PvIB Presentation: Breach & Attack Simulation

ATTACKIQ

The official definition of “breach and attack simulation” technologies:

Gartner defines breach & attack simulation (BAS) technologies as tools “that allow enterprises to continually and consistently simulate the full attack cycle (including insider threats, lateral movement, and data exfiltration) against enterprise infrastructure, using software agents, virtual machines, and other means.”

Presentation & Workshop By: AttackIQ
Jose Barajas, Director of Global Engineering – jose.Barajas@attackiq.com
Maarten Kok, Sales Director Northern Europe – maarten.kok@attackiq.com

Functionality of Breach & Attack Simulation

ATTACKIQ

1. Allows enterprises to automatically emulate comprehensive, multistage adversary campaigns using software agents, virtual machines, and other means.

2. Provides a detailed summary of results and efficacy of security controls, as well as the personnel that support them.

3. Enables security analysts to find protection failures and capability gaps, strengthen security posture, and improve incident response capabilities.

4. Assesses readiness and validates that enterprise security systems are performing as originally intended, guaranteeing a return on investment.

5. Provides automation that enables platforms to work autonomously and at scale to support business growth.

6. Enables analysts to see in real time how changes to configurations or administration can open new risks.

Industry challenges creating the need for security control validation

ATTACKIQ

1. Security controls fail everywhere, and they do so constantly and silently.

2. Companies deploy on average 47 different cybersecurity solutions and technologies.

3. 82 percent of enterprise breaches should have been stopped by existing security controls but weren't, Verizon estimates.

4. When a cybersecurity control fails, either through misconfiguration or operational execution, it can go unnoticed for months.

5. The only way to assess cybersecurity effectiveness is, therefore, with an unquantified assessment, a “finger in the air” of how the program feels on a given day

As a result, security teams are faced with three critical obstacles...

3 Critical Obstacles

ATTACKIQ

1. Complexity and inefficiency
On average, companies deploy 47 different cybersecurity solutions and technologies in their environment. There's no good way for them to ensure they're working efficiently and cost effectively without a breach and attack simulation platform.

2. The alternative to BAS for penetration testing and control validation - “red teaming” - is very people intensive
Without a proper BAS platform, most organizations have a red team either on their own staff or contracted externally. The challenge is that red team testing is infrequent, and the coverage delivered is therefore limited by personnel hours; as a result, coverage is unfortunately smaller than the scale of the security team's defenses. Humans can also only cover limited terrain compared to an automated solution.

3. Lack of an automated control validation platform leads to breaches
Manual control validation is also a common tactic that often leads to silent failure of controls. Security teams who rely on this tactic only leave the organization more vulnerable to breaches.

Why breach and attack simulation is important for cybersecurity teams

ATTACKIQ

- Gartner Blog: The quantification companies use to present risk and security is often expressed in terms of money and likelihood of damage. These calculations, Gartner contends, “are often based on assumptions and 'expert opinion' that essentially dictate the result, rather than real quantitative business assessment. Using the veneer of quantification to get what you want does not support improved cybersecurity.” Cybersecurity teams need real quantification..

- This is where breach and attack simulation comes in. It emulates real-world attacks so that organizations can test and validate how their security controls (composed of people, processes, and technologies) perform against existing threats.

- Furthermore, as adversaries have accelerated attacks, a paradigm shift is occurring. Chief information security officers are putting a strategic emphasis on proactive prevention and insights using automation, rather than relying only on reactive detection and response controls. Regulation is increasing significantly with each year, which leads to more intrusive processes (including questions and assessments) by regulators.

- By automating control validation, security teams benefit from a “force multiplier” effect that enables them to conduct more simulations, more quickly, and with greater insights that can be shared across red, blue, and risk teams. By taking a purple team approach, teams are able to continually improve the effectiveness and efficiency of their security programs in a dynamic and fast-paced threat landscape.

