The BioCatch Analyst Station provides fraud analysts with the visibility they need in order to easily identify, investigate, and act upon potentially fraudulent activity in user accounts. This BioCatch platform component is used to facilitate post-session data analysis whenever an in-depth investigation is required.

**Context at a Glance**

The Analyst Station automatically reveals critical details related to the latest sessions including risk score, geo-location, threat indicators, user ID, and date and time. By having these key high-level insights readily available, fraud teams can gain critical context within seconds and kick off deeper investigations with ease.

**Understanding the Risk Score**

With exposure to detailed session information and analysis such as user behavioral anomalies, criminal and genuine indicators, device statistics, networks, API responses, and session flow including copy and paste activity, fraud analysts can easily understand exactly what contributed to a session’s risk score and conduct investigations more efficiently.
Armed with a powerful visualization tool that allows analysts to reconstruct exactly how the user behaved during a session, including a step by step video breakdown of user activity and detailed behavioral insights, fraud teams can gain better visibility into incidents and feel more confident in their course of action.

**Conducting In-depth Investigations**

Within the Analyst Station fraud teams can construct queries using an array of filters to facilitate in-depth investigations. The querying functionality satisfies two major use cases: complex case resolution and fraud trend visibility.

In the event a high-risk session requires additional investigation to determine course of action, fraud analysts can leverage the query and user history functionalities to gain additional context from previous sessions. For example, within the Analyst Station, fraud analysts can compare behaviors exhibited in the most recent session to the user’s previous sessions or to other fraudulent sessions to more confidently assess risk level.

Querying is also beneficial in identifying or validating fraud trends. For example, if an analyst notices an uptick in social engineering voice scams and wants to report this finding to upper management, they can easily search for all relevant sessions to showcase prevalence over time.

Further, to keep tabs on certain threats or behaviors, queries can be automated to run on a regular basis and outputs can be automatically sent to selected recipients to optimize workflow and drive regular reporting efforts.

BioCatch pioneered behavioral biometrics, which analyzes an online user's physical and cognitive digital behavior to protect users and their data. Today, customers around the globe leverage BioCatch's unique approach and insights to more effectively fight fraud, drive digital transformation and accelerate business growth. With nearly a decade of data, over 50 patents and unparalleled experience analyzing online behavior, BioCatch is the leader in behavioral biometrics. For more information, please visit www.biocatch.com