



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

This course is intended for host or network cyber threat hunters and covers developing and refining analytic tests used in hypothesis-based hunting. Data collection/refinement, scripting/querying essentials, descriptive statistics, and visualizations will be leveraged to find "useful patterns" left behind by a potentially malicious actor.



Prerequisites

While there are no formal prerequisites for this course, experience as a host or network threat hunter and/or with scripting languages (ideally Python or PowerShell) are recommended.



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:



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.