RELIAQUEST

SOLUTION BRIEF

RELIAQUEST GREYMATTER

Automate across the security lifecycle.

SECURITY LEADERS LACK THE INTEGRATION TO ENABLE EFFECTIVE AUTOMATION

Security organizations are overwhelmed. In a recent study of more than 400 security leaders, nearly all respondents say that better visibility into the results of their security program (94%) or integration and automation of disparate tools (93%) would allow them to get more benefit out of their security spend*. But because of too many tools, too many manual, repetitive tasks, and too many alerts, they aren't getting the visibility they need to secure the business and confidently automate.

The industry at large is looking at automation as the answer, but many of the tools available today take a narrow and siloed approach—they focus only on the ability to automate remediation. In reality automation is challenging to implement and scale due to fragmented data, a lack of documentation, standard operating procedures, and confidence that appropriate controls are performing as expected. **This leaves security leaders to wonder**:

Do we understand the ideal workflows from which to build automation?

Do I want to invest in the expertise to build integration across tools, or in analysts who can protect the business?

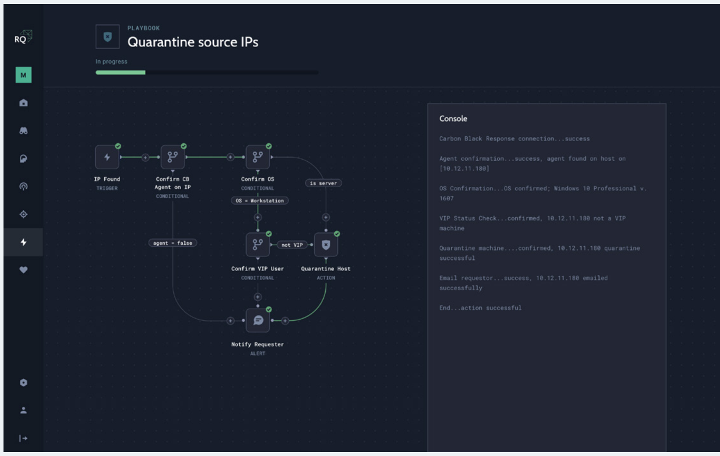
Can we build automation when we have so many false positives?

AUTOMATION, FROM FRONT TO BACK

ReliaQuest's GreyMatter SaaS security platform takes a longer and more holistic view—enabling automation across the security lifecycle. Having run security operations centers (SOCs) for Fortune 1000 organizations for more than a decade, ReliaQuest knows automation is the key to a healthy, efficient and resilient security program.

How does it work?

When ReliaQuest implements detection capabilities in a customer's SIEM or EDR, each use case is assigned a unique code. When a use case triggers, a GreyMatter automation play keys off of these codes to auto-query related technologies, de-dupe, and enrich the data—from historical information, to threat intelligence-and creates a high-fidelity research package at machine speed. The research package provides the analyst with all of the information they need from a single view—no running multiple queries across multiple tools from multiple interfaces. **Fifty percent of what the industry used to think of as the investigative process is done before an analyst even clicks a button.**



Console

```
Carbon Black Response connection...success

Agent confirmation...success, agent found on host on
[10.12.11.180]

OS Confirmation...OS confirmed; Windows 10 Professional v.
1607

VIP Status Check...confirmed, 10.12.11.180 not a VIP
machine

Quarantine machine....confirmed, 10.12.11.180 quarantine
successful

Email requestor...success, 10.12.11.180 emailed
successfully

End...action successful
```

As part of that research package, GreyMatter also pulls from automation playbooks linked to the technologies in your environment. These range from simple responses like blocking an IP address or emailing a user to multi-step, multi-technology responses like banning hashes, creating watchlists, or running IOC lookups against multiple technologies. GreyMatter offers packaged playbooks, tested against our existing customer base, and gives you the ability to customize playbooks or complement existing security orchestration, automation and response (SOAR) technologies. **That's the power of the GreyMatter platform—unified data collection, enrichment and standard operating procedures mapped to playbooks to investigate and respond to threats faster.**

*Source: ***Security Technology Sprawl Report***,
ReliaQuest, December 2019

BEYOND AUTOMATED RESPONSE

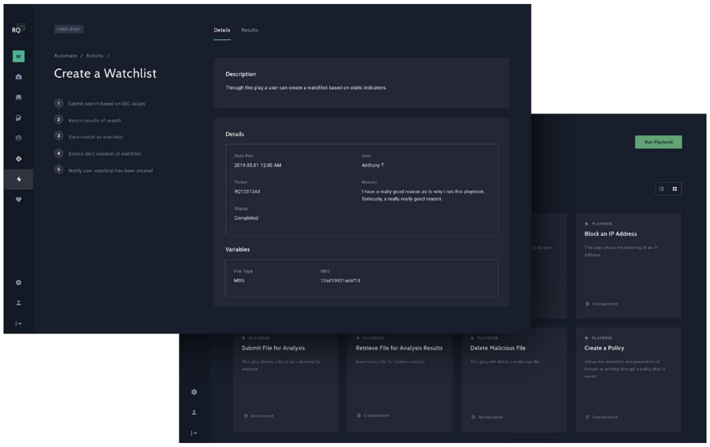
Going beyond response, let's talk about continuous assurance and improvement. It's great to have the latest technologies in place, but ultimately it comes down to knowing that the content and controls you've labored over are actually working. With automated attack simulation, you can continuously validate your detection content. With GreyMatter, you can run continuous testing and prioritize fixes based on greatest risk to the business by taking advantage of the simulation library or building your own.

With packaged threat hunting campaigns, in two clicks, GreyMatter will collect required data from across your environment. You can select from packaged threat hunts or customize your own. As results return, you can continue working to address risks, and stop attackers before they do lasting damage.

- Alert-level automation to speed the investigative process
- Self-healing security environment corrects misconfigurations
- Machine-learning driven threat hunting campaigns
- Autonomous attack simulations
- Automation across multiple technologies to bolster confidence and speed response

A more productive, more engaged team

Get your teams out of the business of tedious, repetitive, low value tasks. Let machines do them instead, thanks to the power of GreyMatter.



Automate / Activity /

Create a Watchlist

1. Submit search based on IOC values
2. Return results of search
3. Save search as watchlist
4. Enable alert creation of watchlist
5. Notify user watchlist has been created

Description

Through this play a user can create a watchlist based on static indicators.

Details

Date Ran: 2019.05.01 12:00 AM

User: Anthony T

Ticket: RQ1231243

Reason: I have a really good reason as to why I ran this playbook. Seriously, a really really good reason.

Status: Completed

Variables

File Type: MD5

MD5: 12sd13421adsf13

PLAYBOOK
Block an IP Address
This play allows the blocking of an IP Address
Containment

PLAYBOOK
Submit File for Analysis
This play allows a file to be submited for analysis
Enrichment

PLAYBOOK
Retrieve File for Analysis Results
Download a file for further analysis
Containment

PLAYBOOK
Delete Malicious File
This play will delete a malicious file
Remediation

PLAYBOOK
Create a Policy
Allows for detection and prevention of threats or activity through a policy that is saved
Containment

When your technology investments do more for you, you free up the people you've invested in to do the tasks humans are best suited for—making decisions based on experience and evidence, and initiating action based on known risks and best possible outcomes.

With this approach, everybody wins:

- Businesses get better outcomes
- CFOs get ROI
- CISOs get better visibility
- Analysts get better job satisfaction
- Security program is proactive and strategic

ReliaQuest GreyMatter glues together the data and processes from your existing investments, so your team can move from reactive to proactive, leading to security confidence. Let's partner to get you to your version of a best-in-class security program.

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