ATTACKIQ®

TAG CYBER

Article

Using Automated Attack Emulation for Continuous Cybersecurity Control Validation

Jonathan Reiber,
AttackIQ and UC Berkeley Center for Long-Term Cybersecurity

Carl Wright,
AttackIQ

Edward Amoroso,
TAG Cyber and New York University

To properly protect data and assets, organizations must validate the effectiveness of deployed security controls. Since both offensive and defensive cyber actions are increasingly automated, this control validation process must be both proactive and continuous. This report illustrates these functional requirements in the context of adversary attack emulation tools.

Introduction

Enterprise security teams benefit from the collection and analysis of data to determine cyber risk posture. When performed properly, these tasks reduce uncertainty about situational security status by showing how posture aligns with a defined metric. Data collection and analysis provide visibility into how the organization is managing risk. World-class security teams rely on such tasks for their day-to-day work.

An important aspect of the collection and analysis process is the degree to which tasks are continuous. All too often, quantitative data is extracted or derived based on a point-in-time status, which results in information that begins to grow stale immediately after collection. Security tests for annual audits, for example, will often result in measured data that becomes gradually out-of-date until the next scheduled audit.

For this reason, security experts have recently come to recognize the importance of continuous, automated measurement processes for threat and risk management. The idea is to establish an on-going means for obtaining useful information with minimal gaps between successive measurement tasks. This continuous, automated method is particularly important for critical asset protection, where a stale understanding of security status can lead to significant consequences.

Collection and analysis are not done, of course, only to obtain quantitative data — but rather to serve as the basis for the critical business objective of control validation. Rather than use subjective observation or judgment to assess protection controls, the best enterprise security teams use measurements, metrics, and data as the basis for validation, and this requires use of automation to ensure comprehensive coverage.

In this paper, we outline how continuous automated security control validation can drive improved management of cybersecurity risk. This is shown to be best accomplished in modern commercial platforms by running carefully planned adversary attack emulations across security controls to demonstrate their proper operation — or in some cases, to expose degraded security operations that require management attention.

Collecting and Analyzing Security Data

The decision about what security data is available for collection from an enterprise is often determined by the commercial tools that have been installed into the network. A security information and event management (SIEM) platform, for instance, will include connectors to specific endpoints, servers, applications, and other systems — and will come with embedded measurements and other analytic support.

While this generally provides an excellent base of quantitative data, it is also helpful to separately and independently determine the types of measurements that will be most appropriate to reduce risk in the local enterprise. Furthermore, it is important to measure and validate the effectiveness of controls that are in place to enforce policies. The result is a means for validating the effectiveness of systems that validate policy enforcement (see Figure 1).

