Technical Validation

Continuous Validation of Enterprise Cybersecurity Controls with AttackIQ

By Jack Poller, Senior Analyst

January 2019

This ESG Technical Validation was commissioned by AttackIQ and is distributed under license from ESG.

Contents

ESG Technical Validations

The goal of ESG Technical Validations is to educate IT professionals about information technology solutions for companies of all types and sizes. ESG Technical Validations are not meant to replace the evaluation process that should be conducted before making purchasing decisions, but rather to provide insight into these emerging technologies. Our objectives are to explore some of the more valuable features and functions of IT solutions, show how they can be used to solve real customer problems, and identify any areas needing improvement. The ESG Validation Team's expert third-party perspective is based on our own hands-on testing as well as on interviews with customers who use these products in production environments.

Introduction

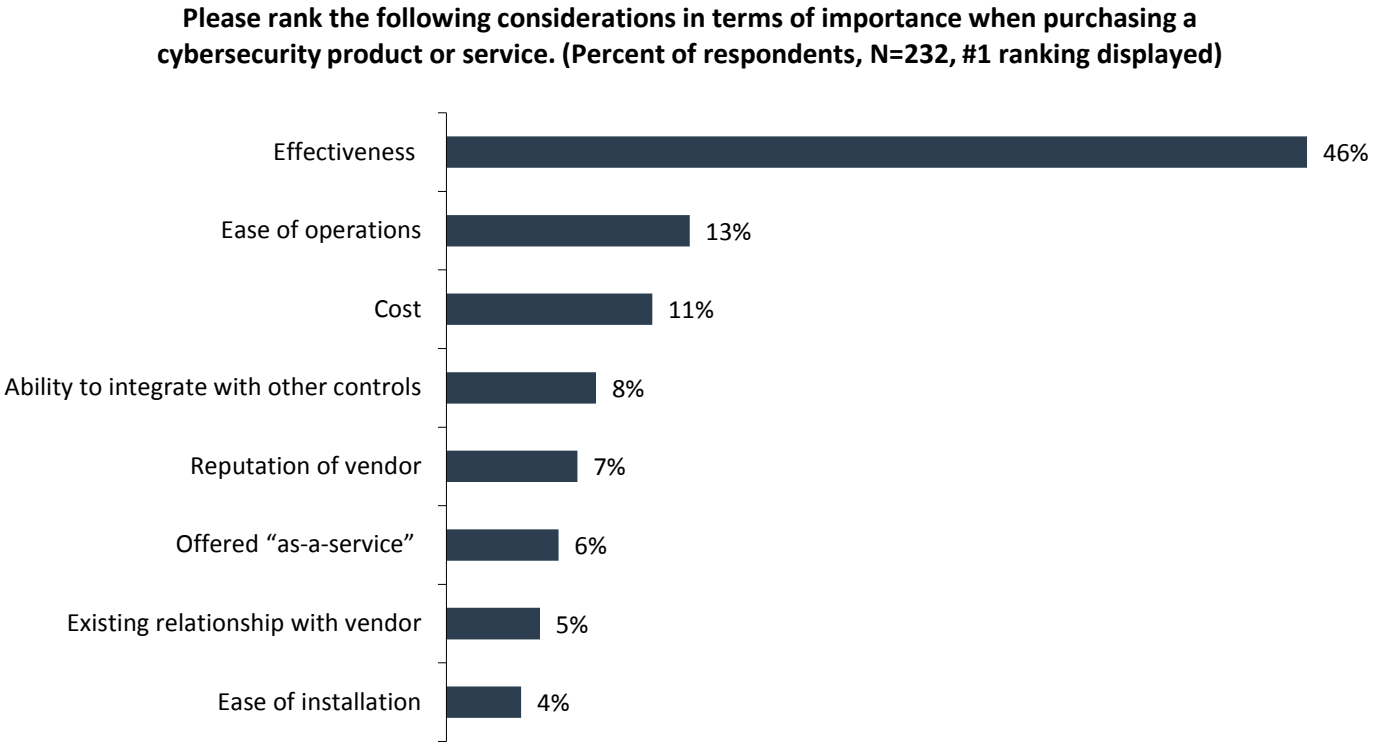
This ESG technical validation detail's ESG's hands-on assessment of AttackIQ. ESG focused on evaluating AttackIQ's continuous validation of cybersecurity controls. The evaluation was designed to explore how the solution can ensure an organization maximizes the effectiveness of its cybersecurity toolchain.

Background

The ever-increasing volume and velocity of threats has made cybersecurity one of the top IT concerns. According to ESG research, 37% of respondents—the largest percentage—believe that strengthening cybersecurity is the business initiative that will drive the most technology spending at their organizations over the next 12 months. This drive to secure their organizations is complicated by the global cybersecurity skills shortage—53% of organizations report that they have a problematic shortage of cybersecurity skills in 2019, up from 51% in 2018.[1]

As a result, organizations evaluating their options for strengthening cybersecurity are seeking more efficient and effective tools. Indeed, according to ESG research, effectiveness is by far the most important and most often cited consideration for organizations investing in cybersecurity products or services (see Figure 1).[2]

Figure 1. Considerations When Purchasing Cybersecurity Products or Services



Source: Enterprise Strategy Group

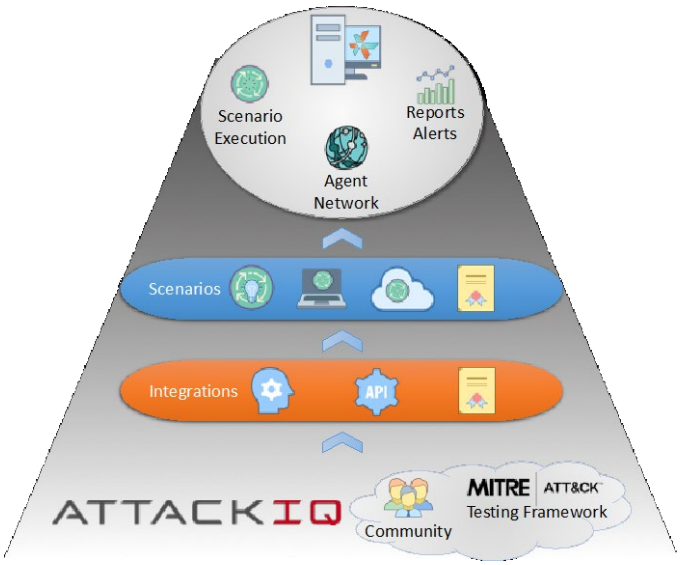
Organizations looking to improve their cybersecurity posture need to answer a key question: how do I know my tools are working correctly? What is needed is a solution that can continuously validate an organization's tools and cybersecurity teams, identifying gaps in detection and response.

