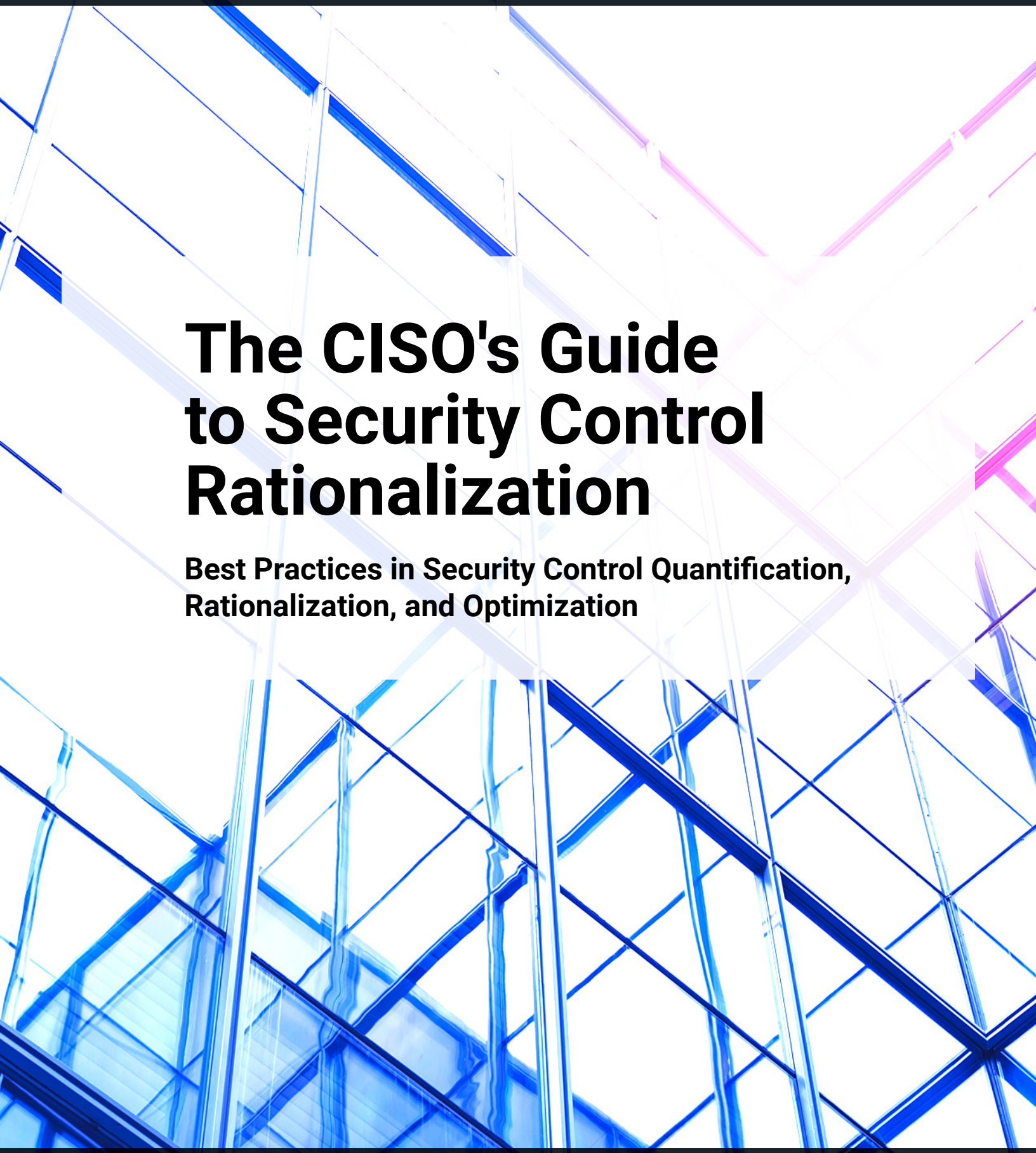


The CISO's Guide to Security Control Rationalization

Best Practices in Security Control Quantification, Rationalization, and Optimization

Notice

This publication is provided for information purposes only. At the time of publication, all of the information within this publication is as accurate and current as could be determined. Any additional data since publication will not be added or updated to this report. AttackIQ, Inc. is not responsible for errors or omissions in the context of this report or for damages arising from the use of this report under any circumstances. Finally, please note that this publication may be updated or changed without notice.

