ATTACKIQ

Datasheet

Optimize Your Security Program

Automate Insights to Efficiently and Effectively Optimize Your Cybersecurity Investments

AttackIQ's Security Optimization Platform enables organizations to build a threat-informed defense program, providing automation around a cycle of continuous testing, measuring, and remediating security controls, improving the overall security program end-to-end with better insights, better decisions, and real security outcomes.

Problem

Mounting an effective cyberdefense has always been difficult. The pressure on Chief Information Security Officers (CISOs) has risen further with COVID-19. Adversaries are ramping up attacks, while security resources are becoming increasingly scrutinized. According to Gartner, the urgency to treat cybersecurity as a business decision has never been greater. AttackIQ comprehensively addresses these challenges with its best-in-class software platform, deep partnerships, and investment in the practice of threat-informed defense.

Solution

The AttackIQ Security Optimization Platform was built from the ground up by former security practitioners to help security leaders move beyond fighting fires and cost reduction to a strategic security program that delivers both improved effectiveness and efficiency.

The AttackIQ Security Optimization Platform enables risk and security practitioners to continuously assess and improve critical security controls within their production environment, optimizing their end-to-end security posture and providing trend reporting for demonstrable improvement over time.

By surfacing better, automated insights, teams are able to make smarter investment decisions and deliver on both business continuity and greater program effectiveness.

Threat-informed Defense

Leadership

Cybersecurity leaders are in a new era of increased attacks, heightened geopolitical risk, and budget scrutiny. In this new normal, the AttackIQ Security Optimization Platform arms cybersecurity teams with better insights, better decisions, and real security outcomes — effectiveness and efficiency. AttackIQ delivers a best-in-class software platform, deep industry partnerships, and threat-informed defense practice enablement for customers.

SOLUTIONS

- Testing and Audits
- Security Operations
- Security Architecture
- Security Risk and Strategy

ATTACK SCENARIOS

- Attack Chains
- MITRE ATT&CK Tactics
- Threat Actors

BUSINESS OUTCOMES

- Align Business Desired Outcomes with Security Operations Tactics
- Prove Operational Resilience
- Justify Security Spend and Priorities
- Rationalize and Validate Security Investments and Capabilities
- Improve Operational Remediation Cycles
- Meet Governance, Risk, and Compliance Assessments (GRC)

SECURITY PILLARS

- Testing and Audits
- Security Operations
- Security Architecture
- Security Risk and Strategy
- Solutions
- Purple Team Exercises
- Gap Analysis/Attacker Emulation
- Security Technology Validation
- SOC Training
- M&A Security Assessment
- Industry Security Performance Baseline
- MITRE ATT&CK Coverage Mapping
- Security Product Comparison
- Industry Security Performance Baseline
- MITRE ATT&CK Coverage Mapping
- FFIEC CAT Maturity
- NIST 800-53 Enforcement Control Testing

ATTACK SCENARIOS

- **Full Kill Chain Support**
- **MITRE ATT&CK Tactics**
  - Initial Access
  - Execution
  - Persistence
  - Privilege Escalation
  - Defense Evasion
  - Credential Access
  - Discovery
  - Lateral Movement
  - Collection
  - Command and Control
  - Exfiltration
  - Impact
- **Threat Actors**
  - Nation-state / APT
  - Insider Threat
  - Cybercriminals

With AttackIQ, you can:

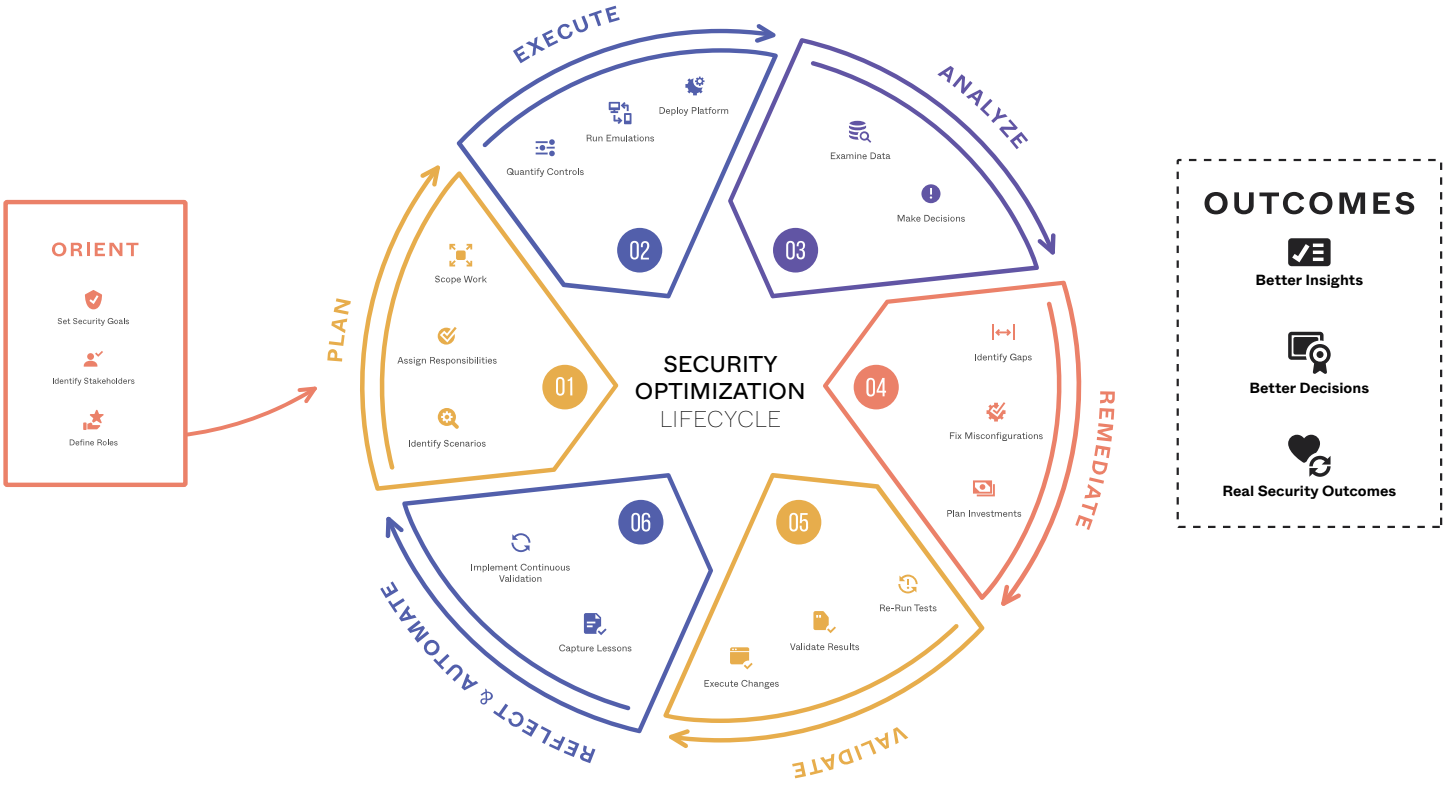
- Make objective, data-driven decisions.
- Provide evidence of your security capabilities.
- Improve security program effectiveness and efficiency.

