NICE Actimize

Factsheet

IFM Dark Web Intelligence: Proactive Intelligence to Radically Reduce Fraud

Unrivaled combination of human intelligence and proprietary technology delivers proven ROI via drastic reduction of fraud losses and financial crimes.

Instantly actionable, customized, and continuously refreshed intelligence and monitoring across post-breach pre-fraud scenarios.

Comprehensive multilingual coverage of Dark and Deep Web, malware networks, botnets, private messaging platforms, and underground fraudster infrastructure and communities.

Transform Fraud Detection from Reactive to Proactive

- Comprehensive coverage across customer account takeovers, compromised payment cards, and mule accounts via three curated, proprietary, highly-differentiated data feeds.
- Significantly reduce operational costs in areas related to fraud prevention and investigation.
- Designed for ease of use and streamlined integration with X-Sight Connect into IFM using existing systems without any need for downstream processing or analysis.
- Conclusively detect and respond to suspicious activity throughout various interactions and transactions without inconveniencing customers.
- Build and optimize fraud prevention models according to both current and new attack vectors.
- Leverage shared intelligence to augment and empower financial crime, AML anti-fraud and information security teams.

Real-Time Intelligence. Immediate Fraud Detection

Mitigate Customer Account Takeover Attempts

Financial Institutions (FIs) can use Dark Web to combat difficult-to-detect account takeovers and a broad range of financial crimes, across all payments channels. Detect account takeover attempts in real time and immediately remediate the compromised account to prevent takeover and the resulting customer friction.

Block Mule Activity with Dark Web Monitoring

Broad, data-driven visibility into mule accounts enables FIs to detect illicit financial transaction events involving mules and take anticipatory action. Dark Web Intelligence provides an actionable data feed detailing mule accounts across FIs, including name, email address, bank account number and phone number. This threat intelligence can be deployed to ascertain if a mule account matches a customer account, if a mule account is connected with a third-party FIs, and to screen new account applications against mule data.

Combat Payment Card Fraud with Zero Customer Friction

FIs can reissue or flag payment cards that have been compromised, and anticipate and forestall occurrences of fraud before it leads to unnecessary customer friction. With a continuously generated data feed regarding jeopardized payment cards that have been stolen by cybercriminals or traded on Dark Web marketplaces, fraud losses at both card-present and card-not-present environments can be mitigated in real time. The Compromised Payment Card feed can further help FIs perform common point of purchase analyses to accurately identify merchant breaches that expose payment card data and safeguard their card portfolios.

→ Ready to get started? Learn more here.