RELIAQUEST

SOLUTION BRIEF

RELIAQUEST FOR NEXT-GENERATION SIEM PRODUCTS

Security Information and Event Management (SIEM) products ingest data from disparate cybersecurity tools from across the enterprise, aggregate the related data, and present it for review. But many traditional SIEM products have been architected with on-premises tools and traditional perimeter-based security strategies in mind. As organizations move to the cloud, it's challenging for SIEMs to keep up with the volume and diversity of events from newer cloud-based technologies. As an answer to overcoming this issue, a new generation of SIEM tools, cloud-native and focused on cloud telemetry, have cropped up. Devo, Microsoft Sentinel, and Sumo Logic are some of the products that are getting increased attention. But these tools still suffer from some of the same challenges extended by their traditional counterparts – proprietary query languages, generic detection rules, and shortages of dedicated, well-trained staff to manage and mature. ReliaQuest helps organizations get the most out of their traditional and next-generation SIEM tools by rapidly maturing the operational effectiveness and increasing the breadth and depth of threat alerting and detection efficacies, as part of an enterprise security operations program.

Drive Maximum Value from Your SIEM Investments with ReliaQuest

The advent and rapid adoption of cloud technologies has dissolved the traditional enterprise perimeter and expanded the attack surface. The security industry has answered this by developing cloud-focused cybersecurity tools, but the traditional problems remain. These products require a sophisticated skill set to manage and keep operational, and while vendors provide a set of detection rules and associated data models, they need to be curated for specific environments to be effective. Additionally, it is critical to continuously develop and deploy new detection rules to keep up with the dynamic threat landscape and IT environment.

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. With full access to constantly updated detection library, analysts are relieved from learning proprietary query languages while staying ahead of threats. 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.

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

ReliaQuest continuously monitors tools under management to ensure events are being received and parsed properly. It monitors system performance to be within utilization ranges and responsiveness for event processing, throughput, data archival, and report performance. Troubleshooting, proactive maturity of integrations as the cloud technologies are enhanced, and an eye on data integrity help drive confidence in detections.

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, conduct investigations, 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, excessive account lockouts, Kerberoasting activity detection
Execution: Detects techniques threat actors leverage to execute controlled code on a local or remote system.	PowerShell remote execution, execution bypasses, service account interactive logon, removable drive followed by execution
Persistence: Detects techniques threat actors leverage to maintain access to systems across restarts, credential changes, etc.	Local admin creations, AWS admin account creation, reverse web shell request, WMI persistence via event filters
Privilege escalation: Detects techniques threat actors leverage to gain higher-privileged permissions on a system or network.	Sensitive plist modification, Meterpreter getsystem pipe, AWS root account usage, self-generated IAM access key
Defense evasion: Detects techniques threat actors leverage to avoid detection throughout their compromise.	Abnormal compiler execution, double extension process, log clearing with WevtUtil, AWS EBS default encryption disabled
Exfiltration: Detects techniques threat actors leverage to retrieve data from an environment.	DNS TXT beaconing, rclone config creation, Tor exit node traffic, outbound file transfer connections