The evolution from BAS to Security Optimization

ATTACKIQ

While cybersecurity risks have continued to increase, budgets remain uncertain, and the socio-economic impacts of the COVID-19 pandemic linger, BAS is no longer considered a tool for breach and attack simulation or security control validation exclusively — but as a way to provide business value by maximizing resources and decreasing management burdens on teams.

Organizations are leveraging a new generation of innovative platforms built on BAS technology to maximize the effectiveness and efficiency of their cybersecurity program as a whole through security optimization, from technical effectiveness to regulatory compliance.

Security optimization requires competence in three areas:

1. Identifying and quantifying cybersecurity risks by measuring the performance of existing security controls against actual threats
2. Prioritizing measurements and security investments based on a “threat-informed defense” strategy that measures security program performance against known threat actor tactics, techniques, and procedures
3. Continuously calibrating staff skills, processes, and technology to maintain the desired security posture, given existing budget constraints.

Top 3 benefits of automating Breach & Attack Simulation

ATTACKIQ

1. **Enhanced insights:**

A reliable BAS platform will generate insights and improve decisions across the complete security organization, from risk to operations and compliance — and offer a rich depth of use cases to improve effectiveness across the security program. The three pillars of insight of a threat-informed defense strategy are known threats (aligned to the MITRE ATT&CK® framework), security control efficacy, and risk management on the basis of key compliance frameworks (like NIST 800-53).

2. **Better business decisions**

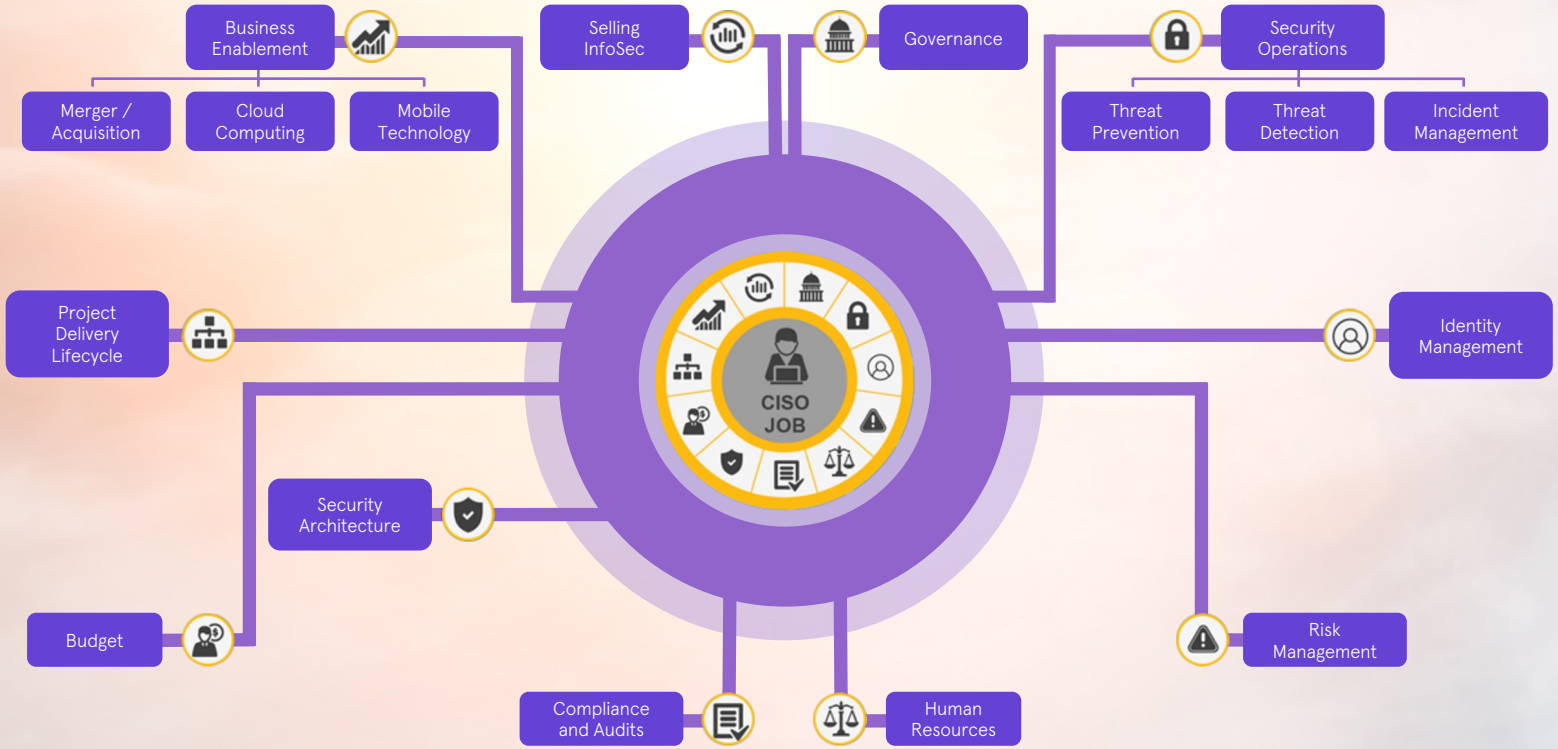
- Make better decisions about people, processes, and technologies.
- Maximize return on investments and inform future investment decisions.
- Identify control and organizational weaknesses so your program performs as planned.

