



Own the Unknown

with GreyMatter Digital Risk Protection

Proactively Mitigate Threats Across the Open, Deep, and Dark Web

Identify and prioritize legitimate threats without overwhelming your security team.

Stay ahead of attackers with expert insights from the ReliaQuest Threat Research team, including deep-dive analyses of targeted threat actors.

Neutralize risks both inside and outside your perimeter with precision.

Organizations often struggle to see the full scope of threats lurking across the open, deep, and dark web—leaving them vulnerable to advanced attacks. Without a complete picture of an organization’s external threat landscape, security teams are often left reactive rather than proactive.

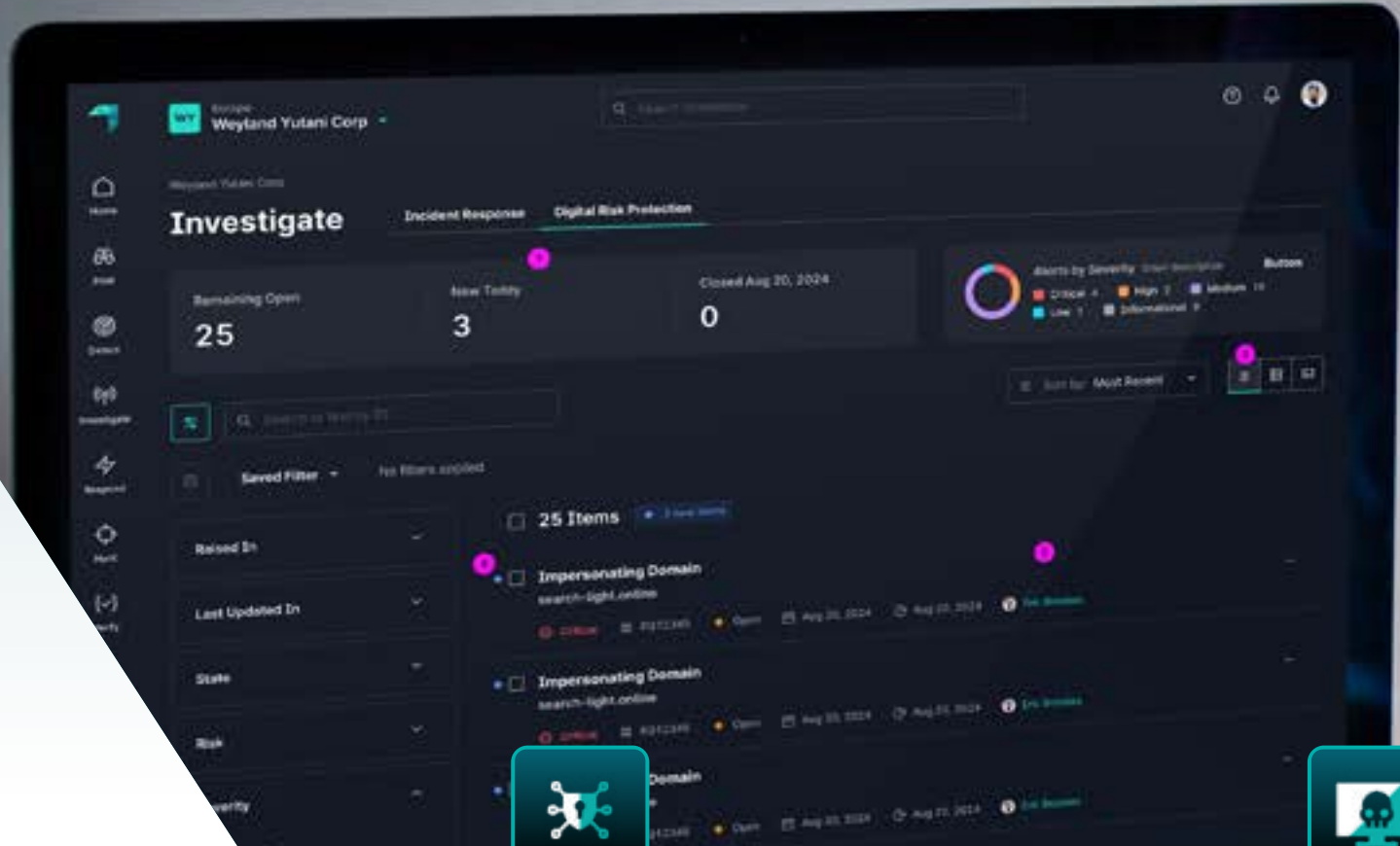
With **ReliaQuest GreyMatter Digital Risk Protection (DRP)**, your organization gains the visibility, context, and actionability needed to address emerging risks, safeguard sensitive data, and stay ahead of attackers.

