ATTACKIQ

White Paper

The CISO's Guide to Security Optimization with AttackIQ

Optimize your security program for better business outcomes

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

CISOs Thrive at the Junction of Technology and Business Value

Despite relentless pressures and shifting responsibilities, the best Chief Information Security Officers (CISOs) persist and thrive in their positions, because "they feel they and their security teams are making a difference."[1] So how do you gauge your impact on your organization? Perhaps you revel in triaging security incidents before they damage the business. Or you may pride yourself in staying abreast of evolving security and privacy regulations. But in the boardroom, according to Gartner estimates, 30 precent of your effectiveness will be directly measured on your ability to create value for the business.[2]

Against a backdrop of increasing cybersecurity risk and uncertain budgets under the extraordinary onset of the novel coronavirus, the most prudent way to create value is to maximize the effectiveness and efficiency of your cybersecurity programs. This requires competence in three areas:

1. Identifying and quantifying cybersecurity risks through the collection of accurate data on the performance of existing security controls against actual threats;
2. Prioritizing security investments based on an understanding of the impact of the quantified risks on business outcomes;
3. Continuously calibrating staff skills, processes, and technology to maintain the desired security posture, given existing budget constraints.

At AttackIQ, we refer to these competencies collectively as **security optimization**. To help organizations of all sizes achieve security optimization, we have bolstered the breach and attack simulation (BAS) capabilities of the AttackIQ Security Optimization Platform, created blueprints for threat-informed defense best practices, and expanded our collaborations with industry partners.

AttackIQ's security optimization initiatives and offerings are outlined in the following pages.

Start with a Solid Technology Foundation

The AttackIQ Security Optimization Platform

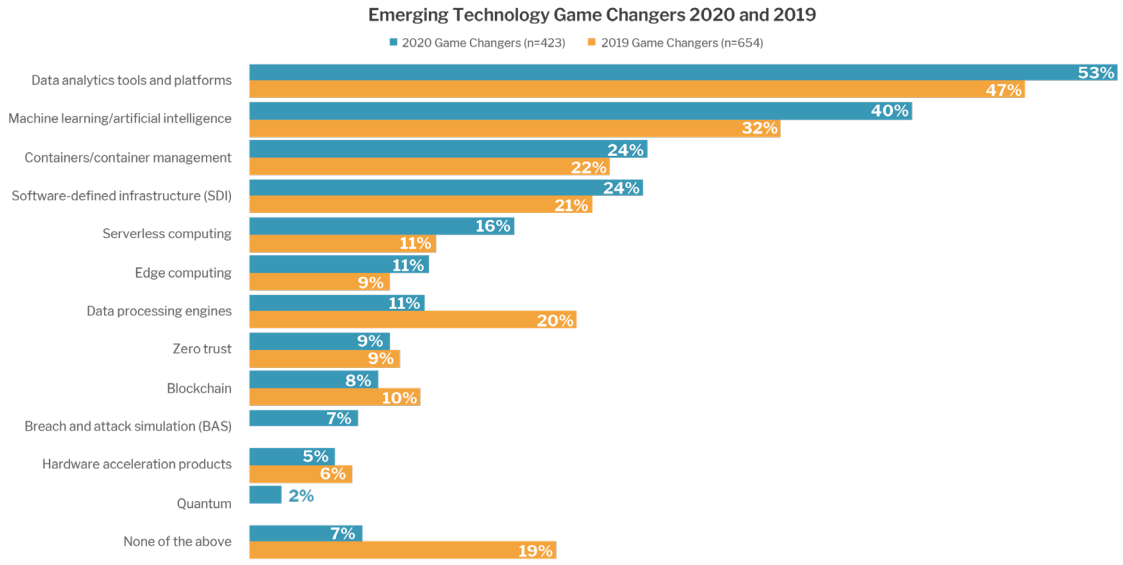
Most security teams cannot demonstrate to corporate leadership that their controls are effective. Even worse, they are not aware of the gaps. Verizon estimates that 82 percent of successful enterprise breaches should have been stopped by existing controls, but weren't.[3]

This is not surprising given that security controls are complex systems composed of technologies, people, and processes. The only way to know if security controls are working at any point in time is to test them. But point-in-time testing, as practiced in red team exercises, doesn't convey the ongoing effectiveness of security controls into the future. The other problem with red teaming is that it can't scale to the entire enterprise. Even the largest companies lack the time and the staff to test all of their controls. What enterprises need is a way to test security controls in an automated and continuous way and to diagnose and report on the control failures detected.

