The Definitive Guide to Selecting a Continuous Security Validation Platform

ATTACKIQ

Contents

Notice 3

Executive Summary 4

The Cyberwar Escalates 6

Business Drivers for Continuous Security Validation 8

Continuous Security Validation Platforms —The Basics 11

- Deploy Agents 11
- Run Your Scenarios 12
- View Results and Improve Defenses 12
- Objective Assess Risk 12

Continuous Security Validation Platforms — Essential Requirements 13

- Utilize Attacks Developed by a Trusted and Authoritative Party 13
- A Common Lexicon 13
- Prioritize, Select, and Run Attacks From Any Step Within an Expanded Kill Chain 14
- Table 1 : MITRE ATT&CK Tactics 14
- Assemble and Execute the Cyber Kill Chain Like a Real Attacker 16
- Automation is Essential to Run Your Assessments Continuously 17
- Validate Your Existing Security Controls 17
- Validate Security Against Known Threats 18
- Validate Security Against Unknown Threats 18
- Integrate With Your Cyberdefense Ecosystem 18
- Provide Objective and Actionable Results 18
- Track Risk Trends Over Time 18
- Flexible Deployment Options for Cloud and On-Premise 19
- Support Both Isolated Testbeds and Production Environments 19
- Use an Open Systems Approach to Build Your Own Scenarios 19
- Use an Open Systems Approach to Benefit From Industry 19
- Use an Open Systems Approach to Benefit From Community 19

Cautions and Concerns 20

- Continuous Security Validation Must be Unbiased and Independent 20
- Avoid Black Box Continuous Security Validation Technologies 20