3. **Real security outcomes**

BAS verifies security capabilities across your entire enterprise, raising efficiency, productivity, and effectiveness by measuring security program performance against known threat behaviours.

About AttackIQ - Our Mission

ATTACKIQ

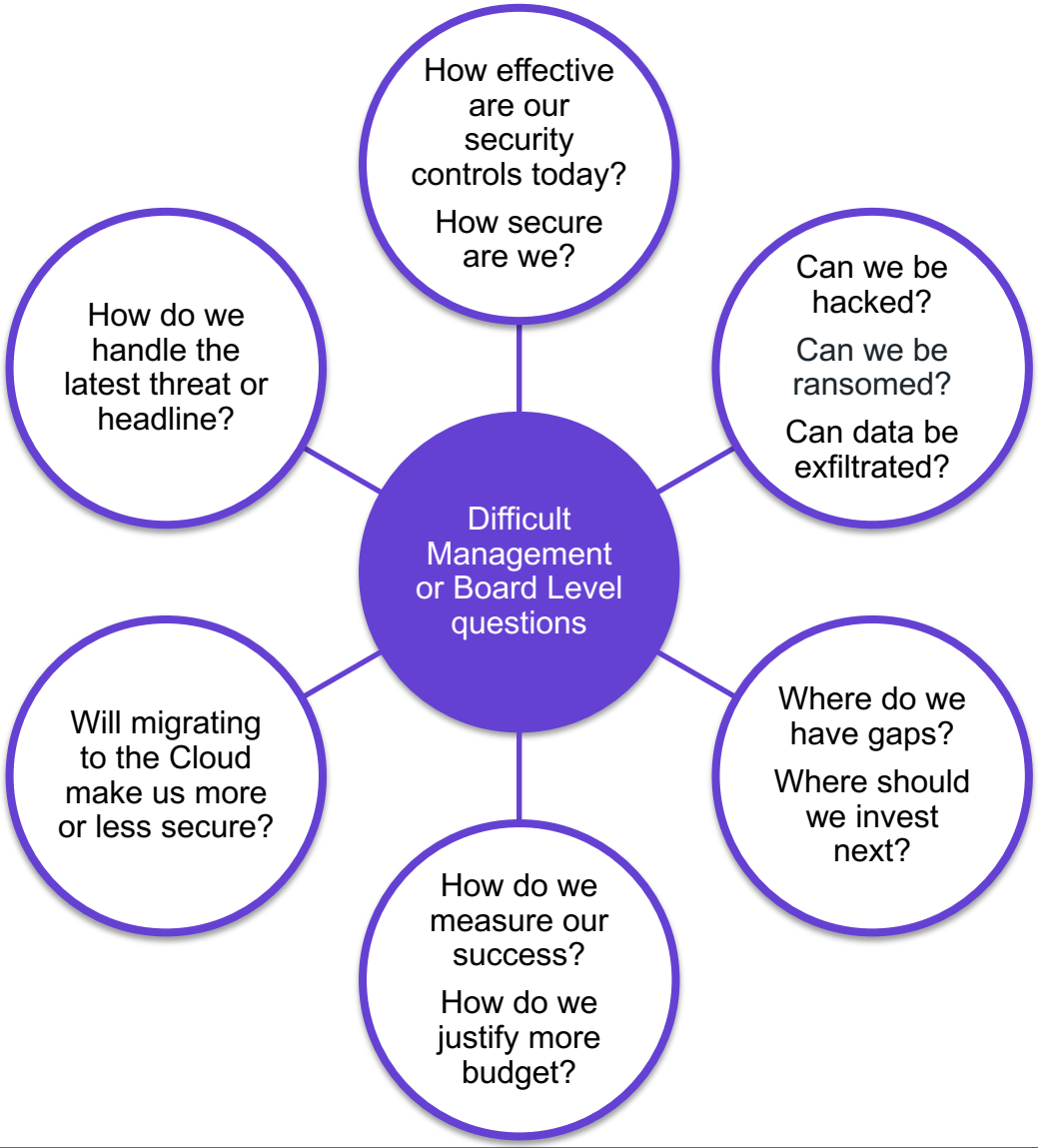


Help CISOs achieve their mission by delivering a Threat-Informed decision support system:

- From ad hoc and open loop *to planned and closed loop*
- From a matter of lore *to a matter of engineering*
- From ineffective and inefficient *to effective and efficient*
- From a source of fear *to a business enabler*

