RELIAQUEST®

Solution Brief

Comprehensive Digital Risk Protection Tuned to Your Business Needs

Continuous monitoring of deep and dark web sources to isolate legitimate threats and provide real-time alerting and fast remediation

As threat actors become more active and more sophisticated, they increasingly exploit the growing digital footprints of businesses. To effectively protect an organization's assets and customer data, security teams need to understand how these threat actors operate, how the risks manifest, and have the ability to take action to reduce their organization's risk

In order to collect the necessary data to understand these growing threats, security teams are at risk of drowning in an overwhelming amount of threat and security data. Even for the most sophisticated teams, getting a comprehensive picture of the threats and exposure is a considerable challenge.

ReliaQuest GreyMatter® Digital Risk Protection (DRP) solves these problems by continually monitoring open, deep, and dark web sources to isolate legitimate threats and provide quick and easy remediation. By focusing on automated actions, enhanced workflows, and integrated alerts, GreyMatter DRP enables security teams to dramatically reduce the time to respond to threats and lessens the risk to the business.

Reduce Triage Time by 70% with Automated Playbooks

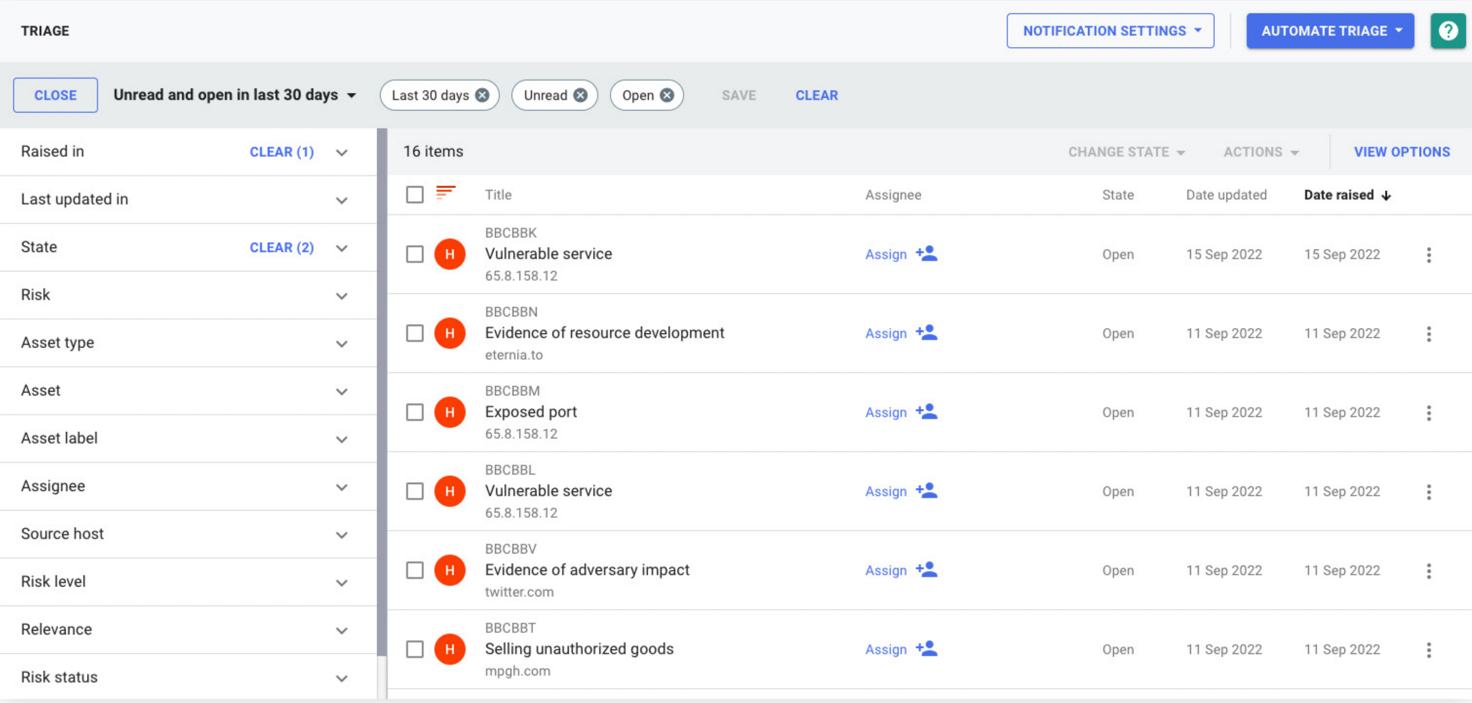
Key Benefits:

- Protect online brands by detecting brand and domain impersonations, monitoring social media profiles, and detecting phishing and business email compromise attempts.
- Prevent data loss and exposed credentials and documents by monitoring online file stores, code repositories, criminal forums, and dark web sites.
- Reduce attack surface threats by identifying network vulnerabilities and weaknesses, outdated software, open ports, or expired/expiring certificates.
- Reduce time to remediate with Automated Playbooks.
- Seamlessly integrate with the ReliaQuest alert process and workflow.

