Q-Audit

Enterprise Audit for Mission Critical and Insider Threat Initiatives

Q-Audit: Analytics for Enterprise Audit, Based on The Gold Standard for Audit Policy

At Qmulos, we are committed to offering an out of the box, prescriptive audit policy that holistically defines what one should audit and log on their network to support compliance efforts. Powered by Splunk for scalability on the largest enterprises, Q-Audit supports compliance efforts, informs security operations, and enables insider threat detection efforts with the ability to monitor, analyze, and alert on anomalies. Q-Audit provides an enterprise class solution with access to real time analytics and alerts with support for enterprise, cloud, and hybrid environments.

Today, National Security Systems are mandated for enterprise audit capabilities based on the Intelligence Community Standard (ICS) 500-27. We have adopted the intelligence community's current gold standard for insider threat audible events as well as NIST, DoD, NISPOM, and commercial audit best practices and built Q-Audit to give our customers the premier software to monitor their network. The app is defensible to auditors, improves security in real time, and gives providers ultimate visibility through customizable dashboards.

By leveraging machine data, coupled with insider threat analytics and dynamic alerting, Q-Audit provides immediate feedback on anomalies and drives risk decisions and risk reduction actions on a near real-time basis, with real-time dashboards for executives, operational security, risk, and compliance staff.

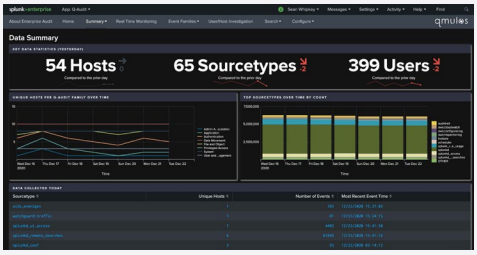
ADVANTAGES

- Out-of-the-box Compliance for **ICS 500-27, NIST, and FedRamp Audit Controls**
- **Reduces** manual efforts & costs
- **Identifies** potential insider threats
- **Alerts** on suspicious events
- Monitors analytics in **real-time**
- **Investigates** malicious activity
- Quick **time-to-value**
- **Satisfies** the auditors

ICS 500-27 AUDITABLE EVENTS

- Authentication events
- File & object events
- Writes/Reads to external devices & media
- User management events
- Group management events
- Use of privileged & special rights
- Admin or root-level access
- Privilege & role escalation
- Audit & log data access
- System reboot & shutdown
- Print to a device
- Print to a file
- Application initialization
- Export of information
- Import of information

SUMMARY DASHBOARD

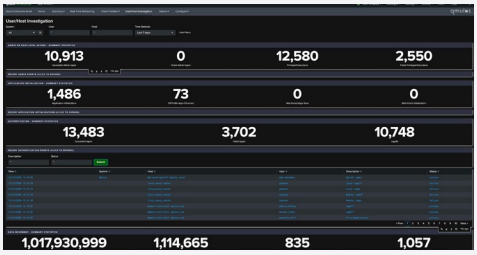


- Updates customers regarding data sources & alerts if sources stop generating data
- Gives customers the flexibility to monitor all recent events across all event families
- Features a historical summary and the option to dynamically change custom features

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