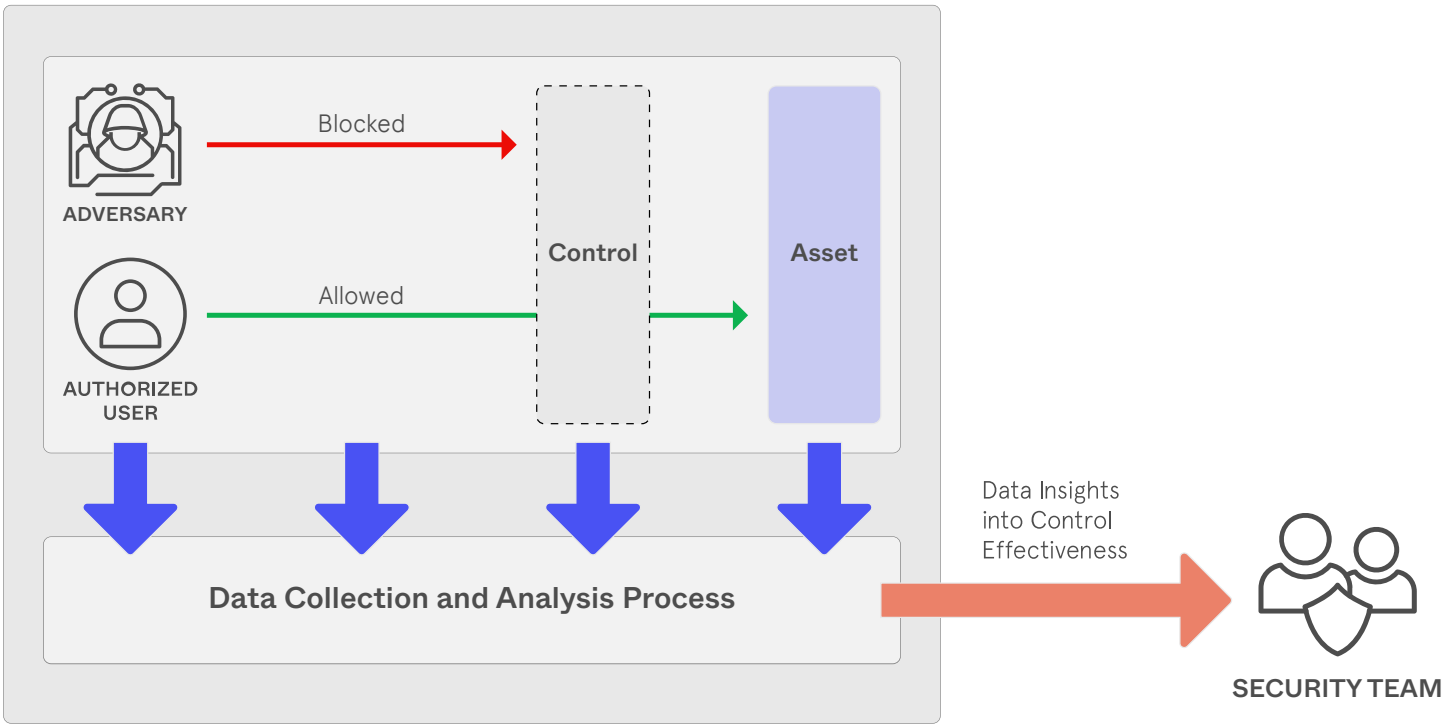

Figure 1. Validation Process for Security Controls

Continuous Security

A major challenge for any attempt to determine control effectiveness is the frequency with which this process is done. Most existing validation methods are designed to capture point-in-time data about some property of interest such as patching levels or existence of known policy exceptions. These quantitative snapshots are certainly accurate when taken, but they begin to degrade once the analysis has been initiated.

For this reason, the security industry has begun to rely on validation methods that provide on-going data about control effectiveness. The result is improved visibility into real-time security posture, as well as the ability to observe offensive activity more clearly (see Figure 2) and over time.