Asset-Based Alerting

GreyMatter DRP provides access to the widest range of data sources and access to the expertise needed to turn that data into intelligence. We identify more than 38 pre-defined risks by monitoring online data sources including code repositories, criminal locations, social media, technical sources, and file stores.

We work with you to register your company assets for protection, including domains, brands, document markings, and key corporate employees.



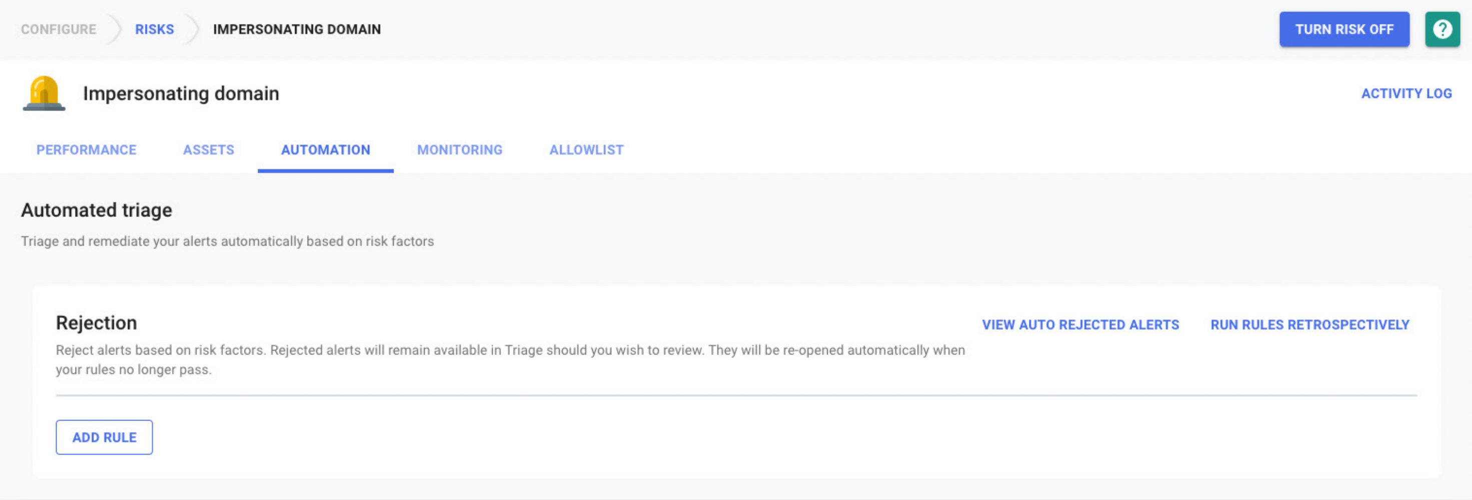
□		Title	Assignee	State	Date updated	Date raised ↓
□	H	BBCBBK Vulnerable service 65.8.158.12	Assign	Open	15 Sep 2022	15 Sep 2022
□	H	BBCBBN Evidence of resource development eternia.to	Assign	Open	11 Sep 2022	11 Sep 2022
□	H	BBCBBM Exposed port 65.8.158.12	Assign	Open	11 Sep 2022	11 Sep 2022
□	H	BBCBBL Vulnerable service 65.8.158.12	Assign	Open	11 Sep 2022	11 Sep 2022
□	H	BBCBBV Evidence of adversary impact twitter.com	Assign	Open	11 Sep 2022	11 Sep 2022
□	H	BBCBBT Selling unauthorized goods mpgh.com	Assign	Open	11 Sep 2022	11 Sep 2022

Integration with the ReliaQuest Portal

Powerful Digital Risk Protection is now available to GreyMatter customers providing a unique 360-degree view of security threats both inside and outside of the organization. If a risk is detected, GreyMatter DRP customers receive context-rich alerts with clear response steps via the ReliaQuest portal alert process and workflow, including alert assignment, automated actions, and mitigation recommendations.

Automated Playbooks

GreyMatter DRP makes working with threat intelligence insights simple, facilitating action through a combination of prebuilt playbooks and automation features that reduce triage workloads. With these capabilities, security teams spend up to 70% less time on triage.



Automated triage

Triage and remediate your alerts automatically based on risk factors

Rejection

Reject alerts based on risk factors. Rejected alerts will remain available in Triage should you wish to review. They will be re-opened automatically when your rules no longer pass.

