ATTACKIQ

Intelligent Security Decisions

VALIDATE THE EFFICACY OF YOUR CYBERSECURITY INVESTMENTS

AttackIQ's continuous security validation enables organizations to measure and validate their security controls, and prioritize remediation.

PROBLEM

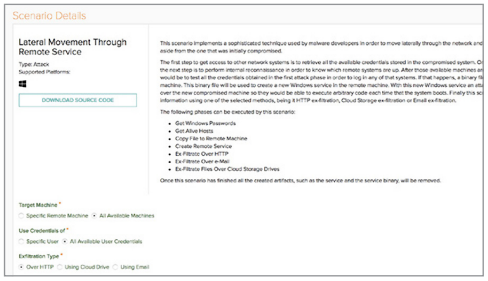
Security teams are playing a reactive game, and as a result are often losing the defensive cyber battle. Organizations must identify protection failures before the adversary does, to close the security gap before it can be exploited. With attack surfaces increasing rapidly, enterprises must implement automated security assessments to continuously validate their security controls, processes, and people.

SOLUTION

AttackIQ leverages the MITRE ATT&CK framework to analyze adversaries' tactics, techniques, and procedures (TTPs) against your existing and planned security controls. AttackIQ can be a catalyst for faster, more efficient and more comprehensive assessments and analysis.

RED TEAM

AttackIQ augments the red team's ability to run exercises and validation scenarios on your enterprise security controls and incident response workflows. Your team is able to identify how each individual asset in your security program responds to thousands of common attack scenarios.



AttackIQ Red Team Scenario - Lateral Movement Through Remote Service

You'll be able to generate comprehensive reporting on test results to then clearly communicate the impact of the threat assessment to the C-suite. You'll see clear metrics on the readiness of common attack vectors like Credential Access, Exfiltration, and Command & Control.

RED TEAM

- **Automate repetitive tasks to conserve resources**
- **Scale effortlessly as security program grows**
- **Deliver clear, comprehensive reporting to CISO**

AT A GLANCE

Features

- Real-time test scenarios
- Custom test scenarios
- Scenario repository
- Executive reporting
- Light weight agents
- Central knowledge base
- Critical security metrics
- Intuitive management
- Active user community

Benefits

- Validation scenario will verify point-product effectiveness and ROI
- Compare current security posture against historical baselines
- Continuous automated testing as your network changes and evolves
- Integrations into major SIEM technologies and log management tools to measure detection and prevention effectiveness

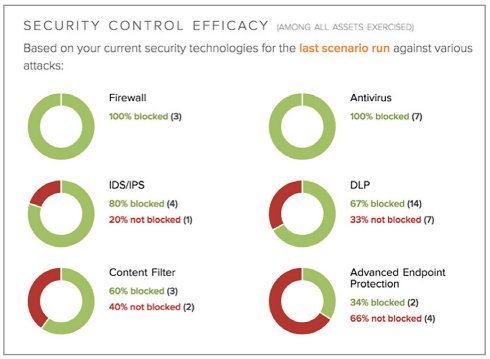
Technology Testing

- Access / Routing
- Data Loss Prevention
- Content/Web Filtering
- EDR
- Firewall
- Network and Host IPS
- AntiVirus (AV)
- SIEM
- SSL Certificates

Intelligent Security Decisions

BLUE TEAM

While the Red Team leverages AttackIQ and MITRE ATT&CK to assess organizations' ability to block and detect known attacker TTPs, the Blue Team continuously validates that security controls are configured properly and able to deter both the Red Team and cyber attackers. AttackIQ provides the Blue Team with comprehensive situational awareness and visibility into the state of organizations' security posture.



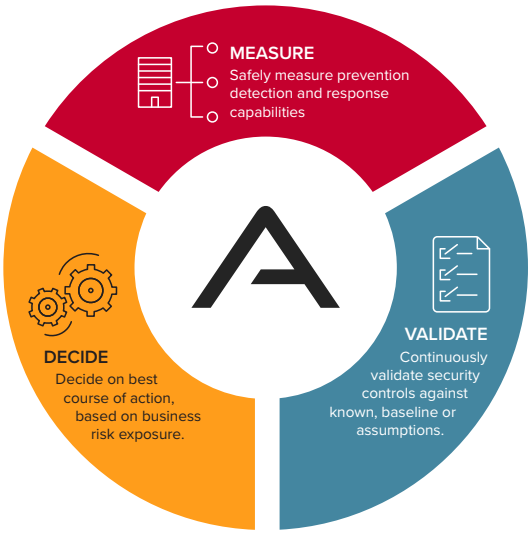
AttackIQ Blue Team Scenario - Security Control Efficacy

With this daily report, security management and engineering can more easily identify critical problems for remediation and understand if security investments are achieving the desired ROI

BLUE TEAM

Use attack scenarios to exercise the existing security controls and incident response workflows.

- **Safely measure prevention, detection and response capabilities**
- **Continuously validate security controls against known, baseline or assumptions**
- **Decide on best course of action based on business risk exposure**



OUTCOME

By leveraging AttackIQ and the MITRE ATT&CK framework, organizations can more effectively validate security controls on a continuous basis to reduce risk and improve their cyber defenses.

KEY BENEFITS

- **Automate time consuming manual processes**
- **Extend the depth and coverage of validation efforts**
- **Gain a deeper understanding of vulnerabilities and risks**
- **Free up Red Team to focus on critical priorities**

According to a recent ESG product lab evaluation, "Before investing in yet another cybersecurity tool, organizations wanting to strengthen their security posture should prioritize investing the few minutes necessary to evaluate AttackIQ, a tool that can continuously validate the effectiveness of their existing cybersecurity toolchains, identify gaps, and help remediate issues."

ATTACK SCENARIOS

Stages

- Persistence
- Privilege Escalation
- Lateral Movement
- Access to Data Stores
- Command and Control
- Data Exfiltration

Threat Actors

- Nation State Actors
- Insider Threats
- Cyber Criminals

People & Processes

- Incident Response
- Red Team Playbook
- Table Top Exercises

ABOUT ATTACKIQ

AttackIQ, a leader in the emerging market of continuous security validation, built the industry's first platform that enables red and blue teams to test and measure the effectiveness of their security controls and staff. With an open platform, AttackIQ supports the MITRE ATT&CK framework, a curated knowledge base and model for cyber adversary behavior used for planning security improvements and verifying defenses work as expected. AttackIQ's platform is trusted by leading companies around the world.

ATTACKIQ

1.888.588.9116

sales@attackiq.com
www.attackiq.com

9276 Scranton Road, Suite 100
San Diego, CA 92121