A Business Value White Paper, sponsored by AttackIQ

The Business Value of the AttackIQ Security Optimization Platform

RESEARCH BY:

Christopher Kissel
Vice President, Security & Trust Products, IDC

Megan Szurley
Senior Research Analyst, Business Value Strategy Practice, IDC

July 2022 | IDC Doc. #US49454222

Navigating this White Paper

Click on titles or page numbers to navigate to each section.

Executive Summary

The "outcome" is the key. An outcome is what happens in prevention, detection, and response to stymie or mitigate the attacker. However, the worst time to worry about an outcome is when the network is under duress.

Often, a network is safe in theory — the security operations center (SOC) believes it has visibility of all assets; it maps its server, routing, and switching tables; the configurations appear safe; and the major vulnerabilities have been patched. A network is fluid, however, and the chasm between theory and practice may be significant.

Businesses would be wise to stress test their networks against specific threats and network conditions. A business may deploy a number of security control tools such as device vulnerability scanners, antivirus, endpoint detection and response (EDR) platforms, and firewalls. To understand its security posture, a company will often hire a red team or penetration testing service to attempt a controlled breach. These testing services, however, provide limited coverage and test only at a point in time. Remember that the desired outcome is more than just determining if a business is safe against the most publicized threat; a business needs to have a comprehensive idea of how its tools perform and how the SOC reacts against a range of adversary behaviors. Ultimately, the business needs the proper insights to adjust its cybersecurity posture.

AttackIQ provides a security optimization platform that offers automated security control validation solutions through breach and attack simulation (BAS). With the use of AttackIQ, organizations can test and validate their overall IT security posture to proactively identify and remediate gaps. IDC conducted research and interviews with five organizations that had direct experience with and knowledge about the benefits of using the AttackIQ platform.

Overall, IDC calculates that study participants achieved significant business value by:

- Improving the overall efficiency of SOC and red security teams and helping organizations break down counterproductive silos between red and blue teams
- Fostering better staff collaboration, thereby improving security postures including threat identification and remediation, while reducing the impact of breaches when they occurred
- Significantly reducing the cost of security breaches while maintaining leaner security staff profiles
- Providing ongoing continuing education to help security teams better anticipate the changing tactics used by attackers

Situation Overview

Inefficiencies and ineffectiveness in a security operations team and a security operations center can easily lead to a breach when security controls fail. The problems are always mounting in the SOC, and there are many factors involved (some that cannot be readily observed). Evolving policies do not convey across all tools. Security tools are misconfigured. Network and security teams have slightly different agendas. The SOC could still be on point with changes such as these, but sometimes new versions of operating systems (OSs), applications, and patches do not upload as expected or break existing functionality.

Consequently, the tools and processes fail repeatedly and silently due to a lack of continuous testing and performance data. For the sake of argument, let's suggest that a BAS assessment is conducted 50 times. One answer might be that the cybersecurity tools and processes stopped the threat 35 out of 50 times. A better answer might be the firewall prevented the attacker 37 out of 50 times; the EDR picked up the threat 33 out of 50 times; the alerts were carried to the SIEM or SOAR and successfully acted upon by the SOC 32 out of 50 times; and last, the time to detect threats ranged from 2 minutes 37 seconds to 48 minutes. Security teams — and security controls — can improve their performance through continuous exercising and testing.

All of this seems obvious enough, but there are practical impediments to realizing outcomes such as these with traditional red teaming or penetration testing:

- **Safety.**
  If a test is poorly conducted, devices can be damaged (which is an argument against black box testing). Routing tables could be destroyed and applications broken. This is an argument against red teams, black boxes, and penetration testing.
- **Context.**
  Security software often produces too many alerts or no alerts at all about an incident, confusing or misleading the security operations team. Any number of events can disrupt the operational context of security controls, including misconfiguration and poorly designed connectors between tools.
- **Availability.**
  Network performance is difficult enough in a nontest environment, as load balancing and network performance monitoring help ensure optimal conditions for employees, contractors, and visitors alike. It could be potentially disruptive to run an exercise during peak network activity. A business such as an online flower shop would rather gamble on a gap in security than compromise its network's ability to process orders on the week leading to Mother's Day.
- **Timing.**
  Red team/blue team exercises and penetration testing require a specific time ordinal and dedicated resource. If a new malware variant occurs after an intensive test, it is not as if a security team can instantly "get the band back together" to test the security program against it effectively.
- **Expense.**
  Pricing is subject to change and what types of insights are expected; however, the majority of penetration testing services start at $100,000+.