Find and Act on Threats from the Deep and Dark Web

Hidden threats can surface anywhere, from stolen credentials on dark web marketplaces to impersonating domains designed to deceive. GreyMatter Digital Risk Protection (DRP) gives you the visibility to uncover these risks and the ability to take immediate action. From protecting your brand to safeguarding your assets and critical data, GreyMatter DRP equips your team with actionable intelligence to anticipate and outpace attackers.

Use Cases: How GreyMatter DRP Protects Your Organization

Digital threats target everything from employee credentials to executive reputations, often through unexpected channels. GreyMatter DRP helps you proactively identify and respond to these risks with precision and speed.



Exposed Credentials:

Detect compromised credentials or sensitive company data being circulated or sold on the dark web to prevent unauthorized access.



Impersonating Domains:

Identify and take down fraudulent login pages designed to deceive users and harvest credentials.



Executive Impersonation:

Stop attackers posing as company leaders to damage your reputation or mislead customers.



Leaked Sensitive Data:

Prevent attackers from exploiting leaked access keys or sensitive technology to compromise your systems.



Dark Web Mentions:

Track dark web forums, stolen data exchanges, and sales of initial access to your corporate environment.



Exploitable Vulnerabilities:

Identify and patch weak spots or misconfigurations that attackers can exploit.

Reduce Risk Inside and Outside Your Organization

With GreyMatter Digital Risk Protection, you'll gain comprehensive visibility into threats —whether they're targeting your organization from inside or outside the perimeter.

Open, Deep, and Dark Web Monitoring:

Spot brand mentions, leaked company data, and emerging threats across web sources, including private messaging apps.

Managed Takedowns:

Quickly remove spoofed websites and social media accounts impersonating your brand or leadership team.

Automated Containment Actions:

Trigger automated responses—such as resetting compromised credentials —based on pre-defined threat events.

Unified TDIR:

Combine threat intel, DRP, and automated responses for comprehensive, efficient Threat Detection, Investigation, and Response (TDIR).

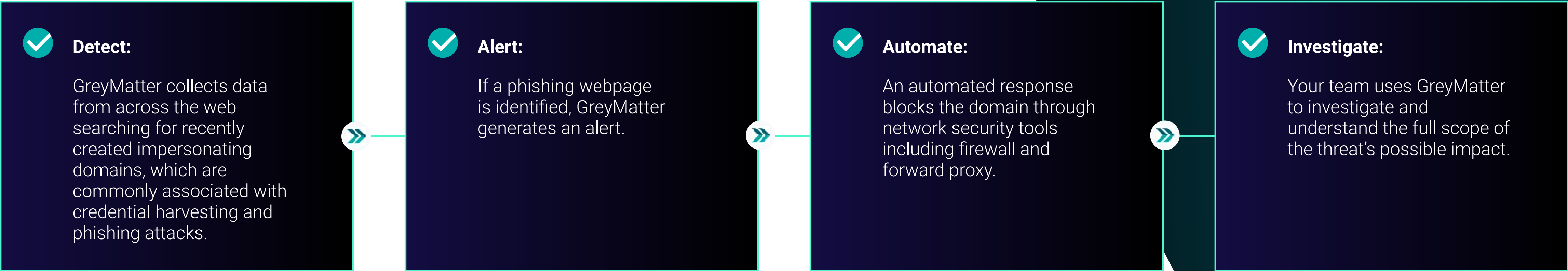
External Attack Surface Management:

Proactively address weaknesses in your endpoints, networks, and cloud environments before attackers can exploit them.

GreyMatter in Action: Neutralizing Impersonating Websites

Imagine attackers create a fraudulent website mimicking your company’s branding to deceive employees or customers into divulging sensitive information. With GreyMatter DRP, you can identify, act on, and remove these threats before they cause harm.


Here’s how the process works:



REQUEST A DEMO



 reliaquest.com

 800.925.2159

 info@reliaquest.com