Build confidence with intelligence base evidence

ATTACKIQ



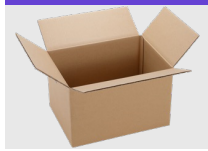
AttackIQ Security Optimization Platform

ATTACKIQ

Scale

Safe Production Testing

Openness



Open Testing Platform

Vision

People, Process & Control Effectiveness

Broadest & Deepest Content

MITRE ATT&CK

MITRE ENGENUITY | Center for Threat Informed Defense
FOUNDING RESEARCH PARTNER

Community & Practice

INFORMED DEFENDERS

ACADEMY

Purple Hats CONFERENCE

Services

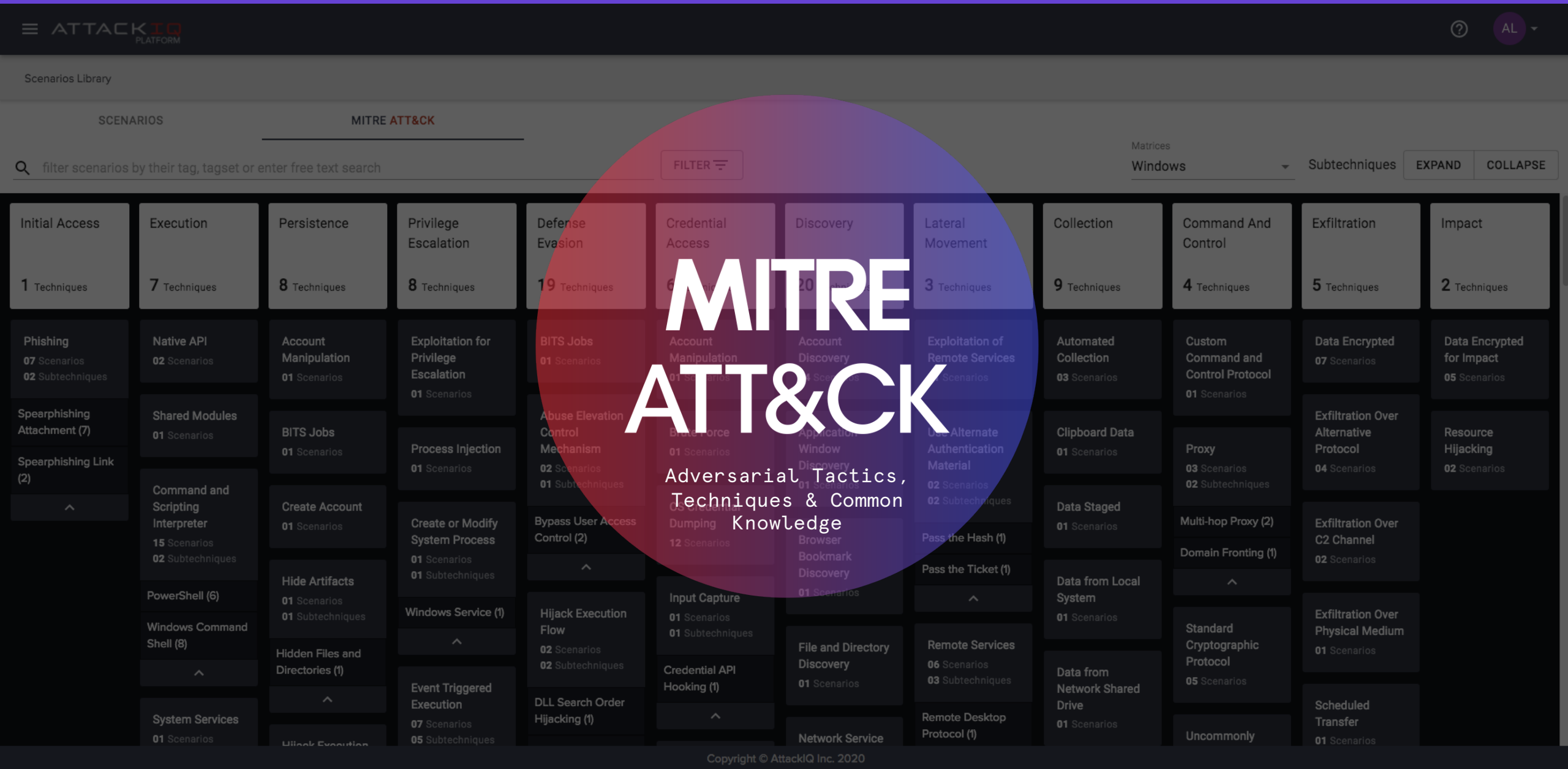
AttackIQ Vanguard:
Helping security teams identify control gaps before the adversary does.