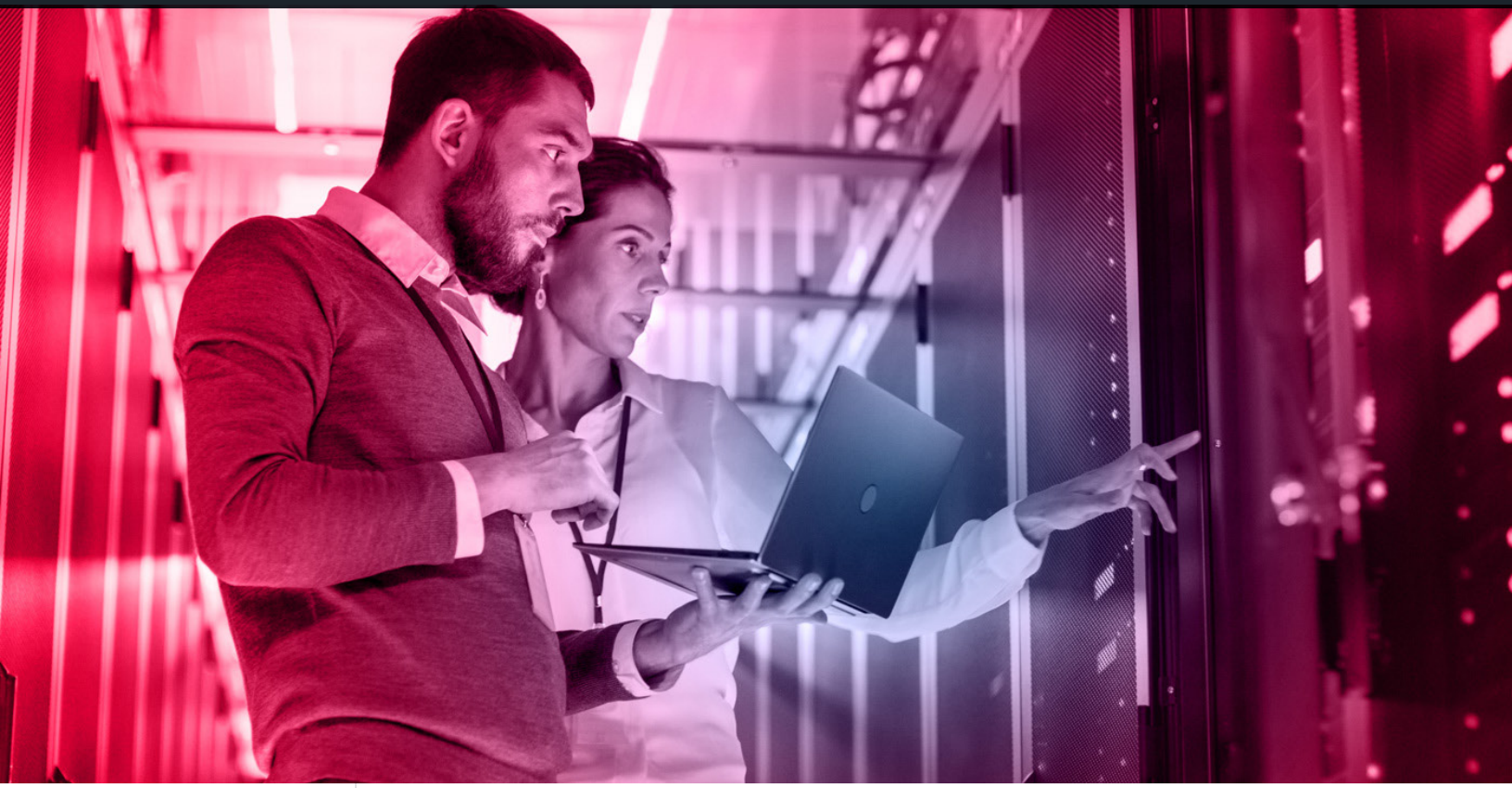
Introducing AttackIQ® 21

- AttackIQ Differentiation 22
- Table 2 : AttackIQ Differentiation Empowers the Strongest Defense 23

Expert Opinion 24

Notice

AttackIQ® publications are made available solely for general information purposes. The information contained in this publication is provided on an "as is" basis. Any additional developments or research since the date of publication will not be reflected in this report.



Executive Summary

Cyberattack risks continue to escalate as the techniques, tactics, and procedures of cyberattackers grow in depth, breadth, sophistication, and resiliency. Funded by organized crime and, in many cases, directly supported by nation states, the tools and techniques they use are evolving more rapidly than the defenses we can put in place.

We truly find ourselves in a cyberwar. As a result, the efficacy of enterprise security matters deeply. Organizations, communities, and individuals are now completely dependent on technology for every aspect of our lives. There is a global epidemic of malicious activity which is trying to capitalize on this dependency. All of this places our commercial business, government, and democracy at high risk.

Enterprise security also underperforms, leaving us all vulnerable to attacks on highly-fragile systems. Enterprise security underperforms because it is missing a critical component: a continuous improvement loop based on precise measurement and feedback.

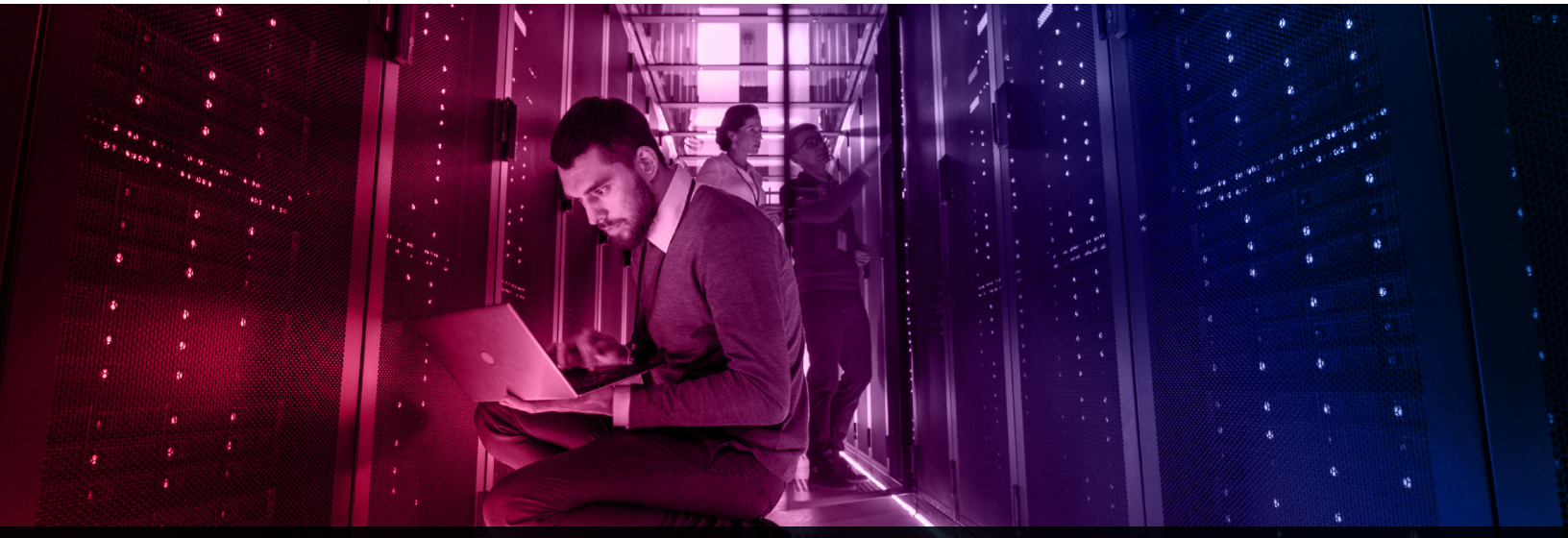
Every other complex solution to a hard problem gets better with time because you see what doesn't work and you fix it. With most cybersecurity controls, you can't see if it's not working, so it never gets better. Continuous security validation initiates this continuous improvement loop, realizing improved effectiveness from the enormous investment of time and money spent on security.

