RELIAQUEST

SOLUTION BRIEF

RELIAQUEST FOR USER ENTITY AND BEHAVIORAL ANALYTICS PRODUCTS

As exploits and attack techniques become more and more sophisticated, security defenders have augmented their traditional signature-based detection capabilities with behavior-centered analysis. Well-known User Entity and Behavior Analytics (UEBA) products include Exabeam, and Securonix. While these solutions are effective in identifying malicious activities and emerging attack strategies, they need to be constantly tuned and curated to specific environments based on their risk appetite and concerns. Many times, security teams either do not have the time or the skills to train and operate these sophisticated products resulting in underutilization of these investments. ReliaQuest helps organizations get the most out of their UEBA tools by getting them operational and keeping them tuned and optimized so they can detect and respond to sophisticated attacks as part of a comprehensive security strategy.

Empower Your UEBA Investments with ReliaQuest

While behavioral analytics have proven to be a critical part of threat detection and analysis, many security teams are challenged to implement, optimize, and derive value out of these products. The products provide rich use cases and data models, out of the box, but they are not curated to the needs and challenges faced by individual organizations. Additionally, a changing threat landscape demands newer detection rules to protect the enterprise.

ReliaQuest detection developers specialize in tuning existing detection rules and adding detected IOCs for highest fidelity. Using a cloud-native platform, GreyMatter, data from UEBA investments are unified with other sources such as SIEM, EDR, CASBs, threat intelligence, and any other technologies to provide context, enrich investigations, and drive fast response for proactive protection.

BENEFITS:

- Tune and optimize analytics models to ensure highest-fidelity detections and reduce noise
- Ensure optimal performance with continuous monitoring of health and system performance
- Combine the power of behavioral analysis with signature-based detection for faster insights
- Leverage 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 and system performance is within utilization ranges and responsiveness. ReliaQuest validates all software updates, upgrades, and patching to ensure optimal performance of the technology, assuring longevity of and maximizing returns in security investments.

Key Capabilities

24/7/365 monitoring: Leveraging its cloud-native GreyMatter platform, ReliaQuest offers continuous monitoring of UEBA 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 of behavioral detection rules: Stay ahead of threats and reduce the impact of events with behavioral detection use cases configured to your 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.

Improve fidelity with curated detection content: Continuously updated detection content helps reduce noise and identify threats that are specific to your environment.

Leverage automation across the security lifecycle: Automation playbooks for data enrichment, containment, investigation, and remediation help reduce analyst fatigue and reduced 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
Privileged user abuse: Undesirable or illegal actions by users with higher level access of IT systems.	• Tracking authentication and access • Compromised account detection • High valued assets access
Exfiltration of data/data leak: A primary concern of organizations where sensitive PII, PHI, and PCI data is stolen.	• Monitoring suspicious outbound activity • Download/access of large amounts of information
Infiltration: Methods used to penetrate an organization's cloud services via account hijacking, network, or systems.	• Impossible traveler scenarios • Abnormal authentication scenarios • Abnormal domain access
Exploitation: Detection and protection against attack methods such as metadata service abuse, resource hijacking, backdoors, and others.	• Unusual program access/installation • Compromised host/system detection

RELIAQUEST

Make Security Possible™

(800) 925-2159 www.reliaquest.com info@reliaquest.com