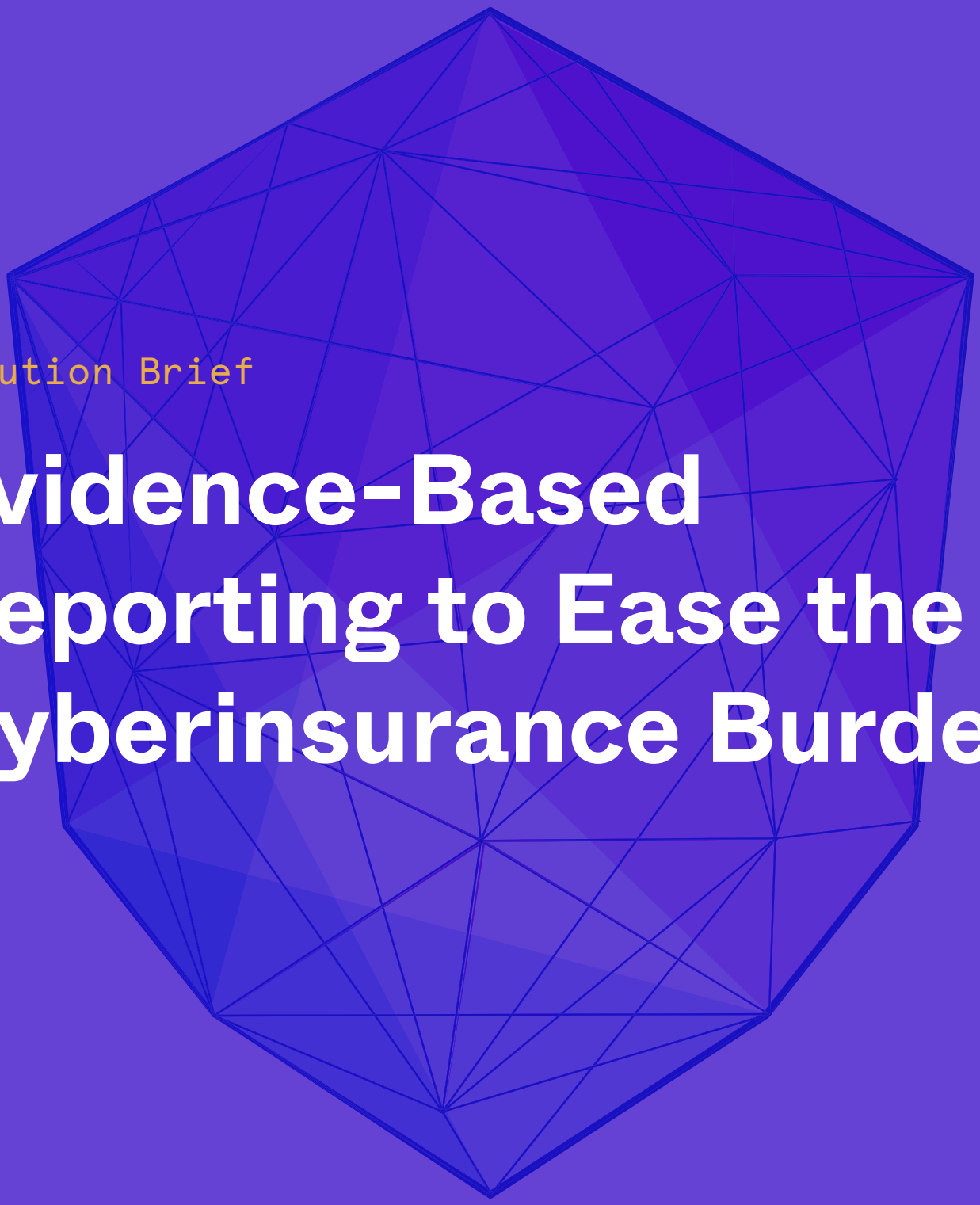
ATTACKIQ®



Solution Brief

Evidence-Based Reporting to Ease the Cyberinsurance Burden

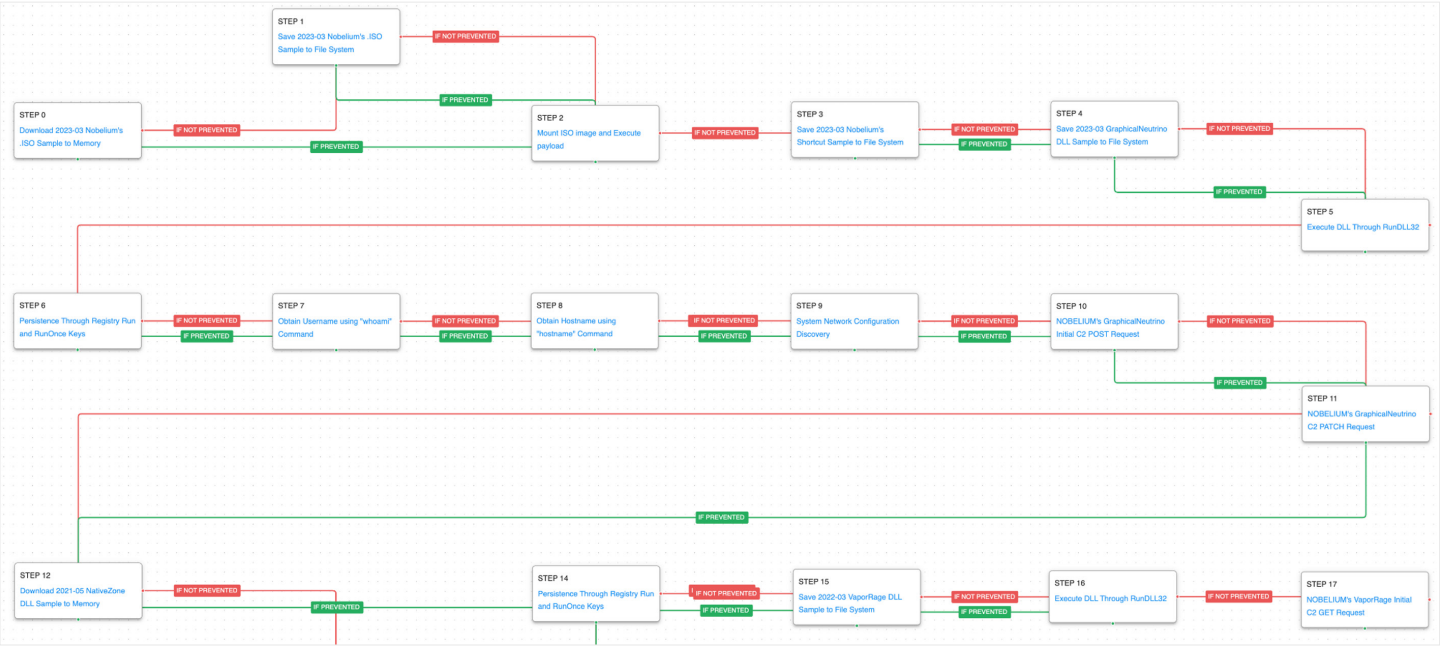
AttackIQ customers save time and decrease their cybersecurity premiums by demonstrating their cybersecurity readiness to insurance underwriters through continuous security control validation. Both customers and insurers achieve savings by automating testing and reporting, reducing insurance premiums and operational costs through evidence-based reporting and analysis.

Solving the Insurance Questionnaire Problem

The process of acquiring cyberinsurance has grown more difficult. Annual or semi-annual insurance questionnaires have been the historic means for insurers assessing a client's risk exposure and making underwriting decisions. The questionnaire approach presents a two-fold challenge: For insurers, questionnaires fail to provide granular data to make scientifically informed decisions. For prospective clients, answering the questionnaires can take weeks if not months to complete and require security teams to work with their legal and audit teams to prove compliance.

> *"You must answer truthfully to the best of your knowledge and not put yourself at risk by answering incorrectly. We leveraged the AttackIQ Security Optimization Platform to find the answer we were looking for and to either share or have that documented in case of a breach, and we were held accountable for those responses."*
>
> - Director of IT Security, Leading Biosciences Company

There is a path to ease the burden for both security leaders and insurers by measuring cybersecurity readiness through continuous security control validation against real-world adversary tactics, techniques, and procedures (TTPs). AttackIQ customers emulate ransomware and threat group behaviors to generate real-time data about their cybersecurity performance. By measuring security control performance, companies quantify risk and then take steps to reduce risk by remediating identified security gaps and improving their security effectiveness against threats.

