RELIAQUEST

Continuous Attack Simulations:

How to Identify Risk, Close Gaps, and Validate Your Security Controls

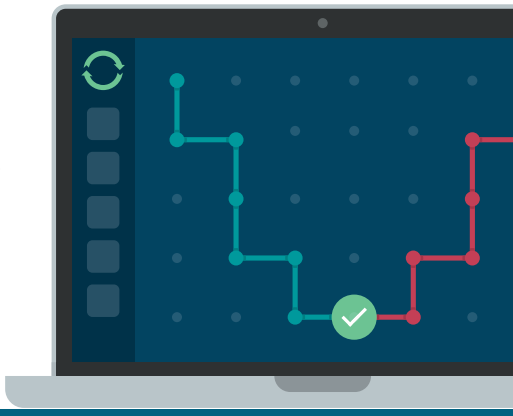
How confident are today's security teams in their readiness to respond to threats?

Introduction

Cyber threats are more sophisticated than ever, requiring precise intelligence into malicious activity – and demanding a high level of confidence in security models. At the same time, enterprises' security models have grown in complexity in terms of product configurations as well as automated and manual processes – not to mention the overall networking environment. Building confidence in readiness has typically required time-consuming, ad hoc, and costly testing, such as the traditional red teaming or penetration tests. But as attackers get savvier and swifter about breaching defenses – and digital transformation accelerates business change – security teams don't have the luxury of time. And the money that teams spend on penetration testing might be better deployed in simulations that can deliver actionable answers on where the threats are and how to stop them.

Today, there is a better way to gain confidence in security models: continuous attack simulations, which automate adversary behavior in a controlled manner and on a consistent basis. This method of continuous testing overcomes the barriers posed by traditional testing, such as time and cost. It can also span many more processes and security controls, without disrupting day-to-day business operations.

However valuable attack simulations are, they can't close security gaps and strengthen security models on their own: reports on which expected alarms didn't fire are only the first step in understanding the success of your security model. The attack simulation results must be paired with actions to close gaps. Continuous testing is part of an ongoing holistic security strategy – not a stand-alone tool that's deployed from time to time.



Attack simulation software continuously mimics real-world threats to highlight gaps in security systems, enabling organizations to improve security controls and respond to incidents.

In this paper, you'll learn:

WHY continuous attack simulations can improve confidence in security models

WHICH common security weaknesses can be identified through attack simulations

HOW to integrate attack simulations into your overall security operations

What's the difference between traditional testing and attack simulations?

TRADITIONAL TESTING

- Test scope tends to be limited – for example, testing the impact of a phishing attack on C-level computers. That means other potential threat vectors won't be tested.
- Results are often delayed – in many cases, they are not reported back to organizations for a month or longer.
- Findings are from a specific point in time, and therefore, are difficult to tie back to long-term security trends. Since security controls evolve rapidly, one-time options like penetration testing can't keep up with "security decay."
- Costs can be high – and go higher as the scope of the test is broadened, or more third-party consultants are added to the testing project.
- Traditional testing has the potential to upend normal operations in the production environment – for example, inadvertently causing denial of service.

ATTACK SIMULATIONS

- Attack simulations provide an ongoing view of security in a way that traditional testing cannot, better aligning with the dynamic nature of the security environment.
- They're not limited by project scope and can validate security controls on a much larger scale.
- The tests are designed to be conducted repetitively without the costs and setup time of traditional testing.
- Machine learning enhances ongoing testing and findings are reported continually, giving security teams more data about day-to-day performance of their security models.
- Attack simulations can be designed to run on production environments.

How do attack simulations fit into security operations?

To achieve their goal of building confidence in security models, attack simulations should not be conducted via stand-alone software, operating outside of overall security stacks and alert sources. Attack simulations are a means to an end – which is more effective security, without gaps.

Here's how to ensure that attack simulations produce actionable insights.

TEST ASSUMPTIONS.

Continuous testing validates security teams' assumptions about the efficacy of security controls. As teams research attack kill chains to determine threats their security controls successfully recognize – as well as the threats that go undetected – attack simulations validate that their environment will perform as expected when under attack.

COVER BASIC RISK FACTORS.

Attack simulations should cover basic risk factors that do not change, which can be the highest-level threat vectors – as opposed to every possible weak point. For best results, focus on where attackers get in and how.

UNDERSTAND POSSIBLE OUTCOMES.

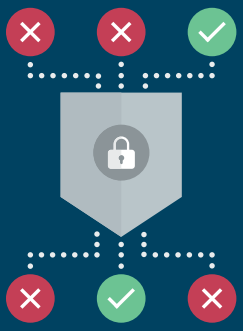
Use continuous testing to validate the security team's expectations of what baseline results should look like. If your team runs tests without understanding outcomes – for example, which alarms will fire, and which data sources are generating data that's used to trigger alarms – you won't know if the simulations were successful or not. There's a common misconception that most attacks are sophisticated and complex. But in reality, many attacks perform in similar ways – and that's what your team can most effectively test for.

