RELIAQUEST

GreyMatter Platform Guide

Outcomes for Enterprise Security Teams

CHALLENGES FOR TODAY'S SECURITY LEADERS:

In order to secure the business, security programs assemble a portfolio of best-of-breed tools. The lack of integration and visibility across those tools often leaves teams stuck in reactive mode, chasing down false positives, getting whiplash from working across dozens of UIs and languages, and unable to implement solid detection content or automation. **Security leaders struggle to make the most of their existing investments and lack confidence in their ability to mitigate risk for the business.**

ReliaQuest GreyMatter, the first SaaS security platform, overcomes these challenges to deliver security confidence. Through a robust set of features, GreyMatter provides true visibility, end-to-end automation across the security lifecycle and continuous measurement ensuring you get the most out of existing security investments to improve your security posture over time.

This guide highlights the outcomes our customers receive today with GreyMatter – ones that your enterprise can experience, too.

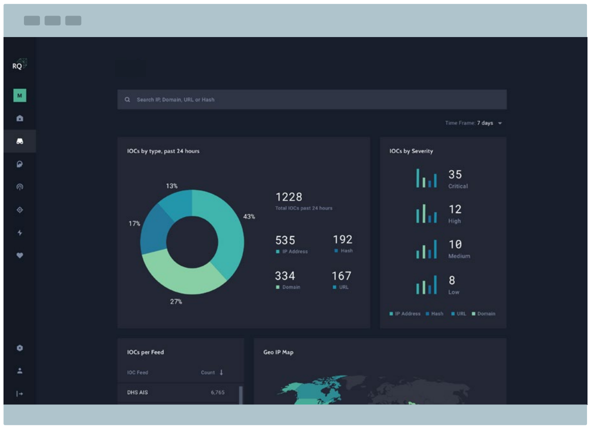
Let's Dive Into What GreyMatter Can Do For You

CENTRALIZE THREAT INTELLIGENCE

High fidelity threat intelligence specific to your organization, integrated seamlessly with your SIEM and EDR.

Before GreyMatter:
There are many open source, government, and commercial feeds that gather and distribute indicators of compromise (IoCs). Reliance on one feed leaves an enterprise at risk of exposure. However, adding multiple sources introduces new challenges: duplicate entries, inconsistent formatting, and large datasets without any way to prioritize IoC consumption.

With GreyMatter:
Higher alert fidelity with relevant threat intelligence for your SIEM and EDR.



CURATED INTEL THAT HAS BEEN DEDUPLICATED, CONTEXTUALIZED, AND PRIORITIZED
Only receive the highest fidelity threat intelligence, so your security controls report fewer false positives. Our own research team validates and scores the various threat intelligence feeds and tunes them based on trends from across our customer base.

OUT OF THE BOX ACCESS TO OVER 40 FEEDS
Actionable view of existing and emerging threats through general and industry-specific threat feeds, including the ability to add your own commercial providers.

THE BENEFITS:

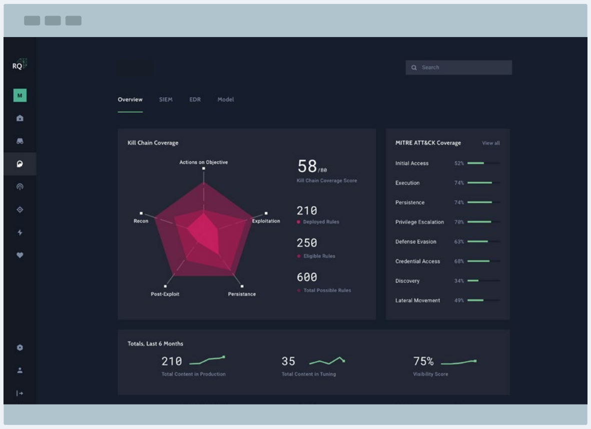
- Increase true positives by 15%
- Integrate with existing feeds
- Calibrate for your specific industry
- Enhance threat detection accuracy

LEVERAGE THREAT DETECTION CONTENT CUSTOMIZED FOR YOUR ENVIRONMENT

Threat detection content tuned to your environment and mapped to frameworks like the Kill Chain® and MITRE ATT&CK®

Before GreyMatter:
Generic content is ineffective at detecting threats in enterprise environments. If content is left untuned or unvalidated, you could be leaving open doors for attackers and thereby increasing your risk.

