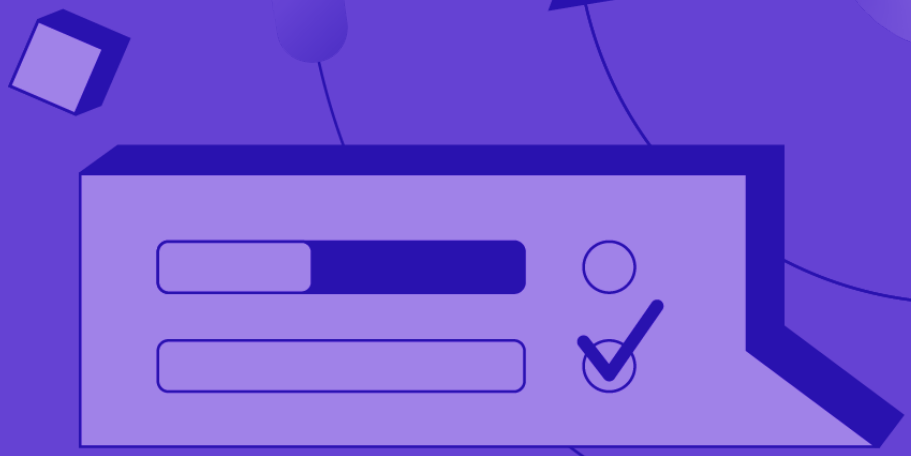
ATTACKIQ®

LogRhythm™

Solution Brief

AttackIQ® and LogRhythm® Integration Enables Routine Continuous Testing and Validation of SIEM Effectiveness



AttackIQ® and LogRhythm® Integration Enables Routine Continuous Testing and Validation of SIEM Effectiveness

Cybersecurity professionals rely on the effectiveness of security information and event management (SIEM) solutions to alert them to potential threats and anomalies in their networks. While SIEMs are an important part of a security strategy, organizations may require additional services.

That is why SIEM provider LogRhythm teamed up with security optimization platform provider AttackIQ.

As a SIEM, LogRhythm is a repository of information from security control systems such as firewalls, endpoint detection and response (EDR) solutions, intrusion detection systems and intrusion prevention systems (IDS and IPS), and data loss prevention (DLP) software. LogRhythm collects, structures, and processes this information, and presents it in a format that security analysts can search for signs of malicious events.

The LogRhythm NextGen SIEM Platform provides holistic visibility across users' environments, enabling effective and efficient incident detection, investigation, and response. The LogRhythm XDR Stack is a comprehensive set of capabilities that make up the NextGen SIEM Platform. The platform enables SOC teams to add components and increase their security sophistication as their needs evolve. With the LogRhythm XDR Stack, IT can monitor and hunt for threats, investigate threats, and respond to incidents from a single platform.

With such capabilities, security analysts are well positioned to detect and respond to malicious behavior detected anywhere on the network. However, these capabilities will work properly only if:

- LogRhythm is configured optimally for data import and alerting, and
- its communication with the security control solutions is also operational.

However, Analysts cannot address events that they never see.

What AttackIQ Testing Brings to LogRhythm Customers

AttackIQ is a leader in the emerging market of continuous security validation and security optimization using the MITRE ATT&CK framework. The AttackIQ Security Optimization Platform automates both red-team attacks—attempted breaches of defenses with the goal of finding gaps—and blue-team activities designed to defend against those emulated attacks by looking for events and alerts from the security controls. The AttackIQ Security Optimization Platform combines both approaches into "purple-team" testing, with automation that reduces the manual workload for human analysts. As a result, it enables organizations to efficiently and effectively validate that their controls are functioning properly.

LogRhythm and AttackIQ engineers collaborated to develop tight integration between the two solutions. Specifically, the AttackIQ Security Optimization Platform can now query LogRhythm to assess whether emulated attacks show up in the SIEM as properly formatted events.

What AttackIQ Testing Brings to LogRhythm Customers (cont.)

For example, the instance of the AttackIQ Security Optimization Platform that is installed on a customer's network might attempt to perform a command-and-control (C&C) address retrieval and contact a server outside the network (the red-teaming portion of the testing). In an actual attack, the goal would be to exfiltrate customer data. However, in this case, the goal is to trigger an appropriate response from security solutions on the customer's network.

This is illustrated in scenario #2 in Figure 1. The emulated security event should be logged by the company's firewall and then routed to the SIEM. If the firewall integrates with AttackIQ, then after initiating the event, the AttackIQ Security Optimization Platform will query the firewall to determine whether it detected the C&C action and responded appropriately. Then the AttackIQ tool will query the LogRhythm SIEM to determine whether the forwarding mechanisms are working and whether the event reached the SIEM.

Automated testing by the AttackIQ platform will also validate whether the SIEM alerting capability within LogRhythm is meeting expectations.

