RELIAQUEST

SOLUTION BRIEF

RELIAQUEST FOR SECURITY INFORMATION AND EVENT MANAGEMENT PRODUCTS

Security Information and Event Management (SIEM) products are a critical component of a comprehensive cybersecurity strategy. Originally conceived to ease the analysts' burden of security alert management, they ingest data from disparate security tools from across the enterprise, then aggregate and correlate it for review. IBM QRadar, Splunk, and LogRhythm are established and well-known SIEM products. While these solutions are very effective in aggregating and correlating events, they can be challenging to deploy and keep optimized to derive continuous value. They each have their own proprietary query languages and require dedicated support to continuously optimize and reduce noise. Detection rules need to be curated and constantly updated for specific environments, and correlating events across hybrid environments is not optimized. ReliaQuest helps organizations get the most out of their SIEM tools by getting them operational, keeping them continuously optimized against a changing threat landscape, and tuning them to detect and respond to sophisticated attacks as part of an enterprise security strategy.

Drive Maximum Value from Your SIEM Investments with ReliaQuest

ReliaQuest detection developers specialize in tuning existing detection rules and adding detected IOCs for highest fidelity while developing new ones curated to the customer organization. The focus is on efficient data consumption and relieving the analyst of learning proprietary query languages. Using a cloud-native platform, GreyMatter, data from SIEM investments are unified with other sources across cloud, hybrid and on-premises, such as EDR, CASBs, threat intelligence and any other technologies to provide context, enrich investigations, and drive fast response for proactive protection, leveraging built-in automation plays.

ReliaQuest continuously monitors tools under management to ensure events are being received and parsed properly and system performance is within utilization ranges and responsiveness. Customers save time and maximize their investments with complete management of these tools including software upgrades, performance tuning, and troubleshooting.

BENEFITS:

- Continuously tune and optimize detection content to reduce noise and identify emerging threats
- Ensure optimal performance with continuous monitoring of health and system performance
- Drive faster insights by enhancing SIEM alerts with contextual telemetry from other security tools and threat intelligence
- Relieve security teams from learning proprietary query languages
- Leverage early warnings from learnings from our global customer base to proactively protect your organization

Key Capabilities

24/7/365 monitoring: Leveraging its cloud-native GreyMatter platform, ReliaQuest offers continuous monitoring of SIEM tools for real-time situational awareness improving alerts prioritization and support for higher fidelity investigations.

Comprehensive threat protection and response: Leverage ReliaQuest MDR services and Open XDR technology to centralize alerts, reduce false positives, drive fast response, and stay ahead of evolving threats.

Continuous tuning and development of detection rules: Stay ahead of threats and reduce the impact of events with curated detection rules, plus continuous updates based on non-stop research and learning from across a growing customer environment.

Monitor for health and system performance: Detect and rectify any outages and degradations by continuously monitoring technology for optimal operations, responsiveness, and systems performance.

Save time with managed integrations: Ensure currency of technology with timely patching, performance tuning, troubleshooting for any core components, software updates, and maintenance, including installation and testing of vendor product upgrades.

Get proactive with threat hunting: Leverage automated threat hunting packages developed from learnings across a wide customer base to identify IOCs and be prepared to prevent attacks.

Leverage automation across the security lifecycle: Automation playbooks for data enrichment, containment, investigation and remediation help reduce analyst fatigue and reduce response times.

MITRE ATT&CK framework mapping: Mappings to MITRE ATT&CK framework and Kill Chain stages help plot coverage and uncover areas for focus to improve security posture.

Industry peer benchmarking: Know how you are doing against your peers when it comes to visibility, team performance, and tool fidelity.

Customer success focus: Gain a dedicated customer success manager who gives you personalized attention, ensuring our services are curated to your needs and exceed your expectations.

Sample Threat Types and Example Use Cases

SAMPLE THREAT TYPES	EXAMPLE USE CASES
Credential access: Detects techniques threat actors leverage to steal credentials such as account names and passwords.	Shadow file access, password spraying, pass-the-hash attack detection, Kerberoasting activity detection
Execution: Detects techniques threat actors leverage to execute controlled code on a local or remote system.	Scheduled task creation, PSEXEC pivoting, service account interactive logon, LOLBIN leveraged
Persistence: Detects techniques threat actors leverage to maintain access to systems across restarts, credential changes, etc.	WMI persistence, sudo file modifications, scheduled task changes, shim injections
Privilege escalation: Detects techniques threat actors leverage to gain higher-privileged permissions on a system or network.	Local admin creations, cloud root account usage, UAC bypass detection, service registry modification, setuid privilege escalation reconnaissance
Defense evasion: Detects techniques threat actors leverage to avoid detection throughout their compromise.	Audit log clearing and log file editing, HISTFILE modification, abnormal PowerShell creation, AMSI bypasses
Exfiltration: Detects techniques threat actors leverage to retrieve data from an environment.	DNS TXT beaconing, ICMP exfiltration, outbound file transfer connections, abnormal removable drive usage
Discovery: Detects techniques threat actors leverage to gain knowledge about the system and internal network.	Internal port scan, account guessing, malicious zone transfer