ATTACKIQ®

Datasheet

AttackIQ® Informed Defense Architecture (AIDA) Product Upgrade

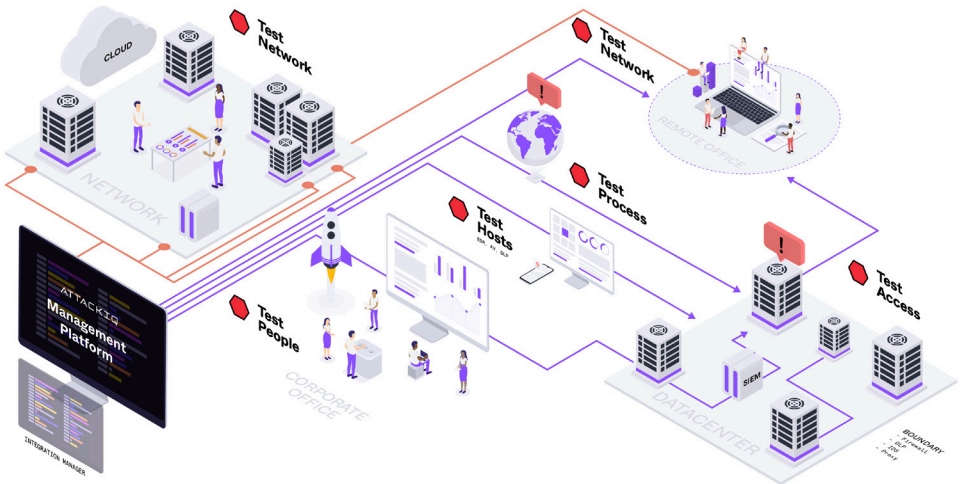
AttackIQ® Informed Defense Architecture (AIDA) Product Upgrade

In an Industry First, the AttackIQ Platform Now Automates the Validation of Artificial-Intelligence- and Machine-Learning-Based Security Technologies.

To validate cybersecurity effectiveness against real-world threats, organizations need a platform that can emulate the adversary with specificity and realism at every step in the cyberattack process. This is no small feat. On the basis of cutting-edge research, AttackIQ is proud to announce a series of technology innovations to its Informed Defense Architecture (AIDA) that will help customers better validate their cybersecurity effectiveness against known adversary behaviors.

This innovation accounts for significant evolutions in security technologies. In recent years, advanced persistent threats have increased the sophistication and impact of their cyberattacks. Concurrent to the evolving threat, our partners have matured their cyberdefense technologies. The cybersecurity industry's adoption of machine learning (ML)- and artificial intelligence (AI)-enabled defense capabilities has improved the world's security posture against advanced persistent threats. Yet one should never assume that the best technologies, the best personnel, and the best processes will always perform as intended. Every cyberdefense capability needs to be constantly tested and validated to ensure effectiveness.

On this basis, AttackIQ has extended its "Informed Defense" Architecture (AIDA) to better emulate adversary campaigns while concurrently making it easier for cybersecurity teams to consume adversary behaviors to test their cyberdefense capabilities. AttackIQ now offers the industry's only adversary emulation architecture built to test AI- and ML-based cyberdefense technologies in production, while emulating comprehensive, multi-stage attacks. These innovations simplify the process of evaluating security control performance across distributed environments and accelerate customers' adoption of a threat-informed defense across the security program. The result is that customers can better test their people, processes, and defensive technologies against advanced threats.