Security Operations

Security Optimization puts the power in the hands of you and your team to manage your estate from evidence, not assumptions, enriched by the insight from your Cyber Threat Intelligence program.

With AttackIQ, you can:

- Demonstrate the function of your security controls by using the relevant tactics, techniques, and procedures (TTPs) of the adversaries that pose the greatest threat to your environment.
- Immediately be alerted of environment drift within your security configurations.
- Compare emerging security vendor technologies to ensure you purchase an effective technology.
- Rationalize your security stack and eliminate overlapping and redundant security capabilities.
- Build a threat-informed defense program around testing and measuring your security readiness and capabilities in order to optimize your end-to-end security posture.



Threat-informed Defense Across The Security Pillars

By leveraging AttackIQ's Security Optimization Platform, organizations can more effectively leverage threat intelligence and validate security controls on a continuous basis to reduce risk and improve their posture across all security pillars.

AUTOMATED

Testing & Audits

Automated Testing Team Enablement	Red/Blue/Purple
Control Audits	Automated Continuous Control Validation
MSSP Testing	MSSP SLA Validation

Security Risk Management & Strategy

Control Framework Assessment	Automated & Continuous Control Framework Dashboarding
Security Strategy and Investment Decision Support	Outcome Analysis of Adversarial Emulation to Drive Top Line Initiatives
Project SDLC Automation	Actor-aligned & TTP-weighted

Regulatory & Compliance

Continuous Compliance Reporting & Dashboarding	Use Adversarial Emulation Testing to Demonstrate Compliance Readiness

OPERATIONS

Security Operations

Security Pipeline Validation	Exercising the Detection and Alerting Technology Stack to Validate End to End Effectiveness
Post IR Remediation	Prove Post IR Remediations are Effective
Threat Hunting	Stimulate the Environment as an Attacker Would to Validate SOC Process

Technology Operations

Change Management Risk Assessment	Automate & Test the Impact to Infrastructure & Application Changes
CI/CD(S)	Automate Adversarial Emulation Testing as Part of Software Release

Analyst Training & Exercises

Analyst Training & Certification	Use Threat Hunting and Complex TTPs to Express Analyst Readiness
Exercise Enablement	The "Cyber Opposition Force" (OpFor). Make Injects Real
ML/AI Engine Training	Exercise Adversary Emulation to Train Automated Engines

ENGINEERING & ARCHITECTURE

Security Technology/Service Evaluation

COTS Security Control Evaluations & Bakeoffs	Adversary Emulation to Define Functional Requirements
MSSP Evaluations & Bakeoffs	Adversary Emulation to Define Functional Requirements
COTS vs. Opensource Evaluations & Bakeoffs	Adversary Emulation to Define Functional Requirements

Security Architecture & Rationalization

Control Rationalization	Benchmark Coverage Overlaps and Gaps to Optimize
Architectural Strategy Rationalization	Define and Assess Differing Security Strategies (i.e. Preventive vs Detective Centricity)
Software Security Development Lifecycle Security Validation	ATT&CK-based Threat Modelling as Part of Lifecycle Security Assessment

BUSINESS LINES

Security Vendor Tool Development

Automated Quality Testing	Use Adversarial Emulation to Validate Technology Effectiveness
Sales	Use Adversarial Emulation in Presales Motions (PoCs)

Business Lines & Other

Merger & Acquisition	Evaluate and Onboard M&A'd Company Infrastructure/Systems
Cyberinsurance Underwriting	Validate Organizational Security Posture Continuously for Underwriting Purpose

ATTACKIQ

U.S. Headquarters
9276 Scranton Road, Suite 100
San Diego, CA 92121
+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.