With GreyMatter:
Increase alert fidelity and threat detection coverage with content using your integrated technologies and covering all attack scenarios.



BEST-IN-CLASS CONTENT
Critical visibility into business risks through custom content, integrated with leading threat intelligence applied across your technology stack.

CONTINUOUSLY TUNED
Consistent building and integration of threat detection content, along with data parsing capabilities, increases the visibility and effectiveness of your existing SIEM and/or EDR.

THREAT GAP ANALYSIS
Understand business risk in real time and identify gaps in threat detection by viewing your existing content coverage, mapped to the Kill Chain® and MITRE ATT&CK® frameworks.

THE BENEFITS:

- Development and tuning continuously reflects your evolving environment
- Reduce time to deploy
- Map intel to detections and investigations
- Decrease false positives
- Improve risk awareness

CUSTOMER SUCCESS STORY:

$6+ Billion Fortune 500 Data and Analytics Organization

Problem: This customer was trying to understand their threat coverage against MITRE ATT&CK® techniques using a manual and time-consuming process

Solution: ReliaQuest GreyMatter provided real time insight into MITRE ATT&CK® coverage visualizing where gaps were across the environment

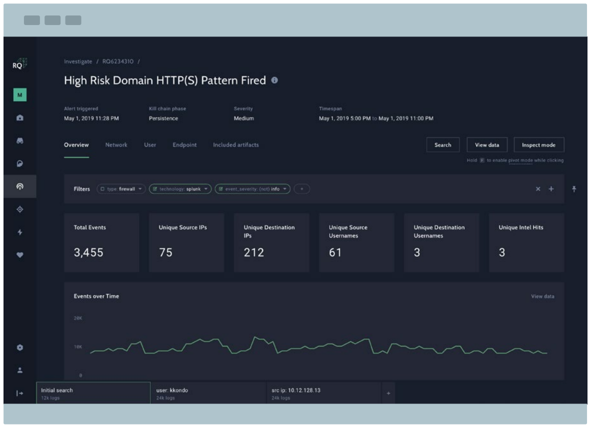
Result: Optimized MITRE ATT&CK® coverage across 50 techniques while creating a strategic and consistent correlation rule roadmap

CONDUCT AUTOMATED INVESTIGATIONS

Alert-level automation, powered by GreyMatter's proprietary universal translator, provides your analysts unified data on-demand from SIEM, EDR, multi-cloud and critical business applications to investigate and respond from a single interface.

Before GreyMatter:
Each tool uses different field names, data structures, and syntax, making it difficult to get an accurate picture of your environment or trust the data you need to take the next step towards remediation. Furthermore, the extensive time wasted pivoting between tools leaves more time for an attacker to do damage.

With GreyMatter:
Faster threat detection and response using on-demand data aggregation and alert-level automation.
On average our customers are able to reduce duplicate SIEM alerts by 41% and EDR alerts by 43% helping to cut response times in half.



Investigate / RQ6234310 /

High Risk Domain HTTP(S) Pattern Fired

Alert triggered	Kill chain phase	Severity	Timespan
May 1, 2019 11:28 PM	Persistence	Medium	May 1, 2019 5:00 PM to May 1, 2019 11:00 PM

Filters
type: firewall
technology: splunk
event_severity: (not) info

Total Events	Unique Source IPs	Unique Destination IPs	Unique Source Usernames	Unique Destination Usernames	Unique Intel Hits
3,455	75	212	61	3	3

Events over Time

Initial search
12k logs

user: kkondo
24k logs

src ip: 10.12.128.13
24k logs

NO MORE TOOL PIVOTING

The GreyMatter universal translator gathers and normalizes data on-demand from your existing security and enterprise technologies in a single, unified view.

