IBM Security
Solution Brief

Beat insider threats with integrated user behavior analytics

Highlights:

- Detect insider threats faster, easier and more accurately using IBM® QRadar® Security Intelligence with the IBM QRadar User Behavior Analytics (UBA) app
- Leverage a user-centric view to identify at-risk users, create watchlists and calculate user risk scores—all from a single dedicated dashboard
- Monitor privileged users and high-priority assets to detect unusual or anomalous behavior that can indicate an insider threat
- Act with speed and confidence based on insights derived from advanced behavioral analytics and machine learning algorithms
- Integrate easily and quickly with enterprise directories like LDAP or Active Directory
- Download the app from the IBM Security App Exchange and obtain insights within hours

Understand the insider threat

Trusted insiders were involved in 60 percent of security incidents in 2016[1]. Yet, despite common perceptions, insider threats are typically not just malicious employees who have a grudge against their employer or are out for financial gain. Instead, most insider threats stem from well-intentioned users who either make genuine mistakes or fall victim to phishing scams, thus granting insider access to external bad actors. Regardless of who the threat actor is, once they are inside network, operating under the guise of trusted employees or contractors, they can go undetected for months or years[2] – all the while scouring your network, learning your company secrets and stealing data or money.

The best way for organizations to detect these stealthy threats is to analyze user behavior and look for anomalies that can indicate either an employee is about to go rogue or their legitimate credentials were compromised by a cybercriminal. By spotting these behavioral anomalies, security teams can detect insider threats earlier in the attack cycle and take steps to contain and eradicate the attacker before damage can be done.

Monitor user activity to detect anomalies indicative of an attack

IBM QRadar User Behavior Analytics (UBA) addresses this problem. The behavioral analytics and machine learning algorithms in UBA continuously monitor and analyze users' behavior to create a 'normal behavior' model of each user. It then identifies behaviors that deviate from this normal and are indicative of an active insider threat. Security analysts can easily keep track of high-risk users and high-risk user activity, as well as create custom watch lists for users who require continuous oversight.

[1] *"Reviewing a year of serious data breaches, major attacks and new vulnerabilities," IBM X-Force Research*

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

Stay ahead of insider threats

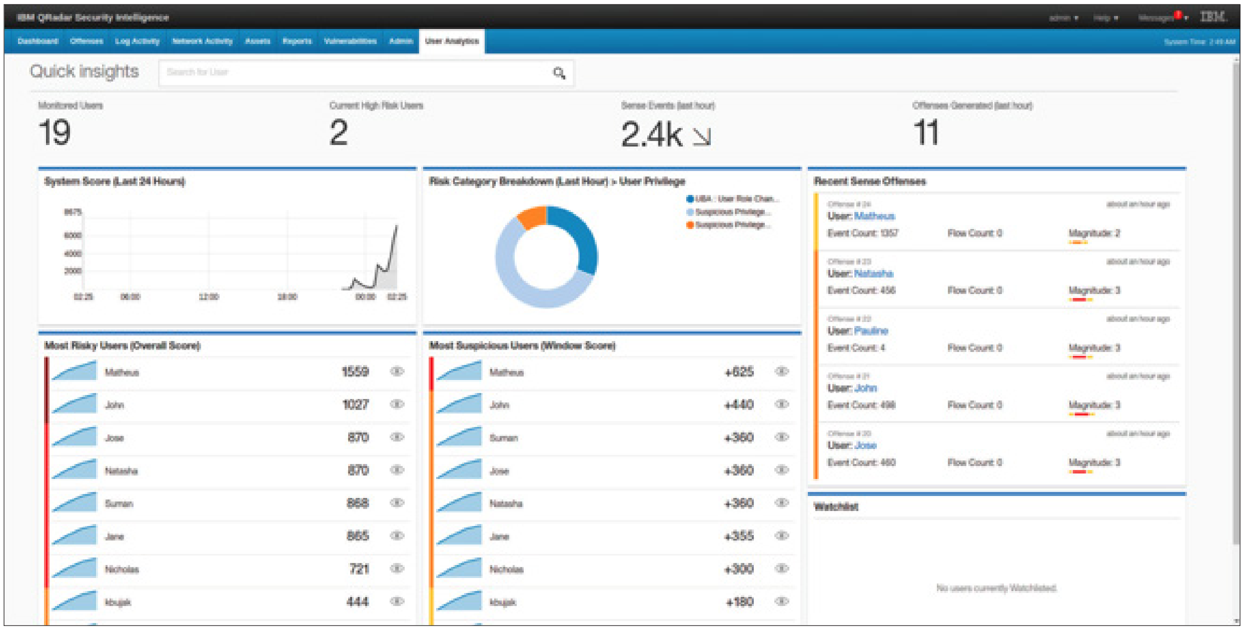
With insider threats on the rise, security teams need to monitor users and quickly investigate suspicious activity—whenever and wherever it occurs. The IBM QRadar Security Intelligence Platform helps security teams do precisely this. At the core, IBM QRadar Security Information and Event Management (SIEM) collects, analyzes and correlates data – including logs, network flows, vulnerability information and threat intelligence – to uncover threats and alert security teams to high risk incidents. QRadar User Behavior Analytics (UBA) adds user context to this information to help security teams:

- Identify high-risk insiders before they go rogue
- Expose cyber criminals operating with compromised credentials
- Monitor and manage privileged user activities
- Monitor access to intellectual property
- Understand and quantify the risk profile of the environment
- Drill down into potential threats and gain insights for corrective action

Analyze abnormal behavior

QRadar UBA continuously monitors user activity to learn what's normal both for individual users and user groups. The solution integrates with Lightweight Directory Access Protocol (LDAP) directories, and Active Directory to gain valuable insight into users and user groups. By establishing a baseline of "known normal," the solution can then detect anomalies that may indicate either a user is about to go rogue or a user's credentials have been compromised by an attacker.

Available for download from the IBM Security App Exchange, QRadar UBA seamlessly integrates into existing QRadar SIEM deployments, providing out-of-the-box analytics and algorithms designed to detect insider threats. Security analysts can customize it to assign specific point values to actions defined as risky, such as when someone visits a malicious website or set it to scale the risks automatically depending upon how much a user deviates from their own "known normal" or that of their peer groups. These points are then combined into a composite risk score for each user. A centralized, dedicated dashboard reveals details such as the top five highest risk users and a scrolling list of the most recent suspicious activities. From here, security analysts can easily keep track of the highest risk individuals or their risky activities.



Monitored Users	Current High Risk Users	Sense Events (last hour)	Offenses Generated (last hour)
19	2	2.4k ↘	11

Most Risky Users (Overall Score)

Matheus	1559
John	1027
Jose	870
Natasha	870
Suman	868
Jane	865
Nicholas	721
kbujak	444

Most Suspicious Users (Window Score)

Matheus	+625
John	+440
Suman	+360
Jose	+360
Natasha	+360
Jane	+355
Nicholas	+300
kbujak	+180

Recent Sense Offenses

Offense # 24 — about an hour ago
User: Matheus
Event Count: 1357 Flow Count: 0 Magnitude: 2

Offense # 23 — about an hour ago
User: Natasha
Event Count: 456 Flow Count: 0 Magnitude: 3

Offense # 22 — about an hour ago
User: Pauline
Event Count: 4 Flow Count: 0 Magnitude: 3

Offense # 21 — about an hour ago
User: John
Event Count: 498 Flow Count: 0 Magnitude: 3

Offense # 20 — about an hour ago
User: Jose
Event Count: 460 Flow Count: 0 Magnitude: 3

Watchlist

No users currently Watchlisted.