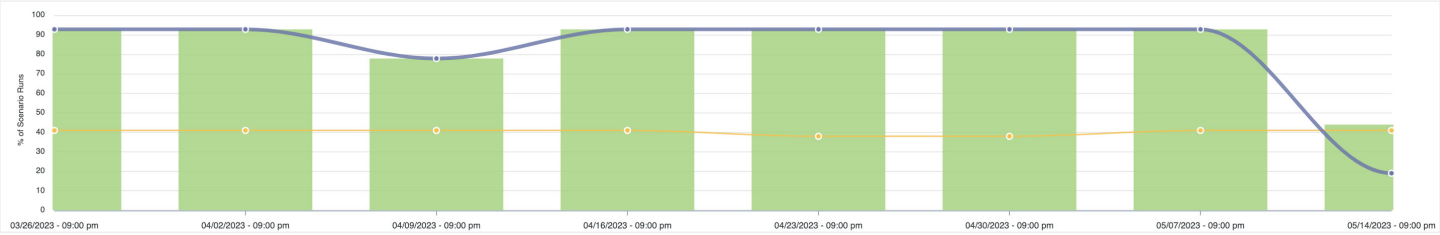


AttackIQ attack graph emulating the Russian state-sponsored Nobelium attack group, discussed here. Nobelium targets European Union countries to gather intelligence on countries supporting Ukraine in the ongoing Russia-Ukraine war.

Cybersecurity insurers require clear information about their clients'security posture to assess their viability as insurable entities. They spend time scrutinizing an organization's security controls, internal processes, and compliance. By reviewing a client's performance data from AttackIQ, insurers can validate security effectiveness and make data-informed decisions as a part of the underwriting process.

Security Control Validation as Evidence

AttackIQ customers generate detailed, historical, and up-to-date data on their security controls effectiveness for a range of defensive capabilities, including Multi-Factor Authentication (MFA), least-privilege, network and micro-segmentation, data protection, and continuous monitoring and logging of suspicious activity. In addition, customers demonstrate the effectiveness of Endpoint Detection and Response, Extended Detection and Response (XDR), Next Generation Firewalls (NGFW), endpoint antivirus, inbound email filtering, and Web Application Firewalls (WAF) technologies.



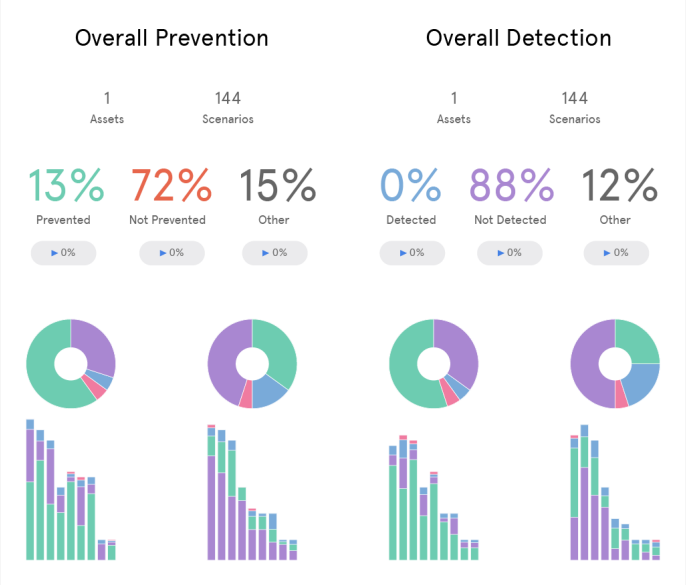
Example of a weekly detection and prevention performance report for an advanced endpoint security control.

Organizations take advantage of advanced in-production automated emulation and testing capabilities to assess internal security policies, processes, procedures, and cybersecurity awareness training for resiliency. Companies use the AttackIQ Security Optimization Platform's validation and reporting capabilities in tabletop and purple-teaming exercises to quantify incident detection, response, and continuity plans and SLAs and then improve on potential weaknesses. Resilient and stress-tested processes allow organizations to improve their chances of qualifying for insurance.

