ADVANCED THREAT MANAGEMENT

EXCLUSIVE SIEM/MDR/ UEBA HYBRID

SD-IQ BENEFITS SUMMARY

- Robust Advanced Threat Intelligence
- Real-Time Threat Management Detection and Response
- Distinct Threat Recognition - Only Credible, High Priority Threats
- Data Analytics that Go Beyond Rules & Analysis from Other External Engines
- Advanced Artificial Intelligence with Actionable Remediation Information - Continuous Learning About Normal Network Activities
- 24x7 SOC Monitoring and Management - Proactive Automated and Human Interactive Resolutions
- Organization-wide Situational Visibility
- Adaptive & Comprehensive Visualization
- Powerful Compliance Reporting
- Customizable Alert and Remediation Policies

SDIQ

Introducing SD-IQ.

More Efficient than SOC. Superior to SIEM. Beyond CLM & UEBA. And Faster than MDR.

SD-IQ is an advanced threat management that visualizes, detects, and eliminates threats in the network—in real-time.

Features and Benefits

SD-IQ is the powerful complement to a Next Generation Firewall (NGFW) secured perimeter defense plan enabling both gateway and in-network security. It adds unparalleled visibility into East-West, as well as North-South traffic throughout the network, regardless of network size or design.

SD-IQ combines:

1. Comprehensive Visibility:
- Ingests raw streaming data (Flows, Logs, Identity), with millions of enrichment features
- Logically auto discovers and creates asset groups
- Works transparently with encrypted traffic

2. Proactive Threat Detection:
- Dynamic Threat Engines
- ML + AI with actionable intelligence combined with leading feature engineering for threat detection of known and unknown threats
- Zero-Day, Zero-Trust Models

3. Containment & Elimination:
- Auto-Remediation of threats in real-time
- Provides clear actionable steps to eliminate threats
- >50% SOC productivity improvement

4. Compliance Analytics & Reporting:
- Reports for regulatory compliance (HIPAA, PCI, NIST, FINRA, GDPR, etc.)
- Security operation and investigation support
- Long-term data analytics

SD-IQ installs and is fully functional "out of the box." (virtual or premise-based).
- There is minimal, if any, provisioning.
- There are no rules to import and customize.
- No signatures to pull in.
- No complicated filters that need optimization.

Once in place, SD-IQ's machine learning and heuristics-enabled collector and analytic "engine" immediately begins to absorb behavioral patterns and traffic flow to establish and recognize normal network activity.

Please contact us at **800.729.1316**, or email: **SDIQ@securedesigns.com**