[1] Source: ESG Research Report, *2019 Technology Spending Intentions*, to be published.
[2] Source: ESG Master Survey Results, *Cybersecurity Landscape: The Evolution of Enterprise-class Vendors and Platforms*, October 2018.

The AttackIQ Platform

The AttackIQ platform was designed to seamlessly integrate into any existing network to deliver immediate visibility into an organization's security program. AttackIQ's goal is to mitigate risk and maximize ROI by validating the effectiveness of the organization's cybersecurity toolchain and security teams.

AttackIQ's methodology focuses on attack scenarios that provide immediate feedback and insight, along with the ability to track results over time. Scenarios mimic the behavior of real-world malware and attack methodologies, such as those in the MITRE ATT&CK framework. Running scenarios enables the organization to validate security tools' detection and response and instrument the environment, enabling organizations to confirm the entire cybersecurity tools, processes and people are functioning as intended.



AttackIQ continuously creates and curates new scenarios based on emerging threats, and provides the source code for each attack scenario, enabling organizations to customize scenarios to their specific environment and needs. Organizations are encouraged to contribute scenarios to the community, increasing the breadth and depth of security toolchain validation over time.

Passive test agents, deployed across the network, are the sensors for AttackIQ, receiving and executing selected scenarios on-command for live security testing. AttackIQ supports all major operating systems and can be deployed on-premises or through the cloud. The lightweight agents ensure simple and rapid scalability as needs change.

AttackIQ provides fully customizable automated reporting, giving security teams and executives a clear picture of security status, and changes and improvements or regressions over time. An interactive dashboard provides comprehensive visualization of events in real time. The solution is designed for all tiers in the cybersecurity team:

- Red team engineer—build and run attack scenarios that imitate real and pervasive threats targeted against the organization and measure the response.
- Blue team engineer—receive immediate validation of changes to security posture, enabling blue teams to catch up to red teams.
- CISO—review impact reports that provide a real time snapshot of overall security posture as compared against the MITRE ATT&CK matrix, as well as improvements (or regressions) over time.

Organizations deploying AttackIQ benefit from:

- Quantification of baseline security posture, and measurements of changes to security posture over time.
- Immediate feedback on how the cybersecurity toolchain responds to threats.
- Real-time reporting to enable data-driven decisions.
- Measurement of effectiveness of security tools, processes and people, with reports to justify existing and new cybersecurity investments.

ESG Technical Validation

Getting Started

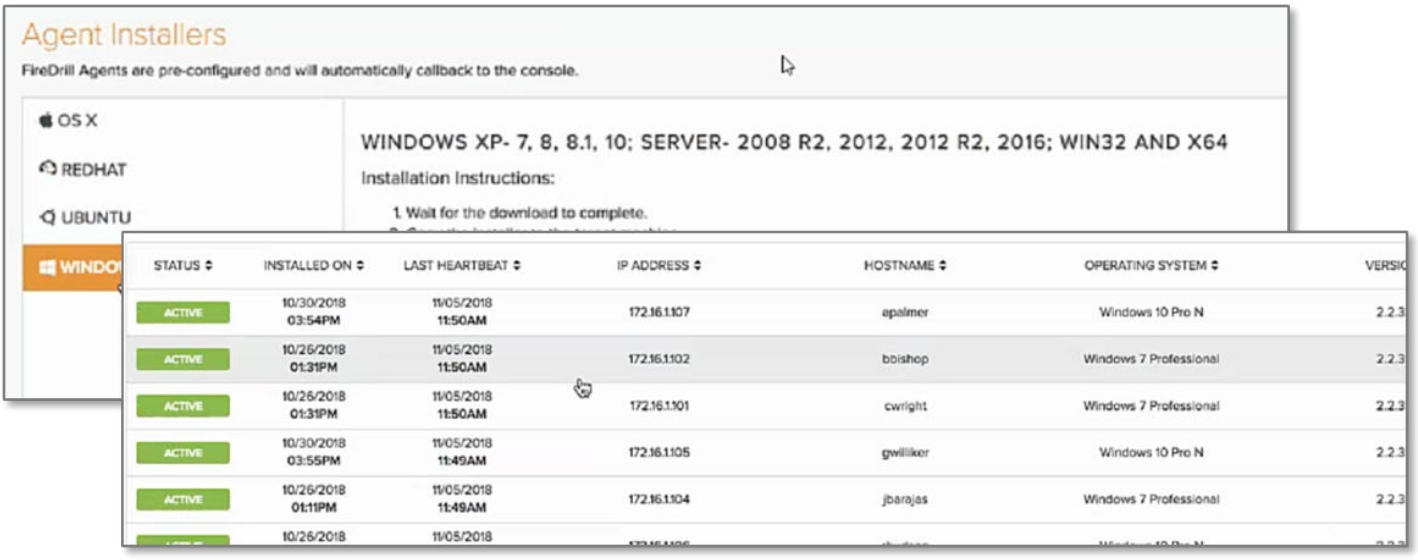
AttackIQ was designed to require minimal setup time and few resources to implement, enabling organizations to obtain results almost immediately. Organizations deploy lightweight agents to run attack scenarios. The agents are passive and wait for commands to execute. When the AttackIQ user selects and runs a scenario, AttackIQ sends a set of commands to the selected agents and waits for the results.

ESG Testing

ESG began by logging in to AttackIQ and deploying a set of agents to a selected set of systems in the environment. The first step was to download the agent from AttackIQ. Custom downloads are available for Apple OS X, Redhat and Ubuntu Linux, and Windows.

Next, ESG installed the agent on select systems. Once installed, the agent registers with AttackIQ, using custom configuration information provided in the download, enabling AttackIQ to distinguish between customers. The agents provide IQ with asset configuration information including OS and version, displayed in the AttackIQ dashboard, as shown in Figure 2. AttackIQ provided a variety of methods to group assets for ease of management and use.