Table of Contents

Executive Summary

Quantification, Rationalization, and Optimization: The Path to Security Effectiveness

In today's cybersecurity organizations, complexity and conflicting signals make it hard for decision makers to set good priorities and manage risk across the enterprise. The average chief information security officer (CISO) manages dozens of security controls and is responsible for meeting hundreds of standards and regulations. CISOs are drowning in data about their organization's security effectiveness, and the data they do have is often irrelevant, outdated, and full of subjectivity.

There is an underlying problem in the cybersecurity ecosystem that no CISO can solve on their own. Verizon estimates that 82 percent of successful enterprise breaches should have been stopped by existing controls, but weren't. Why? Because security controls are complex systems formed of technologies, people, and processes, and they fail silently. They fail largely for two reasons—misconfiguration or operational execution error—and the only way to know if they are working is to actively test them on a continuous basis. It takes a lot for a modern information security program to function properly. Red-team testing is manual and sporadic, and red teams can only test a small percentage of the total attack surface. While valuable for some lessons, third-party penetration testing provides a limited point-in-time perspective on security control effectiveness and sometimes may not even offer meaningful guidance on how to improve your defenses. Consequently, despite over a decade of increasing investment in cybersecurity, most organizations lack real data about their cybersecurity effectiveness.

The situation is further complicated by resource scarcity in a period of acute economic change. CISOs and their teams need to optimize their cybersecurity programs to improve effectiveness, productivity, and efficiency—and now they need to do so with less resources.

To address these challenges, CISOs need to invest in security control quantification and security control rationalization and begin to actively, continuously measure their security program's effectiveness.

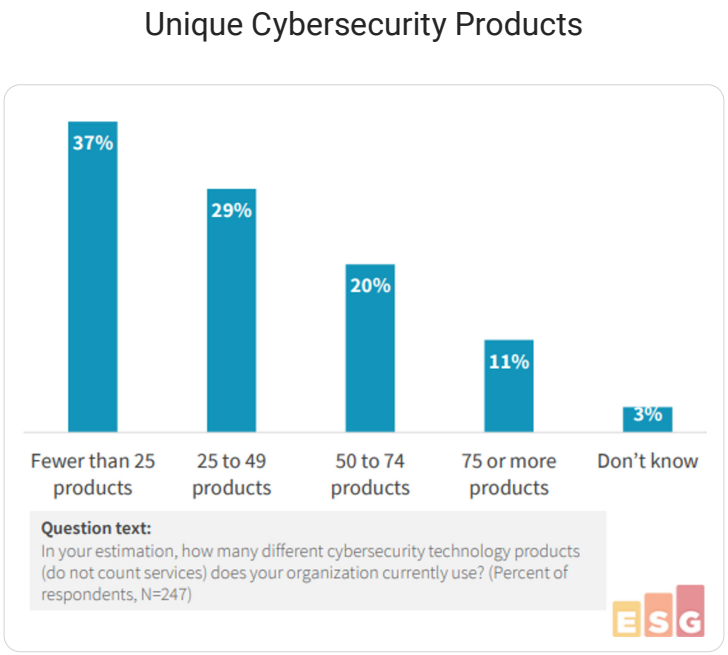
What does this mean? Security control quantification is the process of determining what controls you have and, where they're placed, building an inventory of your security controls, and then measuring the security you have against your organization's baseline cybersecurity requirements and regulations. Security control rationalization is the process of assessing your security controls' effectiveness; identifying and resolving gaps and overlaps in your security control stack; conducting a risk assessment of your security vendors; and then prioritizing, consolidating, and eliminating unnecessary security controls. Security optimization is a management practice of maximizing the efficiency and effectiveness of your total security program (people, process, and technology), by ensuring that existing security investments are measured, monitored, and modified continuously from a threat-informed perspective.