"Continuous security validation platforms are on the front line of the ongoing cyberwar. Regardless of the strategy you deploy for your enterprise, your cyberdefense will not work if the security controls do not perform as you expect. In order to meet this challenge head-on, continuous security validation platforms must provide the core capabilities that are absolutely essential for your success."

Brett Galloway, *Chief Executive Officer*, AttackIQ, Inc.

Continuous security validation platforms represent a rapidly growing and critically important toolset for information technology and security operations teams. Existing security controls can provide high value and stop attacks, but only if they are configured correctly. Continuous security validation platforms bridge the gaps within your security operations teams to automate the detection of misconfigurations, blind spots, and oversights that will likely be identified and targeted by cyberattackers.

This report will review those critical core capabilities and overview some of the basic functions essential to the successful deployment of a continuous security validation platform. We will share insight into the strong economics driving the deployment of continuous security validation platforms.



The Cyberwar Escalates

Worldwide spending on information security products and services reached more than $114 billion in 2018 and is projected to grow an additional 8.7 percent in 2019, reaching $124 billion. In addition to these expenditures, the worldwide cost of successful cyberattacks is estimated to be another $200 billion to as much as $600 billion per year. Many cyber incidents are not reported, so this range is likely conservative. This cost to industry and government is expected to rise to between $2 and $3 trillion or more by 2022, possibly reaching those levels as early as 2021. At a macro level, the average cost of a cyberattack for a single enterprise grew to $1.3 million in 2017.

"The traditional perimeter defense used in both enterprise and government has been softened and made porous by the move to mobile devices and the cloud. Attackers have gained the knowledge and skills to create and escalate new attacks against this new extended enterprise and will do so with increasing intensity into the foreseeable future.

Continuous security validation provides the only real-time assessment of organizational security controls and also objectively defines performance and identifies critical gaps that may leave an organization exposed. This then helps the enterprise justify and invest in the additional actions, security controls, and personnel necessary to remediate these gaps and reduce risk."

Carl Wright, *Chief Commercial Officer*, AttackIQ

In contrast to the massive expenses incurred by both enterprise and government, the financial leverage held by organized crime remains incredible. Organized crime spends hundreds of millions of dollars a year to retain the cyberattackers that build, deploy, and manage malware tools. That's the likely budget for the thousands of hackers that are creating the malware and generating most of the attacks we are experiencing today. For every dollar organized crime invests, they can reap hundreds to thousands of dollars in rewards. That's a massive return on investment. The incentive for organized crime to escalate the current cyberwar is at least as great, and with much lower risk, than most of the other illicit activities in which they engage.

Organized crime's investment is the part of the iceberg we can see. Rogue nation states are also part of the problem; this is the part of the iceberg we often cannot see. In terms of investment, these rogue nation states work quietly with hidden budgets and programs in the many hundreds of millions to billions of dollars to develop the tools and techniques to compromise a broad variety of enterprise and government systems. Beyond the immediate theft of funds or data exfiltration, the goal of these incursions is to create backdoors or place sentient malware into adversary systems. This is part of their strategy for asymmetric warfare - they cannot compete in a military race centered around troops, bombs, and sophisticated fighter jets, but deploying a strategy for asymmetric warfare using cyber tools is compelling, enables them to rapidly reach threat parity, and brings substantial results and leverage at the lowest cost.

Business Drivers for Continuous Security Validation

There are many strategies that an enterprise or a government agency might deploy to defend their critical information technology infrastructure assets. The result is that the average large enterprise has deployed over 75 security control tools, often with significant overlap and redundancy. For most enterprises, it is unclear how well these security controls really work and what areas and gaps require additional investment. Continuous security validation testing helps you develop a smart strategy, validates that you have a resilient security control architecture, and objectively supports your budgeting decisions.

Existing security controls are often not configured correctly or integrated well with your security ecosystem. Continuous security validation platforms identify potentially costly misconfigurations that will be identified and targeted by malicious actors. In any scenario, your cyberdefense will not work if the security controls do not perform as you expect.

Penetration team testing is highly useful, but still inadequate to test and validate the full depth and breadth of your security controls. The volume of required testing and the precision of test execution cannot be done as well by penetration testing teams as by the automation in tools such as CSV. CSV provides more consistent, accurate, and comprehensive testing and can work to support and enhance the efforts of your cybersecurity personnel and procedures.

The threat of cyberattacks remains a prime driver for information security budgets. These threats continue to grow and morph to take advantage of new opportunities. Over the past year, for example, illegal cryptocurrency mining has grown rapidly and gained prominence, even displacing ransomware in terms of impact to enterprise customers in the United States. Cryptomining malware is deployed to take over the targeted computing resources, which can then be used to mine new cryptocurrency. This is not limited to organized crime - nation states such as North Korea have worked diligently to illegally mine cryptocurrency using the computing resources of other nations, such as South Korea. North Korea's state-sponsored attackers have also been actively targeting cryptocurrency banks and related digital currency repositories. This is just one example of a new and rapidly emerging risk area that may need a specific set of security controls. This is further dependent on the risk profile of your business and your overall strategy for the deployment of your security controls.