Figure 2. Installing AttackIQ Agents

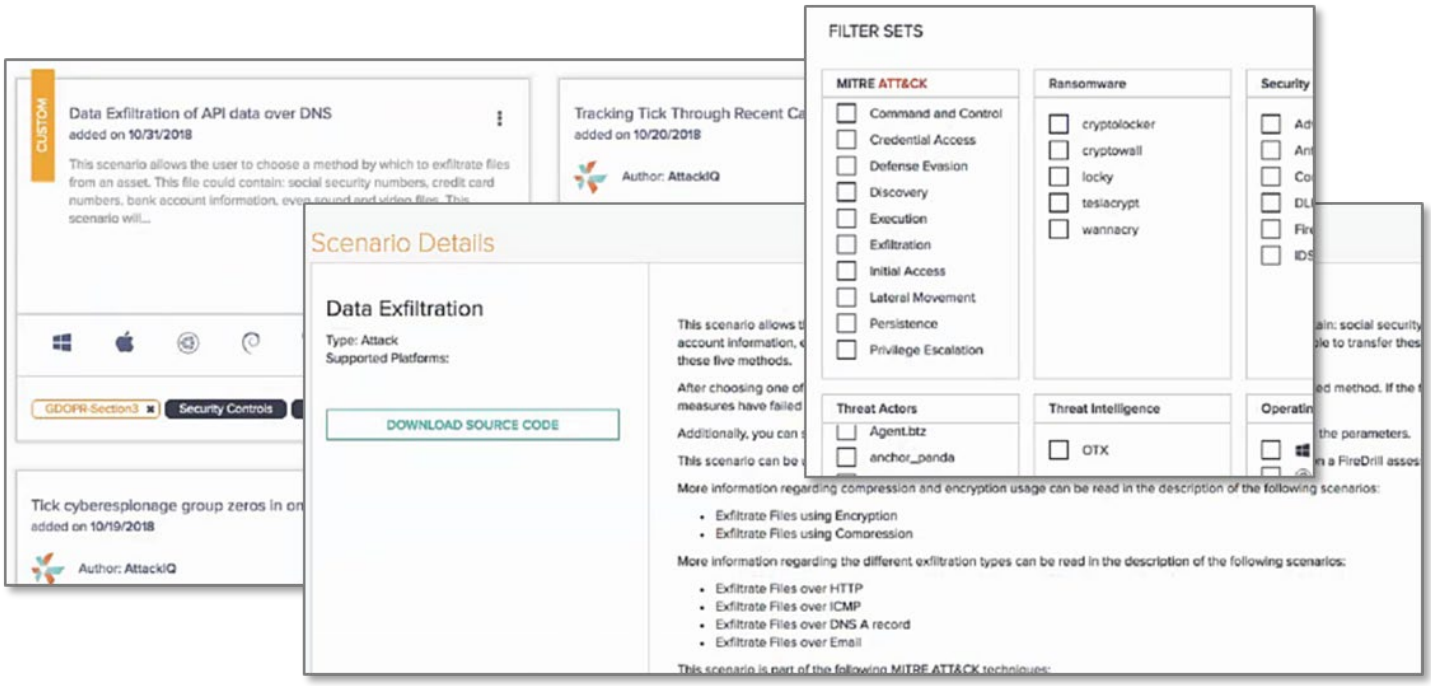


Source: Enterprise Strategy Group

The next step was to select a test scenario to be executed. We browsed the scenario library, as shown in Figure 3. AttackIQ's extensive scenario library is displayed as a set of cards organized by use case. Each card provides the scenario title, description, target OS, and tags which map the attack to the MITRE ATT&CK framework, as well as regulations and industry-standard benchmarks such as GDPR, HIPAA, CIS, etc.

Users can filter the scenario library using categories such as OS, MITRE ATT&CK stage, threat actors, threat intelligence provider, security controls, or ransomware type. We selected the ***Data exfiltration*** scenario, which brought up a popup with detailed information on the scenario and provided us with the ability to download the source code and to specify files to exfiltrate, along with the exfiltration protocol (HTTP, ICMP, DNS, email).

Figure 3. Scenario Library

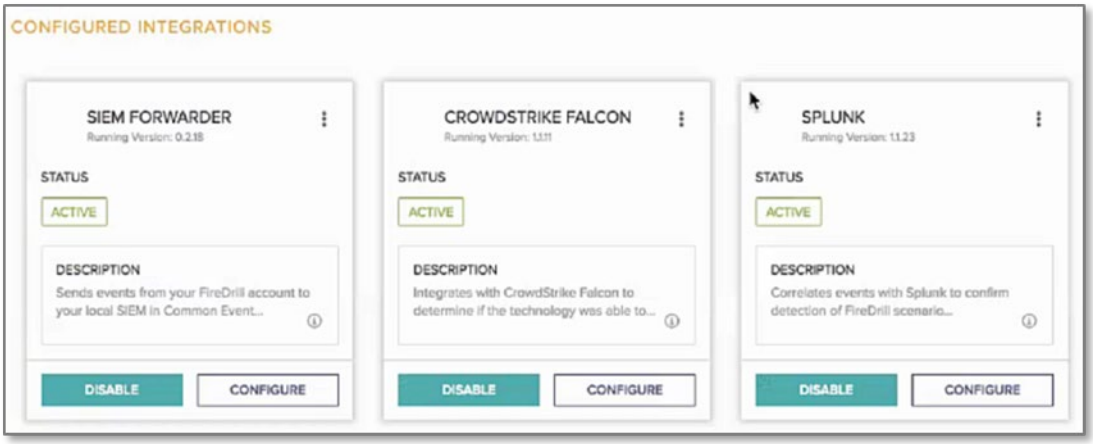


Source: Enterprise Strategy Group

Next, we selected and configured AttackIQ's integration with SIEM and other log management and analysis systems. As shown in Figure 4, integrations are shown in cards similarly to attack scenarios. A key part of the integration is enabling AttackIQ to filter its own activities from the cybersecurity logs, preventing false positives from appearing in reporting and analyses.

For example, when a scenario simulates a data exfiltration attempt, AttackIQ needs to verify that the simulated attack was appropriately logged. Once verified, the log entry needs to be removed to prevent that simulated attack from being counted and analyzed as a real attack against the organization.