5 ways to use attack simulations to validate security controls

To bring your security model from zero to hero, you need to understand how to leverage the full security stack effectively. This is where attack simulations come into play: They can ensure your security solutions can detect and mitigate the risks that threats pose to the network. Attack simulations can test for the five common security weaknesses on the next page.

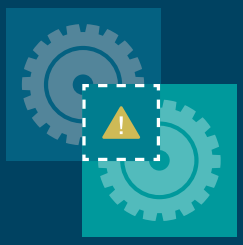
1. MISCONFIGURATIONS:

Many teams are so inundated with false positives that they end up turning off or ignoring their alerting from certain sources to their SIEM (security information and event management) systems, which leads to breaches going undetected and increasing adversary dwell time. By replicating breaches and seeing their impact, teams recognize how to properly configure technology to prevent attacks or detect them faster.



2. SECURITY DECAY:

Over time, as enterprises add security tools and those tools continue to function without being patched, and new malware and exploits are developed, the systems and network security posture decays. As changes such as patching and new configurations are made to network tools, security decay is compounded, since teams can't be certain how changes will affect the overall security environment. Attack simulation tools can diagnose and prevent security decay because they allow teams to continuously test systems to ensure they're up to date and remain secure.



3. OVERLAP:

Another challenge comes when enterprises have rapidly adopted new cybersecurity technologies and now have tools that duplicate capabilities. Companies end up spending resources on tools they don't need because they can't measure the effectiveness of the coverage they already have. By using attack simulations, companies can identify where coverage is strong as well as unproductive overlap, thereby reducing the cost of their product spend.

4. TOOLS THAT DON'T WORK IN YOUR ENVIRONMENT:

Every organization has a unique security environment, in which not all tools will work effectively. You can validate potential tools in your own environment before making the purchase, instead of only testing them in the vendor's lab environment.

5. INCIDENT RESPONSE TRAINING:

For many security team members, live security incidents are their first opportunities to build incident response skills. They have to respond on the fly and hope their approaches are the correct ones. With attack simulations, teams can safely learn about incident response without putting live systems at risk. Attack simulations can drill teams on proper mitigation techniques and threat hunting, so they're ready when the real threats occur.

In the 2019 ReliaQuest Security Technology Sprawl Report, more than half of IT professionals say the number of security tools is so burdensome that it adversely impacts security posture. Disparate tools and processes can leave gaps in security models – but continuous testing can help identify those gaps and plot a course for closing them.

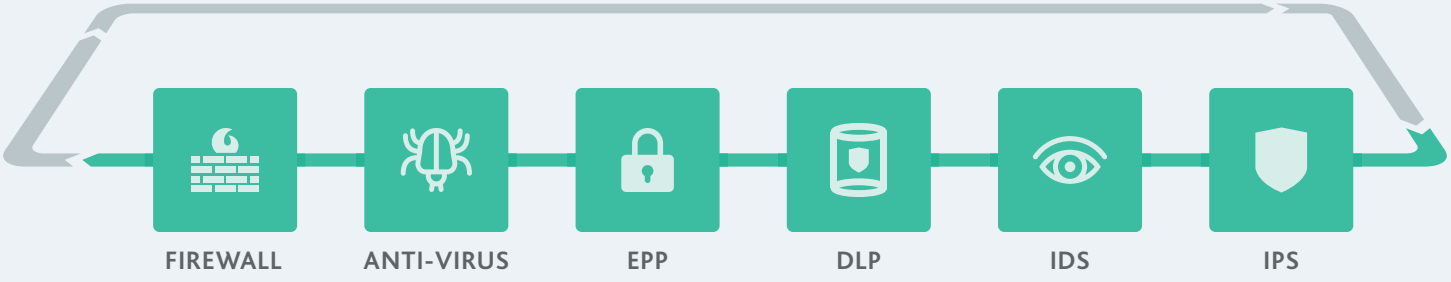
How to take action on test findings

Discovering vulnerabilities is an important step in building confidence in security – but it's only the first step. If the discovery phase is disconnected from the "take action" phase, then security gaps will persist. Testing of security controls should work hand-in-glove with managing security models.

Traditional attack simulation solutions only offer half the story. They can't provide the insights that lead to immediate actions – which then improve security.

TO CLOSE THE LOOP, ATTACK SIMULATIONS NEED TO:

- Integrate with security controls to recognize which data is required to generate alarms, the sources of the data, and the configuration of these sources.
- Monitor your security controls with recognition of which alerts should fire from an attack simulation.
- Provide immediate feedback on where threat detection and response are impaired.
- Easily identify the failed controls and prioritize or automate remediation based on the highest level of impact.
- Map both attack techniques and security control content to security frameworks such as MITRE ATT&CK, in order to recognize potential and validated threat coverage.
- Map to, and integrate with, automated playbooks that reflect common actions or series of steps to remediate threats once discovered.



WITH AN INTEGRATED APPROACH, IF ALARMS DON'T FIRE:

- You know which attack type or scenario you're currently at risk of missing.
- You know if data sources are no longer generating information to trigger the alarm.
- You know if misconfigurations in your environment are leaving you vulnerable to an attack.