AttackIQ Overview

The flagship product for AttackIQ is the AttackIQ Security Optimization Platform, a breach and attack simulation solution that allows clients to emulate adversarial behavior and validate security control performance. It consists of a management platform that can be deployed as a SaaS or on premises. The management platform manages a constellation of agent-based test points that are deployed throughout the company's infrastructure. It comes with a broad and diverse scenario library that allows security teams to test real-world techniques, tactics, and procedures (TTPs) in a production environment. Clients can leverage AttackIQ's API-based integrations with a broad range of cybersecurity tools from companies like Splunk, Microsoft, Cisco, VMware, Cybereason, Check Point, and CrowdStrike, among others, to increase performance visibility and lead coordinated vendor responses to issues. Detailed reports on test results provide data that is used to find and resolve gaps for improved security posture and for updating compliance teams and auditors.

Common use cases for the platform are security control validation, operationalization of the MITRE ATT&CK framework, threat emulation, cloud security optimization, and compliance optimization.

The AttackIQ Security Optimization Platform is based on the AttackIQ Informed Defense Architecture (AIDA). The best way to think of AIDA is that it helps AttackIQ achieve everything: from security and compliance gaps to detections, and onto which remediation playbooks to deploy. AIDA is also an adversary emulation architecture built to test artificial intelligence (AI) and machine learning (ML) cyberdefense technologies in a production environment. The architecture supports TTPs similar to what a red team would do and generates results of how the blue team performs, a true mélange; the dual exercise is called "purple teaming." AIDA allows the AttackIQ Security Optimization Platform to test multiple assets in a customer's environment against any number of adversary assessments (i.e., APT29, FIN6, or Muddy Water) concurrently.

Clients can add modules to the platform, such as the AttackIQ Network Control Validation module, which allows them to replay traffic using packet capture (PCAP) reply between an attacking asset and a target asset to determine whether the inline security controls detect and prevent the attack. It then provides clear mitigation recommendation options for customers to improve their security posture.

The company also offers a comanaged service model, called AttackIQ Vanguard. Describing Vanguard as purely a BAS gives it short shift. Vanguard is a comanaged service under which AttackIQ subject matter experts and data scientists advise clients on their testing strategy, assessments, and scenarios to run. The Vanguard team uses assessments and attack graphs in the AttackIQ Security Optimization Platform to run realistic adversary emulations against advanced cyberdefense technologies, to include heuristic AI- and ML-enabled defenses like CrowdStrike. AttackIQ maps the network and allows it to gain threat-informed insights into the network, end users, the perimeter, and the hosts. Last, the AttackIQ Security Optimization Platform dashboard presents point-in-time and longitudinal testing data through graphical representations of security control performance, risk management effectiveness, and MITRE ATT&CK tactics, techniques, and procedures, among other analytic offerings designed to help the security operations team make better informed decisions.

A few points are noteworthy. The AttackIQ approach is that its platform is installed with the intent to find gaps in the security posture by validating network controls; this is proactive and preventative in nature. The platform then derives data-driven insights to suggest which steps in remediation are needed to optimize tooling and procedures; this is a closed-loop approach. While the AttackIQ platform provides scenarios, clients can also create their own using open APIs. Last, while BAS taken at face value provides security insights, security teams will also receive compliance reporting, an idea of how well individual tools work, as well as their overall platform, and can make informed decisions on which vulnerabilities to address first based upon risk.

The Business Value of AttackIQ

Study Demographics

IDC conducted research that explored the value and benefits for organizations in using AttackIQ to reduce cyberthreats and improve their overall risk profiles. The project included five interviews with organizations that were using the solution. Interviewed organizations all had experience with and knowledge about the impacts of its use and were asked a variety of quantitative and qualitative questions about their IT profiles and security operations.