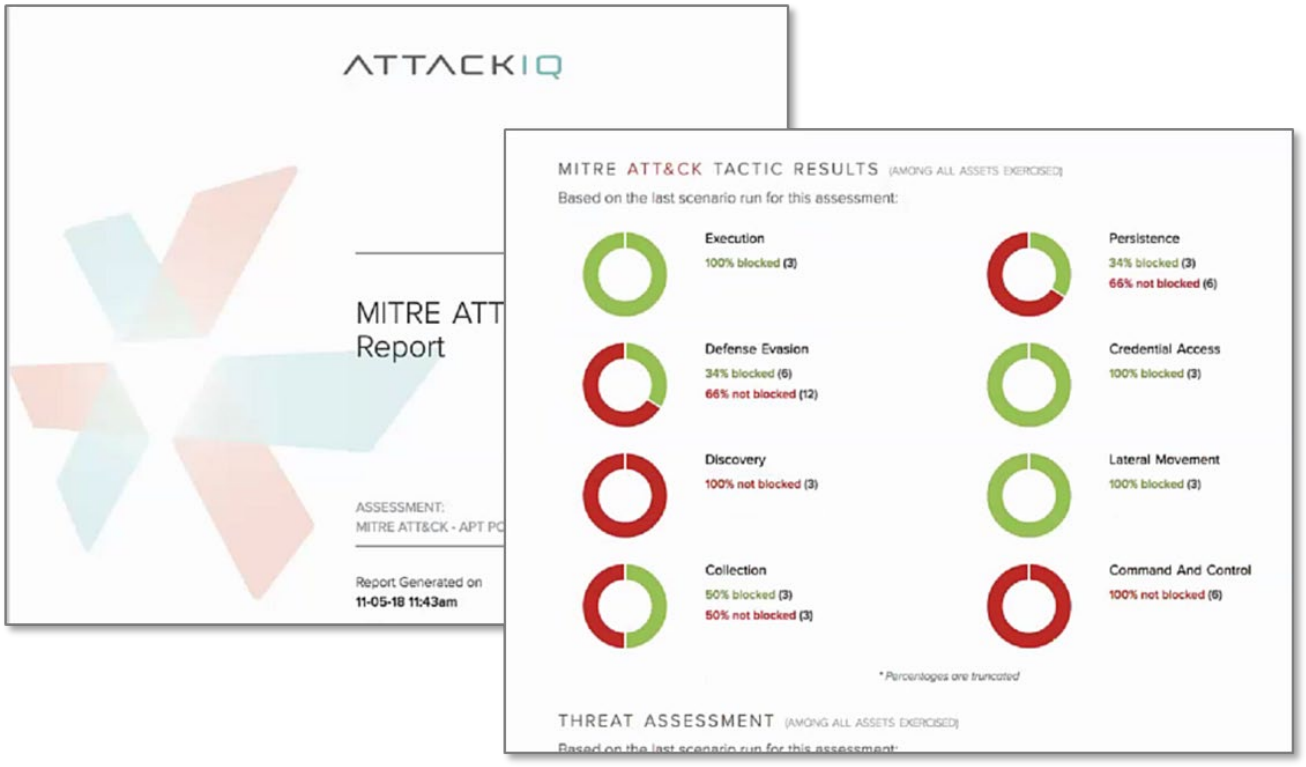
Figure 4. Integrations



Source: Enterprise Strategy Group

After executing the simulated exfiltration attack, we ran a standard on-demand report, as shown in Figure 5. The report provided both summary information as well as a detailed analysis of all attempted scenarios, organized to the MITRE ATT&CK framework. Users can configure AttackIQ to routinely email reports.

Figure 5. Reports



Source: Enterprise Strategy Group

Why This Matters

Facing perpetual cybersecurity skills shortages, organizations cannot afford to invest in complicated products with extensive learning curves, requiring significant efforts and time to install and obtain initial results.

ESG validated that installing AttackIQ is quick and simple. We were able to download and install agents in just a matter of minutes. We found the user interface intuitive and were able to rapidly progress through configuration to running our first simulated attack scenarios. AttackIQ's reporting provided readily understandable results—suitable for both security practitioners and C-suite executives—demonstrating the current security posture and historical trends.

Assessments

The typical AttackIQ use model is to configure a set of assessments of the organization's cybersecurity infrastructure. The security analyst runs assessments—sets of attack scenarios—to establish a baseline for the organization, and then schedules assessments to run on a routine basis to continuously validate the cybersecurity posture, identifying improvements and regressions.

ESG Testing

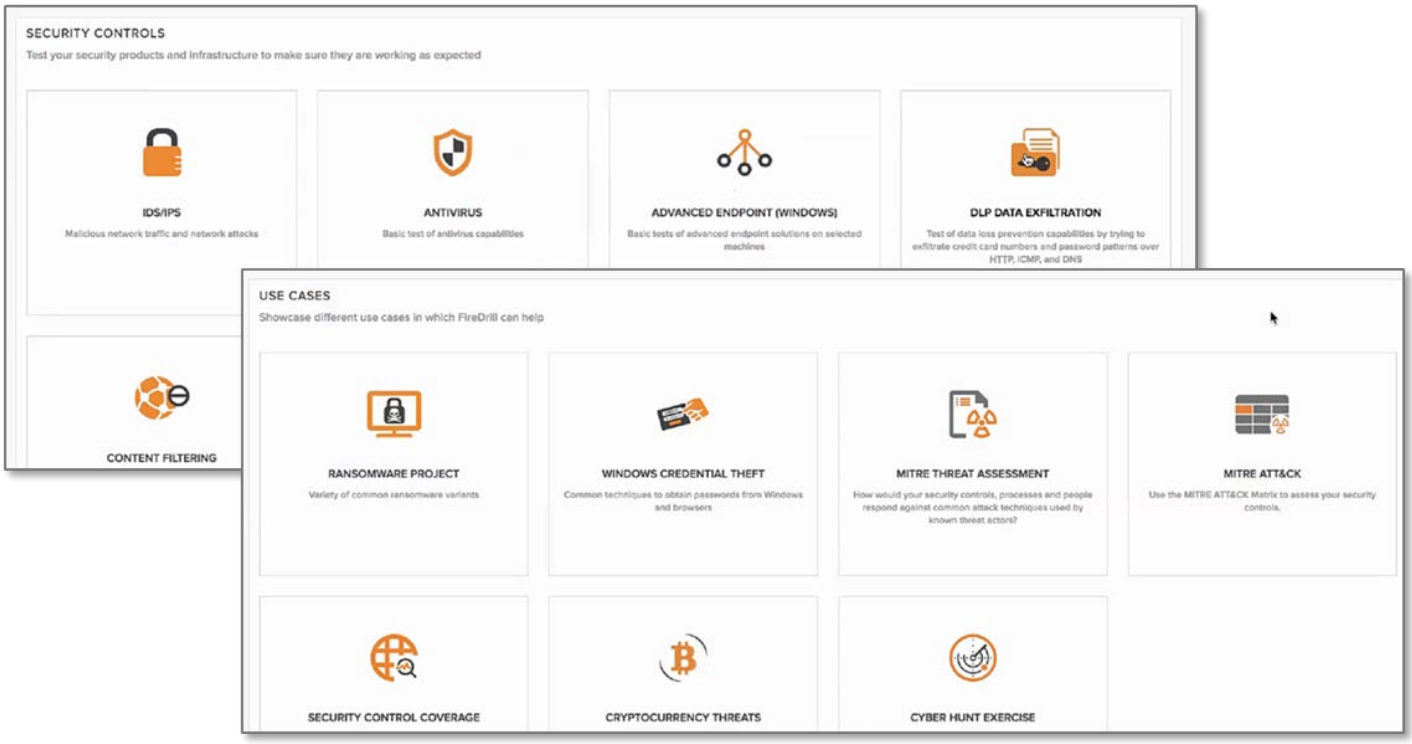
First, ESG created a customized assessment based on existing assessment templates. We browsed the template library to select an assessment. As shown in Figure 6, AttackIQ organized assessments by use case, such as IDS/IPS, antivirus, Windows endpoints, DLP, ransomware, credential theft, MITRE threat assessment, or MITRE ATT&CK.