As security models improve and provide enterprises with greater visibility and threat coverage, attack simulations validate those visibility and threat coverage improvements. And as both the environment and threat landscape change, attack simulations ensure that levels of visibility and threat coverage remain intact.

Attack simulations are the great security equalizer – shedding light on long-held assumptions and hidden gaps and providing confidence that security models are aligned to risks.

Discovering vulnerabilities is an important step in building confidence in security – but it's only the first step. To take action on findings and close security gaps, attack simulations need to integrate with your existing security controls.

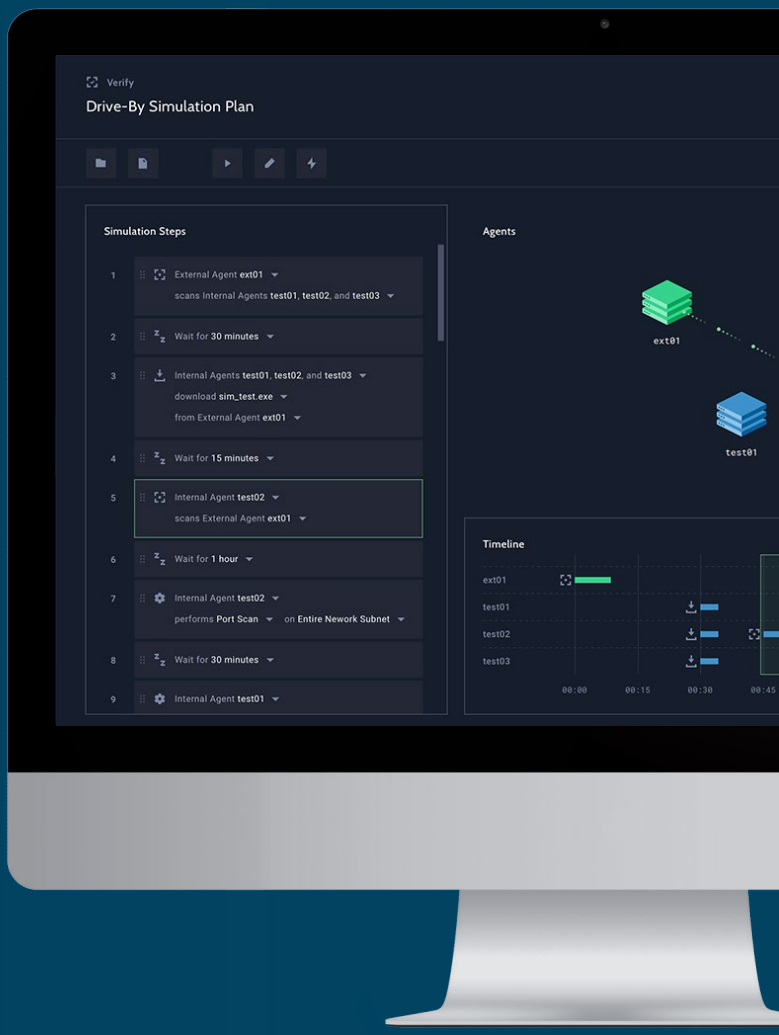
How ReliaQuest Validates Security Programs

ReliaQuest fortifies the world's most trusted brands against cyber threats with GreyMatter, its SaaS platform for increasing enterprise visibility while automating threat detection and response. It does this by unifying and integrating existing SIEM, EDR, multi-cloud, and third-party apps, to deliver a centralized, transparent view across the environment. The platform's analytics provide actionable reporting and metrics that measure ongoing improvement of the security program to improve the effectiveness of security investments while better enabling the business.

ReliaQuest GreyMatter includes integrated attack simulations that ensure enterprise security controls will perform as expected when attacks occur. This capability uses persistent and dissolvable agents, certified integrations, and flexible attack simulations with impact ratings to enable cyber assurance across disparate environments, providing continuous, actionable results. It integrates across a wide range of security controls and enables the deployment of automated responses to remediate threats when they are discovered.

More than 250 Global 2000 enterprises rely on ReliaQuest to achieve security confidence. ReliaQuest is a private company headquartered in Tampa, Fla., with locations worldwide, visit www.reliaquest.com

LEARN MORE ABOUT RELIAQUEST GREYMATTER



ReliaQuest GreyMatter's integrated attack simulations continually integrate across production environments, including existing security controls, multi-cloud environments, and third-party apps to ensure fast recognition and resolution of security program gaps.

RELIAQUEST

Make Security Possible™

(800) 925-2159 www.reliaquest.com info@reliaquest.com

Copyright © 2018 ReliaQuest, LLC. All Rights Reserved. ReliaQuest, RQ, and the ReliaQuest logo are trademarks or registered trademarks of ReliaQuest, LLC of its affiliates. All other products names and/or slogans mentioned herein may be trademarks or registered trademarks of their respective companies. All other information presented here is subject to change and intended for general information. Printed in the USA.