

Defenses at Every Attack Stage:

GreyMatter Attack Scenario Coverage

When it comes to modern cyber threats, focusing on threat vectors alone is no longer enough.

Phishing, for example, doesn't just involve a message in an inbox; it's a chain reaction. A user could click a malicious link that leads to a credential harvester, or they could download an attachment that deploys ransomware. This is the attack scenario—the complete sequence of events that could unfold beyond the initial entry point.

ReliaQuest GreyMatter provides complete coverage and control across the top attack scenarios by unifying your existing control domains—email, network, endpoint, and more—into a single command system.

Detect, investigate, and remediate threats at every stage of the attack.

Phishing and BEC

Leverage advanced detection and automatic containment for phishing attempts and BEC attacks. GreyMatter protects users from credential theft and fraudulent communications by identifying suspicious email behavior and blocking malicious messages.

Control Domains:



Email
Security



Authentication &
Identity and Access
Management



Endpoint
Security

Malware and Ransomware

Protect against both traditional malware and sophisticated ransomware attacks with GreyMatter. It detects malicious files and behaviors across endpoints and networks, automatically isolating infected devices and blocking further spread.

Control Domains:



Endpoint
Security



Network
Security



Application
Security



Authentication &
Identity and Access
Management

Data Loss

Safeguard sensitive data from unauthorized access and prevent data leakage. GreyMatter detects abnormal access patterns, unauthorized transfers, and data exfiltration attempts, triggering automatic containment actions to avert data loss.

Control Domains:



Data
Security



Authentication &
Identity and Access
Management



Network
Security

Cloud Threats

Ensure protection across cloud environments by detecting and responding to cloud-specific threats, including misconfigurations, unauthorized access, and vulnerabilities in cloud infrastructure. GreyMatter monitors cloud service activity and provides containment and remediation capabilities tailored to cloud platforms.

Control Domains:



Cloud
Infrastructure
& SaaS



Authentication &
Identity and Access
Management



Network
Security

Credential Theft and Account Compromise

Ensure coverage against credential theft, password spraying, and account compromise attempts. GreyMatter monitors authentication events and login behaviors to automatically detect and respond to suspicious activities, locking compromised accounts immediately.

Control Domains:



Email
Security



Authentication &
Identity and Access
Management



Endpoint
Security

Insider Threat

Monitor user behavior to detect potential insider threats, whether malicious or unintentional. GreyMatter identifies unusual activity from employees, contractors, or privileged users that could lead to data breaches, intellectual property theft, or security violations.

Control Domains:



Endpoint
Security



Authentication &
Identity and Access
Management



Network
Security

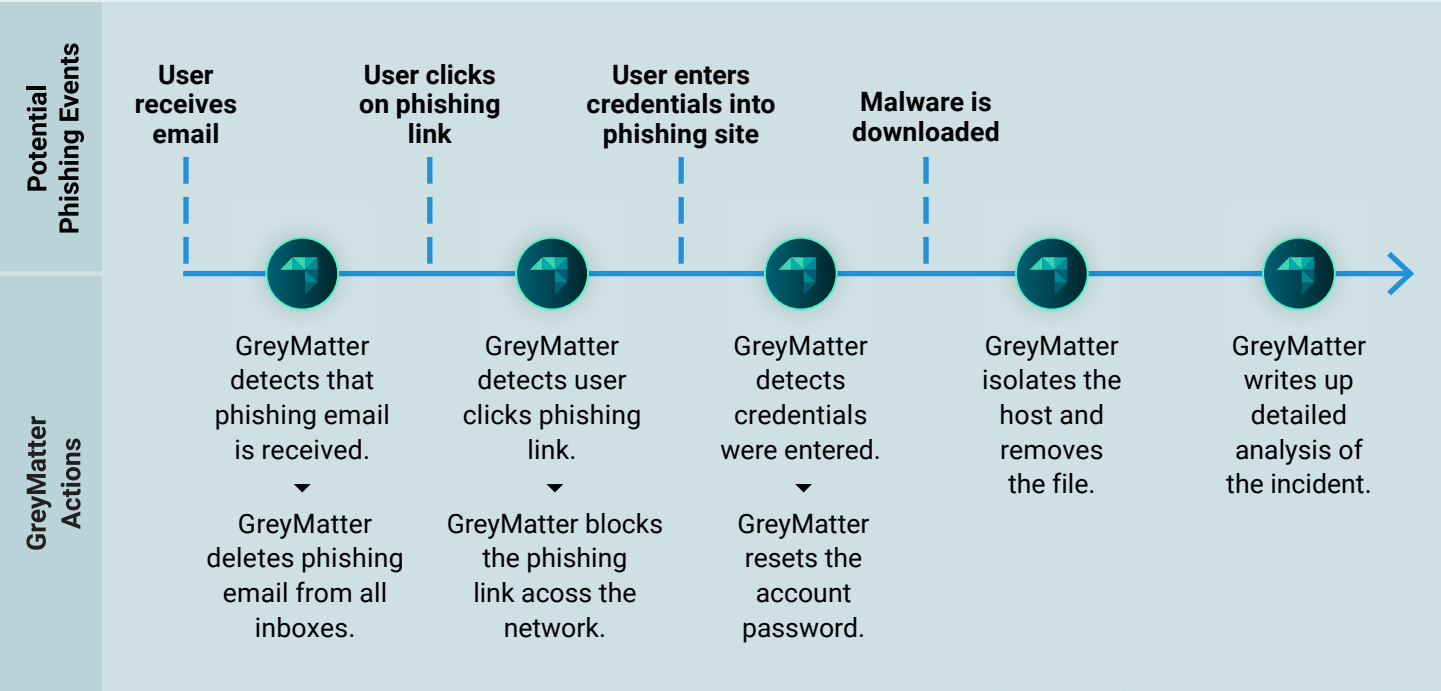
Operational Technology Risk

Comprehensively cover your OT and IoT environments to protect critical infrastructure and connected devices from cyberattacks. GreyMatter detects unauthorized access, system anomalies, and malicious activity within OT and IoT systems, ensuring secure operations.

Control Domains:



Phishing & BEC Attack Scenario with GreyMatter Defenses



Attackers don't stop at the entry point, and neither should your defenses.

With GreyMatter, you can uncover, understand, and counter any attack scenario—no matter how complex or multi-faceted. From phishing and ransomware to insider threats and cloud risks, GreyMatter empowers you to detect and contain threats before they escalate.

Don't settle for partial visibility or fragmented responses. Take control of your security operations with GreyMatter and achieve complete coverage and control across the attack scenarios that matter most. It's time to stop reacting to threats and start owning the fight.

With over 1,000 customers and 1,200 teammates across six global operating centers, ReliaQuest Makes Security Possible for the most trusted enterprise brands in the world. **Learn more at www.reliaquest.com.**