NightOwl

Over a decade of real-world experience makes Secure-IQ's NightOwl the industry's leading Security Information and Event Manager (SIEM) for corporate and enterprise networks. Our intuitive user interface and advanced event correlation capabilities help protect valuable network and computing resources without adding staff. With 56 separate detection algorithms, our event correlation engine separates real security threats from false positives.

Built from the ground up with scalability, performance, and intelligence in mind.

The ideal security management platform for service providers and MSSPs.

No costly third party software licensing fees.

Capabilities

+ Pinpoint accuracy and rapid threat detection help customers identify and isolate security breaches as they happen
+ Open source database keeps pricing low as the number of monitored devices increases
+ Integrated trouble ticket system
+ Designed to handle extremely large volumes of firewall and IDS event information
+ Infinite Horizontal Scalability™ makes it easy to increase system capacity and resiliency by adding servers in parallel
+ Software installs on industry standard Wintel hardware on standalone and blade servers and VMware virtual machines
+ Extensive reporting capabilities including message and ticket volume trends

Benefits

+ Dramatically improved security and reduced threat exposure through early detection
+ Affordable pricing structure in comparison with other SIEM solutions
+ Simplified training requirements and reduced staff levels with our intuitive dashboard user interface
+ Strong revenue generation for Managed Security Service Providers
+ Support for all major brands of network components, including firewalls, VPNs, and intrusion detection systems
+ High performance database responds rapidly under heavily loaded conditions
+ Various installation options, including on-premise, MSSP, and remote management
+ Designed for white labeled sales

Specifications

+ Key Features
- Alert reduction, ticket reduction
- Improved security analyst effectiveness
- Improved incident response time and reconciliation
- Advanced data replication and segregation
- Improved security posture awareness
- Infrastructure behavior trending
- High system availability with fault tolerant architecture
- Linear pricing as the number of monitored devices increases
- No third party software licensing fees

+ Core Capabilities
- Receives Syslog events
- Receives and supports SNMP
- Receives and supports Checkpoint LEA
- Archives pre-filtered events
- Filters non-security related events
- Generates reports
- Generates alerts
- Generates alerts based on historical trends
- Easily create customized alert signatures
- Correlate events on one or more devices into a single alert
- Advanced data replication and segregation

+ Service Components
- Sentinel, models 1200, 1408, and 2412
- Gateway
- Database
- Intelligent Correlation Engine (ICE)
- Security Portal
- Customer Relationship Management

+ Supported Security Devices
- Cisco ISR, ASA, and PIX series
- ISS Proventia
- Fortinet
- Checkpoint VPN-1 Pro and VPN-Edge Series, Firewall-1 Express
- Juniper NetScreen
- ISS RealSecure

+ Security Console (Dashboard) Tracking Components
- Service Metrics
- Alert Conditions
- Security News
- Unresolved Problem Ticket Status
- Change Request Status
- IDS Device Status
- Message and Ticket Volume Trends
- Top Sources
- Top Countries

+ System Administration
- Fine grain security policy
- Multi-layer user administration, 4 levels
- Built-in two factor token-based authentication
- User customizable dashboards

+ IDP/S Report Types
- Executive summary report
- Weekly service summary report
- Top signature classification report
- Top attacking source IPs report
- Top attacked destination IPs report
- Top attacked ports/services report
- Security analyst summary report
- Compliance reporting

+ Server Platform
- Runs on industry standard Wintel server hardware
- Available as software for installation on customer provided servers, blade servers, or VMware virtual machines
- Linux operating system with Java JRE 1.5 or above

+ Hardware Requirements
- Minimum dual core 2.00 GHz processor
- 4GB RAM memory
- 500GB local storage
- Dual NICs (preferred)

+ API
- Communicate with external applications via JDBC, ODBC, Remedy API, etc.

+ Supported Web Browsers
- Microsoft Internet Explorer 7 and 8
- Mozilla Firefox 3 and 4

About Secure-IQ

Secure-IQ is a leading global provider of network security solutions. Built to perform reliably on a 24x7x365 basis, our products and services are used in some of the world's largest carrier networks, including AT&T, BT, and Tata Communications. Our pioneering technology and streamlined workflow processes help companies save money through improved operational efficiency and reduced staff levels. The high performance and intelligence built into all of our products is the end result of our many decades of collective network security experience. It is your assurance of our unwavering commitment to quality, innovation, and customer satisfaction.

All trademarks are the property of their respective owners. ©2011 Secure-IQ