"Continuous security validation platforms enable you to emulate an adversary and their abilities to customize attacks to fit your risk profile precisely. You can focus on security drivers relevant to your industry and test the specific controls you require to meet your cybersecurity and compliance goals. The current threat landscape and the growing requirements of compliance position continuous security validation as highly compelling for both enterprise and government."

Stephan Chenette, *Co-Founder & Chief Technology Officer*, AttackIQ, Inc.

Compliance is also a prime driver for greater investment in security controls. Today, per a recent survey, approximately 69 percent of companies see compliance as a key driver for their information security budgets. Compliance now impacts data and threat protection control technologies in many areas. It brings increased requirements for audit, logging, and reporting. Compliance may specify the use of specific technologies such as data loss prevention (DLP), encryption, and tokenization. It may also require the use of other technologies such as digital rights management (DRM, which can help protect data distributed on mobile devices), single sign-on (SSO), and two-factor authentication (2FA).

Core and center to compliance is the global trend for the rollout of data privacy legislation. Data privacy and the security controls that support it are the key factors addressing legislation such as the EU's General Data Protection Regulation (GDPR). GDPR stipulates massive, almost existential, fines for noncompliance and has cost the average corporation over $1 million for implementation alone.

California's Data Protection Act, which goes into force in 2020, along with the pending American Data Dissemination Act very recently introduced by Marco Rubio, portend an even more complex mix of data privacy compliance requirements. This new wave of compliance requirements will make the baseline of controls, policies, and procedures required within the security operations center more challenging than ever before.

The mix of control technologies used by enterprises can vary substantially and depends on the specific types of devices in their networks, the types of endpoints and applications, the mix of on-premise and cloud, the porosity of their networks, and many other factors. There is no single approach to implementing the right levels of data security and threat protection - it varies by industry, application, and compliance requirements.

Continuous Security Validation Platforms —The Basics

Continuous security validation technology allows enterprises to automatically simulate the full attack and expanded kill chain against enterprise infrastructure using software agents, virtual machines, and other means. Continuous security validation platforms deliver continuous validation of your enterprise security program. You can find the performance gaps, strengthen your security posture, and improve your incident response capabilities. Continuous security validation assesses readiness and validates that your enterprise security systems are performing as originally intended. Automation enables the platform to work autonomously and to scale to support the largest global enterprise.

Support for live production environments is essential - small changes to configurations or administration can open new vulnerabilities in your cyberdefense. This is the ever-present gap between test environments and live production environments that, undetected, will ultimately compromise the entire organization. For this reason, your live production environments must be subject to the same kill chain of emulated activities that an attacker would seek to execute.

The following are the basic capabilities you should expect of a continuous security validation platforms:

› Deploy Agents

Test point agents and automation distribute and set up your environment for emulation and testing. Test point agents are enabled to receive and execute your assessments to allow for live testing of your security controls in test systems or in your live production environments. The test point agents used should be very lightweight and inactive except during the small testing window, making it feasible to deploy agents on live systems.

› Run Your Scenarios

Scenarios are used to test your technology controls, validate your security posture, and instrument your environment. Scenarios will mimic malware and attack vectors so you can confirm that your security controls are working as expected. The most authoritative and trusted source is the **MITRE ATT&CK™ Matrix**. The MITRE ATT&CK Matrix is the premier knowledge base of adversarial tactics and techniques. It was derived by observing millions of actual attacks on enterprise and government networks. **MITRE ATT&CK** stands for **A**dversarial **T**actics, **T**echniques, and **C**ommon **K**nowledge.

The fast path to productivity is to test your existing security controls to validate they are performing as you expect. If you decide to test by threat, it is to be absolutely sure that your continuous security validation platform shows exactly where the failure happened by security control.

Search is an important component of Continuous Security Validation. For example, you can search for the relatively new threat "APT28" and immediately find a scenario and customizable template to meet your needs.

› View Results and Improve Defenses

SIEM integration is an essential requirement for your continuous security validation system.

Automation delivers real-time alerts and summary reporting to applications such as your SIEM, email, Slack®, Jira®, and other applications so you can evaluate the risk for attacks quickly. This rapid assessment of results enables you to make fast and accurate decisions on how to best address vulnerabilities and validate the effectiveness of your security controls.

Many security operations teams must manage redundant products and deal with massive volumes of alerts that don't provide meaningful information. Continuous security validation helps you determine the core security products required to secure your enterprise adequately. Continuous security validation allows your team to develop a smart strategy and to build the resilient architecture needed to make it work.