Figure 1: QRadar UBA dashboard

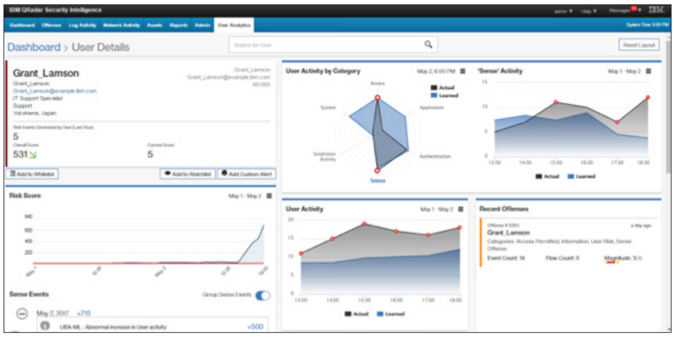
A single click on a User takes the security analyst to more detailed information to drill down into what's driving the risk score. Here, they can substantiate their observations or add the person to a specific watch list. The analyst can easily see an overview of factors contributing to that user's risk score, then quickly drill-down into specific events involving the user's actual versus predicted behavioral patterns.

Machine Learning

QRadar UBA comes with advanced behavioral analytics and machine learning algorithms that augment the robust analytics engine within QRadar SIEM. These algorithms are packaged and delivered in the Machine Learning (ML) App, which comes bundled with QRadar UBA.

Over half a dozen machine learning algorithms in the ML App analyze users' activities and creates a behavioral model for each individual user. The app ingests users' log data from the preceding 4 to 6 weeks, and within hours of installation, it understands the normal activity patterns of each monitored user. These algorithms are then able to predict users' future activities and the frequency of those activities. When a user's activities fall outside of the predicted range, the algorithms flag these activities as anomalous behavior.

Security analysts can dynamically scale the risk score assigned to users depending upon the magnitude of a users' deviation. So a user who deviates within 1 standard deviation from the normal may get 5 points, but the user who deviates 2 standard deviations may automatically be assigned a risk score of 10 points.



Grant_Lamson
Grant_Lamson
Grant_Lamson@example.ibm.com
IT Support Specialist
Support
Yokohama, Japan

Risk Events Generated by User (Last Hour): 5
Overall Score: 531
Current Score: 5

May 2, 2017 +715
UBA ML : Abnormal increase in User activity +500

Offense # 5263
Grant_Lamson
Categories: Access Permitted, Information, User Risk, Sense Offense
Event Count: 14 Flow Count: 0 Magnitude: 3/10

Figure 2: QRadar UBA user view

The machine learning algorithms in QRadar UBA can be used for:

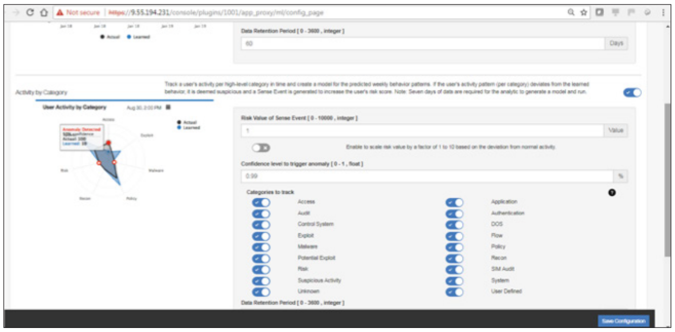
i) Detecting Users' deviation from themselves

The multi modal Gaussian analysis in the QRadar UBA app monitors users' behavior across multiple categories of events. A user's behavior is modeled in 18 different categories of user activities, such as authentication, network access, firewalls accept/denies, application activity, port or network scans, denial of service type events, malware or other malicious software activity etc. Figure 3 shows the 18 categories of activities modeled by these algorithms.

The anomalies detected by these algorithms are displayed in the form of spider charts (Figure 3) for all categories of events that the user has shown activity.

Examples of anomalies that can be detected include:

- Abnormal increase in user activity level (over time)
- Deviation in a specific type of user activity, such as an increase in authentication requests
- Deviation of the user's risk posture
- Abnormal rate of increase in the user's risky activity
- Deviation or increase in a user's local to remote activity (helps detect exfiltration activities)
- Changes made to a user's systems, software installation etc.



https://9.55.194.231/console/plugins/1001/app_proxy/ml/config_page

Data Retention Period [0 - 3600 , integer]
60 Days

Track a user's activity per high-level category in time and create a model for the predicted weekly behavior patterns. If the user's activity pattern (per category) deviates from the learned behavior, it is deemed suspicious and a Sense Event is generated to increase the user's risk score. Note: Seven days of data are required for the analytic to generate a model and run.