Table 1 presents study demographics. The organizations that IDC interviewed had an average of 108,700 employees with an average IT staff of 191. In terms of geographic distribution, three companies were based in the United States with the remainder in the United Kingdom and Denmark. The vertical markets represented in the study included the healthcare (3), IT, and financial services sectors.

TABLE 1

Firmographics of Interviewed Organizations

Firmographics	Average	Median	Range
Number of employees	108,700	50,000	4,000–400,000
Number of IT staff	191	50	6–800
Number of assets managed	68,920	45,000	12,600–170,000
Annual revenue	$37.4B	$12.4M	$529M to $120B
Countries	United States (3), United Kingdom, and Denmark		
Industries	Healthcare (3), IT, and financial services		

Source: IDC Business Value Research, May 2022

Choice and Use of the AttackIQ Platform and Services

The organizations that IDC interviewed cited the reasons for their choice of AttackIQ as a core partner for their security operations. In most cases, some form of a security breach or ransomware attack prompted a need for these organizations to significantly shore up their cybersecurity programs and validate security operations and policies. Study participants called out the platform's reliability and significant time-saving features and noted that it provided the ability to solve and remediate complex security breaches.

They elaborated on these and other benefits:

- **A reliable way to test security controls:**
  "In February 2020, my organization was hit by a ransomware attack. It took the servers down for a month. As a result, IT security gained a lot of focus. It was significantly ramped up and centralized. We now have the responsibility for endpoint security controls, so we needed a way to test reliably."
- **Time-effective approach to security validation:**
  "I'm a big proponent of breach and attack simulation. My organization did its own in 2015 simulations when there was no software. We have a smaller team, with some red team capabilities, and doing everything in-house is very expensive. In selecting AttackIQ, I was looking to take advantage of the automation and playbooks that some vendors have to offer. Also, it's a time-saver, and can run simulations as often as desired, and allows us to more continually validate security."
- **Helpful in solving complex security breaches:**
  "My organization has an ongoing obligation to regulators to maintain security. We had numerous breaches and wanted to ensure that we could meet our obligations. It was difficult and expensive to solve very complex issues, but putting more money toward it did not move the needle. We had to fundamentally change how we handled security and decided to invest in AttackIQ."
- **A source of cybersecurity posture development:**
  "AttackIQ was viewed [as] part of the continuous development on our cybersecurity posture."

Study participants discussed additional selection criteria. Interviewed companies reported that AttackIQ represented a cost-effective approach to validating security policy without sacrificing robust functionality. They noted that it offered a diverse set of playbooks, simulations, and content and was a fully mature product that was backed by a supportive senior management team. Study participants also appreciated the fact that AttackIQ was an agile partner that helped them customize the platform according to their unique needs. Integration with Microsoft 365 was also cited as a core benefit.

Participants commented on these and related benefits:

- **Relationship with senior management team:**
  "There was a focus from senior management at AttackIQ on achieving my organization's desired outcomes versus a simple customer supply relationship and margin. The executive team listened and wanted to help us customize goals."
- **Diverse playbooks and partnership with MITRE:**
  "My organization likes the AttackIQ tool and how it operates, and there were a lot of the playbooks that covered diverse topics. Also, the partnership with MITRE is a big plus because they mapped very well to MITRE ATT&CK."
- **Cost-effective approach to simulations:**
  "AttackIQ stood out from the others in terms of product functionality and company knowledge. The pricing is also appreciated, and we like the service they offer where their experts run simulations on our network."

- **Large volume of content available:**
  "The AttackIQ product is streamlined and easy to use. We are a thin team and so ease of use is important. The open platform was also a big attraction. I have pretty sophisticated developers on my security team, and they want to be able to tie this into other workflows and codevelop it along with operational programs. Last, the volume of content is pretty striking and its diversity in terms of testing content. The ways that you can emulate, the scenarios, the playbooks, and the attack chaining functionalities were all great."
- **Mature product with integration into Microsoft 365:**
  "AttackIQ had official integration with Microsoft 365 and was the more mature and streamlined product on the market. It focuses on simulations based on the attack framework and does it very well. Also, the support staff were friendly and helpful."