Vulnerability Intelligence

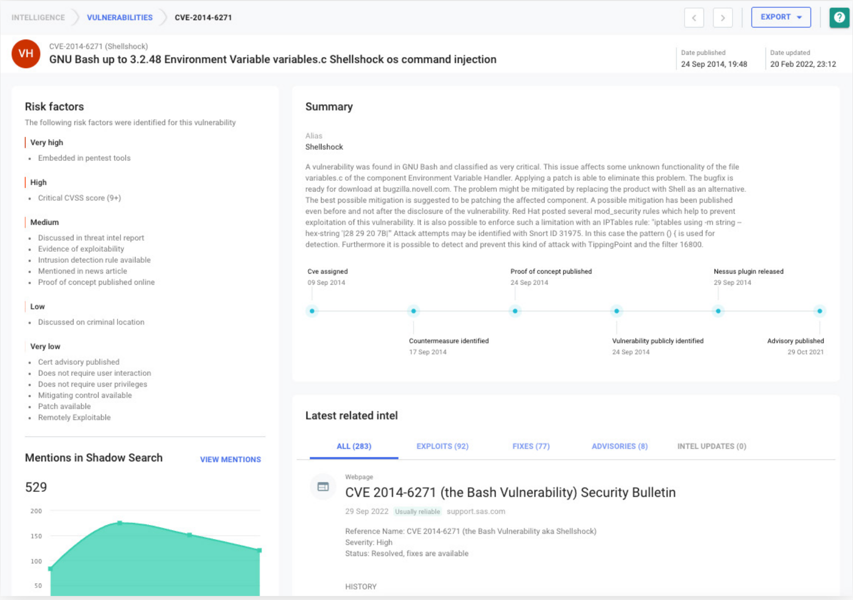
GreyMatter DRP customers have unlimited access to the SearchLight Intelligence Repository, which includes intelligence updates, actor profiles, MITRE techniques, and a vulnerability intelligence module. The vulnerability intelligence module helps to prioritize vulnerabilities, enabling users to quickly identify which vulnerabilities to respond to first. With intuitive filters built into the dashboard, users can search for Common Vulnerabilities and Exposures (CVEs), Common Platform Enumerations (CPEs), product families, and vulnerability aliases to get intelligence on specific areas of interest.

How It Works

GreyMatter DRP has four stages. At each of these stages, GreyMatter acts as an extension of an organization's security team to help identify and configure its key assets, collect from hard-to-reach sources, analyze and detect risks, and mitigate impact.

Configure

Register company assets for protection, including domains, brands, document markings, and key corporate employees. GreyMatter DRP will automatically discover domains and code repository assets to ease the load, and GreyMatter DRP users benefit from a dedicated Asset API.



CVE-2014-6271 (Shellshock)

GNU Bash up to 3.2.48 Environment Variable variables.c Shellshock os command injection

Date published 24 Sep 2014, 19:48

Date updated 20 Feb 2022, 23:12

Risk factors

The following risk factors were identified for this vulnerability

Very high

- Embedded in pentest tools

High

- Critical CVSS score (9+)

Medium

- Discussed in threat intel report
- Evidence of exploitability
- Intrusion detection rule available
- Mentioned in news article
- Proof of concept published online

Low

- Discussed on criminal location

Very low

- Cert advisory published
- Does not require user interaction
- Does not require user privileges
- Mitigating control available
- Patch available
- Remotely Exploitable

Mentions in Shadow Search

529

Summary

Alias

Shellshock

A vulnerability was found in GNU Bash and classified as very critical. This issue affects some unknown functionality of the file variables.c of the component Environment Variable Handler. Applying a patch is able to eliminate this problem. The bugfix is ready for download at bugzilla.novell.com. The problem might be mitigated by replacing the product with Shell as an alternative. The best possible mitigation is suggested to be patching the affected component. A possible mitigation has been published even before and not after the disclosure of the vulnerability. Red Hat posted several mod_security rules which help to prevent exploitation of this vulnerability. It is also possible to enforce such a limitation with an IPTables rule: "iptables using -m string --hex-string '|28 29 20 7B|'" Attack attempts may be identified with Snort ID 31975. In this case the pattern () { is used for detection. Furthermore it is possible to detect and prevent this kind of attack with TippingPoint and the filter 16800.

Cve assigned 09 Sep 2014

Countermeasure identified 17 Sep 2014

Proof of concept published 24 Sep 2014

Vulnerability publicly identified 24 Sep 2014

Nessus plugin released 29 Sep 2014

Advisory published 29 Oct 2021

Latest related intel

Webpage

CVE 2014-6271 (the Bash Vulnerability) Security Bulletin

29 Sep 2022 Usually reliable support.sas.com

Reference Name: CVE 2014-6271 (the Bash Vulnerability aka Shellshock)

Severity: High

Status: Resolved, fixes are available

Collect

We utilize insights from the widest collection of sources across the open, deep, and dark web. GreyMatter DRP comprehensive alerting options ensures no stone is left unturned.

Detect

A combination of technology and analysts, alongside automated playbooks, removes more than 95% of noise and provides a prioritization score.

Alert

Built-in playbooks, context, takedown options, and integration with the ReliaQuest alert process ensures a rapid response with recommended actions.

Additional Solutions

Managed Takedown Service

By identifying malicious brand, company, and executive impersonations of your organization as well as threat actor mentions and data leaks, ReliaQuest proactively mitigates threats to your company name and brand(s) online. The Managed Takedown Service provides customers end-to-end management of submitting, chasing, and confirming takedown requests across all available risk categories.