› Objectively Assess Risk

Continuous security validation platform test results add high value towards building out a complete and objective risk analysis. Risk assessment is a cornerstone of most compliance regulations and provides your board of directors, perhaps for the first time, with the objective measurement of cyberdefense effectiveness and enterprise risk. This helps in supporting budget requests, as you can objectively delineate risk areas and the exposure they bring.

Continuous Security Validation Platforms — Essential Requirements

Utilize Attacks Developed by a Trusted and Authoritative Party

AttackIQ uses the MITRE ATT&CK framework, the most authoritative, comprehensive, and complete set of up-to-date attack techniques and supporting tactics in the world. MITRE ATT&CK is a globally-accessible knowledge base of adversary tactics and techniques based on real-world data. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

MITRE's stature in the cyber community and the independence of its intellectual property in the ATT&CK matrix make it the ideal platform from which security operations management, executive staff, and the board of directors can objectively evaluate and measure cybersecurity controls' performance, risk, and capability.

A Common Lexicon

MITRE ATT&CK has brought a well-matured taxonomy of the tactics and techniques that may be leveraged by any prospective attacker. This provides, for the first time, a common lexicon that enables business stakeholders, cyber defenders, and vendors to clearly communicate on the exact nature of a threat and the objective assessment of the cyberdefense plan that can defeat it. This common lexicon brings a universal language that can be used to describe the procedures of an attacker or attack tools and exactly the techniques which they deploy. The precise lexicon of MITRE ATT&CK enables a more precise assessment of threats and a faster, better-targeted response.

Prioritize, Select, and Run Attacks From Any Step Within an Expanded Kill Chain

MITRE ATT&CK provides the largest depth and breadth of attack scenarios, suggested mitigation techniques, detection procedures, and other important technical information. MITRE has expanded the kill chain to include the widest variety of tactics, which are then supported by detailed techniques. This organized approach enables you to methodically select the attack you need to validate your security controls and to understand the gaps so you can rationally expand your security controls set.

Table 1 : MITRE ATT&CK Tactics

Name	Description
Initial Access	The initial access tactic represents the vectors adversaries use to gain an initial foothold within a network.
Execution	The execution tactic represents techniques that result in the execution of adversary-controlled code on a local or remote system. This tactic is often used in conjunction with initial access as the means of executing code once access is obtained, as well as with lateral movement to expand access to remote systems on a network.
Persistence	Persistence is any access, action, or configuration change to a system that gives an adversary a persistent presence on that system. Adversaries will often need to maintain access to systems through interruptions such as system restarts, loss of credentials, or other failures that would require a remote access tool to restart or alternate backdoor for them to regain access.
Privilege Escalation	Privilege escalation is the result of actions that allows an adversary to obtain a higher level of permissions on a system or network. Certain tools or actions that require a higher level of privilege to work are often necessary at many points throughout an operation. Adversaries can enter a system with unprivileged access and then take advantage of system weaknesses to obtain local administrator or SYSTEM/root level privileges. A user account with administrator-like access can also be used. User accounts with permissions to access specific systems or perform specific functions necessary for adversaries to achieve their objective may also be considered an escalation of privilege.
Defense Evasion	Defense evasion consists of techniques an adversary may use to evade detection or other defenses. Sometimes these actions are the same as or variations of techniques in other categories that have the added benefit of subverting a particular defense or mitigation. Defense evasion may be considered a set of attributes the adversary applies to all other phases of the operation.

Credential Access	Credential access represents techniques resulting in access to or control over system, domain, or service credentials that are used within an enterprise environment. Adversaries will likely attempt to obtain legitimate credentials from user or administrator accounts (local system administrator or domain users with administrator access) to use within the network. This allows the adversary to assume the identity of the account with all of that account's permissions on the system and network, and it makes it harder for defenders to detect the adversary. With sufficient access within a network, an adversary can create accounts for later use within the environment.
Discovery	Discovery consists of techniques that allow the adversary to gain knowledge about the system and internal network. When adversaries gain access to a new system, they must orient themselves to what they now have control of and what benefits operating from that system give to their current objective or overall goals during the intrusion. The operating system provides many native tools that aid in this post-compromise information-gathering phase.
Lateral Movement	Lateral movement consists of techniques that enable an adversary to access and control remote systems on a network and could, but does not necessarily, include execution of tools on remote systems. The lateral movement techniques could allow an adversary to gather information from a system without needing additional tools, such as a remote access tool.
Collection	Collection consists of techniques used to identify and gather information, such as sensitive files, from a target network prior to exfiltration. This category also covers locations on a system or network where the adversary may look for information to exfiltrate.
Exfiltration	Exfiltration refers to techniques and attributes that result or aid in the adversary removing files and information from a target network. This category also covers locations on a system or network where the adversary may look for information to exfiltrate.
Command and Control	The command and control tactic represents how adversaries communicate with systems under their control within a target network. There are many ways an adversary can establish command and control with various levels of covertness, depending on system configuration and network topology. Due to the wide degree of variation available to the adversary at the network level, only the most common factors were used to describe the differences in command and control. There are still a great many specific techniques within the documented methods, largely due to the ease with which one can define new protocols and use existing, legitimate protocols and network services for communication.