Avoid Guessing — Know Your Risk with Breach and Attack Simulation

A recent Gartner blog post pointed out that the quantification companies use to present risk and security is often couched in terms of money and likelihood of damage. These calculations, Gartner contends, "are often based on assumptions and 'expert opinion' that essentially dictate the result, rather than real quantitative business assessment. Using the veneer of quantification to get what you want does not support improved cybersecurity."[4] We agree; you need real quantification.

This is where breach and attack simulation comes in. It emulates real-world attacks so that organizations can test and validate how their security controls (composed of people, processes, and technologies) perform against existing threats. According to 451 Research, part of S&P Global Market Intelligence, Voice of the Enterprise Digital Pulse: Budgets & Outlook 2020 study, BAS is an emerging technology that is gaining attention among security professionals. Last year, 451 Research added BAS (along with quantum computing) to the list of selected "emerging technologies" highlighted in Voice of the Enterprise Digital Pulse: Budgets & Outlook 2020 study, which also includes artificial intelligence, data analytics, zero trust, and edge computing.[5]



Opt for AttackIQ's Robust, User-Friendly SaaS Solution

Breach and attack simulation solutions vary widely in their effectiveness and ease of implementation. As an early innovator in BAS, AttackIQ has operationalized the tactics, techniques, and procedures (TTPs) of the highly regarded MITRE ATT&CK framework. The AttackIQ Security Optimization Platform uses MITRE ATT&CK TTPs to test security controls in production, at scale, and across the entire kill chain. The AttackIQ platform has been proven in large and mission-critical networks and in those with sensitive data that are prime targets of cyberattackers.

Even with its robust capabilities, the AttackIQ Security Optimization Platform is easy to implement. We are flexible; our management system can be deployed remotely as software as a service (SaaS) or directly on-premises. And our agents are lightweight and easy to install. We do not require dedicated test points, and this makes us dramatically more scalable than other solutions. The AttackIQ platform quickly deploys across your network, runs scenarios continuously or as needed, and presents the results in a way that enables operational insight even for non-cybersecurity professionals.

One organization in the nonprofit sector handles the personally identifiable information (PII) of more than 1.5 million customers. With such sensitive information, the organization cannot afford to rely on guesswork or subjective data to ensure that its security controls are working. AttackIQ's easy deployment architecture allowed the nonprofit to implement the platform and test points rapidly out of the box.

With AttackIQ's broad and comprehensive scenario testing library, the organization automatically runs simulations of the full attack and expanded kill chain against its infrastructure. Important scenarios include credential caching, as well as email, web, and DNS exfiltration scenarios. With the AttackIQ Security Optimization Platform, the nonprofit is assured that its security controls are effective and efficient and that customers' data is secure.