Risk Value of Sense Event [0 - 10000 , integer]
1

Enable to scale risk value by a factor of 1 to 10 based on the deviation from normal activity

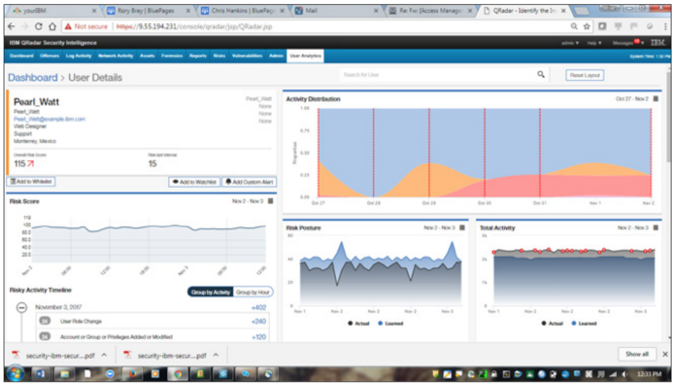
Confidence level to trigger anomaly [0 - 1 , float]
0.99 %

Categories to track

✓	Access	✓	Application
✓	Audit	✓	Authentication
✓	Control System	✓	DOS
✓	Exploit	✓	Flow
✓	Malware	✓	Policy
✓	Potential Exploit	✓	Recon
✓	Risk	✓	SIM Audit
✓	Suspicious Activity	✓	System
✓	Unknown	✓	User Defined

Data Retention Period [0 - 3600 , integer]

Figure 3: Tuning Machine Learning Algorithms



Pearl_Watt
Pearl_Watt
Pearl_Watt@example.ibm.com
Web Designer
Support
Monterrey, Mexico

115
15

November 3, 2017 +402
User Role Change +240
Account or Group or Privileges Added or Modified +120

Figure 4: Activity Distribution graph

ii) Detecting change in user's activity vs. frequency

QRadar UBA takes these machine learning algorithms a step further to understand the detailed mix of activities that a user may be engaged in and the frequency of each of these different types of activities at any given point time. Leveraging Latent Dirichlet allocation and Kullback–Leibler divergence, QRadar UBA creates an activity and frequency distribution model over time for each user.

Figure 4 shows the graphical representation of a user's activity with a frequency distribution over one week. Any time the user's activity or the frequency of that activity changes (ie. the actuals deviate from the predicted values of the algorithm), it is flagged as an anomaly.

These algorithms can help detect instances when a user's credentials are compromised or when a user with legitimate credentials changes the frequency of certain tasks he or she regularly performs. Examples of the anomalies that can be detected are:

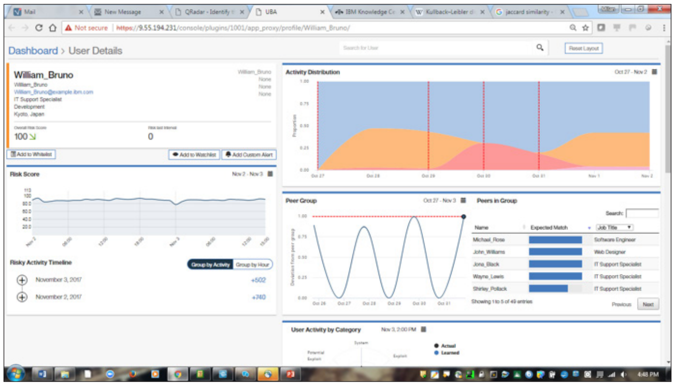
- If a person with the stolen credentials engages in different types or patterns of activity, the algorithms would immediately detect the change in activity and increase the user's risk score
- If an internal user (an employee or contractor) with legitimate credentials changes the frequency of his/her normal activity, (Ex: increased access to or download from a regularly-accessed asset) this change will be detected and the user's risk score will be raised

iii) Anomalous deviation from Peer Groups

The above referenced algorithms and analytics are very effective in understanding each individual user's behavior and detecting any time the user deviates from their normal known behavior. The third set of machine learning algorithms in the QRadar UBA take these individual users' behavior models and create behavioral clusters of similar users.