Identifying Control Regressions

A national bank scheduled an AttackIQ assessment of a critical security control to run every hour. Months later, the assessment suddenly failed, alerting the security team.

An investigation revealed that an OS upgrade included a subtle change to how a security control was implemented, exposing a security hole. The organization was able to identify and remediate the regression in a matter of hours, preventing potentially catastrophic losses.

Figure 6. Assessments and Use Cases



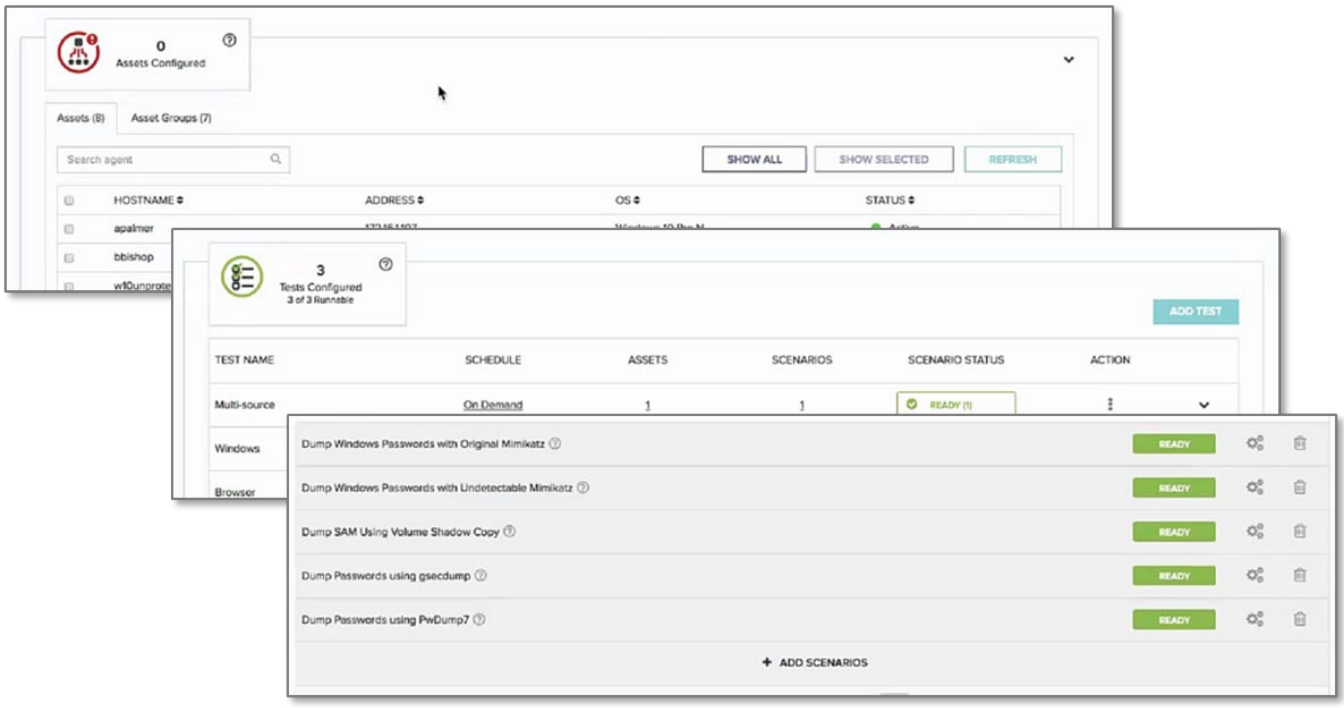
Source: Enterprise Strategy Group

We selected the ***Windows credential theft*** template, which created a new assessment. AttackIQ provided a step-by-step configurator to configure the assessment, as shown in Figure 7. Following the steps, we selected assets to be assessed from the list of configured assets.

Next, we reviewed and configured the assessment scenarios. The assessment groups scenarios into a set of tests. Clicking on the expand arrow on the far right of the test list expanded the test. We could customize the test by adding additional scenarios and could customize each scenario.

The last step was to schedule the assessment, and we chose to run immediately.

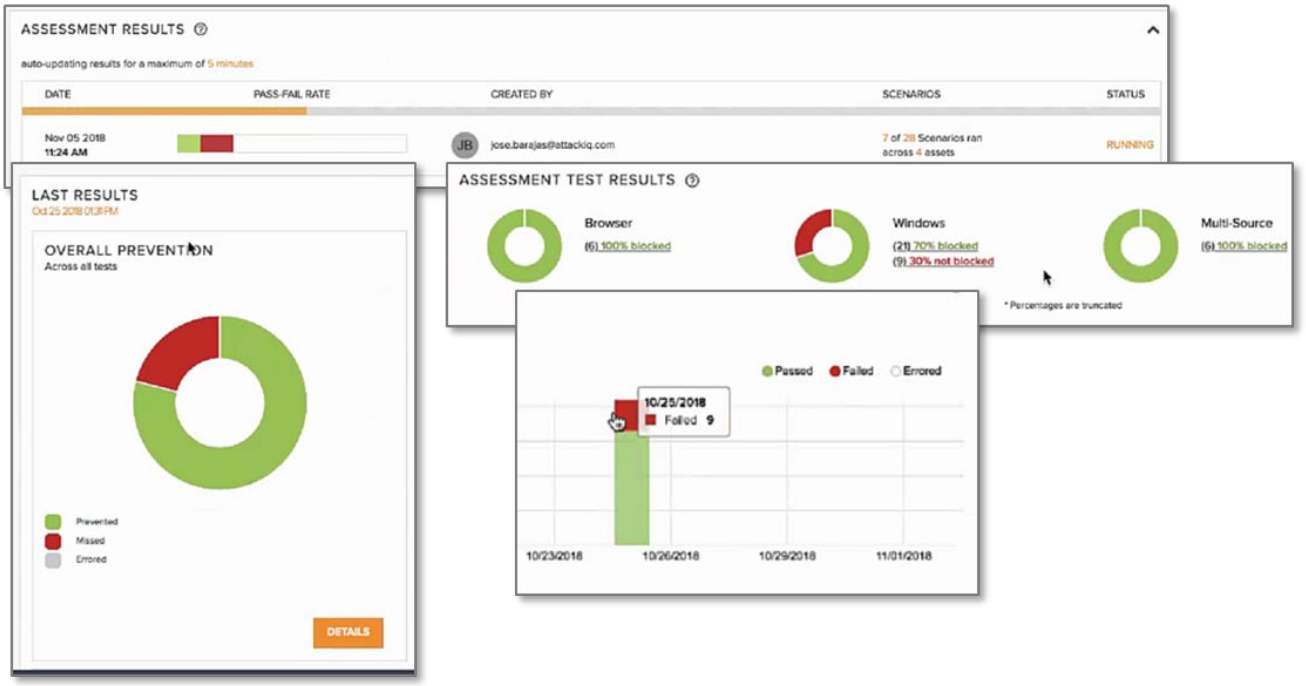
Figure 7. Configuring an Assessment



Source: Enterprise Strategy Group

AttackIQ displayed a progress bar, automatically updating results as they became available, as shown in Figure 8. Once complete, we used the results interface to review summary and detailed results, presented as donut and bar charts. Scenarios that were detected and prevented are classified as passed and shown in green, while those not detected or prevented are classified as failed and shown in red.