Use the Tactics, Techniques, and Procedures of a Real Attacker

It is critical to take on the mindset of the attacker. Imagine that one or more cyberattackers are working full time, with no other goal in mind than to break, enter, and compromise your intellectual property, damaging or destroying your information technology infrastructure. Sophisticated attackers are not set back by a few counter defenses - instead, they continue to probe and try to work through these defenses. Your continuous security validation platform must allow you to similarly change the plan, giving you every opportunity to probe and find vulnerabilities. Your continuous security validation platform must provide the flexibility and capability to allow your red team to structure and execute these tests to meet the likely threats in your environment.

"In order for companies to improve their security strategy, they need to realize that controls can fail. Controls fail over time, and the worst outcome is that there is a breach because they had a control in place that should have detected the threat. By continuously validating your security controls, you minimize the risk of misconfiguration, administration error, or some other problem that opens up your entire enterprise to breach."

Stephan Chenette, *Co-Founder & Chief Technology Officer*, AttackIQ, Inc.

Assemble and Execute the Cyber Kill Chain Like a Real Attacker

Most important is the need to assemble the events that constitute the likely kill chain variations your organization may face and to understand how your security controls perform from the assumed point-of-breach and forward. There are many goals you can now set and measure. These include identifying and stopping the attacker before they can exfiltrate data. Stopping attacker breakout is job one - measuring your organization's ability to detect or block breakout before breach is of paramount importance. Security investments must be evaluated as an integrated defense-in-depth stack - this is necessary to detect and stop malicious adversary breakout and successful exfiltration.

When analyzing performance with modeled kill chains, breach is not the endpoint. Detection of breach is the beginning of your successful defense. Your ability to test and manage the unfolding kill chain variations successfully will be the difference between success in stopping the attacker and suffering a catastrophic data breach, operational damage to IT systems, or much worse.

Automation is Essential to Run Your Assessments Continuously

Automation gives your red team the ability to run exercises and validation scenarios on your enterprise controls and incident response workflows. Your red team is able to identify how each individual security control responds to the many thousands of possible common attack scenarios. The red team will be able to generate comprehensive reporting on each test result and clearly communicate the impact of the threat to management.

Automation gives your blue team the ability to continuously validate that security controls are configured properly and that they can meet (and defeat) the red team attacks as well as deter actual cyberattackers. Automation delivers daily reports, such that security management can rapidly and easily identify critical problems for remediation. These regular reports also help document how existing security investments are achieving the desired return on investment (ROI).

Validate Your Existing Security Controls

Start simply by validating your existing security controls. As mentioned earlier in this report, the typical enterprise has an average of 75 security controls per enterprise, so some redundancy and inefficiency exist. A continuous security validation system provides objective and actionable data about the state of security control technology based upon the way they are configured and deployed. By starting with your existing security controls, you will understand the state of your current cyberdefenses and the efficacy of the components as they are configured, enabling you to quickly identify any configuration errors.

With Continuous Security Validation, you can comprehensively validate your security controls. You can rapidly determine if the security controls are configured to maximize performance and highlight gaps that require immediate remediation.

Validate Security Against Known Threats

You should be able to rapidly deploy and validate protection against the latest attacks that target your enterprise or industry. This enables you to validate protections for these new attacks and to verify that you have set up your security controls so that they meet (and defeat) these threats per the vendor guidelines.

If you test by threat, the most important thing is to be absolutely sure that your continuous security validation platform shows exactly where the failure happened by security control. This should be front and center in your reports.

Validate Security Against Unknown Threats

Your red team can customize and build new attack scenarios that allow you to test your controls against variations in tactics and movement that a determined attacker may use as they continue to move against your defenses.

Integrate With Your Cyberdefense Ecosystem

An integrated cyberdefense ecosystem builds out the layers of a competent defense-in-depth strategy. During testing, alerts will flow through control security technologies to your SIEM so that they can be reviewed and triaged. This not only tests the integrity of your security controls as configured but also helps your blue team perfect their response.

Integrate with major vendors such as ThreatStop, CarbonBlack, Phantom, Endgame, Splunk, CrowdStrike, and many others. If you have special integration needs, ask your continuous security validation vendor and they should accommodate your requests.

Provide Objective and Actionable Results

Security operations management, chief information security officers, chief information officers, compliance and governance teams, executive staff, and boards of directors all ask the same questions. How do our security controls work to protect against the threats we expect? Are they being configured optimally? Where do we need new security controls to better protect against threats? How are we doing over time - are we improving? These are exactly the questions that continuous security validation will answer.