These algorithms leverage Gaussian mixture, Jaccard similarity to identify and cluster users into peer groups of users with similar activities. It then uses Kullback–Leibler divergence to detect when a user deviates from his or her peer group to sense any anomalous activity. Figure 5 shows a user's activity and their deviation from the peer group, along with the names of members of this peer group. Any time a user deviates 1 standard deviation from the peer group's normal, the app raises an anomaly and raises the users' risk score.

Peer group analytics give yet another lens into a user's activities and helps identify anomalous or malicious activity when the user deviates from a peer group of employees with similar roles and responsibilities.



William_Bruno
William_Bruno
William_Bruno@example.ibm.com
IT Support Specialist
Development
Kyoto, Japan

100
0

November 3, 2017 +502
November 2, 2017 +740

Name	Expected Match	Job Title
Michael_Rose		Software Engineer
John_Williams		Web Designer
Jona_Black		IT Support Specialist
Wayne_Lewis		IT Support Specialist
Shirley_Pollack		IT Support Specialist

Showing 1 to 5 of 49 entries

Figure 5: Peer Group analysis

Prioritize users and assets

The QRadar UBA app can prioritize both users and assets with a higher risk profile, so security teams can respond quickly to the most critical issues. Out-of-the-box rules and analytics can be customized to fit the unique requirements and risk profile of your organization. The app also enables security teams create their own rules based on organizational policies, such as segregation-of-duties and user access permissions.

Let's say an organization wants to get a handle on its privileged user activities. QRadar UBA can monitor for anomalous access by privileged users—such as the first time they access a high-value system; access during unusual times or from unusual locations; or access from a canceled, suspended or closed account. The solution can prioritize the alert on the dashboard and notify the SOC analyst so he or she can begin investigation and take appropriate remediation action.

More importantly, organizations need to be able to detect and prevent the use of stolen credentials – particularly privileged credentials. QRadar UBA can monitor for abnormal changes in account usage—such as multiple login failures; access using rarely used privileges; time-space disagreements (logging in from two different locations at the same time, for example); or account usage deviating from peer group behavior (such as making large data transfers during off-business hours, for example). Each of these anomalies can indicate that a privileged user's credentials have been compromised and are actively being used by a remote bad actor. QRadar UBA can prioritize these alerts to rapidly notify analysts of a potential compromise.

Respond to Insider Threats Faster

Detecting threats early in the attack cycle is a critical step in stopping attackers before they take off with your sensitive data or wreak havoc on your IT systems. Yet, it's only the first step. The IBM Security Intelligence Platform offers add-on apps and out-of-the-box integrations with complementary solutions to help analysts accelerate investigation times, contain attacks faster and more quickly recover from incidents.

- **QRadar Advisor with Watson** uses cognitive intelligence to help security teams dramatically accelerate investigation times. When a threat is detected, analysts can use QRadar Advisor with Watson for further analysis. Operating up to 60 times the speed of manual threat investigations, it helps show the scope of an attack, uncover new threat patterns, triage threats and identify the root cause of an attack.
- **i2 Analyze** enables security analysts to visualize activity associated with an incident and easily share analysis with fellow team members. Analysts can map out high risk users, their relationships with the organization and the actions they've taken leading up to and following an incident.
- **Identity Governance and Intelligence** shares information on user groups and user entitlements, providing context to user behavioral patterns, and can receive information regarding high risk users and activity. When a user engages in a particularly high-risk activity, the solution can be notified of the activity and automatically suspend the user's account access to avoid further damage.
- **Resilient Incident Response Platform** enables security teams to orchestrate and automate incident response processes. When insider threats are detected, security analysts can use pre-defined playbooks to orchestrate the response, contain the threat and quickly recover from the attack.