Teams rationalize their security controls and optimize their security programs on a continuous basis to achieve effectiveness, efficiency, and productivity. A robust breach and attack simulation platform can facilitate the process by grounding organizations in a shared understanding of adversaries and their behaviors using the MITRE ATT&CK framework. Through continuous testing with real-world adversary behaviors, a breach and attack simulation platform can increase defenders' insights about their cybersecurity effectiveness by producing evidence of control technology and visibility platform function. Armed with better insights, security leaders can make better informed decisions about people, products, and processes continuously—and that leads to an overall improvement in security and business outcomes.

The CISO's Dilemma

Security Control Proliferation

Today, CISOs face the challenging task of managing and assessing a sprawling proliferation of cybersecurity controls, testers, attempts at "single panes of glass," and code scanners. According to a 2020 presentation by Jon Oltsik, Senior Principal Analyst and Fellow at ESG, a typical enterprise may utilize between roughly 10 to 75 or more security controls across the security organization. The sheer number of cybersecurity vendors and unique security controls can become overwhelming in a large organization burdened by regulatory and compliance demands.



Graphic 1 - ESG Survey Question on Number of Cybersecurity Products

Security Magazine's June 2019 survey of over 200 enterprise security leaders revealed that the average team is managing 57.1 discreet security tools. More than a quarter said they run more than 75 security controls. Despite having so many controls in place, less than a third could measure the efficacy of their existing tools in driving down cybersecurity risks.

A Dangerous Cybersecurity Environment

The nature of the cyberthreat makes the problem more complicated. According to Accenture's Ninth Cost of Cybercrime Study, which surveyed senior leaders in 355 companies across 11 countries, organizations have seen a 67 percent increase in security breaches the past five years and an 11 percent increase in security breaches in the past year alone. The average total estimated cost of a data breach is $3.92 million. Outside of financial goals, nation-state adversaries seek to disrupt democratic discourse and foster mistrust in institutions across society in order to achieve their geopolitical goals.

Security Control Quantification: Identify Investments

What are the key steps for a CISO to take to in the quantification, rationalization, and optimization ladder? The first step is to select a security framework to inform their cybersecurity strategy, like the National Institute of Standards and Technology (NIST) Special Publication 800-53. Second is to build a cyber defense team. Third, the team needs to align the organization's security controls to the framework.

To align security controls, you first need to quantify your security control inventory. You cannot begin to improve your inventory without knowing what you have in it. You need to assemble all of your data about users, data, systems, and software and then identify the relevant security controls that you have to secure the enterprise, as well as their locations. All cybersecurity assets must be identified, enumerated, and documented. These include software, systems, controls, critical data stores, and applications—any device, data, or component in the environment that supports cybersecurity-related activity.

Security Control Rationalization: The Art of the Possible

Once you have quantified your inventory, security teams need to identify cybersecurity gaps and areas of overlap. A gap can be a missing security control or a gap can be a security control that is not working. Organizations may also have redundant security controls. As Johna Till Johnson, CEO of Nemertes Research, says, "Most cybersecurity organizations have too many tools, but CISOs are afraid to eliminate products for fear they're hurting their cybersecurity operational effectiveness." She advocates for a risk-based approach to optimize effectiveness, saying, "Taking a risk-based approach to assessing cybersecurity technology effectiveness can help streamline their product portfolios while maintaining or improving cybersecurity operational metrics." This is what it means to rationalize your security controls.

Set Strategic Goals

Organizations should set a specific strategic goal as they begin the process of security control rationalization. Organizations need to clarify their desired end state and the steps they need to take to get there. Key questions for companies to consider as they alter their investments in the rationalization process: Will this change break the business? What is our execution strategy? Did the elimination or consolidation of a security control produce a better result or reduce our ability to prevent known adversary behaviors? Did we eliminate overlap? These are essential questions to consider in the process of security control rationalization.

Threat-Informed Defense: Use the MITRE ATT&CK Framework

To measure efficiency, you need to be able to test and exercise your security controls against real-world threats at scale, safely, and in production. And you need to be able to test and validate a security control continuously to assure effectiveness. The MITRE ATT&CK framework provides a foundation for scalable testing and validation. MITRE ATT&CK is a globally available, free, open framework of known adversary tactics, techniques, and procedures (TTPs). Knowledge of adversary behavior was previously reserved for elite operators or national security practitioners in a classified environment. The MITRE Corporation, a federally funded non-profit research and development organization working in the public interest, built the ATT&CK framework to help defenders all over the world focus on the threats that matter most.