Track Risk Trends Over Time

It is critical to provide a real-time assessment of your security controls that is supported by objective data reporting. Once you have established baseline reporting of the objective data with respect to your controls' performance, you can show trends over time. These trends and the associated measurement of control performance provide an important dashboard to department operations, which can be used to assess performance, adjust budgets, and calibrate risk.

Flexible Deployment Options for Cloud and On-Premise

Don't get locked into a software architecture that cannot go where you do. Plans and business direction can change. Mergers and acquisitions happen. Your continuous security validation platform must have the flexibility to be cloud and on-premise deployable. Your management console should either sit in the cloud or be installed locally on-premise.

Support Both Isolated Testbeds and Production Environments

Tests that successfully validate control performance in an isolated testbed environment often fail in a production environment. Why? Because the configuration and administration often introduce errors that open up vulnerabilities. Many of the recent data breaches in IaaS clouds have been caused by misconfigurations in the production environments. Chinese hackers, identified as the Rocke Group, have deployed malware that is engineered to gain administrator access on a given cloud instance. Once this administrator access is obtained, the malware is then able to uninstall the software just as any credentialed administrator.

Use an Open Systems Approach to Build Your Own Scenarios

Basic scenarios and playbooks provide the essentials for testing your security controls. Your environment is always unique, and open system approaches should allow you to customize any existing scenarios or to create new ones. You can see all of the code and your team will be able to validate the control defenses necessary for your enterprise or agency. This is a "white box" approach - completely open, shareable, and extensible. This is in sharp contrast to a closed "black box" continuous security validation platform.

Use an Open Systems Approach to Benefit From Industry

The composition of critical information technology and communications infrastructure varies by industry. For example, in the health care industry, networks contain a high number of internet of things (IoT) devices and medical devices. These require special controls and network segmentation for protection, and, when infected by malware, they are often extremely difficult to remediate. Security validations can be adjusted to meet the specific needs of health care networks and to accommodate these unique vulnerabilities.

Use an Open Systems Approach to Benefit From Community

The composition of critical information technology and communications infrastructure varies by industry. An open systems approach can provide shared scenario templates that can save you time, reduce your costs, help you better target vulnerabilities and threats, and improve your return on investment.

Cautions and Concerns

Continuous Security Validation Must be Unbiased and Independent

Continuous Security Validation technologies are the decision support systems for the tactical, operational, and strategic teams that support and defend your institution. These systems must remain agnostic and unbiased in their reporting.

In order to achieve this goal, you must verify that your intended CSV technology sets are not owned or directed by an organization that produces the very technology that must be measured and validated. This is essential to deliver an independent, objective, and fair assessment of your defenses.

Avoid Black Box Continuous Security Validation Technologies

Be cautious and avoid "black box" continuous security validation technologies. What is a black box technology? As mentioned earlier, a black box technology is a software system and technology which is closed. Black box technologies provide no visibility into internal operations and no access to these mechanisms. Black Box technologies are not open, do not provide application program interfaces (API) for customers or partners, do not allow sharing or development of customizations, and do not allow introspection into the operation of any simulation or results. They substantially reduce the return on investment for your continuous security validation platform, slow down implementation, and don't allow you to evaluate the many possible types of emerging threats

Introducing AttackIQ®

AttackIQ provides the industry's premier independent continuous security validation platform. AttackIQ requires minimal setup time and few resources to implement. This rapid time-to-value means you're able to start seeing results almost immediately. Once you've deployed test point agents, you'll be able to set automated scenarios to run continuously and launch targeted scenarios on demand. This gives you real-time insight into how your products, people, and processes respond to known and emerging threats.

With AttackIQ, you can download shared scenarios from the community and then customize them. You can add or manipulate data you wish to try to exfiltrate and can specify exactly how you want the structure of a test that seeks to obtain the data across the specified boundary, while deploying different test points to access security controls that would block this exfiltration attempt.

AttackIQ uses a distributed client-server architecture and can support your deployment in test and production environments, both on-premises and in the cloud. AttackIQ deploys test point agents into your test environment to initiate simulated attacks. It provides downloadable executables that work with Microsoft Windows XP® Embedded to current OS versions of Windows, Linux®, and Mac® and supports a full range of endpoints, servers, mobile devices, and more. AttackIQ is tightly integrated with a scenario library based upon the MITRE ATT&CK framework.

The MITRE ATT&CK framework acts as a playbook for the cybersecurity industry, offering a vast knowledge base that allows organizations to clearly see the steps of complex attacks and what

procedures are linked to a specific adversary behavior. This cybersecurity lexicon levels the playing field for security teams. It allows cybersecurity analysts, penetration testers, and threat intelligence teams, as well as red, blue, and purple teams, to see specific trends between attacks and adversary styles. It allows security executives to think systematically about the adversary environment in which they must establish a security program and to determine if every security dollar spent is effective in preventing or detecting all known attacker behaviors. With the broadest implementation of the MITRE ATT&CK framework, AttackIQ provides enterprises of all sizes the ability to automate the assessment of their cyber readiness.