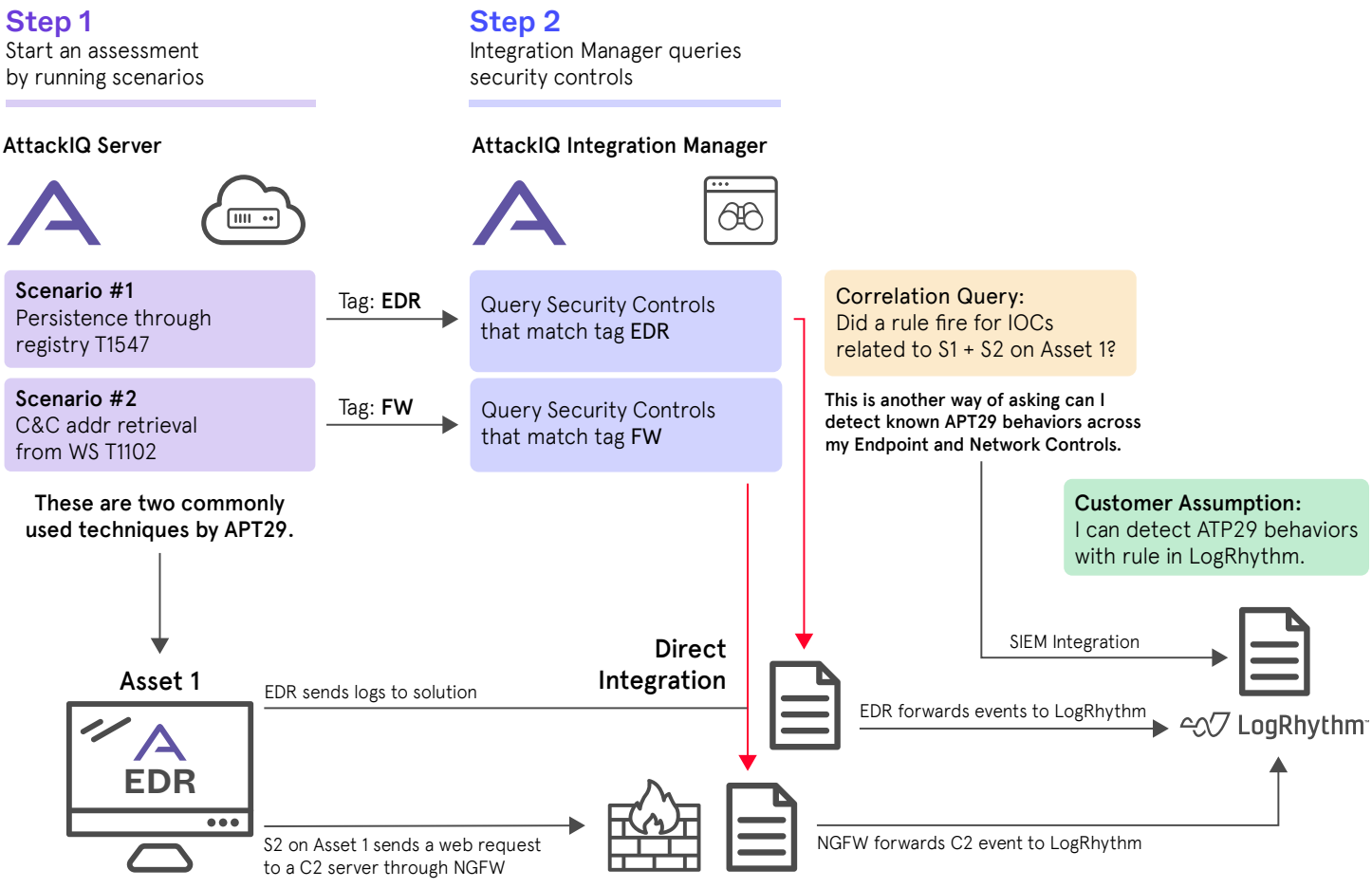


Figure 1: Process for AttackIQ testing of LogRhythm security controls.

Evidence of Security Measures' Effectiveness

For users of LogRhythm, the benefits of this integration are clear: By testing their SIEM, they can make sure this critical solution is meeting their needs. They can ensure that security events are being logged and properly imported for analyst review. Thus, security teams can have confidence—built on evidence—that if an attacker is able to enter the network, the security solutions in place will perform as advertised. Such testing also gives security teams practical information they can use to measure, monitor, and modify their existing security investments from a threat-informed perspective.

A data breach is the hard way for a company to learn that its security controls are not effective. Automated purple-team testing of a SIEM is much less painful, for the corporate executives, the communications staff, and the cybersecurity pros.

About LogRhythm

LogRhythm empowers more than 4,000 customers across the globe to measurably mature their security operations program. LogRhythm's award-winning SIEM Platform delivers comprehensive security analytics; user and entity behavior analytics (UEBA); network detection and response (NDR); and security orchestration, automation, and response (SOAR) within a single, integrated platform for rapid detection, response, and neutralization of threats. Built by security professionals for security professionals, LogRhythm enables security professionals at leading organizations like NASA, KIA, Bloomin Brands, and Temple University to promote visibility for their cybersecurity program and reduce risk to their organization each and every day. To learn more, please visit logrhythm.com.

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 plan security improvements and verify that cyberdefenses work as expected, aligned with the MITRE ATT&CK framework. The Company is committed to giving back to the cybersecurity community through its free AttackIQ Academy, open Preactive Security Exchange, and partnership with the MITRE Center of Threat Informed Defense.

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