AttackIQ Vanguard Edge

AttackIQ Vanguard Premier

Automate MITRE ATT&CK Framework

ATTACKIQ

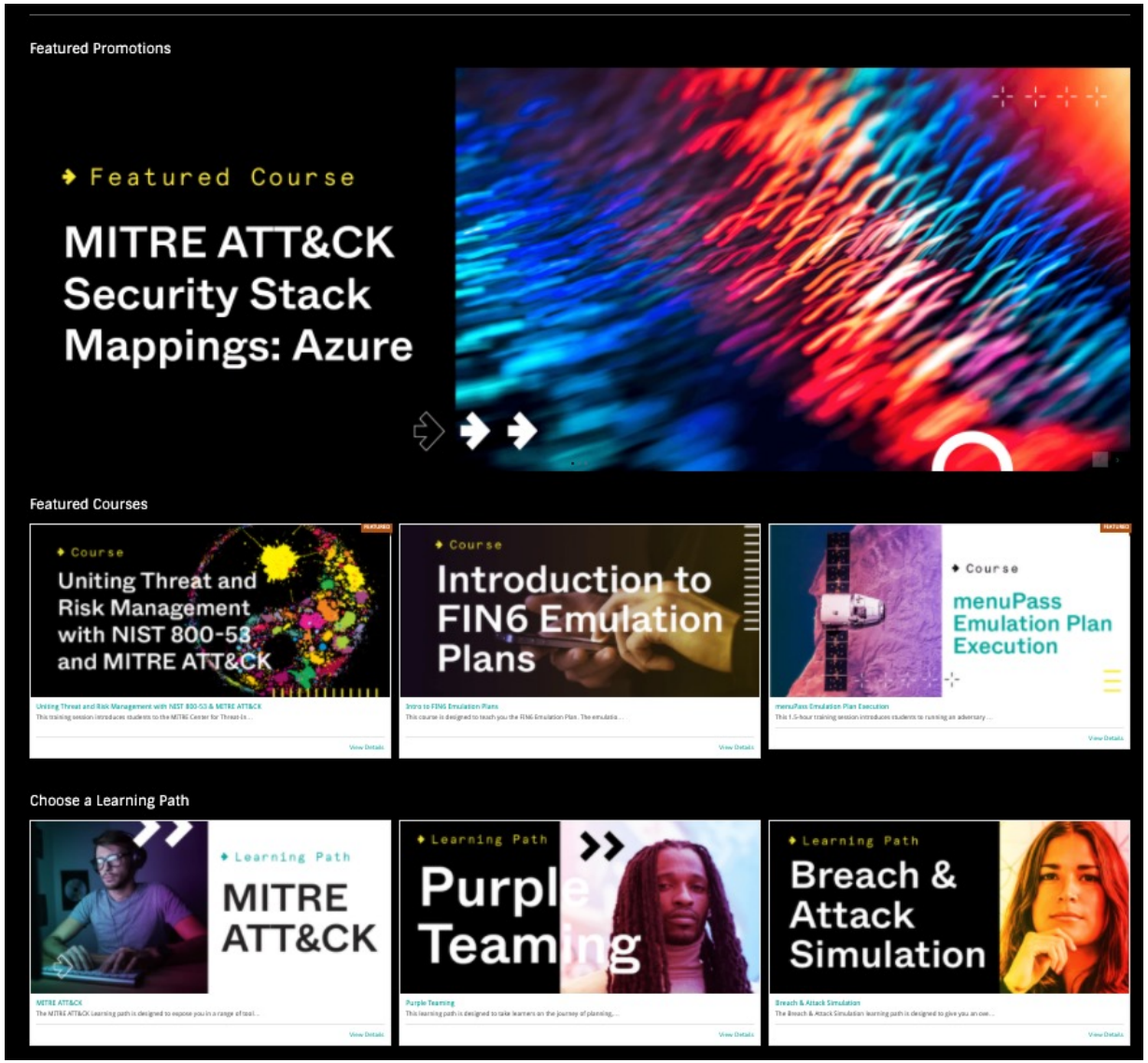


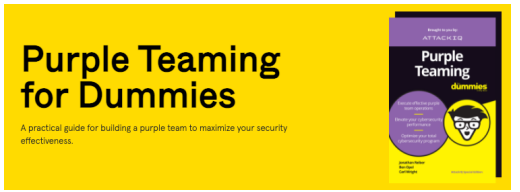
AttackIQ Academy

Practice Creation + Community

27,000+ Cybersecurity Students from 180+ countries

ATTACKIQ





https://academy.attackiq.com/

https://academy.attackiq.com/courses/beyond-atomic-testing-with-attack-flows

Additional resources:

ATTACKIQ

AttackIQ Academy, for free-of-charge, high quality training: https://academy.attackiq.com/

Breach & Attack Simulation 101 Guide download: https://attackiq.com/lp/breach-and-attack-simulation-101-guide-ty/

MITRE ATT&CK: https://attackiq.com/mitre-attack/

AttackIQ Breach and Attack Simulation: https://attackiq.com/breach-and-attack-simulation/

AttackIQ Community: https://attackiq.com/who-we-are/attackiq-community/

AttackIQ Security Optimization Platform: https://attackiq.com/platform/

Recent Case Study with ISS World Services: https://attackiq.com/pdf-case-study-iss-world-services/

AttackIQ Customers: https://attackiq.com/customers/

ATTACKIQ

MITRE ENGENUITY™

Thank You.

Questions?