Figure 8. Assessment Results

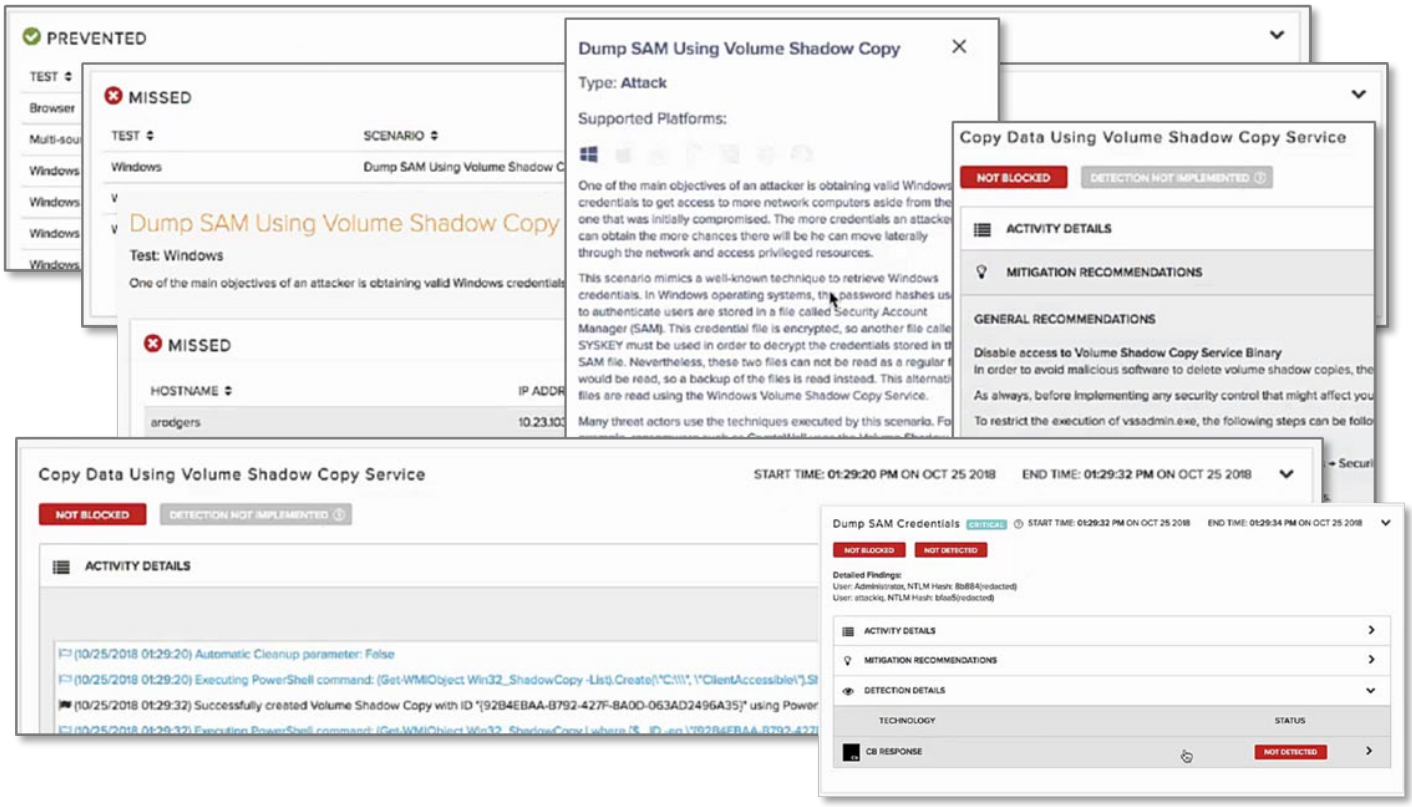


Source: Enterprise Strategy Group

The interface presented assessment results over time, enabling us to compare current and previous results identifying improvements and regressions. We could also click on a result to drill down for more information. We clicked on the ***Overall Prevention*** results from the current run, and AttackIQ provided details for the three groups in this assessment, ***Browser, Windows,*** and ***multi-source.***

Next, we clicked on Windows to expand and show results for each of the five scenarios in the Windows test group. We drilled down to obtain the details and perform a failure analysis, as shown in Figure 9. AttackIQ provided exceptional fidelity of results, and we were able to review the exact step where the scenario succeeded by dumping SAM using volume shadow copy. AttackIQ also provided detailed descriptions and suggested remedial actions for each step in the attack. We could then proceed to fix the issue and quickly retest to validate the remediation.

Figure 9. Assessment Details and Failure Analysis



Source: Enterprise Strategy Group

Why This Matters

Traditional red team efforts to validate cybersecurity control effectiveness take months to plan and execute, and even more time to analyze and report results. Often, red team exercises are structured around audits, leaving organizations exposed as changes escape validation.

