

**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](mailto:jose.Barajas@attackiq.com)

Maarten Kok, Sales Director Northern Europe – [maarten.kok@attackiq.com](mailto:maarten.kok@attackiq.com)

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.

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...**

## **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.

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.

## 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

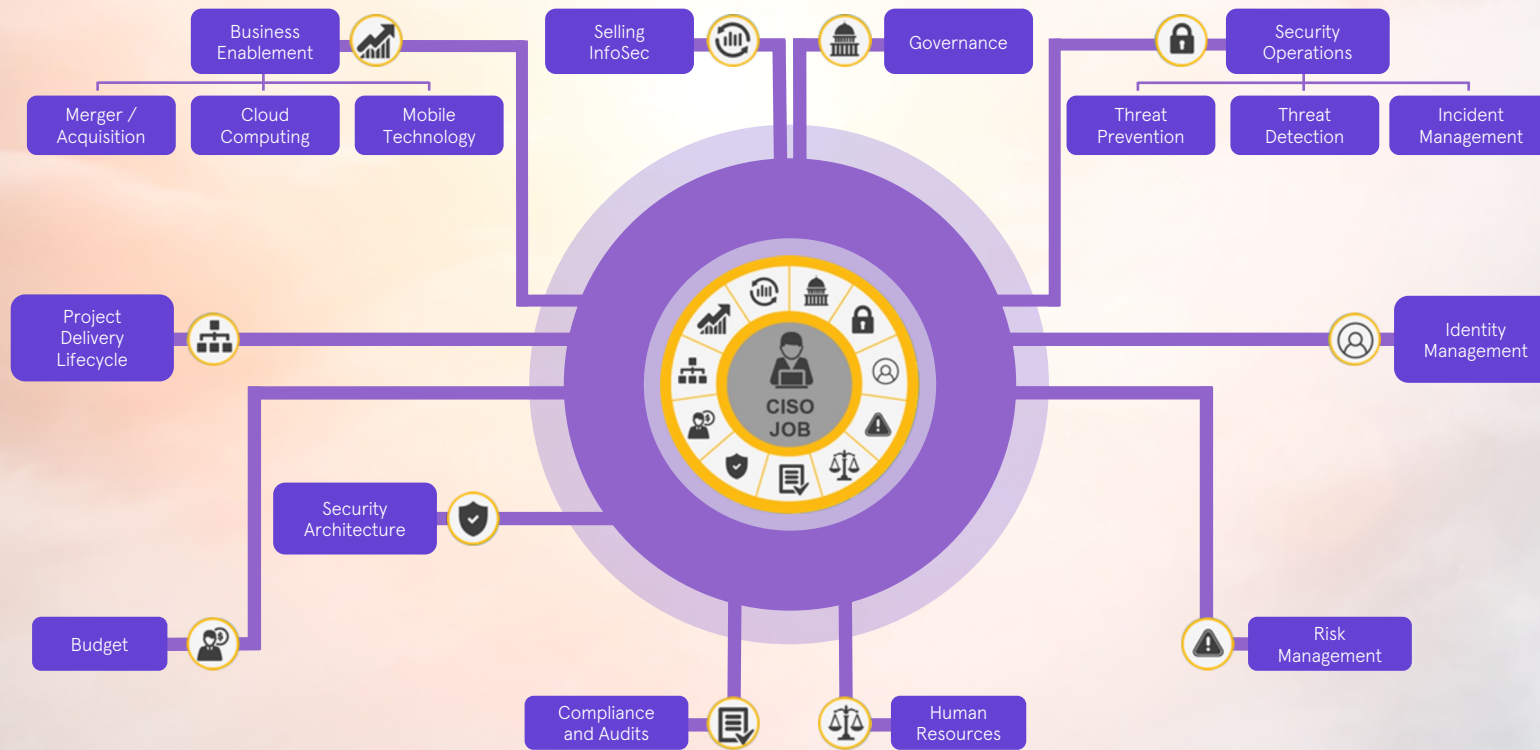
- Make better decisions about people, processes, and technologies.
- Maximize return on investments and inform future investment decisions.
- Identify control and organizational weaknesses so your program performs as planned.