Table 2 lays out the average organizational usage of AttackIQ based on interviews conducted. A large number of applications were optimized by AttackIQ (2,764), showcasing the value organizations saw in improving their security posture. The overall IT footprint was similarly substantial with 57,200 endpoint devices and 3,825 virtual servers/instances. Additional metrics are presented.

TABLE 2

Organizational Usage of AttackIQ

	Average	Median
Number of applications optimized by AttackIQ	2,764	1,500
Number of datacenters	5	3
Number of sites/branches	887	45
Number of endpoint devices	57,200	20,000
Number of virtual servers/virtual instances	3,825	3,300

Source: IDC Business Value Research, May 2022

Business Value and Quantified Benefits of AttackIQ

Interviewed organizations attributed substantial improvements in security operations to their use of the AttackIQ platform. The solution helped companies improve the efficiency of their SOC and red security teams while helping their organizations break down inefficient silos between red and blue teams (purple teams). Better collaboration improved their overall security operations, including threat identification and remediation.

AttackIQ allowed organizations to complete real-time testing and validation of their security policy, including controls that helped them identify performance problems. This capability enabled them to proactively fix problems before a major breach occurred and created greater confidence in their existing programs. With a diverse set of timely playbooks, the platform also gave organizations better ability to measure the effectiveness of their security posture and manage threat scenarios driven by the constantly shifting techniques of attackers.

Importantly, these organizations appreciated having a knowledgeable and supportive partner. Besides creating efficiencies for security teams, AttackIQ delivered financial benefits by significantly reducing the cost of security breaches while maintaining a more productive security staff. In addition, AttackIQ provided ongoing continuing education programs to help security teams anticipate the changing nature of threats and threat actors.

Interviewed customers spoke to the most significant impacts of their use:

- **Strong partnership:**
  "The partnerships made all the difference along with all the product features. Other solutions simply didn't compete. The big winner for AttackIQ is the whole approach to my organization as the customer."
- **Diverse playbooks and real-time testing:**
  "The biggest benefit is definitely the real-time testing. AttackIQ offers validation of controls and points things out that weren't working properly, which is an even bigger benefit than the validation process that finds some of the things we missed. Another big advantage is the timeliness of a lot of the playbooks. When I present to the board of directors, it's great to be able to say that we made these changes to our environment and now our protection against some particular threat group has gone up by 20% or whatever that number is."
- **Real-time team testing and validation:**
  "We appreciate the real-time testing and automated validations from AttackIQ. They save a lot of time for our teams because this is all tested by the AttackIQ teams."
- **Confidence from real-time and automated testing:**
  "The biggest benefits for my organization are real-time testing, automated testing, and confidence in the controls."
- **Ability to measure and manage cybersecurity:**
  "The largest benefit of AttackIQ is the ability it gives us to measure and manage our cybersecurity."

The Benefits of AttackIQ for Security Teams

To better prevent and remediate cyberattacks, organizations need to shift to a proactive mindset from a reactive one. Incident readiness programs are an important step in elevating any organization's cybersecurity program. Incident readiness helps organizations prepare in advance to make the right decisions when a crisis emerges so that the damage and duration of a cyberattack can be minimized.

AttackIQ is designed to help meet these challenges by providing multiple levels of functionality that benefit the different types of security teams providing the front line of defense against attacks. The platform enables teams that are often overly siloed to work together to achieve a better security posture while enhancing the skill sets of team members. AttackIQ automates a variety of routine tasks, including writing simulations and attack records, and gives security teams the ability to effectively test and analyze their current security policies to ensure that policy is rigorously adhered to by end users.

Study participants commented on these and related benefits:

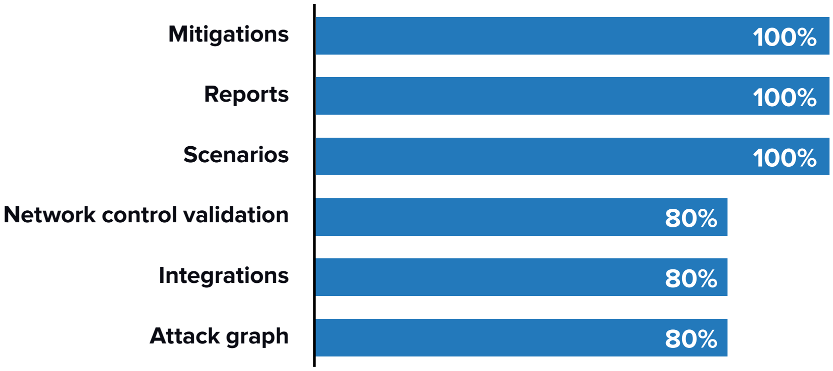
- **Efficient way to test and analyze cybersecurity posture:**
  "AttackIQ has given my organization the ability to test and analyze the results, and then come up with mitigations to iterate and improve our cybersecurity."
- **Less siloed approach to security:**
  "AttackIQ has brought people together in a cross-functional way."
- **Better security policy implementation due to simulations:**
  "AttackIQ has helped break down silos in my organization because it has been good at getting cooperation from other teams to implement policy. One thing is the security team often doesn't control a lot of the things where security policies need to be implemented. Sometimes it's much more convincing if I can say not only is it bad, but we ran this breach simulation, and this ransomware attack would have succeeded because this is turned on. It is good at giving some of the concrete proof of why some things need to be done."
- **Automation of tasks to save time:**
  "AttackIQ frees up time in running simulations, it automates a lot of tasks that saves time. Also, it brings attacks that are out there for simulation versus writing own script, which can be a time-consuming and costly process."
- **Greater productivity in writing attack records:**
  "Our Security Assessment Team (SAT) is more productive because they don't have to spend time writing attack records and simulating them. Outside of SAT, all the teams benefit from knowing if something's wrong with the internal controls."

Interviewed organizations recognized the value of the key features and functions of the AttackIQ platform. A majority of companies used all the features available on the platform. More specifically, all used *mitigations, reports, and scenarios* as shown in **Figure 1**. In addition, 80% of companies used *network control validation, integrations, and attack graph.*

FIGURE 1

AttackIQ Features and Functions Used

(% of organizations)



n = 5; Source: IDC Business Value Research, May 2022

Interviewed organizations noted that real-time testing, the availability of diverse playbooks, and simulations all helped their security operations team manage risk and ensure less impactful security events with greater effectiveness. Importantly, this team found that they were not constantly putting out fires and had greater overall confidence in their security posture. In addition, AttackIQ helped them proactively identify anomalies in their security preparedness. With the benefit of an automated platform, security teams did not need a development-focused background. These features helped the team recognize a strong efficiency gain of 47% (see **Table 3**), resulting in benefit of $901,460 in value of staff time per year. Overall, the efficiency gain recognized by this team enabled them to avoid hiring 2+ additional FTE security employees.

TABLE 3

Security Operations Team Efficiency Gain

	Before AttackIQ	With AttackIQ	Difference	Benefit
Total FTE count	19	10	9	47%
Value of staff time per year	$1.9M	$1.0M	$901,460	47%

Source: IDC Business Value Research, May 2022

IDC then looked at the impacts of AttackIQ on security operations center analysts and managers. Organizations found that these teams benefited from the ability to use reports and playbooks generated by AttackIQ to mitigate risk and ensure security policy with greater efficiency. This team, more than others, found particular value in AttackIQ's reporting functionality, which helped them evaluate the performance and controls in place in their organizations. They also noted that the playbooks were especially helpful in ensuring policy. Combined, these benefits enable SOC analysts to be 37% more efficient, as shown in **Table 4**. This efficiency amounted to the team saving the time of seven FTEs, allowing them to be repositioned within the team to focus on other business initiatives. It resulted in an annual value of staff time per year of $670,625 for each organization.

TABLE 4

Security Operations Center Analysts/Managers Efficiency Gain

	Before AttackIQ	With AttackIQ	Difference	Benefit
Total FTE count	18	11	7	37%
Value of staff time per year	$1.8M	$1.1M	$670,625	37%

Source: IDC Business Value Research, May 2022

IDC then looked at the staffing impacts on red teams. These teams are typically charged with challenging security controls within organizations by taking on an adversarial stance designed to look for weaknesses. Study participants reported that after adopting AttackIQ, red teams benefited from the platform's in-depth simulations that helped them evaluate, test, and validate cybersecurity operations. AttackIQ also served to automate routine tasks to free up staff and simplify the process of validation. As shown in **Table 5**, these improvements created an efficiency gain of 57% for red teams and a business value of $79,333.