Add Threat-Informed Defense Best Practices

Blueprints Help You Grow Your Security Optimization Practice

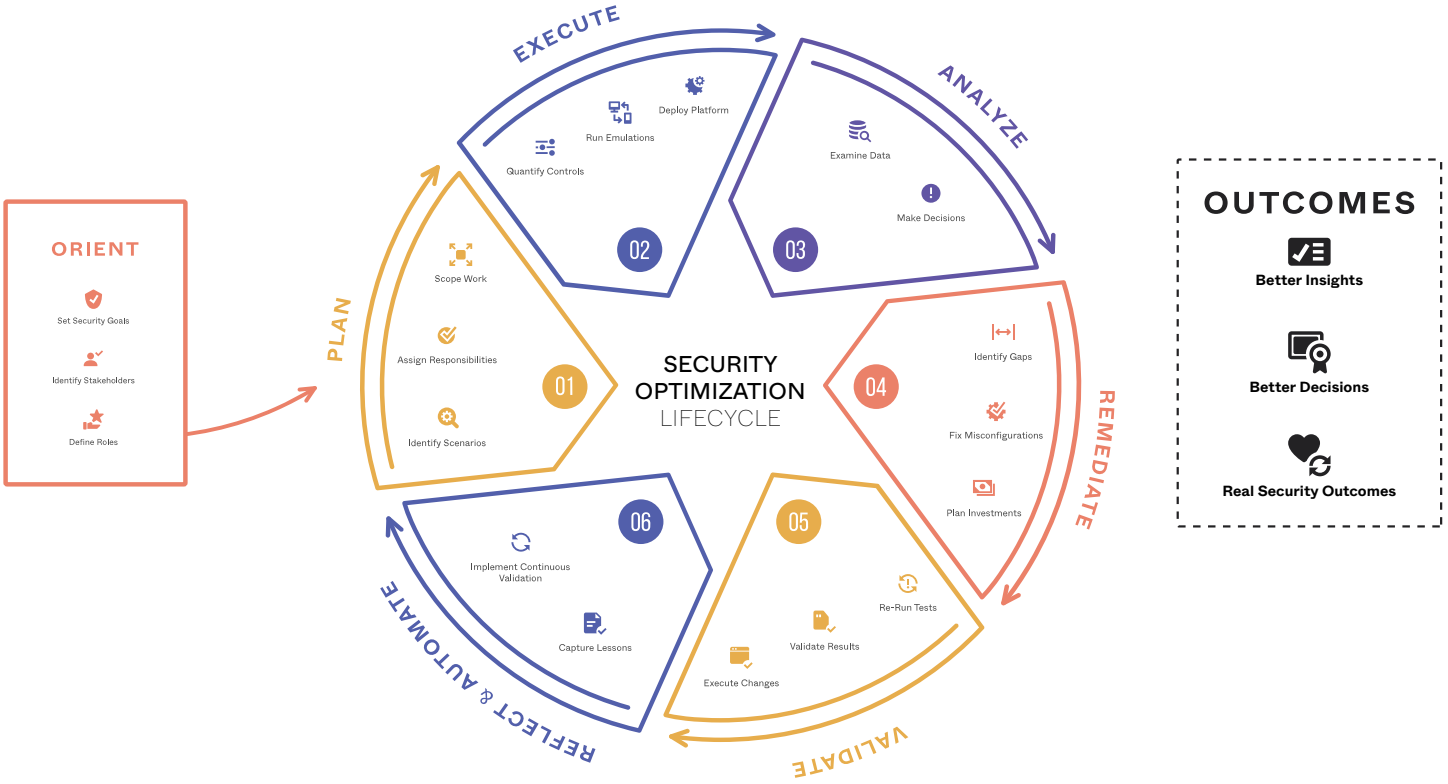
Based on our years of hands-on experience with customers and the expertise of our own security practitioners, AttackIQ has defined a series of security optimization blueprints. These are step-by-step guides to align people, processes, and technology to deliver optimization across the security organization. We have organized the blueprints into four phases that reflect the increasing maturation of an organization's security optimization practice.

Blueprint Phase 1: Automated Security Validation

The initial goal is to achieve a pervasive and continuous testing program with the means to find and close security gaps. As you begin the security optimization process, you could use the AttackIQ platform in a number of ways, to include:

- Automated testing (using red, blue, and purple teams);
- Validations of controls throughout the security pipeline, commercial vendors, and open-source solutions;
- Assessments of managed security service providers (MSSPs) at the proof-of-concept stage of engagement and throughout the contract lifecycle.

Other potential solutions that can be deployed in this phase can be found here.



Blueprint Phase 2: Threat-Informed Operations

As your company seeks to make your security optimization more sophisticated, you can develop more granular performance data and drive improvements in your organization's security and technology governance processes using the following solutions:

- Threat emulation for security optimization;
- Threat-informed technology operations to improve software security and architectural security;
- Projections of software security development lifecycle (SSDL) and modeling.

After gathering this performance information, you have a data-driven, objective change management process to reduce risk. Automation enables you to evolve toward a SecDevOps model. You gain a consistent, automated approach to project security oversight and control.

Blueprint Phase 3: Strategic Defense Posture

If you want to further enhance your effectiveness, you develop meaningful ways to measure and evaluate the performance of your people, processes, and technologies:

- Continuously exercising your analysts against known threats to sharpen your defense capabilities;
- Streamlining compliance by creating dashboards that map real data about your cybersecurity effectiveness to the applicable regulatory requirements;
- Beginning to benchmark your security ROI by rationalizing your controls (overlaps and gaps) and your architectural strategy (e.g., prevention-centric or detection-centric).

Blueprint Phase 4: Comprehensive Security Optimization

Solutions in this phase cover security, risk management, and strategy, with the aim of maximizing the efficiency and effectiveness of your total security program (people, processes, and technology), to ensure that existing security investments are measured, monitored, and modified continuously from a threat-informed perspective.

In this phase you are running a fully actualized security program. A data-driven, threat-informed strategy gives the organization a shared understanding of threats and threat behavior, and this makes security more tractable and manageable. This change in security culture eliminates fear, uncertainty, and doubt. Using real performance data provided by continuous testing, you can prioritize the improvements that matter most for your security posture. Data-driven reporting leaves boards and senior leaders with deeper confidence in the security team's approach and overall effectiveness.