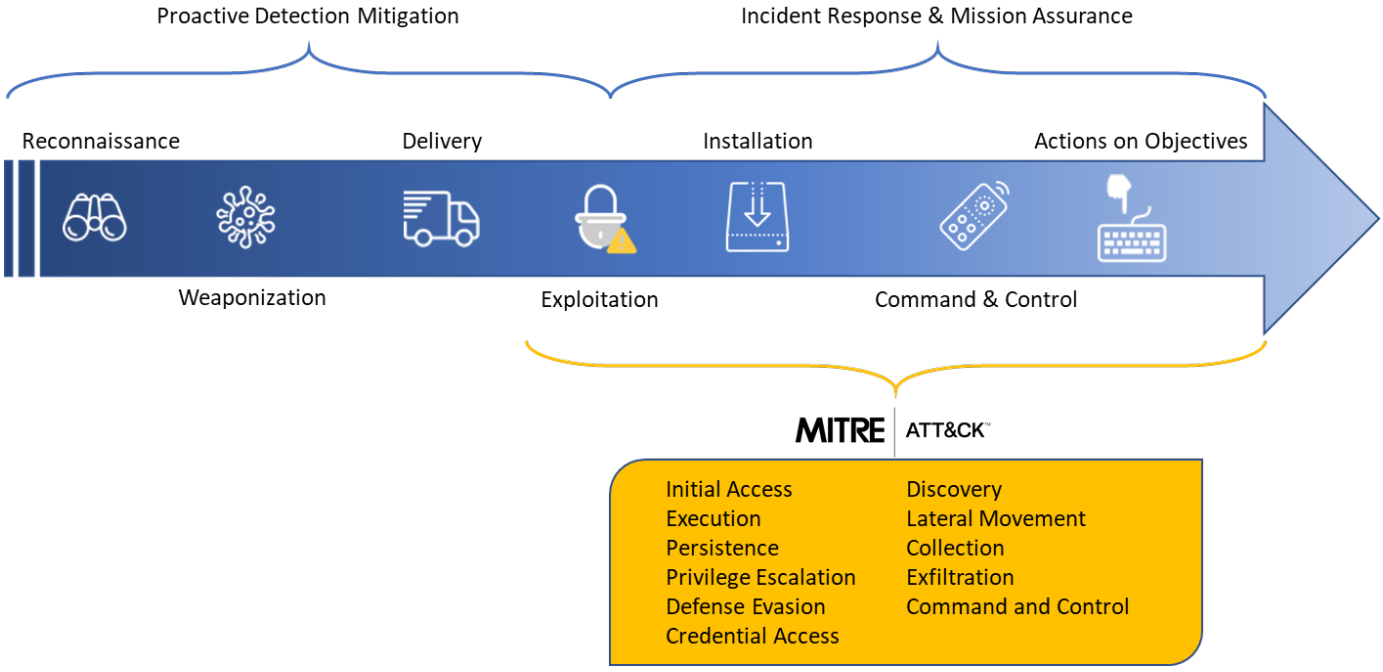
ESG validated that with AttackIQ, we could easily create and schedule assessments to run routinely. We could drill down through results to rapidly identify issues and apply remediations. Using AttackIQ's continuous validation methodology, organizations can assess current toolchain effectiveness and can easily identify regressions and track improvements over time.

MITRE ATT&CK Framework

The MITRE ATT&CK framework expands upon the Lockheed Martin Cyber Kill Chain to provide a deeper level of granularity in describing what can occur during an intrusion. MITRE ATT&CK provides a database of real-world adversary tactics, techniques, and processes (TTP). The 11 ATT&CK TTP categories were derived from the later stages of the kill chain, as shown in Figure 10.

The ATT&CK framework describes the actions an adversary may take to compromise and operate within an enterprise network and can be used to better characterize and describe post-compromise adversary behavior. AttackIQ structures scenarios and assessments according to the ATT&CK framework to help users understand and prioritize cyber threats and the impact on their organization's cybersecurity posture.

Figure 10. MITRE ATT&CK Framework



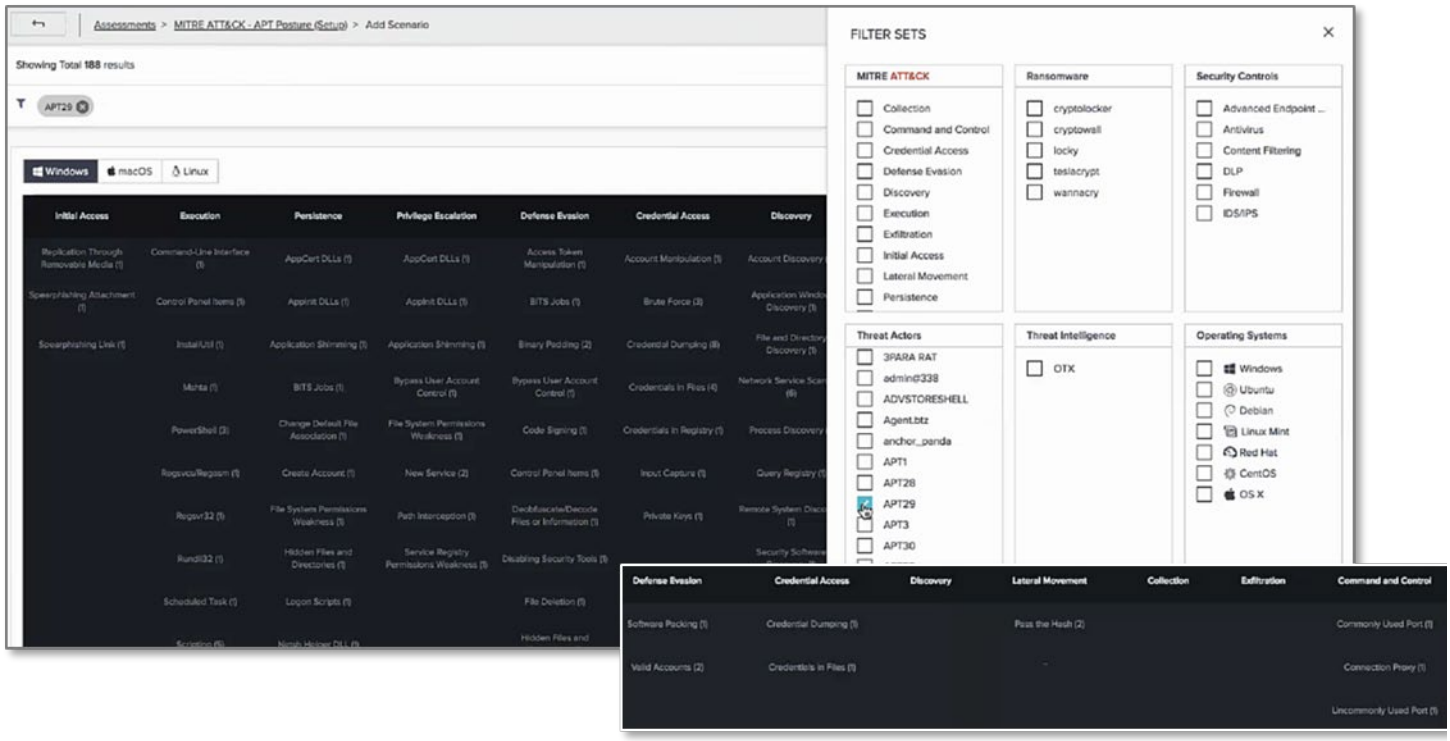
Source: Enterprise Strategy Group

ESG Testing

ESG created a new assessment using the MITRE ATT&CK framework. From the assessment template library, we selected the MITRE ATT&CK framework template. As shown in Figure 11, AttackIQ displayed the comprehensive list of ATT&CK scenarios. Using the filter option, we selected ***APT29*** from the ***Threat Actors*** category, and AttackIQ displayed the filtered set of TTPs associated with APT29. We then clicked on ***select all*** and added the scenarios to the assessment. We also added scenarios for TTPs associated with threat actors APT3 and APT28.