TABLE 5

Red Team Efficiency Gain

	Before AttackIQ	With AttackIQ	Difference	Benefit
Total FTE count	1.4	0.6	0.8	57%
Value of staff time per year	$140,000	$60,667	$79,333	57%

Source: IDC Business Value Research, May 2022

Another important aspect of optimal security operations is the coordination of team efforts. Study participants reported that AttackIQ helped their organizations break down silos that existed between red teams (offensive orientation as described) and blue teams (defensive stance).

The platform helped both teams continuously work together as a purple team. As one study participant noted: "*My organization used purple teaming to reduce the number of actual alerts we were getting. We are now much more confident that we're able to detect what we need to. We also have, at the same time, reduced the number of trigger alerts and have reduced by 100-fold the situations that actually require alerts.*"

These staff improvements also served to help build skill sets and confidence and enhance knowledge transfer for red and blue teams working together. The end result was that these organizations could better detect and create alerts for threats proactively. As shown in **Table 6**, threat response due to better purple teaming had significant financial impacts and resulted in total average annual cost savings of $4.7 million for interviewed organizations.

TABLE 6

Cost Savings Using Purple Teaming

	With AttackIQ
Threat response	$4.7M

Source: IDC Business Value Research, May 2022

Cost Benefits of AttackIQ

Interviewed organizations reported that AttackIQ gave them greater confidence in their cybersecurity posture and reduced their overall business risk profiles. After adoption, they gained a deeper understanding of the policies and controls that provide optimal protection against the risk of attack. If for any reason using a particular control posed a risk, study participants could then take preemptive steps to mitigate it. AttackIQ also gave security teams the ability to report to management that the controls they had in place were working at full capacity. In addition, interviewed organizations found that AttackIQ gave them the ability to proactively plan their risk management strategies using improved metrics and to better anticipate attacker strategies via simulation techniques.

Study participants commented on these and related benefits:

- **Reduction in risk due to reporting:**
  "Business risk has been reduced, because with AttackIQ, we can measure where things work well. If something isn't working, we can take steps to address that."
- **Enables planning to deal with operational risk:**
  "AttackIQ enables us to have a plan. We have very weak metrics for how we measure operational risk. Having a strategy that measures performance with a validation component is now the plan … to deal with operational risk management."
- **Simulation of attacker strategies:**
  "AttackIQ helps my organization find some of the clever ways in which attackers can get around things."
- **Proof of effective controls:**
  "AttackIQ shows that the controls actually work. There is a big push in security now for having certain maturity levels assigned where we have to actually show the process working. It's not enough to say they have a control, but my organization has to show controls are repeatable and that they are working. While we are still in the early stages, AttackIQ provides the basis for proving that there are effective controls in place."

Other risk mitigation benefits were financial in nature. Preparation based on emulations, comprehensive testing, and playbooks all combined to help interviewed organizations significantly reduce the potential costs related to security breaches. In addition, with the implementation of AttackIQ, their teams were able to work together to better understand breaches, transfer knowledge, and gain confidence in response plans. As a result of these improvements, they were able to reduce the cost of a potential security breach on average by nearly $4 million annually, representing a 44% improvement (see **Table 7** next page).

TABLE 7

Potential Security Breach Risk Reduction

	Before AttackIQ	With AttackIQ	Difference	Benefit
Total FTE count	$59.7M	$33.5M	$26.1M	44%
IDC operating margin	15%	15%		
Value of staff time per year	$8.9M	$5.0M	$3.9M	44%

Source: IDC Business Value Research, May 2022

IDC further evaluated security cost benefits. Study participants noted that the use of AttackIQ enabled their organizations to consolidate multiple tools into one platform, thereby resulting in significant cost reductions. **Table 8** quantifies this benefit with total average annual savings calculated at $862,254.