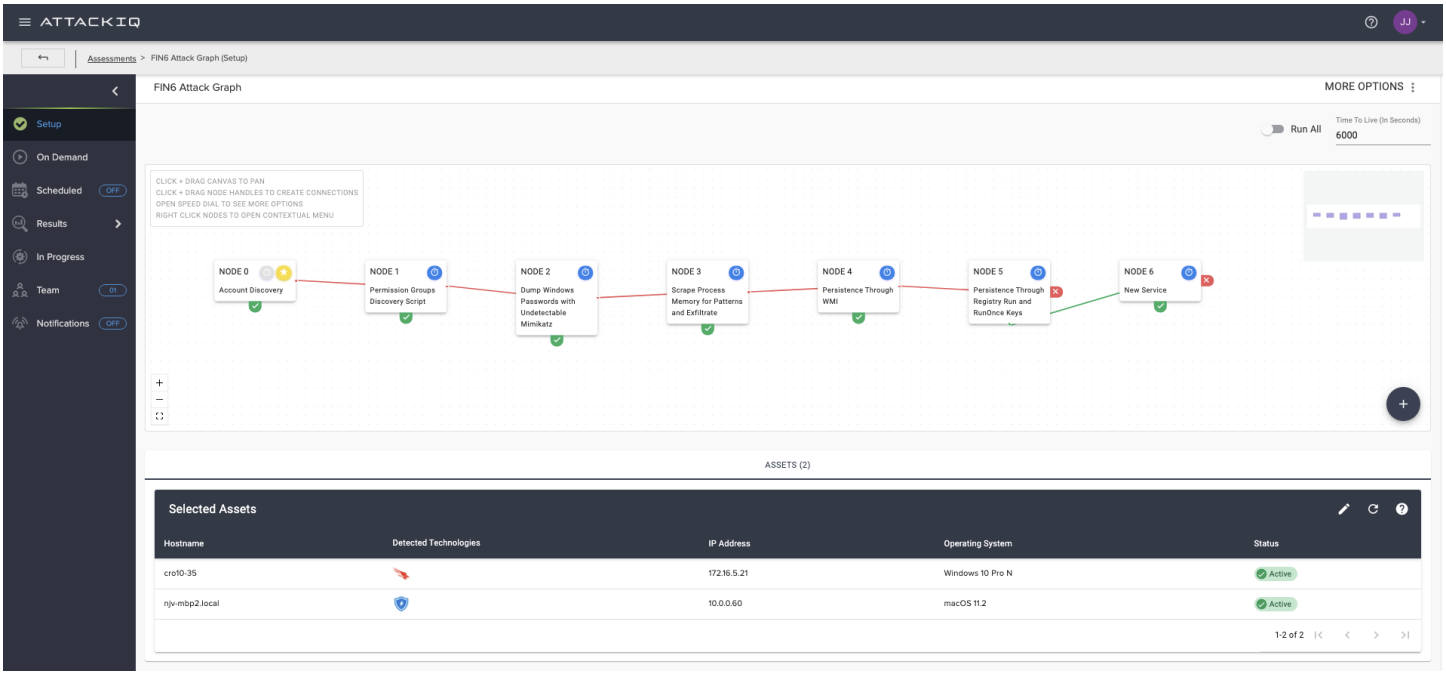


New components in AttackIQ's Informed Defense Architecture:

- **AttackIQ's Anatomic Engine** provides a user defined, multi-stage engine that allows cyberdefenders to emulate entire adversary attack flows and attack campaigns. The Anatomic Engine makes AIDA the industry's only adversary emulation architecture built to test AI- and ML-based cyberdefense technologies in production, while emulating comprehensive, multi-stage attacks.

- **AttackIQ's Network Control Validation Module** combines a new comprehensive network topology map with adversarial attack replays. This helps organizations to rapidly exercise the end-to-end validation of network-deployed security controls and gives technology-specific remediation guidance, ensuring that customers get the most out of their cyberdefense investments.

- **The AttackIQ Hosted Agent** simplifies the process of deploying the Security Optimization Platform, improving the customer experience by providing a managed, external source and target, making it simple to emulate advanced adversary behaviors.



The net result is that no matter the defensive technology type — including technologies based on complex, behavioral models — AttackIQ provides unique insights into the state of a customer's total security program from network to endpoint, on-premises or in the cloud. And it does so with industry-leading ease of use.

How do these AIDA innovations deliver improved cybersecurity effectiveness?

- **The Anatomic Engine** makes it easy for operators of all skill levels to create complex adversary attack graphs (or attack flows) that are purpose built for emulating attacker patterns. Enumerating complete kill-chain sequences in this manner provides high-level efficacy when testing modern ML- and AI-based security controls.
- **AttackIQ's Network Control Validation** uses already-deployed AttackIQ test points on the network, AttackIQ's Network Control Validation module evaluates the performance of network-deployed security controls. It then provides prescriptive mitigation guidance to maximize the value of investments in next-generation firewalls (NGFW) and similar technologies.
- **The AttackIQ Hosted Agent** allows you to rapidly begin testing network boundaries and Internet-facing control technologies in a simple, fast deployment cycle. With the AttackIQ Hosted Agent, you no longer need to deploy anything to address north-to-south and south-to-north testing; you can now emulate the adversary easily in a single place

Better Insights, Better Decisions, Real Security Outcomes

With these platform innovations, AttackIQ customers will improve their cyberdefense effectiveness in a number of ways. AttackIQ's Anatomic Engine combines the industry's leading atomic testing capabilities with the most comprehensive adversary emulation capabilities available on the market. By chaining attacks together in a graph, the Anatomic Engine allows organizations in a user interface to measure their defenses against a series of attacker patterns. With the AttackIQ Network Control Validation Module, customers who use next-generation firewalls and other AI- and ML-based defense technologies can operate with increased confidence in their network security effectiveness. Lastly, with hosted agent innovations, the AttackIQ Security Optimization Platform deploys with greater ease, freeing up the security team's time and energy for other matters.

AttackIQ has moved its Security Optimization Platform forward. With these innovations, customers can operate their security program with confidence knowing that they are testing their most advanced cyberdefenses against comprehensive and multi-stage adversary emulations. The outcome is an increase in defense capability and performance.

These upgrades are available **April, 2021**. Please contact the AttackIQ sales team for further details at info@attackiq.com.

ATTACKIQ
U.S. Headquarters
171 Main Street Suite 656
Los Altos, CA 94022
+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 identify 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 MITRE Engenuity's Center for Threat Informed Defense.

For more information visit www.attackiq.com. Follow AttackIQ on Twitter, Facebook, LinkedIn, and YouTube.

© 2021 AttackIQ, Inc. All rights reserved. Confidential and proprietary. Do not distribute.