Security teams can measure their control efficacy in measurable, clear ways by deploying automated adversary emulations against their defenses using MITRE ATT&CK. ATT&CK brings a standard language taxonomy for your entire security, network, and information technology teams that they can all share and understand. It helps you answer a simple question: Is a security control mitigating an adversary attack emulation? The data you derive from an emulation helps you rationalize your security controls.

Security Optimization: Threat-Informed, Data-Driven Effectiveness

After you quantity and rationalize your security controls, security optimization is the next step in the process of improving your security program's performance. Security optimization is a management practice that maximizes the effectiveness and productivity of a security program, while simultaneously ensuring that existing control performance is measured and improved continuously from a threat-informed perspective. At its core, security optimization uses data about your teams' and tools' performances against real world threats to improve effectiveness, efficiency, and productivity. It helps you to align people, processes, and technology to achieve better results.

We have introduced another term here in our discussion of optimization. What does it mean to adopt a threat-informed defense? The term "threat-informed defense" was coined by the MITRE Corporation as it made the MITRE ATT&CK framework operational. As MITRE says, a threat-informed defense strategy "applies a deep understanding of adversary tradecraft and technology to protect against, detect, and mitigate cyber-attacks." MITRE ATT&CK is a foundational framework for testing your security against known threats. Only with performance data about your team's performance against real-world threats can you make informed decisions to optimize your security and achieve effectiveness.

MITRE's threat-informed defense approach has gained global support since the ATT&CK framework first emerged in 2015. Most recently, in the summer of 2020 the office of the Prime Minister of Australia referenced the importance of the ATT&CK framework in the face of escalating nation-state attacks against Australian infrastructure, calling out the Australian government's ATT&CK-focused approach. This governmental focus reflects broader trends across the industry. As one customer told the AttackIQ research team, "MITRE ATT&CK gave us the ideal framework to meet our target use cases … we could continually validate the performance of our production system security controls in real time." An automated adversary emulation platform helps transform an organization from taking an ad hoc approach to security operations to adopting a data-driven, threat-informed approach. To achieve security optimization, you need a platform to automate testing and generate performance data.

Automate with Breach and Attack Simulation

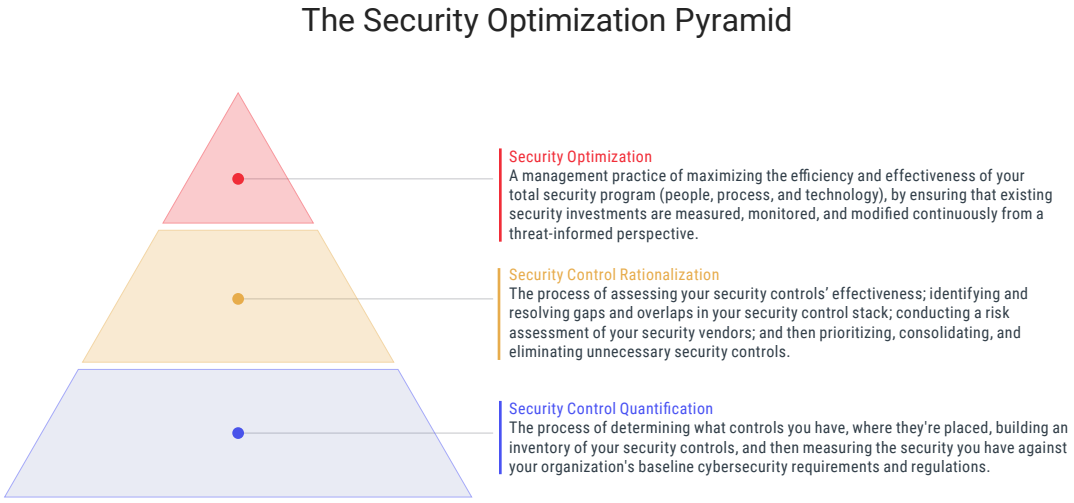
With a strong breach and attack simulation (BAS) platform, you can measure the performance of your security controls and assess the state of your defenses continuously. Once you understand the gaps and identify overlapping capabilities, and you can optimize your security investments: correct configuration issues, improve performance, and change your architecture to maximize your return on investment.