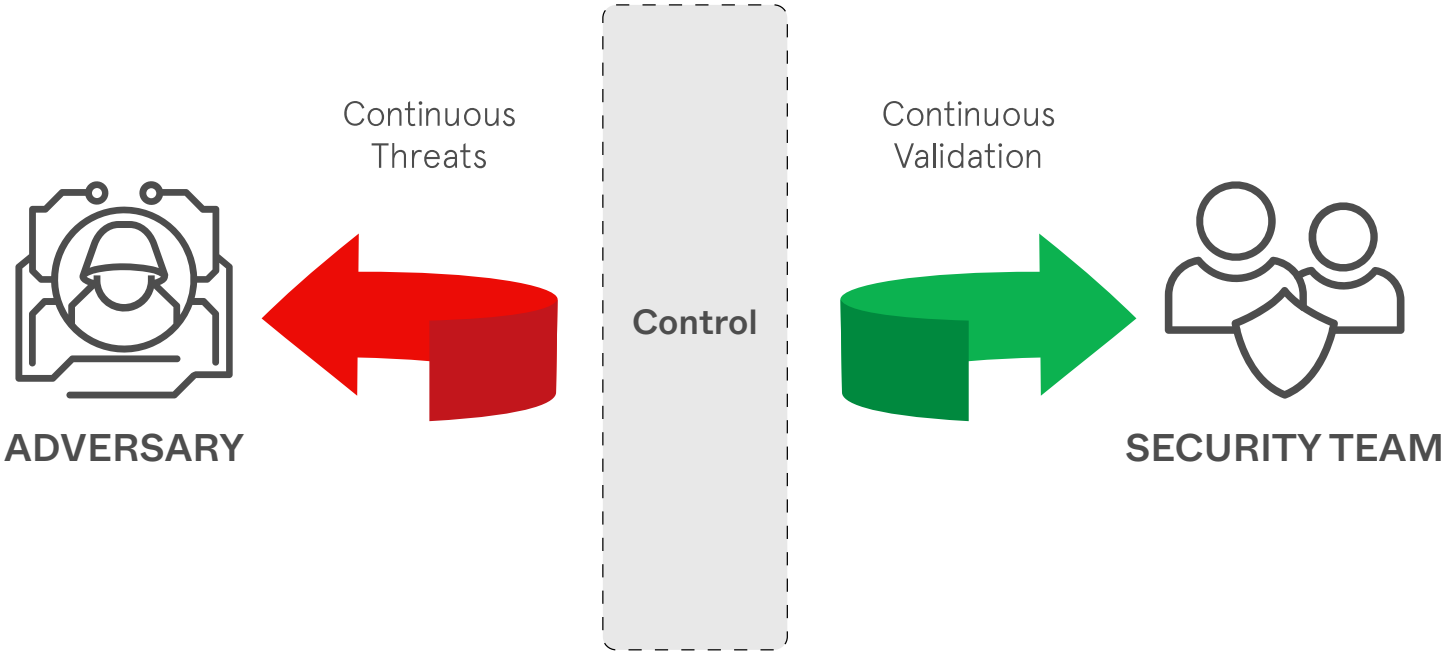

Figure 2. Continuous Control Validation Process

Attack Emulation

An effective means for validating the on-going effectiveness of security controls involves the realistic emulation of attacks. Such a process offers a controlled means for testing whether controls have been configured correctly, whether they are sharing data and output sufficiently, and whether the required protection capability is functioning as expected. The approach offers insights to security teams about malicious adversary activity.

As one would expect, the degree to which such testing is automated influences the continuous aspect of the process. Red team testing, for example, can be done using human experts, but, except for the more extraordinary situations (e.g., military environments), such initiatives cannot be performed in an on-going manner because the human expertise can only be provided on a project-by-project basis.

Instead, modern organizations must rely on automated attack emulation platforms that provide a suitable balance between continuous testing, detailed insights on potential gaps, and support for automation to keep up with on-going threats. Furthermore, automation allows for use of complete attack taxonomies such as MITRE ATT&CK® to ensure completeness of threat coverage (see Figure 3).