The net result of comprehensive security optimization is that your cybersecurity posture works effectively and efficiently. Technology performs as intended; costs are streamlined; organizational weaknesses and vulnerabilities are identified, fixed, or filled with new capabilities. You now operate under a robust cybersecurity posture with the AttackIQ Security Optimization Platform at the center. You can tell the CEO and board a data-driven story about your cybersecurity effectiveness to achieve the outcomes you seek.

Take Advantage of Easy Access to Best Practices and Education

AttackIQ Security Validation Service

All organizations, regardless of size and security staffing levels, should be able to start on the road to security optimization. This is especially important in light of the COVID-19 pandemic. Security teams are stretched thin as many staffers are redirected to implement work-from-home security controls and manage the other unforeseen impacts of pandemic-related business reorganization.

AttackIQ's Security Validation Service (SVS) is a managed engagement model that enables your organization to take advantage of AttackIQ's best practices and security expertise to realize the substantial benefits of a continuous security validation program. Designed to work closely with your executive management and security team, SVS helps you achieve situational awareness and visibility into both the effectiveness and efficiency of your security programs, as well as overall resilience. AttackIQ SVS includes detailed operational reporting and remediation recommendations that facilitate risk management and budgeting discussions with your corporate leaders.

AttackIQ Academy

AttackIQ works closely with the MITRE Corporation to promote the practice of threat informed defense with its popular AttackIQ Academy. AttackIQ Academy features free instructor-led courses leading to (ISC)² CPE credits in critical concepts such as foundations of operationalizing MITRE ATT&CK, foundations of breach and attack simulation, and foundations of purple teaming. You and anyone from your organization can join the more than 1,600 learners who have registered for Academy courses since its launch.

"The AttackIQ Purple Teaming course was an excellent primer on what it takes to get a Purple Team up and running with clearly defined processes to support a long-term program. I was impressed by the instructor's depth of knowledge and experience. I recommended this to my team already and would recommend to all security practitioners interested in improving cyber defense."

–Tom Needham,
Director Cyber-Security Operations
Cyber Threat Action Center, Abbott

Benefit from Deep Integration and Collaboration with Security Partners

The Preactive Security Exchange (PSE)

It takes a village of vendors, across a broad array of technologies and services, to help a CISO construct a successful security program. The Preactive Security Exchange is a comprehensive, category-first partner program to help mutual customers be proactive about preventable failure. Through the Preactive Security Exchange, AttackIQ and its partners collaborate on technological integrations with security vendors in live production environments. These solutions are API-first and highly configurable, keeping them open for all. Equally important is our shared mission to enhance the effectiveness of organizations' security controls for the benefit of our mutual customers.

Industrywide Community of Practice

AttackIQ also participates in established frameworks and communities to share threat intelligence and defense best practices. The company was selected as one of the 13 founding members of the MITRE Center of Threat Informed Defense (CTID).

MITRE ENGENUITY™
A Foundation for Public Good

This open, collaborative forum builds on the MITRE ATT&CK framework, a matrix of attacker TTPs that is widely used for modeling adversary behavior. The CTID is an organization within MITRE that conducts applied research and advanced development to improve cyberdefense at scale for the global community. It brings together the best cybersecurity researchers from across the globe.

Be Ready to Optimize for Any Business Outcome

Real-World Approaches

While the AttackIQ blueprints provide an overarching roadmap for security optimization maturity, security teams often need specific data-driven insight quickly. This is particularly true in 2020 under the onset of the novel coronavirus, a historically disruptive event that impacts every part of our lives. The COVID-19 era presents CISOs with a radically new security environment. Adversaries are attacking more vigorously under COVID-19, exploiting the opportunities for attack that have been revealed both by the shift to work from home and the broader socio-economic disruptions accompanying the disease. The coronavirus and its socio-economic impact have made the United States and countries around the world more vulnerable to data exploitation, destruction, and to disinformation. All of which impact the CISO dramatically.

If your security budget is locked in for the rest of the current cycle, you may be struggling to rationalize reallocations in security investments that the COVID-19 pandemic has necessitated. You need to know which reallocation plan will yield the greatest business value at the lowest overall risk to the enterprise.

For this and other decisions requiring rapid enablement of threat-informed, data-driven decisions, the AttackIQ Security Optimization Platform stands ready to help. Once you have set up your AttackIQ account in the cloud, you or any of your team can tap into it to acquire and analyze data on security controls' performance.