EFFICIENT INVESTIGATIONS

Every threat detection alert triggers a unique correlation rule and GreyMatter automatically aggregates relevant investigation data to assemble a research package across your entire security tool stack in a fraction of the previous time.

THE BENEFITS:

- Reduce alert fatigue
- Decrease the need for technology specific queries to perform investigations
- Investigate in a fraction of the time
- Speed threat detection and response
- Consolidate all required data in one place, without tool hopping

CUSTOMER SUCCESS STORY:

Fortune 1000 Travel Organization

Problem: Security team had little or no visibility into activity or risk in the environment with previous approaches

Solution: Leveraging ReliaQuest GreyMatter while deploying a new EDR and SIEM solution unified visibility and investigations from across the environment

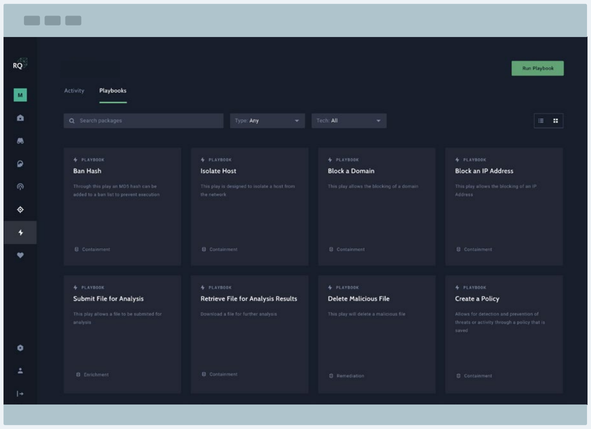
Result: Consolidating an immense amount of data into a single interface using GreyMatter; within a year, visibility grew by 150%

DRIVE FASTER THREAT CONTAINMENT AND REMEDIATION

Use pre-built playbooks to automatically enrich your data and accelerate your response to threat detection.

Before GreyMatter:
Automation isn't a reality for most enterprise security teams because of integration complexities, undocumented standard operating procedures and a lack of trust in the data and controls needed to implement automation. Maintaining playbooks is also resource intensive.

With GreyMatter:
Respond to your threats faster through automation certified to work end-to-end and across your entire environment.



PLAYBOOK
Ban Hash
Through this play an MD5 hash can be added to a ban list to prevent execution
Containment

PLAYBOOK
Isolate Host
This play is designed to isolate a host from the network
Containment

PLAYBOOK
Block a Domain
This play allows the blocking of a domain
Containment

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

INCREASED CONSISTENCY

From alert-level automation for data collection, data enrichment for specific correlations, certified detections tuned to your environment, technology integrations, and pre-built playbooks - achieve consistency across the security lifecycle so that your analysts can concentrate on higher-level decision making for critical threats.

ROI

Recognize areas ripe for automation and remove the overhead of creating, tuning, and maintaining technology integrations and playbooks, giving your analysts more time for priority work.

THE BENEFITS:

- Reduce repetitive tasks
- Decrease complexity of data integration
- Speed response by 50%
- Review historical responses triggered in your environment
- Audit past workflows

CUSTOMER SUCCESS STORY:

$21 Billion Fortune 500 Communications Organization

Problem: Quickly identified that using a manual approach to run their security program was not working. It was too expensive and ineffective

Solution: ReliaQuest GreyMatter centralized both SIEM and EDR technologies giving their team single workflows for investigation and threat detection and response

