Data Sheet

Biocatch Analyst Station

Capabilities

- Monitor and investigate the latest sessions
- Access detailed session data including BioCatch behavioral insights and threat indictors
- Visualize behavioral anomalies indicative of fraud through video reconstruction
- Leverage advanced query and reporting capabilities
- View risky sessions by geo-location using a detailed map view

Benefits

- Optimize fraud investigations with access to detailed session context
- Decrease time to action by understanding the exact behavioral indicators that contributed to a session's risk score
- Drive complex case resolution using a powerful set of visualization tools
- Reveal fraud trends via automated query capabilities

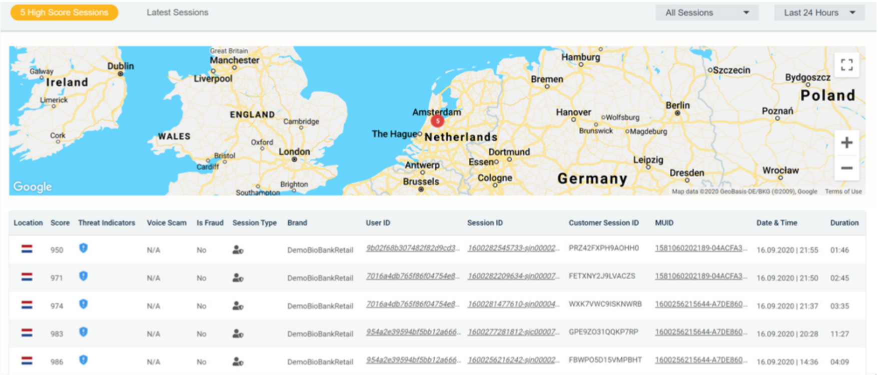
Other BioCatch Platform Components

- Rule Manager
- Case Manager

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 context within seconds and kick off deeper investigations with ease.

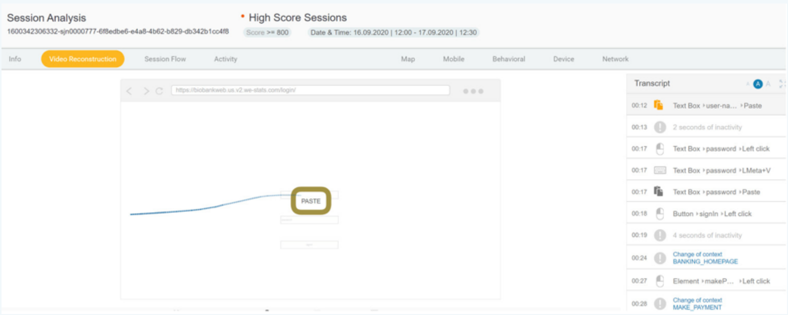


Location	Score	Threat Indicators	Voice Scam	Is Fraud	Session Type	Brand	User ID	Session ID	Customer Session ID	MUID	Date & Time	Duration
🇳🇱	950	🛡	N/A	No	👤	DemoBioBankRetail	9b02f68b307482f82d9cd3...	1600282545733-sjn00002...	PRZ42FXPH9AOHH0	1581060202189-04ACFA3...	16.09.2020 | 21:55	01:46
🇳🇱	971	🛡	N/A	No	👤	DemoBioBankRetail	7016a4db765f86f04754e8...	1600282209634-sjn00007...	FETXNY2J9LVACZS	1581060202189-04ACFA3...	16.09.2020 | 21:50	02:45
🇳🇱	974	🛡	N/A	No	👤	DemoBioBankRetail	7016a4db765f86f04754e8...	1600281477610-sjn00004...	WXK7VWC9ISKNWRB	1600256215644-A7DE860...	16.09.2020 | 21:37	03:35
🇳🇱	983	🛡	N/A	No	👤	DemoBioBankRetail	954a2e39594bf5bb12a666...	1600277281812-sjc00007...	GPE9ZO31QQKP7RP	1600256215644-A7DE860...	16.09.2020 | 20:28	11:27
🇳🇱	986	🛡	N/A	No	👤	DemoBioBankRetail	954a2e39594bf5bb12a666...	1600256216242-sjn00002...	FBWPO5D15VMPBHT	1600256215644-A7DE860...	16.09.2020 | 14:36	04:09

Analyst Station Dashboard

Understanding the Risk Score

With exposure to detailed session information and analysis such as user behavioral anomalies, criminal and genuine indicators, device statistics, and session flow, fraud analysts can easily understand exactly what contributed to a session's risk score and conduct investigations more efficiently.



Session Analysis
1600342306332-sjn0000777-6f8edbe6-e4a8-4b62-b829-db342b1cc4f8
High Score Sessions
Score >= 800
Date & Time: 16.09.2020 | 12:00 - 17.09.2020 | 12:30

00:12 Text Box › user-na... › Paste
00:13 2 seconds of inactivity
00:17 Text Box › password › Left click
00:17 Text Box › password › LMeta+V
00:17 Text Box › password › Paste
00:18 Button › signIn › Left click
00:19 4 seconds of inactivity
00:24 Change of context BANKING_HOMEPAGE
00:27 Element › makeP... › Left click
00:28 Change of context MAKE_PAYMENT

Session Video Reconstruction

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.

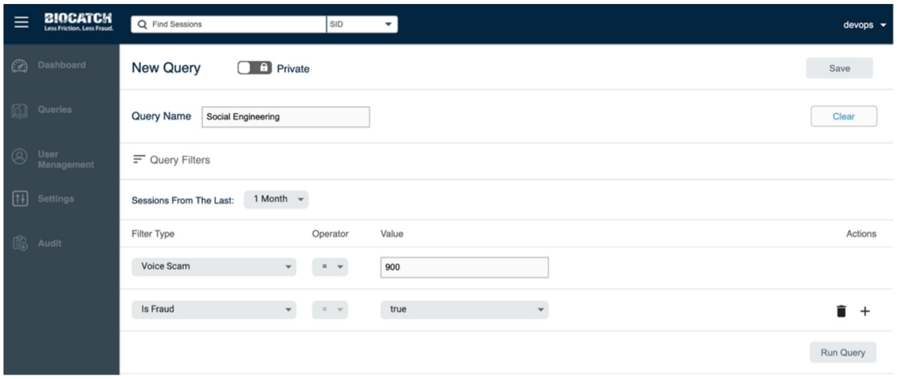
Conducting In-depth Investigations

Within the Analyst Station fraud teams can construct queries using a broad range of filters to facilitate in-depth investigations. 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.

Revealing Fraud Trends

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.



New Query
Private
Query Name: Social Engineering
Query Filters
Sessions From The Last: 1 Month

Filter Type	Operator	Value	Actions
Voice Scam	=	900	
Is Fraud	=	true	🗑 +

Querying Within the Analyst Station

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**

www.biocatch.com

E: info@biocatch.com

@biocatch

in /company/biocatch

Tel Aviv | New York | Boston | London | São Paolo | Santiago | Mexico City | Melbourne | Mumbai