RELIAQUEST

SOLUTION BRIEF

RELIAQUEST GREYMATTER

VERIFY

Assure cyber readiness with continuous attack simulations

Identifying Security Gaps

CISOs need to confidently assert their team's readiness to detect and respond to a growing number of threat types. As the security team evolves their tools, risk increases due to changing product configurations, manual triage processes, ongoing content tuning, and automation relying on technical integrations. This creates areas of unknown risk incurred from introducing unrecognized vulnerabilities. Enterprises need to turn "unknowns" into "knowns" and gain confidence that their security models recognize and mitigate risk as soon as it arises.

- **How do I know whether our existing security investments will perform as expected when they come under attack?**
- **Have we identified all risk areas that could prevent us from seeing or responding to an attack?**
- **Can we effectively evaluate new security controls' ability to perform and complement existing investments?**

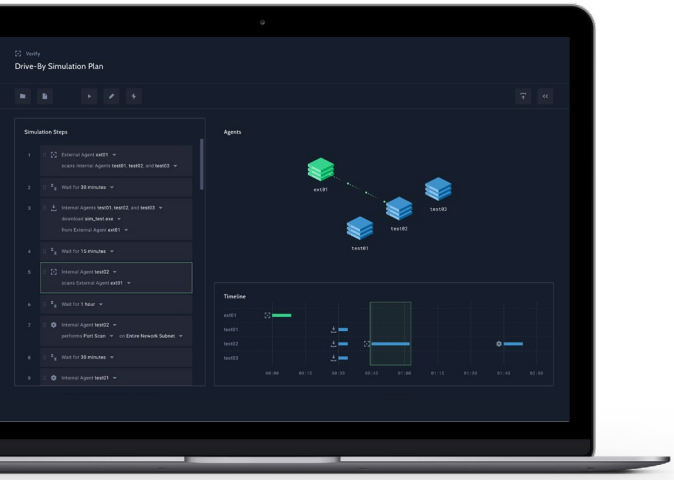
Breach and attack simulations are the primary way to test if your security controls provide visibility, threat coverage, and appropriate methods for response. Common methods for simulating attacks include tabletop exercises, red teaming, or white hat penetration tests. These approaches have shortcomings. The costs, both in terms of the budget for third party consultants and time investments from internal resources, limit scope to testing specific controls. Simulations also feature slow reaction times, taking up to a month to receive reports. While the reports often contain numerous details, they reflect a single point in time without guidance as to prioritization or resolution. These methods are not sufficiently agile to keep pace with the rate of change in modern enterprise environments.

To reduce the manual and ad hoc characteristics of attack simulations, you need an automated approach that provides:

- Continual assurance that security models are operating optimally
- Access to immediate feedback
- Recognition of root causes to control failures, so that controls can be altered and continually re-tested until ideal results are reached

ReliaQuest GreyMatter

Verify is a core capability of the ReliaQuest GreyMatter platform. ReliaQuest GreyMatter increases your enterprise visibility while automating threat detection and response. It does this by unifying and integrating existing SIEM, EDR, multi-cloud, and thirdparty apps, to deliver a centralized, transparent view across your environment. The platform's analytics provide actionable reporting and metrics that measure ongoing improvements of the security model to recognize and communicate success across the enterprise. With a unique combination of technology, analytics, and ongoing enablement, GreyMatter customers see fast, measurable results, averaging 400% improvement in threat detection within the first 90 days of going live.



Cyber Assurance Across All Environments

Verify uses attack simulations, which are one or more techniques, tactics and procedures to mimic real-world threat actor behavior. It also brings series of simulations together in campaigns, which mimic advanced attack scenarios. Enterprises receive real-world results, not lab induced scenarios, by executing simulations with persistent and dissolvable agents designed for production environments. Scheduled, ongoing simulations provide continuous analysis for more immediate recognition of missing data or configurations that would impair security tools from detecting and responding to threats.

- Persistent and dissolvable agents
- Designed to use across production environments
- Perform hundreds of tests per hour

Certified Integrations Ensure Continual Assurance

ReliaQuest certifies integrations across security controls, cloud environments, and third-party applications. Certified integrations ensure successful execution of attack simulations without time-consuming preparations. GreyMatter Verify maps threat coverage to specific attack types and techniques captured in security frameworks such as MITRE ATT&CK.

Visualization of your threat coverage and gaps allows for faster comprehension of the threat types your security controls will recognize and which gaps to address.

ReliaQuest's library of simulations map to MITRE ATT&CK scenarios and common attack techniques

Certified integrations align to your threat coverage and your security controls

Continuously Validate Security Model Effectiveness

ReliaQuest GreyMatter ensures continued integration across your production environments, including your existing security controls, multi-cloud environments, and third-party apps. Findings from your Verify simulations ensure fast resolution of security model gaps by identifying the root security controls. Overall, GreyMatter customers gain confidence in their threat protection with:

- ReliaQuest's maintained security control content library
- Ongoing tuning of security control content to your specific environment
- Visibility into your threat coverage mapped to security frameworks and threat stages
- Continued assurance your security controls detect and respond to threats

This unrivaled level of visibility provides clear assurance while also revealing a tactical roadmap of where to gain coverage and control.

With Verify, enterprises maximize the overall effectiveness of their security model with validated, measurable results.

To learn more about ReliaQuest GreyMatter, please visit us at **https://www.reliaquest.com**.

RELIAQUEST

Make Security Possible™

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