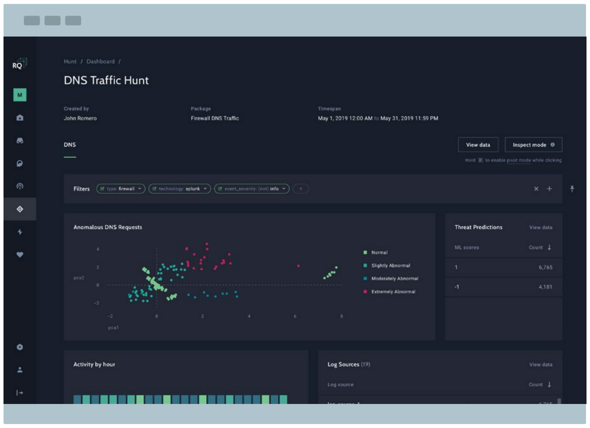
Result: The security team was able to achieve cost savings and be more effective across their security ecosystem

ENABLE EFFECTIVE THREAT HUNTING

Proactively execute threat hunting campaigns to detect anomalies across your environment.

Before GreyMatter:
Threat hunting remains beyond the reach of most enterprise security teams. Effective threat hunting relies on collecting data over extended time periods from across the entire enterprise environment. Both gathering and analyzing this data proves challenging, requiring extensive time and expertise to uncover credible threat activity.

With GreyMatter:
Identify abnormalities through automated data collection and machine-learnining driven threat hunting.



Hunt / Dashboard /

DNS Traffic Hunt

Created by: John Romero

Package: Firewall DNS Traffic

Timespan: May 1, 2019 12:00 AM to May 31, 2019 11:59 PM

Filters: type: firewall · technology: splunk · event_severity: (not) info

Threat Predictions

ML scores	Count
1	6,765
-1	4,181

Log Sources (19)

UNIFYING YOUR DATA FOR MORE MEANINGFUL INSIGHTS

Certified integrations aggregate large datasets across EDR, SIEM, multi-cloud, and business applications over long periods of time to help you differentiate abnormal from normal activity.

FASTER RECOGNITION OF EARLY THREAT ACTIVITY

Perform retroactive IoC hunts or behavioral analysis hunts using machine learning to identify early indicators of threats.

THE BENEFITS:

- Speed threat hunting by 5X
- Automate collection of relevant data without performance impact
- Reduce time to identify network anomalies
- Move from reactive to proactive threat identification
- Proactively identify known IoCs

CUSTOMER SUCCESS STORY:

Fortune 1000 Healthcare Organization

Problem: The team invested in SIEM and SOAR technologies but were not getting the expected ROI

Solution: Leveraging GreyMatter to automatically query large volumes of data unavailable in the SIEM allowed additional visibility and anomaly detection

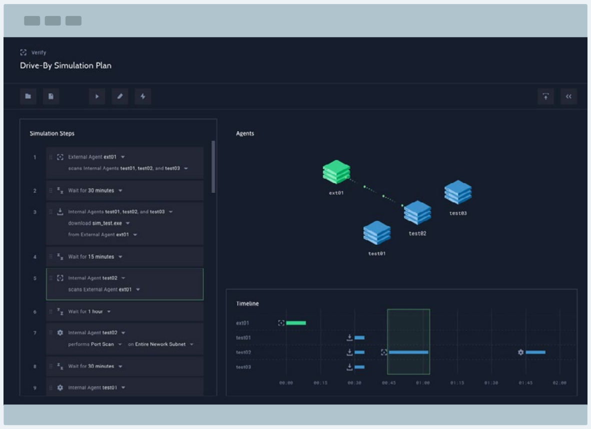
Result: Gained additional visibility into potential reconnaissance activity against the enterprise and accomplished desired automations at a far lower cost

ACHIEVE CONTINUOUS CYBER ASSURANCE

Validate efficacy of controls across your environment.

Before GreyMatter:
One of the common questions for enterprise CISOs is: "How do I know that the tools I've invested in and the processes we've put in place are working?" Traditional ad hoc approaches to answer this question can take weeks to yield results that are outdated by the time they arrive, resulting in continued risk to the business.

