Q-Behavior Analytics and Audit (Q-BA²)

Enterprise-Grade User Behavior Analytics and Insider Threat Detection

Proactively Detect & Mitigate Insider Threats with AI-Driven User Behavior Analytics

Qmulos' Q-Behavior Analytics and Audit (Q-BA²) is an advanced user behavior analytics (UBA) and audit solution designed to meet the mission-critical security needs of government agencies and commercial enterprises. Built on the intelligence community's gold standard for insider threat detection, ICS 500-27, Q-BA² delivers real-time, data-driven insights to proactively identify, investigate, and mitigate security threats across your network.

Powered by Splunk machine data and enriched with artificial intelligence (AI)/machine learning (ML), Q-BA² delivers continuous monitoring, anomaly detection, and dynamic alerting, empowering security and compliance teams with unparalleled visibility into user activities.

Key Capabilities & Benefits

ENTERPRISE-GRADE USER BEHAVIOR ANALYTICS

- **Early Threat Detection** – Detects anomalous user behavior in real-time using AI/ML-driven analytics.
- **Risk-Based Alerts** – Triggers alerts based on risky behavior to quickly identify insider threats and potential security breaches.
- **Comprehensive Visibility** – Provides security teams with rich insights via comprehensive actionable dashboards

AUDIT & COMPLIANCE READINESS

- Prescriptive audit policy as the foundation for complete and quality data
- Meets ICS 500-27, NIST, and FedRAMP audit standards out of the box.
- Reduces manual efforts & compliance costs with automated audit logging.
- Satisfies auditors with defensible, real-time security event tracking.

ADVANCED THREAT HUNTING & INCIDENT RESPONSE

- **Continuous Monitoring** – Monitors all user and host activity to detect privilege abuse, unauthorized access, and data exfiltration.
- **Score Risky Users and Hosts** – Prioritizes threats based on behavioral patterns and security context.
- **Rapid Investigation & Response** – Security teams can triage alerts and respond to threats before damage occurs.

WHY CHOOSE Q-BA²?

- Typical time to value is two weeks or less*
- Out-of-the-box compliance with ICS 500-27, NIST, FedRAMP, CMMC, SOC2, and other frameworks
- Real-time detection & alerting for insider threats & anomalous behavior
- Seamless integration with Splunk for enhanced audit and security insights
- Proactive threat mitigation through AI-driven user behavior analytics
- Scalable and customizable to fit mission-critical enterprise environments

*Splunk instance and data source dependent

User Behavior Analytics: Key Features

Q-BA² DETECTS AND ALERTS ON	EXAMPLES OF ANOMALOUS ACTIVITIES
Unauthorized Access	Admin/root access abuse, role escalation
Lateral Movement	Unusual login patterns, unauthorized system access
Data Exfiltration	Printing sensitive data, exporting/importing files
Malicious Insider Activity	Privileged user misuse, policy violations
External Media Usage	Reads/writes from unauthorized devices

QmulosQ-BA²'s real-time alerting and forensic investigation tools enable Security Operations Centers (SOCs) to quickly identify threats, mitigate risk, and safeguard critical assets.

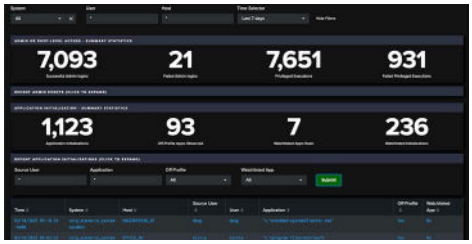
SUMMARY DASHBOARD

- Updates customers regarding data sources and alerts if sources stop generating data.
- Gives customers the flexibility to monitor all recent events across all event families.
- Features a historical summary and the option to dynamically change custom features.

EVENT DETAILS

- Monitor and audit events and activities in each event family.
- Key metrics help to establish baselines and identify anomalies.
- Detailed event-level views of recent activity for analysis.

INVESTIGATION DASHBOARD



- Investigate activities of specific users.
- Investigate events on critical endpoints.
- Query and analyze event data to identify malicious events.

Contact Qmulos

For more information on Q-BA² visit Qmulos.com or reach out to our team today.