TABLE 8

Tool Consolidation Cost Reductions

	With AttackIQ
Tool consolidation cost reductions	$862,254

Source: IDC Business Value Research, May 2022

Continuing Education with AttackIQ Academy

AttackIQ Academy is a value-added learning service that provides free cybersecurity courses to provide real-world, hands-on experience to customers. The programs allow companies to improve their overall cybersecurity postures and to better deal with attack methods that are becoming more targeted, sophisticated, and automated. The curriculum includes topics such as Uniting Threat and Risk Management with NIST 800-53 and ATT&CK, Purple Teaming, and Breach and Attack Simulation and offers badges and certifications upon completion.

Organizations discussed the positive impact that AttackIQ Academy had on their organizations, especially when understanding and operationalizing MITRE ATT&CK. They reported that participants gained a better understanding of the evolving nature of the threats their organizations were exposed to and that the courses gave their security teams an easy way to stay current with best practices.

.Study participants commented on these benefits:

- **Deeper understanding of MITRE ATT&CK:**
  "AttackIQ Academy has definitely helped us operationalize the MITRE ATT&CK. It gave the whole staff more of a feel for what MITRE ATT&CK is, how AttackIQ was going to help with a lot of the stuff. It provided a lot of the background knowledge necessary for everyone to understand the strategy of breach and attack simulation and more evidence-based approaches that I was bringing to the organization."

- **Robust understanding of threats:**
  "Employees who participate in AttackIQ Academy are armed with knowledge and understand the new threats out there that our organization is exposed to. They also learn how those things impact us internally."

- **An easy way to learn:**
  "AttackIQ is an easy way to consume best practices."

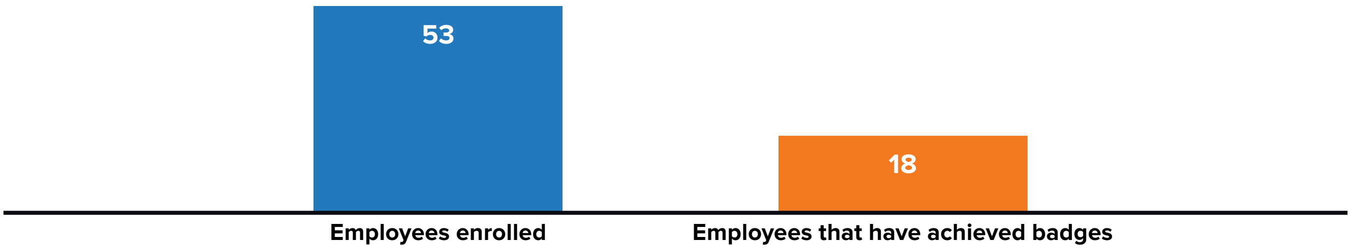
- **Cost-effective approach to continued education:**
  "AttackIQ is both free and very educational."

From these comments, it's clear that interviewed organizations appreciated the value proposition of AttackIQ Academy and the large number of courses that were available. At time of interview, these organizations had an average of 53 employees enrolled in the program (see **Figure 2**). In addition, 18 employees had earned some form of a badge or certification. Interviewed organizations reported that they expected to continue to enroll employees in the program.

FIGURE 2

AttackIQ Academy Participation

(Employees)



n = 5; Source: IDC Business Value Research, May 2022

Challenges/Opportunities

As is often the case in cybersecurity, AttackIQ can be seen as both a complement to cybersecurity tools and a competitor with the chance to displace certain tools. The dynamic holds true for services such as BAS, red teaming, and penetration testing; AttackIQ can improve these services or be used in lieu of them.

There are a handful of challenges that face AttackIQ. The first challenge is its software platform competes against BAS vendors such as SafeBreach and Cymulate. In security instrumentation, Mandiant has its Mandiant Security Instrumentation Platform, and there are any number of well-reputed penetration testers.

The second challenge is a matter of misperception within SOCs. Mature SOCs may believe they have solved their security tool and workflow problems. An advanced SOC may deploy a mix of proprietary and commercial point products. If anything, the mature SOC may favor better point products (a more robust firewall or a more versatile EDR solution), confident that it can integrate and automate tools within its fabric.