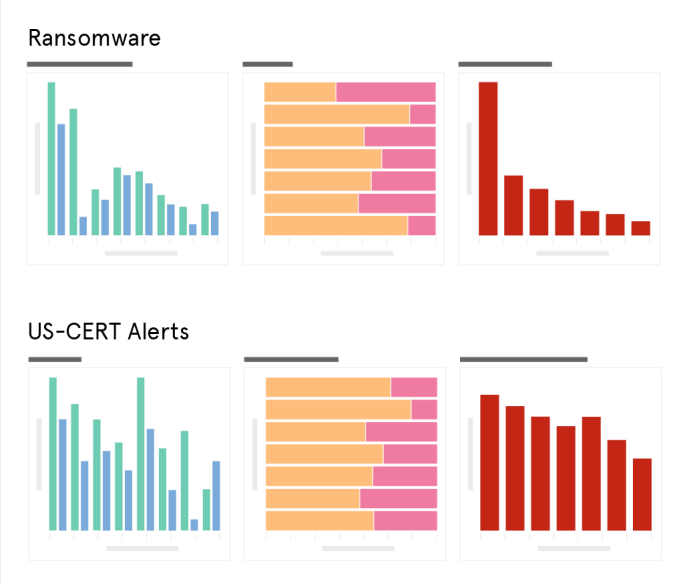
Customers also target specific compliance controls to communicate evidence-based compliance with frameworks like NIST 800-53, CMMC or ISO, and demonstrate adherence to best practices by testing deployed defenses through the MITRE ATT&CK framework. Continuous testing provides an evidence-based and threat-informed baseline measurement of security performance

AttackIQ Reporting and Managed Services

For all the key cybersecurity insurance focus areas, AttackIQ offers concise and automated daily, weekly, and monthly reporting about a security program's performance. This saves teams time and resources during the insurance acquisition process and provides reporting to negotiate and prove effectiveness. AttackIQ customers have negotiated down their insurance premiums, decreasing costs and saving their organizations' significant resources.



Real-time performance data that insurers can use to measure security program effectiveness over time or at a single point-in-time to make informed risk evaluations.



Access to the immediate analysis of emerging threats from the AttackIQ Adversary Research Team.

AttackIQ Ready! and AttackIQ Enterprise Products

Operationally, AttackIQ eases the insurance burden through AttackIQ Ready!, a fully managed breach and attack simulation service, and through AttackIQ Enterprise, a co-managed service that serves as your co-pilot in continuous testing. With AttackIQ Ready! and Enterprise, AttackIQ customers use weekly, monthly, and on-demand reporting to communicate about their security effectiveness. You can read more about AttackIQ's products at www.attackiq.com/products

Example Insurance Questions AttackIQ Answers

Below are some of the kinds of questions from insurance questionnaires that AttackIQ solves.

- Do you have network security firewalls and how well are they performing?
- Do you have micro-segmentation capabilities and how well are they performing?
- Do you have antivirus capabilities and how well they are performing?
- Do you have endpoint detection and response capabilities and how well are they performing?
- What steps are you taking to prevent and detect ransomware?
- Do you use a SIEM provider, and how well is it performing?
- Do you have any third-party assessments of your cybersecurity program's effectiveness?

To answer these and other questions, AttackIQ generates reports about an organization's security program performance, including example reports below:

Daily, weekly, and monthly draft analysis to track security control efficacy and see how well they are blocking, detecting, and reporting against MITRE ATT&CK threat templates.

Proven, measurable data to provide underwriters with a baseline understanding of your security coverage and reassurance of continuous visibility into your security posture.

Sign-up for a demo of AttackIQ reporting capabilities or reach out to our sales team at sales@attackiq.com to learn more. For more about AttackIQ's approach to cybersecurity insurance and to learn more about the issues facing the cybersecurity insurance market overall, check out AttackIQ's podcast interview with Josephine Wolff, author of the best-selling book on this topic, *Cyberinsurance Policy: Rethinking Risk in an Age of Ransomware, Computer Fraud, Data Breaches, and Cyberattacks*.

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 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 Engenuity's Center for Threat Informed Defense.

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