IBM QRadar User Behavior Analytics (UBA)

Automatically detect rogue and potentially compromised users to quickly contain insider threats and limit their impact.

Highlights

- Layers user behavior analytics into the IBM QRadar Security Intelligence Platform to expose and prioritize insider threats
- Includes machine learning and user behavior analytics to detect anomalous activity that may indicate an active insider attack
- Empowers security analysts to rapidly respond to insider threats by automatically measuring and rank ordering the risk associated with suspicious and potentially compromised users
- Immediately begins baselining user activity and delivers insights within 24 hours
- Downloads quickly and easily as a free application from the IBM App Exchange

High profile insider threats have made the headlines in recent years, and studies show that nearly 60% of attacks stem from malicious or accidental insider actions.[1] Trusted insiders can make costly mistakes, fall victim to phishing attacks that inadvertently provide attackers with insider access, or simply turn rogue. As a result, organizations can experience significant data loss, destruction of systems and compliance violations, among other consequences. Because of the trusted nature of authorized insiders, these threats are the most difficult to detect and most remain unnoticed for months to years.[2]

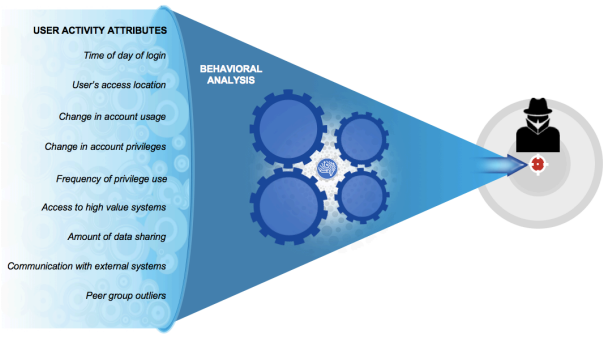
Once an attacker begins operating with insider access, one of the most effective ways to detect the threat is through behavioral analysis. IBM QRadar User Behavior Analytics (UBA) uses advanced analytics to identify early warning signs of insider threats and empower security analysts to take action before damage can be done. Using a combination of machine learning and behavioral analysis, QRadar UBA can:

- Automatically establish a baseline of normal activities
- Identify anomalous user behavior that may indicate an active insider threat
- Prioritize the highest risk users and activities in the organization
- Alert security analysts to potential insider attacks

1. IBM X-Force® Research. 2016 Cyber Security Intelligence Index.

2. Verizon 2017 Data Breach Digest Update. The Insider Threat: Protecting the Keys to the Kingdom

UBA Extension to QRadar SIEM

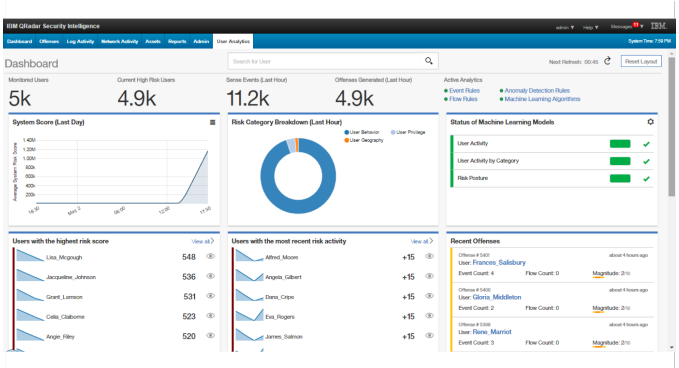


QRadar UBA, which is easily downloadable from the IBM Security App Exchange, is a free, optional component of the IBM QRadar Security Intelligence Platform. The app delivers out-of-the-box rules and algorithms that plug directly into the QRadar advanced analytics engine. This fully integrated solution is designed to add user context to log, flow and vulnerability data collected by IBM QRadar Security Information and Event Management (SIEM). Using this information, QRadar UBA establishes a baseline of normal user access patterns and activities to effectively identify outlying behaviors, generate risk scores for users, and provide security analysts with insight into high-risk and potentially compromised users.

By extending the QRadar Security Intelligence Platform with QRadar UBA, security analysts can become more productive and manage insider threats more efficiently. QRadar UBA jumpstarts an organization's ability to investigate potential insider threats. It quickly exposes high-risk activities and enables security analysts to focus their investigation efforts on specific insiders who have likely either engaged in unauthorized activity or had their credentials compromised by an external, targeted attacker.

When risky activity is discovered, analysts can drill down on any user and in one click obtain a detailed view of the actions and offenses that contributed to that person's risk score. The individual logs and flow data involved can also be viewed by simply clicking on the offense of interest. This centralized view of user activity can help shorten investigation times and enable faster response times.

QRadar User Behavior Analytics



Additionally, the IBM Security Intelligence Platform can be integrated with incident response solutions to automate response processes to reduce the amount of time needed to contain, eradicate and ultimately recover from an insider threat.

QRadar UBA provides a dedicated dashboard that aggregates user data to show information such as the number of users being monitored, high risk users, and events and offenses generated in the last hour. It also shows information on an individual basis, such as the highest risk users by name, recent offenses and risk categories.

QRadar UBA provides intelligent insider threat detection capabilities packaged as a downloadable app that is free of charge and independent of the platform's formal release cycles. All current QRadar clients can add this app to QRadar version 7.2.7 and higher releases to begin seeing a user-centric view of what is happening within their networks.

In conclusion

Insider threats are increasingly prevalent, yet incredibly difficult to detect. As part of the IBM Security Intelligence Platform, QRadar UBA uses advanced analytics to help security teams identify and quickly investigate threats that attempt to hide under the guise of well-intentioned employees. By accelerating detection and investigation processes, QRadar UBA empowers incident responders to rapidly respond to insider threats before attackers have the opportunity to steal data, disrupt business or destroy systems. QRadar UBA is available in the IBM Security App Exchange and offered free of charge to QRadar SIEM customers.

For more information

To learn more about this offering contact your IBM representative or IBM Business Partner, or visit: ibm.com

IBM Corporation

Software Group

Route 100

Somers, NY 10589

Produced in the United States of America

August 2017