AttackIQ is also a completely open platform. AttackIQ is supported by an active community of hundreds of security teams, including some of the largest banks and health care firms. Customers in the AttackIQ community can customize, share, and build scenarios. Vendors can build tests to validate their security controls and then share them with the user community.

AttackIQ Differentiation

AttackIQ empowers the strongest defense by enabling you to proactively identify security control failures before the attacker does. AttackIQ allows you to test your environment on the potential impact of the newest attacks. You can continuously test, probe, and stress your cyberdefenses to build the resiliency and confidence you need to know your security controls are working correctly.

AttackIQ continuously facilitates and enhances the workflow for your entire decision support system. Each operational tier derives immediate value from integrating AttackIQ into existing processes.

Table 2 : AttackIQ Differentiation Empowers the Strongest Defense

Open Platform	› White Box Open Technology › Customizable and Extensible w/API › Community and Industry Assets › Vendor Test Scenarios › Visibility to Platform Operation at all Times
Flexible Architecture	› Cloud or On-Premise › Validate and Test in Test Environments and in Production Environments › Management Console Anywhere › Alerts Integrated With Your SIEM › Other Special Integrations Available or Delivered Upon Request
Flexible Approach By Controls or By Threat	› Validate Security Controls by Technology › Simulate Attacks Using Threats to Immediately Pinpoint Specific Failures in Identified Security Controls › Support for Zero Day threats - anything a human penetration tester can develop can be simulated by AttackIQ
Depth & Breadth of Testing Scenarios	› MITRE ATT&CK Matrix › Authoritative › Trusted › Complete › Extensible › Customizable

Expert Opinion

Gartner

"Security and risk management leaders who are charged with showing that their security programs are effective and a good use of corporate funds should consider using security validation services such as those offered by AttackIQ."

Gartner® Cool Vendors
Monitoring and Management of Threats to Applications and Data
Gartner 2017

CSO MAGAZINE

"Over the course of testing with AttackIQ FireDrill, it became obvious why a testing tool like this that is designed to evaluate other tools can be so helpful in defending modern networks. In one case, we discovered that an antivirus program was blocking all attacks against endpoints, making a secondary defense that was also deployed on them largely unnecessary. In another scenario, an advanced cybersecurity program that should have been blocking attacks leveled at core assets was sometimes failing. The reason was that it had never been taken out of discovery mode on assets that were getting compromised, so it was monitoring the attacks but not actually preventing them. In still another scenario, multiple cybersecurity programs were interfering with one another, leading to decreased efficiency and openings for attackers to slip through. The list of problems and the reasons behind them were extremely interesting and would have been difficult or impossible to discover without the dedicated FireDrill tool.

Not only will FireDrill identify weak spots or flaws in existing defenses, but it will also find areas where misconfigurations or installation mistakes are preventing good cybersecurity tools from operating properly. In this era of incredibly complex networking where everything is a unique environment, FireDrill can help ensure that the best defenses are in place and that they are operating at maximum efficiency."

John Breeden II, *Product Evaluation*
Chief Security Officer Magazine
January 8, 2019
https://www.csoonline.com/article/3331173/network-security/review-attackiq-firedrill-watches-the-watchers.html?upd=1547943355306

"In one scenario, FireDrill [AttackIQ] deployed five agents on five different ATM machines, performing very simple windows harvesting. Of the five ATMs, four were safe, as security measures detected the attack and blocked them. But on one machine, the testing agent was able to harvest credentials. Then, making a lateral movement – one of the 11 tactics identified by ATT&CK – the attacking agent was able to harvest credentials from 300 other ATMs. FireDrill [AttackIQ] demonstrated this situation was possible – crucial data for the client."

Dan Cure, *Product Review*
SCMagazine
October 1, 2018

ATTACKIQ

CONTACT ATTACKIQ

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

OFFICES

New York
Washington, DC
Atlanta, Georgia
Chicago, Illinois
Dallas, Texas
San Francisco, CA
European Operations
Barcelona, Spain

For additional information please refer to our website
http://www.attackiq.com

About AttackIQ

AttackIQ, a leader in the emerging market of continuous security validation, built the industry's first platform that enables red and blue teams to test and measure the effectiveness of their security controls and staff. An open platform, AttackIQ™ supports the MITRE ATT&CK Matrix, a curated knowledge base and model for cyber adversary behavior used for planning security improvements and verifying that defenses work as expected. AttackIQ's platform is trusted by leading companies around the world. For more information visit **www.attackiq.com**. Follow AttackIQ on Twitter, Facebook, LinkedIn, and YouTube.