RELIAQUEST GREYMATTER: VERIFY

Assure cyber readiness with continuous attack simulations

Identifying Security Gaps

Security leaders need to bolster their team's readiness to detect and respond to a growing number of threats against an increasingly dynamic IT environment. As the security team evolves their tools, risk increases due to changing product configurations, manual triage processes, ongoing content tuning, and automation that relies on technical integrations. This creates areas of unknown risk from introducing unrecognized vulnerabilities. The more the security team can turn "unknowns" into "knowns," the more confident they can be that they can quickly mitigate risk.

How do we know whether our existing security investments will perform as expected during an attack?	Have we identified all gaps that could prevent us from seeing or responding to an attack?	Can we effectively evaluate whether new security controls will perform and complement existing investments?

Breach and attack simulations are the primary way to test whether your security controls are effective. Common attack simulations 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 take up to a month to produce results. While the results often contain valuable data, they reflect a single point in time and can't suggest prioritization or means of resolution. These methods are not agile enough to keep pace with modern enterprise environments.

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

- Continual assurance that security models are operating optimally.

- Access to immediate feedback.

- Root-cause analysis of control failures.

ReliaQuest GreyMatter Verify

Verify is ReliaQuest's automated breach and attack simulation capability. Verify allows security operations teams to simulate breaches and identify gaps by mimicking the likely attack paths and techniques used by bad actors.

With ReliaQuest GreyMatter, an Open XDR-as-a-Service platform, customers get fully packaged and field-tested scenarios that operators can run, on-demand or continuously, and get results immediately. Frequent updates to attack scenarios based on the latest threat intelligence help identify risk areas and help teams be better prepared for specific attacks.

Certified Integrations Ensure Continual Assurance

ReliaQuest certifies integrations across security controls, cloud environments, and third-party applications. Certified integrations ensure successful attack simulations without time-consuming prep. GreyMatter Verify maps threat coverage to 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.

Continuously Validate Security Model Effectiveness

ReliaQuest GreyMatter affirms that integrations across your production environments are always up to date. Verify simulations ensure fast resolution of gaps by identifying the problematic security controls. Overall, GreyMatter customers gain confidence in their threat protection with:

- ReliaQuest's living library of security control content
- 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 properly detect and respond to threats
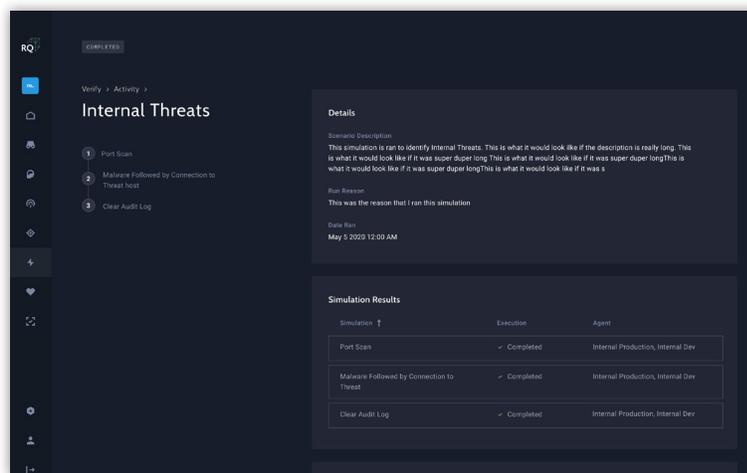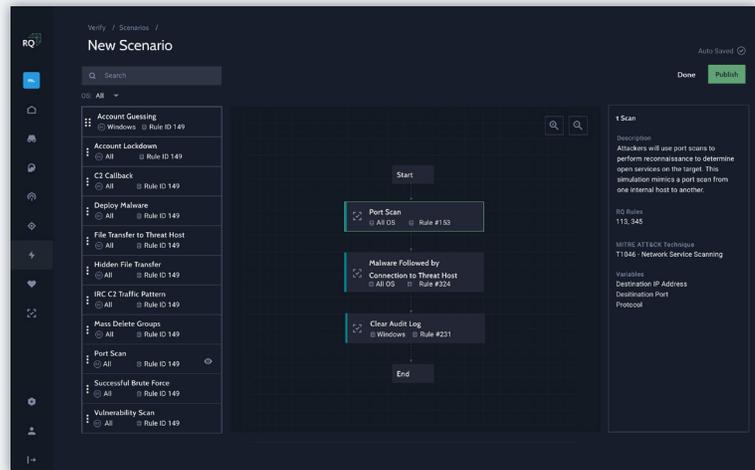
This unrivaled level of visibility provides confidence while also revealing a tactical roadmap of where to gain coverage and control. With Verify, enterprises maximize their security model with validated, measurable results.

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**