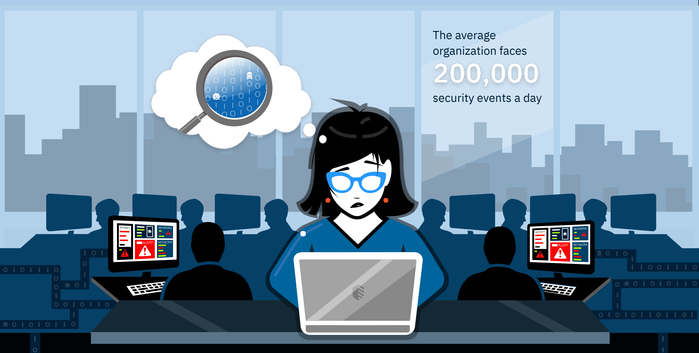
IBM Security

Transforming Noise to Knowledge

With security teams stretched thin and facing an ever-growing stream of threat data, today's analysts are overwhelmed.



A stream of threats and vulnerabilities

Security analysts are faced with thousands of vulnerabilities, threats and attacks each day. QRadar cuts through the network noise to focus on the security events that matter so that security teams can swiftly take actions to defend against them.

USERS

CLOUD

NETWORK

ASSETS

Interpret Data

Normalize log and network flow data in a consistent format for more robust analysis.

Profile Activity

Baseline asset, user, service and network activity to learn normal patterns and enable accurate anomaly detection

Advanced Analytics

Pattern Analysis
Analyzes event attributes in real-time against patterns of known malicious activities to quickly identify and classify active threats.

Anomaly Detection
Detects "normal" behavioral patterns over time and identifies deviations from the known normal that may indicate a threat.

Historical Analysis
Many attackers skip normal steps in an attempt to breach systems. When certain actions are not preceded by expected behavior, historical analysis can flag them for attention.

Statistical Analysis
Statistically analyzes entity behavior to help identify outlying, potentially compromised systems, such as endpoints sending abnormally large amounts of data to unauthorized cloud services.

Entity Behavior
Continuously monitors machine entities for anomalous behaviors, services and connections to more effectively detect compromised systems.

Threshold Analysis
Analyzes activity volumes to identify deviations from the norm, such as increases or decreases across things like bandwidth or service usage.

User Behavior Analysis
Continuously analyzes individual user behavior to detect deviations that can help identify compromised user credentials and malicious insider activity.

Threat Intelligence
Compares event attributes against up-to-date threat information, such as malicious domains or hashes, to more accurately identify the latest known threats.

Forecasting Analytics
Uses a behavioral forecasting model to predict future behaviors and detect when actions or behaviors deviate from what's expected.

Peer Group
Clusters users into peer groups based on similar activities, and continuously looks for anomalous behaviors to more quickly and accurately uncover high-risk or malicious users.

Alert

Fuse related signals uncovered during analysis to establish the end-to-end chain of a security event, determine the severity of the event and generate a a single alert.

Investigate

Cognitive Reasoning

Uses natural language processing to automatically create knowledge graphs, which are then used to determine the root cause, provide an attack overview and identify related IOCs.

Root Cause

Threat Actor

Dramatically improve speed, throughput and accuracy to more effectively defend against cyber attacks.

With QRadar, a security analyst can avoid the confusion and delay caused by thousands of events per day, and instead target suspected incidents with efficiency, based on clear, actionable information.

For more information, contact your IBM Business Partner:

Lighthouse Computer Services
1.888.542.8030 | info@lighthousecs.com
www.lighthousecs.com/

IBM Registered Business Partner

LIGHTHOUSE COMPUTER SERVICES