With GreyMatter:
Turn unknowns into knowns and continuously advance your security posture.



Drive-By Simulation Plan

Simulation Steps

1. External Agent ext01 scans Internal Agents test01, test02, and test03
2. Wait for 30 minutes
3. Internal Agents test01, test02, and test03 download sim_test.exe from External Agent ext01
4. Wait for 15 minutes
5. Internal Agent test02 scans External Agent ext01
6. Wait for 1 hour
7. Internal Agent test02 performs Port Scan on Entire Nework Subnet
8. Wait for 30 minutes
9. Internal Agent test01

CONTINUAL ASSURANCE

Perform ongoing or on-demand attack simulations to review the efficacy of your threat detection rules and the security controls in your environment. Remediate the identified gaps to support the dynamic changes of your enterprise ecosystem.

SEE ROOT CAUSES

Reports identify missed alerts from your security controls to prioritize remediation based on highest risk to the business.

THE BENEFITS:

- Identify gaps in required logging for comprehensive threat detection
- Review recommendations to optimize current security controls
- Map to MITRE ATT&CK® scenarios and techniques
- Alter and re-test controls until ideal results are reached
- Eliminate time-consuming preparation with certified integrations

CUSTOMER SUCCESS STORY:

$3.4 Billion Retail Organization

Problem: New security team inherited a large tool set, was unsure of technology effectiveness and felt they were missing critical threats across their environment

Solution: Assisted customer team in testing MITRE ATT&CK® based attacks to uncover potential issues with downstream detection capabilities and logging challenges through ReliaQuest GreyMatter

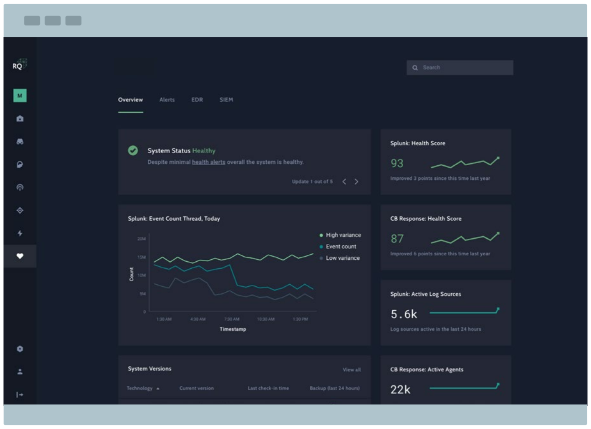
Result: The team was able to confidently report to the Board that it had improved visibility across the environment as well as increased efficacy in detecting threats, reducing business risk

ENSURE SYSTEM HEALTH

Optimize visibility through the health of your existing security investments.

Before GreyMatter:
Your visibility and ability to secure the business suffer if your tools aren't working properly. System maintenance is often reactive, time consuming and leaves enterprise security teams vulnerable with blind spots from misconfigurations and log collection issues. These gaps increase the risk of an attacker penetrating defenses and going undetected.

With GreyMatter:
A unified view to ensure your SIEM and EDR are operating properly.



System Status Healthy
Despite minimal health alerts overall the system is healthy.

Splunk: Health Score
93
Improved 3 points since this time last year

CB Response: Health Score
87
Improved 6 points since this time last year

Splunk: Active Log Sources
5.6k
Log sources active in the last 24 hours

System Versions

CB Response: Active Agents
22k

PROACTIVE, REAL-TIME HEALTH MONITORING
Protect your visibility by consistently monitoring the performance and availability of your SIEM and EDR solutions. Preemptively recognize system misconfigurations and quickly identify log source collection issues to mitigate impacts to your security ecosystem.