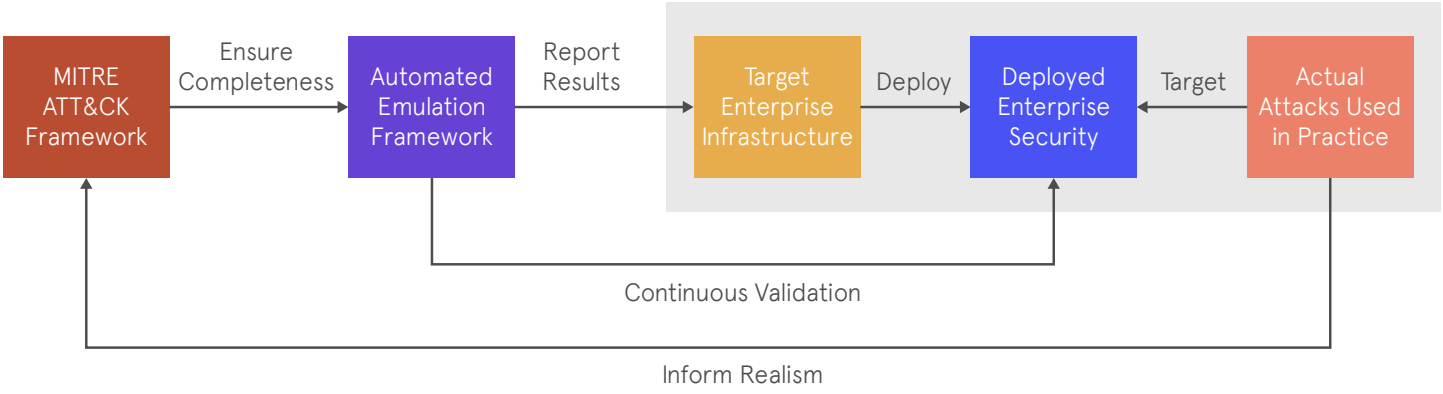

Figure 3. Ecosystem for Automated Attack Emulation Testing

It should be obvious that continuous security assessments are preferable to point-in-time snapshots. Transitioning an enterprise toward this objective, however, will not always be a straightforward process. In most cases, security teams will have to create a methodology for optimizing risk posture assessments through the deployment of continuous security platforms targeting the desired control measurements.

Commercial Platforms

Automated platforms are available today from vendors to support this continuous cybersecurity validation process. These commercial solutions range in their respective emphasis, so buyers should take the time to understand the differences in design, deployment, support, analytics, reporting, and coverage. The availability of such choices is good, because it allows enterprise teams to select a platform that best matches their needs.

For any platform, however, a key requirement is to provide insight into control effectiveness. This is often done by identifying which exploits are successful at causing problems in deployed controls. The AttackIQ platform, for example (see Figure 4), was used to review anonymous data reported by almost one hundred customers, resulting in identification of process hollowing, account discovery using WMI, and pass-the-ticket as top successful tactics that evade organizations' security controls.