A last challenge, that may in fact be an opportunity, is a matter of static assumptions based on legacy cybersecurity architectures. In general, businesses do not understand the multivaried network that they have. The move to cloud includes new surfaces such as PaaS and IaaS; Internet of Things (IoT), 5G networks, and the metaverse are visible on the horizon. The dirty secret in cybersecurity is that security tools and platforms need constant tuning, and this problem is multiplied as more tools are introduced. Beyond tools, the efficacies of the APIs and SOAR platform tools are affected as well.

The opportunity for AttackIQ is it can show that automated controls validation is a synthesis of what can be achieved by BAS, penetration testing, and security platforms that measure configuration drift. Remember that the objectives of security tools are to prevent intrusion in the first place and then help detect the adversary if the network is breached. Pre-validating controls powerfully enforces prevention capabilities, and the sharpening of tools and processes increases the probability of detection and the reduction of the blast surface in fighting the adversary.

Conclusion

The tried-and-true maxim about the SOC is that it is a magical combination of " … people, processes, and technology." What is fascinating though is that no one really thought to test the confluence of this dynamic. The conventional processes have been to uncover the most prevalent vulnerabilities and remediate them (patch, build a firewall to mitigate access, etc.). This leaves out the questions of how tools work together to find vulnerabilities and how to supply the best context for actionable intelligence.

To be fair to SOCs, even the smartest teams deal with a fluid network. Conditions change with each software upgrade. The problem is multipronged; it is difficult to determine if a tool is configured properly or is working in the first place, much less trying to determine if valid alerts are getting into the workflow so that the context is actionable.

Taking another tactic, one of the ways that organizations think about their network is in terms of attack surfaces, often in terms of the externally facing attack surface. The reality is that attacks typically consist of a multiphase campaign — the “kill chain”. There is an attack surface associated with every phase of the attack chain, with security controls put in place to detect or block the adversary behaviors typical of that phase. It is vital to verify that those controls are working to defend that entire attack surface across the beginning, middle, and end of the attack.

We found that AttackIQ in its process runs adversary emulations and attack graphs in a production environment and can run multiple assessments concurrently and at scale across an organization’s security controls. The insights provided include visibility into how an attack progresses, how individual tools and the integrated security stack perform, and how the SOC itself performed. AttackIQ provides a safe, automated, and low network resource–intensive environment allowing a SOC to retest its posture after remediations are made.

AttackIQ represents a logical and extensible approach to how businesses should approach their evolving SOC practices. The return on investment that IDC was able to measure confirms AttackIQ’s mission statement that real-time, data-driven visibility into a company’s security program offers prevention in terms of shoring up a security posture, stronger SOC performance in real-time investigations with the element of practice, and stronger remediation as much is learned about the network and how to limit the blast surface.

Note: All numbers in this document may be inexact due to rounding.

About the Analysts

Christopher Kissel

Vice President, Security & Trust Products, IDC

Chris Kissel is a Research Vice President in IDC's Security & Trust Products group, responsible for cybersecurity technology analysis, emerging trends, and market share reporting. Chris's primary research area is Tier 2 that security operation center (SOC) analytics. The major technology groups within this practice are SOAR, network intelligence and threat analytics (NITA), and XDR. Chris's also contributes to the IDC SIEM, device and application vulnerability practices. The Tier 2 SOC analytics service effectively covers the processes SOC analysts employ to monitor, detect, remediate, and mitigate threat actors attempting to attack a network within a security and vulnerability management and security analytics paradigm.

[More about Christopher Kissel]

Megan Szurley

Senior Research Analyst, Business Value Strategy Practice, IDC

Megan Szurley is a Consulting Manager within IDC's Custom Solutions Division, delivering consultative support across every stage of the business life cycle: business planning and budgeting, sales and marketing, and performance measurement. In her position, Megan partners with IDC analyst teams to support deliverables that focus on thought leadership, business value, custom analytics, buyer behavior, and content marketing. These customized deliverables are often derived from primary research and yield content marketing, market models, and customer insights.

[More about Megan Szurley]

IDC Custom Solutions

This publication was produced by IDC Custom Solutions. As a premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets, IDC's Custom Solutions group helps clients plan, market, sell, and succeed in the global marketplace. We create actionable market intelligence and influential content marketing programs that yield measurable results.

IDC

@idc   @idc   idc.com

Privacy Policy | CCPA