Integrated approach to stop insider threats

IBM Resilient Incident Response Platform

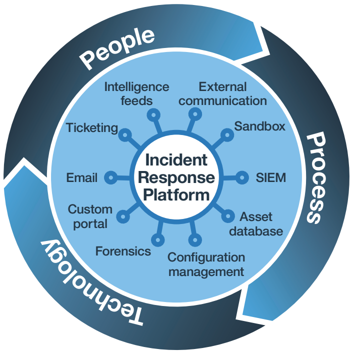
- Detects and records notable user behavior events
- Uses correlation rules engine, anomaly detection engine and reference data
- New tab and dashboard items to research “users”
- New user model to hold context and risk data about users
- Risk engine calculates user risk score from notable user behavior events

+

Risky users

At-risk assets

IBM Resilient Incident Response Platform



Realize the business benefits of integrated behavior analytics

QRadar UBA helps security leaders measure the risk associated with insider threats and track changes in the organization’s risk level over time. From a central dashboard, security leaders can see the number of users monitored by the solution, the number of high risk users in the organization and the number of high risk incidents associated with insiders.

A single platform approach to security analytics – including user behavior analytics – helps security teams reduce the risk associated with insider threats without requiring days or weeks of manual effort. The solution integrates directly into the existing SIEM solution, adding new insights to existing data sources without requiring any customization or integration work. Available for download from the IBM Security App Exchange, the app installs in minutes and can start generating insights within 24 hours.

QRadar UBA adds user context to logs, flows and vulnerability data to help security teams more quickly and accurately detect insider threats. Analysts can clearly see high-risk users, recent risky activities and the underlying events influencing a user’s risk score. Together, this information provides greater context on incidents and enables analysts to more easily investigate and respond to insider threats.

To help manage day-to-day responsibilities, the solution enables security teams to add free-form notes on users and offenses, helping analysts more easily keep track of risks in dynamic environments. Users can be added to – or removed from – watch lists as needed. From a reporting perspective, a single platform approach to security analytics means that all enterprise-wide security data stays in one place, making it easier to report on data and demonstrate compliance come audit season.

The QRadar UBA app improves the speed, efficiency and productivity of SOC analysts when analyzing insider threats.

Why IBM?

IBM Security solutions help detect, address and prevent security breaches through integrated hardware and software solutions. Powered by deep analytics and trusted IBM Security expertise, the robust IBM portfolio of comprehensive, scalable, industry-leading tools delivers unparalleled security intelligence with reduced complexity and lower maintenance costs.

In fact, the QRadar Security Intelligence Platform deploys rapidly regardless of a network's scale and begins delivering results in mere hours. Its advanced analytics engine and stored intelligence can associate related attacks emanating from the same source or corresponding to the same targeted data. QRadar delivers these actionable insights to meet both current and future needs—from advanced threat detection to insider threat monitoring, fraud detection, risk and vulnerability management, forensics investigations, compliance reporting and incident response.

In addition, QRadar Security Intelligence Platform has an open framework that enables easy integration with solutions posted on the IBM Security App Exchange (which is where the QRadar UBA app is available for download). The IBM Security App Exchange allows partners to share apps, security app extensions and enhancements to IBM Security products. All code is reviewed by IBM against set criteria before it appears on the site. Security teams can download and install the solutions at their own convenience. This way, they can apply new security use cases without adding unnecessary solution complexity.

For more information

To learn more about IBM QRadar, please contact your IBM representative or IBM Business Partner, or visit: ibm.com/security

To download the IBM QRadar User Behavior Analytics app from the IBM Security App Exchange, visit: https://exchange.xforce.ibmcloud.com/hub

About IBM Security solutions

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research and development, provides security intelligence to help organizations holistically protect their people, infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. These solutions enable organizations to effectively manage risk and implement integrated security for mobile, cloud, social media and other enterprise business architectures. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 20 billion security events per day in more than 130 countries, and holds more than 3,000 security patents.

Additionally, IBM Global Financing provides numerous payment options to help you acquire the technology you need to grow your business. We provide full lifecycle management of IT products and services, from acquisition to disposition. For more information, visit: ibm.com/financing

IBM Security
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
February 2018
All Rights Reserved