

ATTACKIQ




AttackIQ Academy

Course Catalogue

AttackIQ Academy

The AttackIQ® Academy offers entry-level and advanced cybersecurity training, modularized curriculum, and cyberrange labs to partners, customers, and prospective customers. These labs offer a scalable, cloud-hosted infrastructure that will provide learners with virtual environments for realistic, hands-on cybersecurity labs and exercises. Students practice with real-world scenarios that give them the skills to recognize threats, understand attackers' methods, and quickly shut threats down.



"We created AttackIQ Academy because we believe strongly in the mission of MITRE ATT&CK, the power of Breach & Attack Simulation (BAS), and the innovation of Purple Teaming. Together, they supply the missing ingredient for security programs: closed-loop feedback to optimize effectiveness. You can't defend your organization unless you can plan your defenses against well-defined threats, measure how well those defenses are working, and execute improvements, all on a continuous basis. This coursework is designed to provide concrete instruction in getting this done."

- Carl M Wright, Chief Commercial Officer, AttackIQ

AttackIQ Academy enables Security Teams to:

- Experience real-world threats in a safe and secure environment.
- Learn to rapidly identify and mitigate threats.
- Better defend against current threats, helping to avoid the expense, loss of revenue, and reputational damage of a data breach.
- Adopt and utilize cybersecurity industry best practices, reducing operational expense and saving money.
- Reduce team turnover with improved employee satisfaction and better career paths supported by essential training and certification credits.
- Be better equipped to meet the security operations baselines of industry and government compliance mandates.
- Make better decisions about the selection, deployment, and configuration of security controls.

For the AttackIQ Partner Community, online modules include basics on go-to-market deployment and configuration of AttackIQ's BAS platform and the best practices necessary to fully configure security control performance assessment. Advanced classes will target specific defender techniques to operationalize MITRE ATT&CK to defend against new and emerging threats and to focus threat intelligence data into an actionable program that customers and partners can deploy.

Special training modules, such as Purple Team Enablement and Deployment, offer a unique opportunity for customers and partners to pivot their defensive strategies and better leverage MITRE ATT&CK with a BAS platform. Certifications include those for sales, technology, professional services, and managed security service providers.



"AttackIQ Academy gives us the capabilities we need to help our customers operationalize MITRE ATT&CK and deliver the advanced capabilities needed to meet and defeat the advanced threats in our current environment."

- Matt Stamper, CISO & Executive Advisor, EVOTEK

Course Catalogue

Learning Path: Purple Teaming

- Foundations of Purple Teaming - Entry Level

This training session introduces the state-of-the-art practice of purple teaming and its essential nature as the joint operation of red and blue teams. Students will learn the core concepts, workflows, activities, and artifacts underpinning purple team methods, and complete the class with both a clear understanding of the role of purple teams in a threat-informed defense strategy and with the skills required to plan a foundational purple-team exercise within their own environment.

- Emulation Planning for Purple Teams - Intermediate

This course will delve deeper into concepts from Foundations of Purple Teaming. Students will learn key processes enabling sound threat intelligence integration and organizational threat alignment in support of purple team exercises and will create emulation plans based on the business requirements and IT architecture of a fictional scientific research organization to better understand their own threat environment and actionable plans toward defending it.

- Threat Alignment for Purple Teams - Intermediate

This course will delve deeper into concepts from Foundations of Purple Teaming. Students will learn key processes for enabling sound threat intelligence integration as well as organizational threat alignment in support of purple team exercises. Students will then create threat models based on the threat environment, business requirements, and IT architecture of a fictional scientific research organization to better understand mission alignments with threat-informed defenses.



"The AttackIQ Purple Teaming course was an excellent primer on what it takes to get a Purple Team up and running with clearly defined processes to support a long term program...I recommended this to my team already and would recommend to all security practitioners interested in improving cyber defense."

- Tom Needham, Director Cyber-Security Operations, Cyber Threat Action Center, Abbott

Course Catalogue (cont.)

Learning Path: Breach and Attack Simulation

- Foundations of Breach and Attack Simulation (BAS) - Entry Level

This hands-on training program introduces the capabilities and deployment options of a BAS (breach and attack simulation) platform. Students learn and apply testing methodologies used to emulate adversarial techniques and measure the efficacy of various security control implementations and configurations. The course includes advanced topics such as building a threat-informed defensive strategy and operationalizing the MITRE ATT&CK framework. Hands-on cyberrange labs are included.