## 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

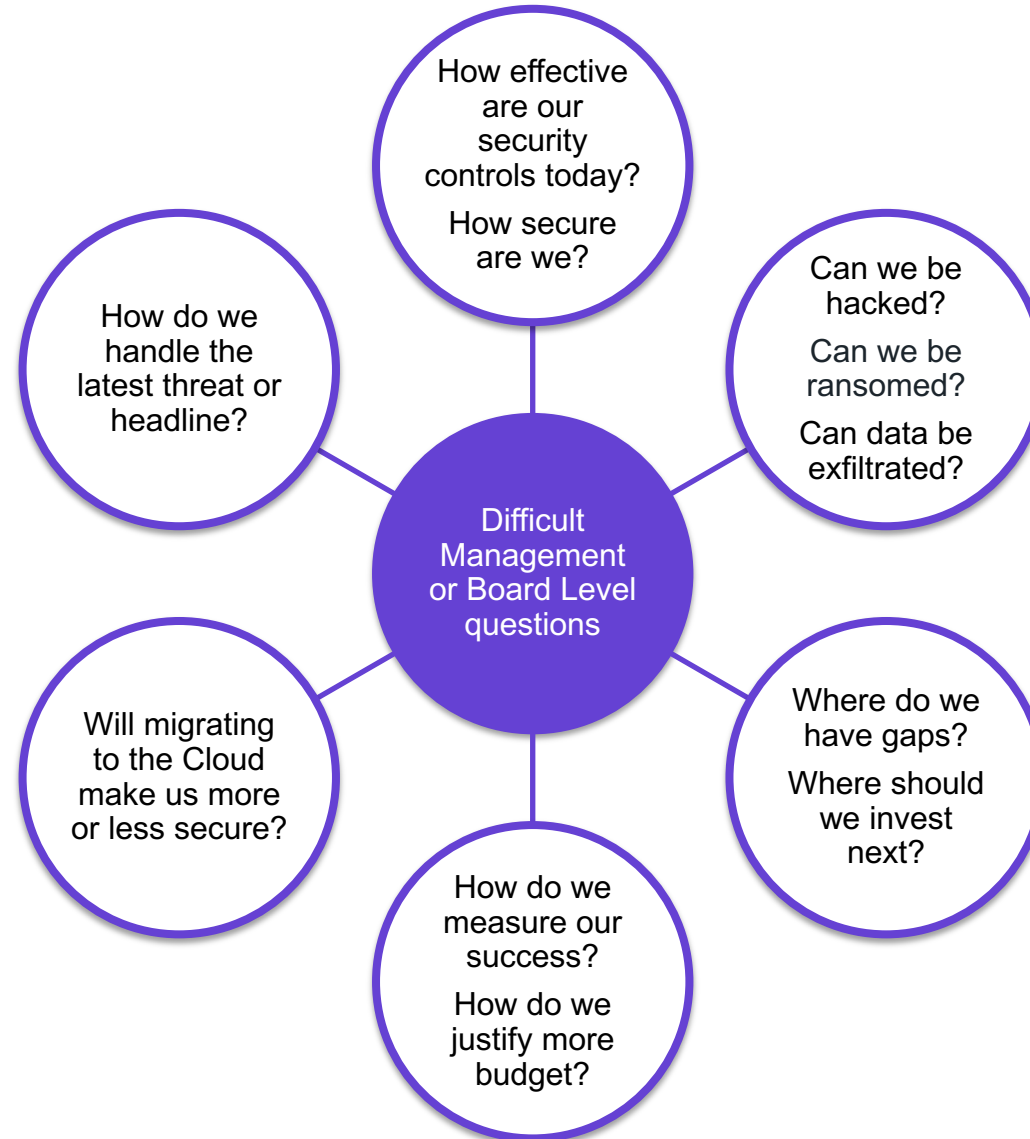


Help CISOs achieve their mission by delivering a Threat-Informed decision support system:

- 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 Security Optimization Platform