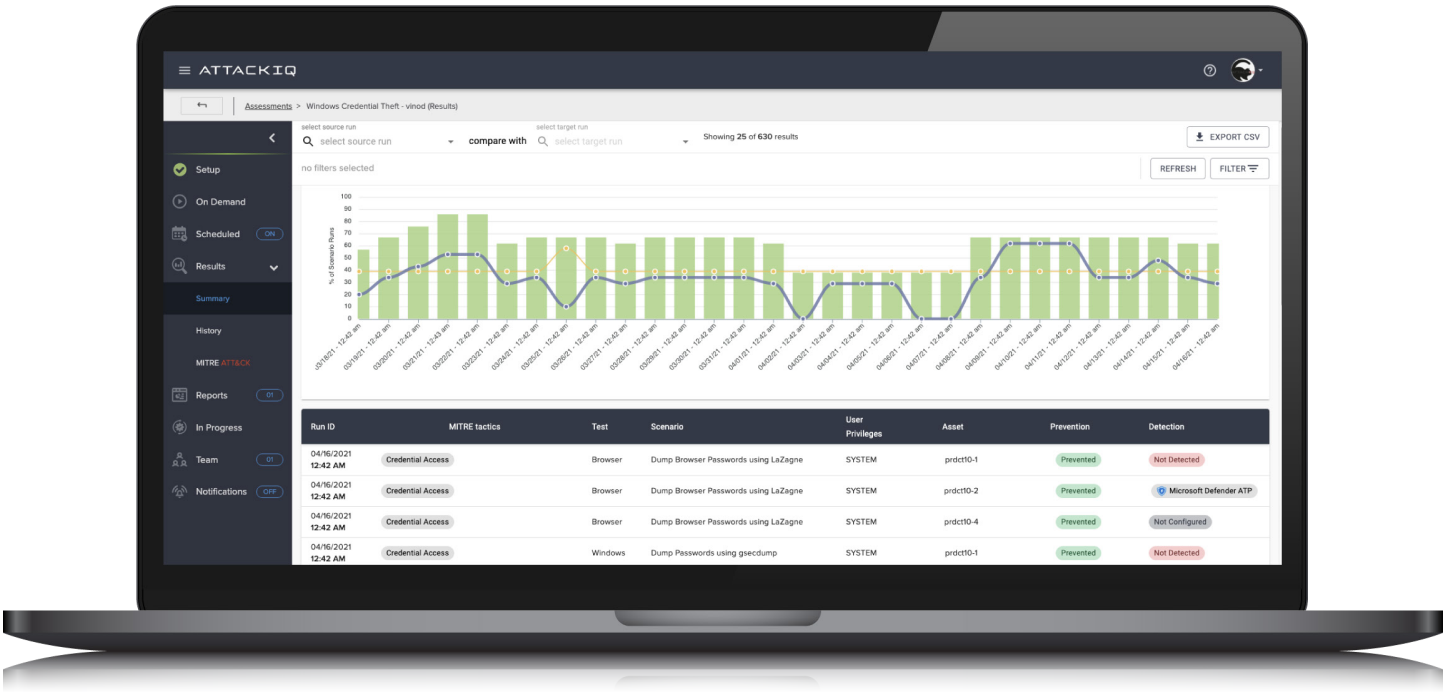

Figure 4. AttackIQ User Interface

Action Plan for Enterprise

Enterprise teams are advised to begin the process of installing and supporting an automated platform to continuously validate the effectiveness of deployed security controls. This should be done through partnership with a world-class commercial vendor. To maximize the impact of such deployment and partnership, an enterprise should also consider developing the following complementary initiatives:

- ☑ Generating key performance indicators (KPIs) to assess the overall security program and determine necessary divestments and investments.
- ☑ Establishing cybersecurity risk reduction during mergers and acquisitions through comprehensive program assessments.
- ☑ Evaluating control framework effectiveness (e.g., NIST 800-53) to identify which control framework is most appropriate for the infrastructure.
- ☑ Reducing an organization's compliance and regulatory burden by mapping compliance controls and measuring compliance effectiveness.
- ☑ Assessing the effectiveness of machine learning and artificial-intelligence-enabled defense capabilities to improve an organization's security posture.

About the Authors

Jonathan Reiber is Senior Director for Cybersecurity Strategy and Policy at AttackIQ and former Chief Strategy Officer for Cyber Policy in the Office of the Secretary of Defense. He is the author of A Public, Private War (Berkeley Center for Long-Term Cybersecurity) and his commentary has been featured in TIME Magazine, The Atlantic Monthly, and DefenseOne, among others.

Carl Wright is Chief Commercial Officer at AttackIQ and former Chief Information Security Officer for the U.S. Marine Corps. Prior to joining AttackIQ, he held executive operational roles at Securify, Decru, and Kidaro, where he contributed to rapid growth and subsequent acquisition by Microsoft, Network Appliance, and Secure Computing.

Edward Amoroso is Chief Executive Officer of TAG Cyber, a research and advisory company headquartered between New York and Boston. He is also Research Professor at the NYU Center for Cyber Security (CCS), where he leads on-going studies in threat sentiment. Ed spent three decades at AT&T where he helped to develop the cybersecurity discipline at Bell Labs.

ATTACKIQ®

U.S. Headquarters
171 Main Street Suite 656
Los Altos, CA 94022
+1 (888) 588-9116
info@attackiq.com

About AttackIQ

AttackIQ, the leading independent vendor of breach and attack simulation solutions, built the industry's first Security Optimization Platform for continuous security control validation and improving security program effectiveness and efficiency. AttackIQ is trusted by leading organizations worldwide to identify security improvements and verify that cyberdefenses work as expected, aligned with the MITRE ATT&CK framework. The Company is committed to giving back to the cybersecurity community through its free AttackIQ Academy, open Preactive Security Exchange, and partnership with MITRE Engenuity's Center for Threat Informed Defense.

For more information visit www.attackiq.com. Follow AttackIQ on Twitter, Facebook, LinkedIn, and YouTube.