- Assessment Design for Gap Analysis - Intermediate

This course brings together the fundamentals learned in Foundations of Breach & Attack Simulation through real-world scenario-based hands-on labs. There will be a strong focus on designing and executing assessments in the AttackIQ Platform. During this course, students will learn how to design a threat-informed assessment and an assessment for purple teaming.

- Assessment Design For Security Controls - Intermediate

This course brings together the fundamentals learned in Foundations of Breach & Attack Simulation through real-world, scenario-based hands-on labs. During this course, there will be a strong focus on designing and executing assessments in the AttackIQ Platform. Students will learn how to design an assessment for security control validation, an assessment for bakeoffs, an assessment for implementation, and an assessment for continuous security validation.

- Custom Scenario: TTP Development - Advanced

This training session will provide an overview of advanced customization options and scenario content development within the AttackIQ Open System Testing Platform. This hands-on, instructor-led course will teach students how to create test scenarios via customization of Parameters, Payload/Scripts, and Python. Students will learn how to share custom content within your organization and the AttackIQ Community. As part of the lab, students will develop FIN7 discovery of data (T1082) will exfiltrate that data (T1043) by designing their very own multi-phase scenario.

- DevSecOps: Leveraging AttackIQ API - Advanced

This three-part series will instruct students on how to develop applications with the AttackIQ Open System Testing Platform API to operationalize and create a fully automated BAS based SecDevOps capability. Through a series of class discussions and hands-on exercises, students will write several platform API applications to create and run security assessments and analyze the effectiveness of their security controls.



"The AttackIQ Academy Purple Team and BAS training courses were a phenomenal activity to listen and learn about from a capability perspective; how the tool evolves with each team's needs...Also, the training was of great value from both a technical and management team perspective."

- Radel Vazquez, Senior Security Engineer, Threat Management, ADP Global Security Organization

Course Catalogue (cont.)

Learning Path: MITRE ATT&CK

- Foundations of Operationalizing MITRE ATT&CK - Entry Level

This training session introduces students to the basics of the MITRE ATT&CK framework. Topics include its history and evolution, reasons why organizations are adopting it, and the basic workflows an organization uses to operationalize MITRE ATT&CK within its security program. The class also covers the tools and resources available to supplement MITRE ATT&CK testing, including ATT&CK Navigator and Joystick.

- Applying MITRE ATT&CK Navigator - Intermediate

This course expands upon the key concepts taught in Foundations of MITRE ATT&CK, with a strong focus on the tools that have been developed to operationalize the MITRE ATT&CK framework. In this training, students will deep dive using the ATT&CK Navigator in hands-on lab activities. During this course, students will learn key concepts of ATT&CK Navigator, Navigator controls, and how to import and export Navigator data.

- Applying MITRE Threat Report ATT&CK Mapper (TRAM) - Intermediate

This course expands upon the key concepts taught in Foundations of MITRE ATT&CK, with a strong focus on tools that have been developed to operationalize the MITRE ATT&CK Framework. In this training, students will learn key concepts of TRAM, how to install TRAM, how to find data sources, and how to analyze and categorize data using TRAM in hands on lab activities.

If you have any questions or would like to learn more about AttackIQ Academy, please get in touch with **Keith Wilson**, Director of AttackIQ Academy, at academy@attackiq.com.

ATTACKIQ

U.S. Headquarters
2901 Tasman Dr. Suite 112
Santa Clara, CA 95054
+1 (888) 588-9116
info@attackiq.com

About AttackIQ

AttackIQ, the leading independent vendor of breach and attack simulation solutions, built the industry's first Security Optimization Platform for continuous security control validation and improving security program effectiveness and efficiency. AttackIQ is trusted by leading organizations worldwide to plan security improvements and verify that cyberdefenses work as expected, aligned with the MITRE ATT&CK framework. The Company is committed to giving back to the cybersecurity community through its free [AttackIQ Academy](#), open Preactive Security Exchange, and partnership with the [MITRE Center of Threat Informed Defense](#).

For more information visit www.attackiq.com. Follow AttackIQ on [Twitter](#), [Facebook](#), [LinkedIn](#), and [YouTube](#).

Copyright © 2020 AttackIQ, Inc. All rights reserved