ATTACKIQ



Scale



Safe Production Testing



Openness



Open Testing Platform



Vision



People, Process & Control Effectiveness



Broadest & Deepest Content

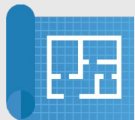
**MITRE** | ATT&CK™

**MITRE**  
**ENGENUITY.** | Center for Threat  
Informed Defense  
FOUNDING RESEARCH PARTNER



Community & Practice

**INFORMED**  
**DEFENDERS**



Services

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

**AttackIQ**  
**Vanguard**  
**Edge**

**AttackIQ**  
**Vanguard**  
**Premier**

# Automate MITRE ATT&CK Framework

Scenarios Library

SCENARIOS

MITRE ATT&CK

filter scenarios by their tag, tagset or enter free text search

FILTER

Matrices

Windows

Subtechniques

EXPAND

COLLAPSE

Initial Access 1 Techniques	Execution 7 Techniques	Persistence 8 Techniques	Privilege Escalation 8 Techniques	Defense Evasion 19 Techniques	Credential Access 6 Techniques	Discovery 20 Techniques	Lateral Movement 3 Techniques	Collection 9 Techniques	Command And Control 4 Techniques	Exfiltration 5 Techniques	Impact 2 Techniques
Phishing 07 Scenarios 02 Subtechniques	Native API 02 Scenarios	Account Manipulation 01 Scenarios	Exploitation for Privilege Escalation 01 Scenarios	BITS Jobs 01 Scenarios	Account Manipulation 01 Scenarios	Account Discovery 01 Scenarios	Exploitation of Remote Services 01 Scenarios	Automated Collection 03 Scenarios	Custom Command and Control Protocol 01 Scenarios	Data Encrypted 07 Scenarios	Data Encrypted for Impact 05 Scenarios
Spearphishing Attachment (7)	Shared Modules 01 Scenarios	BITS Jobs 01 Scenarios	Process Injection 01 Scenarios	Abuse Elevation Control Mechanism 02 Scenarios 01 Subtechniques	Brute Force 01 Scenarios	Application Window Discovery 01 Scenarios	Use Alternate Authentication Material 02 Scenarios 02 Subtechniques	Clipboard Data 01 Scenarios	Proxy 03 Scenarios 02 Subtechniques	Exfiltration Over Alternative Protocol 04 Scenarios	Resource Hijacking 02 Scenarios
Spearphishing Link (2)	Command and Scripting Interpreter 15 Scenarios 02 Subtechniques	Create Account 01 Scenarios	Create or Modify System Process 01 Scenarios 01 Subtechniques	Bypass User Access Control (2)	Dumping 12 Scenarios	Browser Bookmark Discovery 01 Scenarios	Pass the Hash (1) Pass the Ticket (1)	Data Staged 01 Scenarios	Multi-hop Proxy (2) Domain Fronting (1)	Exfiltration Over C2 Channel 02 Scenarios	
	PowerShell (6)	Hide Artifacts 01 Scenarios 01 Subtechniques	Windows Service (1)	Hijack Execution Flow 02 Scenarios 02 Subtechniques	Input Capture 01 Scenarios 01 Subtechniques	File and Directory Discovery 01 Scenarios	Remote Services 06 Scenarios 03 Subtechniques	Data from Local System 01 Scenarios	Standard Cryptographic Protocol 05 Scenarios	Exfiltration Over Physical Medium 01 Scenarios	
	Windows Command Shell (8)	Hidden Files and Directories (1)	Event Triggered Execution 07 Scenarios 05 Subtechniques	DLL Search Order Hijacking (1)	Credential API Hooking (1)	Network Service	Remote Desktop Protocol (1)	Data from Network Shared Drive 01 Scenarios	Uncommonly	Scheduled Transfer 01 Scenarios	
	System Services 01 Scenarios	Block Execution									

MITRE

ATT&CK

Adversarial Tactics, Techniques & Common Knowledge

Featured Promotions

Featured Course

## MITRE ATT&CK Security Stack Mappings: Azure

Featured Courses

- Course: **Uniting Threat and Risk Management with NIST 800-53 and MITRE ATT&CK**
- Course: **Introduction to FIN6 Emulation Plans**
- Course: **menuPass Emulation Plan Execution**

Choose a Learning Path

- Learning Path: **MITRE ATT&CK**
- Learning Path: **Purple Teaming**
- Learning Path: **Breach & Attack Simulation**

ATTACKIQ | Academy

Course Catalog Learning Paths About Academy Testimonials Register Contact Us AttackIQ

## Beyond Atomic Testing with Attack Flows

In this 1.5 hour course, you are introduced to testing EDR or AI-based cybersecurity tools utilizing the AttackIQ Security Optimization Platform. This course will teach you why Attack Flows are important to this testing while giving you practical experience with a lab set in AttackIQ's Cyber Range.

Course

# Beyond Atomic Testing with Attack Flows

**Purple Teaming for Dummies**

A practical guide for building a purple team to maximize your security effectiveness.

**MITRE ATT&CK® For Dummies**

Transform your security program with the MITRE ATT&CK framework.

# Additional resources:

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/>

The background features a dark blue grid. Scattered across the grid are several stylized clouds in shades of purple and blue. Small geometric shapes, including diamonds and dots in orange, purple, and blue, are also placed at various grid intersections.

ATTACKIQ

||| ≡ MITRE  
ENGENUITY™

Thank You.

Questions?