Like our previous assessment, we then selected the assets targeted for testing by this assessment. Next, we scheduled the test to run immediately.

Figure 11. MITRE ATT&CK Tactics and Techniques Scenarios



Source: Enterprise Strategy Group

The results of the assessment are shown in Figure 12. AttackIQ presented current and historical results in bar graph and donut charts, in various groupings, including by ATT&CK phase (execution, discovery, persistence, lateral movement, etc.), and by threat actor.

Figure 12. MITRE ATT&CK Assessment Results

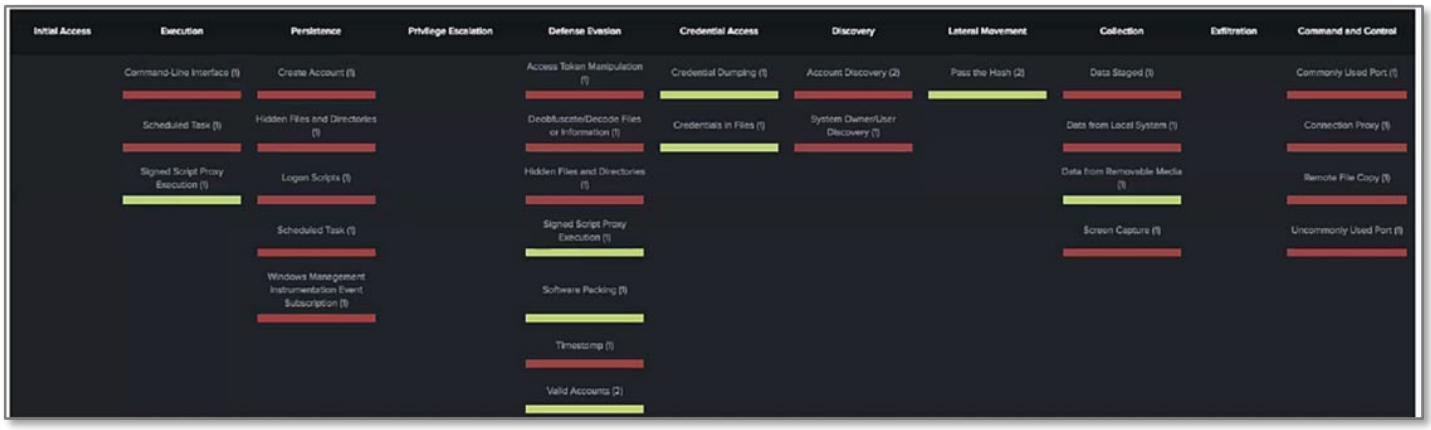
Source: Enterprise Strategy Group

Because AttackIQ maps each scenario to the MITRE ATT&CK framework, it was also able to display an ATT&CK assessment heat map, as shown in Figure 13. We found this useful in understanding the organization's exposure to adversary TTPs and prioritizing our future activities.

Maximizing ROI with ATT&CK TTP Prioritization

A national insurance company has categorized each ATT&CK TTP by the difficulty in execution for the adversary. It then prioritizes its AttackIQ assessment activities based on TTP difficulty, maximizing the ROI of improving its security toolchain effectiveness.

Figure 13. MITRE ATT&CK Heat Map and Historical Results



Source: Enterprise Strategy Group

Why This Matters

The ever-increasing volume, velocity, and variety of threats can overwhelm an organization. What threats are most important to me? How do I know if my security controls protect me from those threats?

ESG validated that AttackIQ assessments are structured to match the MITRE ATT&CK framework, a catalog and organization of real-world adversary tactics, techniques, and processes. AttackIQ users can prioritize their assessment efforts based on this easy-to-understand framework. This helps both red team and blue team engineers: blue teams can focus on securing the organization from the most applicable threat TTPs, and red teams can focus on applying the most salient TTPs in their efforts to validate blue team and security controls.

The Bigger Truth

ESG asked IT executives and professionals to select the most important 2018 IT meta-trends. Twenty one percent cited strengthening cybersecurity tools and processes, making it the most cited option in the list.[3] The traditional approach to achieving this goal is to acquire more tools to address perceived or existing weaknesses in the organization's cybersecurity strategy.

This approach is doomed to fail as it forces organizations to expend more scarce resources—time, money, effort, and, most importantly, staff—on acquiring and becoming experts in each new tool added to the cybersecurity toolbox. Recent ESG research revealed that 55% of organizations use 25 or more cybersecurity products acquired from six or more vendors.[4]

Instead of adding more tools, organizations need to first look at assessing and improving the effectiveness of their existing cybersecurity toolchain.

AttackIQ is a platform that provides such an assessment. Designed to meet the needs of organizations of any size, AttackIQ is an open platform delivering continuous validation of the cybersecurity program. Organizations can use AttackIQ to identify gaps and regressions, strengthen security posture, and exercise incident response capabilities.

During ESG's validation of AttackIQ, we were able to quickly install agents and select and run assessments of the security infrastructure. The interface proved to be very intuitive, with virtually no learning curve. Taking the perspective of a red team engineer, we used the MITRE ATT&CK matrix to select attack scenarios using TTPs typical of threat actors such as APT29. We used these scenarios to simulate attacks against the organization, and to evaluate the results.

Taking the perspective of a blue team engineer, we used the results of the attack simulation to understand the shortcomings of the current cybersecurity toolchain, and to understand and apply remediations. We could then use AttackIQ to re-run the assessment and validate that we had resolved the issues.

ESG validated that structuring assessments around the ATT&CK framework enabled organizations to use AttackIQ to prioritize assessment activities based on the most applicable and salient TTPs, and that routine assessment activities help measure improvement over time and identify regressions that can expose previously protected attack surfaces.

Before investing in yet another cybersecurity tool, organizations wanting to strengthen their security posture should prioritize investing the few minutes necessary to evaluate AttackIQ, a tool that can continuously validate the effectiveness of their existing cybersecurity toolchains, identify gaps, and help remediate issues.

[3] Source: ESG Research Report, *2019 Technology Spending Intentions*, to be published.
[4] Source: ESG Master Survey Results, *Cybersecurity Landscape: The Evolution of Enterprise-class Vendors and Platforms*, October 2018.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.

 www.esg-global.com

 contact@esg-global.com

 P. 508.482.0188