A quality breach and attack simulation platform should present the user with a transparent and manageable attacker kill chain testing methodology and build off of MITRE ATT&CK. It should combine the ability to emulate attacker behavior in the early stages of attack, simulate the attacker's lateral movements, maintained by experts in the sources, methods and behaviors of the adversary, and be technologically up-to-date. It should also ensure that customers and partners have the right content and testing methodology at their fingertips to optimize their security programs.

It is important to note that security optimization is a continuous process of assessment, validation, and adjustment. As one cybersecurity manager at a communications industry firm told the AttackIQ research team, "Our weekly sprints, using MITRE ATT&CK to validate chosen areas, have proven highly productive. In just two to three months, we found many areas requiring improvement and implemented special team programs to get the required mitigations in place." That's the goal of security optimization: to help you sharpen your security team's performance, effectiveness, and productivity.

Production Environment Support

To determine real-world effectiveness against adversaries, an organization needs to be able to test its security controls in a production environment. In production, cybersecurity can be degraded due to changes in the software environment; programs are exposed to the crucible of change. Networks, systems, hybrid clouds, and more undergo constant change to support application delivery and business outcomes. These changes are often poorly communicated to the security program - or sometimes, not at all. Each single change increases the risk that defensive operations and controls will not perform as expected. Implementing a security optimization platform puts insight back in the hands of the security organization to identify change, maximize the efficacy of the program, and reduce exposures. Misconfiguration increases risk by exposing gaps with specific security controls or even exposing data that was expected to be encrypted. Breach and attack simulation tools can help you identify these misconfigurations, restore the expected performance of your security controls, and reduce overall risk.



Graphic 2: The Security Optimization Pyramid

Security control quantification, rationalization, and optimization allow you to baseline the performance of your security architecture and improve your performance while reducing costs and risk. Breach and attack simulation platforms facilitate the process.

Getting Started: Keep It Simple

The security optimization process doesn't happen overnight. It helps to start with MITRE ATT&CK, and it helps to begin by keeping it simple.

As a first step, list the top three to five capabilities you assume are present in your organization and the key reasons why you initially purchased the product. Security control categories might include data loss prevention (DLP), endpoint detection and response (EDR), web filtering, firewalls, and more. Once you have identified your top-tier capabilities, you can map those capabilities to the MITRE ATT&CK tactics and techniques. Once mapped, you can then test the configuration and effectiveness of your security controls.

By using AttackIQ to complete end-to-end testing of critical areas for which you assume you have defensive coverage, the platform gives you data to support the rationalization process and prioritize rationalization. This evidence can be shared with your management team and other business units within your organization to communicate the state of your security posture and make decisions about your investments.

Conclusion

The process of security rationalization and security optimization should improve your cyber defense capabilities, reduce risk, and bring a higher return on investment to any enterprise. Security rationalization and security optimization can both be facilitated through the use of an effective breach and attack simulation platform. A quality platform should provide you with accurate data about your security program's effectiveness against real-world threats. It should also allow you to incorporate up-to-date information about adversary TTPs into the platform to test your security controls.

By implementing a threat-informed defense strategy and using the MITRE ATT&CK framework, you can identify gaps, improve your defenses in an iterative process, and optimize your security performance and investments across the security organization. A breach and attack simulation platform should continuously validate your security control effectiveness and provide an objective measurement of your team's performance. That's how you achieve security optimization.

ATTACKIQ

U.S. Headquarters
9276 Scranton Road, Suite 100
San Diego, CA 92121
+1 (888) 588-9116
info@attackiq.com

About AttackIQ and Threat-Informed Defense
AttackIQ, the leading independent vendor of breach and attack simulation solutions, built the industry's first platform that enables security 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 a 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.

For more information visit: www.attackiq.com. Or follow AttackIQ on Twitter, Facebook, LinkedIn, Vimeo, and YouTube.