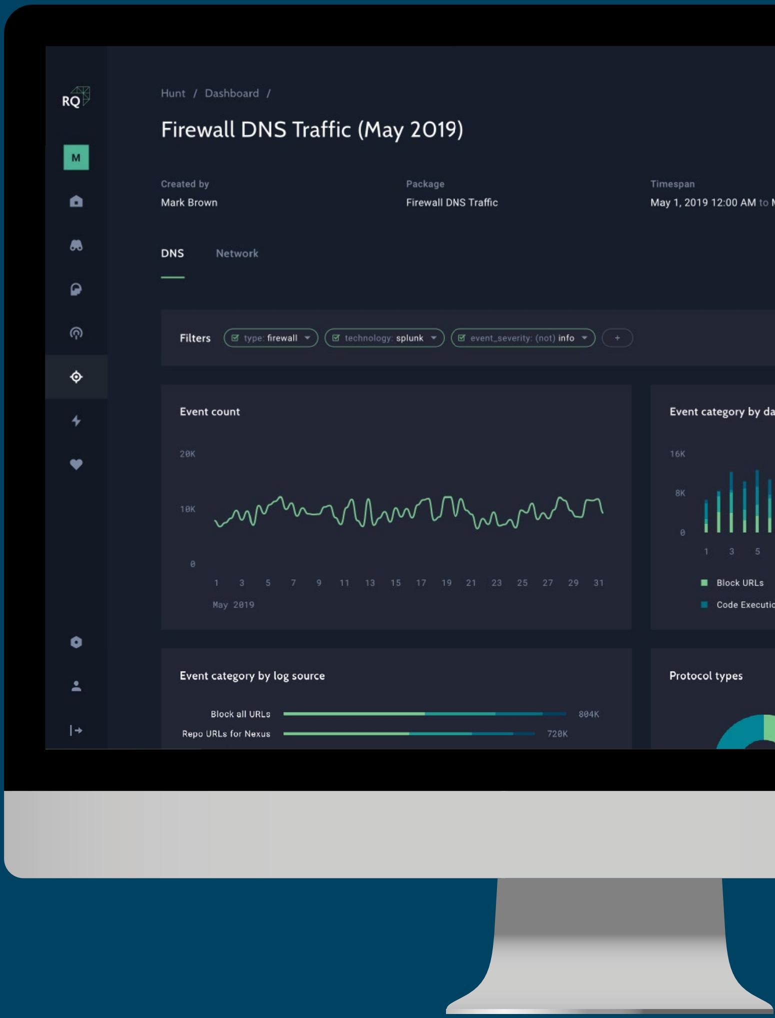
BASELINE ENVIRONMENT AND ALERTS
Actively baseline health conditions to identify problems before operations are interrupted.

THE BENEFITS:

- Optimize SIEM and EDR performance
- Achieve consistent trust in your data and secure monitoring with out-of-band system health alerting
- No impact to infrastructure
- Certify SIEM and EDR upgrades and integrations

About ReliaQuest

ReliaQuest, a global leader in cybersecurity, delivers industry-leading visibility and automation on-demand across complex environments with a platform purpose-built to protect organizations from security breaches. GreyMatter is the first cloud-native SaaS solution that integrates and improves an enterprise's on premise and multi-cloud technologies, unlocking the power of next generation cybersecurity. By increasing visibility through the platform's proprietary universal translator and use of automation and artificial intelligence, GreyMatter saves security teams valuable time and increases effectiveness by enabling automatic and continuous threat detection, threat hunting, and remediation. ReliaQuest is a private company headquartered in Tampa, Fla., with five global locations.



Hunt / Dashboard /

Firewall DNS Traffic (May 2019)

Created by: Mark Brown

Package: Firewall DNS Traffic

Timespan: May 1, 2019 12:00 AM to M

Filters: type: firewall · technology: splunk · event_severity: (not) info

> **ReliaQuest GreyMatter is the foundation for best-in-class security programs providing unified visibility, automation across the security lifecycle and Board-ready continuous measurement enabling security teams to support the business smarter and faster.**

LEARN MORE ABOUT RELIAQUEST GREYMATTER

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.