Conclusion

Security optimization is a management practice designed to maximize the efficiency and effectiveness of your total security program (people, processes, and technology) by ensuring that existing security investments are measured, monitored, and modified continuously from a threat-informed perspective.

To help CISOs, their organizations, and the entire security community thrive, AttackIQ has focused its business on supporting security optimization. We welcome you to engage with us to begin—or to accelerate—your security optimization journey. Learn more at attackiq.com.

One municipality that was coping with strict budget constraints in a worsening threat environment turned to the AttackIQ platform to find performance gaps, strengthen its security posture, and improve overall incident response capabilities. The platform gives everyone in the organization objective, verifiable, threat-informed information specific to their roles. With a strong basis for strategic, informed decisions, the city is now confident in its security posture and in its budgetary expenditures.

Appendix: Common Business Requirements

The following are some of the common business requirements that customers fulfill using the AttackIQ platform. For the full list of solutions that AttackIQ provides, please visit our website at www.attackiq.com.

Security Performance Measurement

Because data collection is the first step in any analysis, most security teams turn to AttackIQ first for security performance measurement. With the broadest coverage of MITRE ATT&CK TTPs, the AttackIQ platform tests security controls, security teams, and the processes they employ to detect and mitigate emulated real-world attacks. The AttackIQ platform then delivers data about successes and failures of specific security controls, the frequency with which emulated attacks compromise the controls, and other measures of cyberdefense effectiveness. Analyst teams can then apply the feedback and retest with the changes in place. Using the AttackIQ platform to augment traditional red team and blue team exercises and support purple team coordination, organizations achieve measurable change quickly.

Security Control Rationalization and Optimization

With increasing calls to improve operational efficiency in the security organization, CISOs need to decide which controls, if any, they can eliminate without significant negative impact on the organization. In this context, CISOs use the AttackIQ platform to assess the effectiveness of all the security controls under consideration. This allows them to identify and resolve gaps and overlaps in the security control stack and conduct a risk assessment of the security tool vendors. By doing so, they can prioritize and consolidate controls, eliminating unnecessary expenses to maximize efficiency.

Business Justification for Additional Control Coverage

If the team has identified gaps in control capabilities, it can use the AttackIQ platform to decide whether to invest or divest in specific areas to mitigate the discrepancy. Because the platform provides data from security tools in production and the data can be collected continuously over time, the security organization can more accurately evaluate the state of the company's security investments and the value the business is deriving from each. It can then present to management more data-driven justifications for requesting additional control coverage. This is even more effective when the security team can also include plans to divest certain controls that it can prove are less effective.

Compliance Mapping

Compliance requirements are often ambiguous, leaving CISOs and their compliance teams to figure out how to achieve the regulatory objectives and demonstrate that they have done so. A security group can use the AttackIQ platform to reduce the company's compliance and regulatory burden by defining relevant controls, conducting continuous tests, and mapping the data from those tests to the compliance framework. During an audit, they can provide regulators with data from the AttackIQ platform to satisfy their expectations for well-established and documented security control processes.

Security Pipeline Validation

In managing its security program, your security operations team needs confidence that it can see and respond to an event efficiently, effectively, and quickly; the security operations team can use the AttackIQ platform to assess all of the security technology sensors within an organization, including the event logs, network security controls, and the Security Information and Event Manager (SIEM), to ensure that the technology works as it should. Whether you are building your security program or choosing a new commercial security vendor for your existing security needs, you can use the Security Optimization Platform to assess competing security technologies and determine which one best meets your needs.

Cybersecurity Insurance Cost Reduction

Insurance companies underwrite cybersecurity insurance policies based on certain constraints. As the company grows and changes over time, the security team can use the AttackIQ Security Optimization Platform to demonstrate to insurers that the company can exercise defenses against prospective attacks and mitigate the risk. The goal is to inspire confidence among insurers that the company's security controls perform as intended.

---

[1] Gary Hayslip, "Why Do CISOs Enjoy Serving In Their Position?" Forbes, June 26, 2019.

[2] Tom Scholtz, "Rethink the Security & Risk Strategy: Why leaders must embrace modern cybersecurity practices." Gartner, 2020.

[3] "Verizon Data Breach Investigations Report", 2019, Verizon, accessed on July 29, 2020.

[4] Meghan Rimol, "Security Experts Must Connect Cybersecurity to Business Outcomes," Gartner.com, May 11, 2020, accessed July 24, 2020.

[5] "Report: Voice of the Enterprise: Digital Pulse, Budgets and Outlook – Quarterly Advisory Report," 451 Research 2020.

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.