sift

Checklist for CISOs

What to Ask, Answer, and Require to Support Your Enterprise Fraud Solution

CISOs are in a new era of expectation, with expanded responsibilities tied to reducing digital risk and growing revenue. As information security leaders refine their relationship with fraud operations to align with their expanded role, there are three mission-critical questions to explore:

1. *What are the biggest challenges you face in detecting and preventing attacks such as account takeovers (ATO) and account opening/account creation fraud (AO)?*
2. *How are you leveraging CIAM and consumer identity in downstream fraud operations?*
3. *How do you measure the efficacy and resilience of your fraud prevention stack?*

With these questions answered, CISOs can offer their endorsement of a fraud prevention solution. The following checklist is designed to help infosec leaders compare functionality across platform types, identify gaps, and directly tie risk operations to increased order acceptance, ROI, and revenue with the right platform.

1 | AI-POWERED Fraud Decisioning

AI-powered fraud solutions accelerate the detection of anomalous behavior patterns indicative of fraud. The ability to leverage real-time risk signals allows CISOs to quickly surface new fraud techniques and stay ahead of evolving threats.

- ☐ *Can the solution leverage a consumer identity graph to detect and analyze an array of risk signals in real time?*
- ☐ *Does it cover unusual outbound network traffic, database read volumes, HTML response sizes, and other critical indicators?*
- ☐ *Does it offer unified threat intelligence?*

2 | Comprehensive BEHAVIOR Analysis, Adaptive Learning, and Advanced Analytics

Deep insights into consumer behavior enable the detection of subtle anomalies that signal the size and scope of potential threats. Adaptive learning capabilities ensure that systems continuously refine their understanding of normal and abnormal patterns.

- ☐ *Is the solution capable of monitoring behavior across the digital consumer journey, spanning account creation, login, payments, chargebacks, policy abuse, money movement, and more?*
- ☐ *Does it offer insights into anomalies like geographical irregularities, device behavior masking, bot traffic patterns, and more?*
- ☐ *Does the solution incorporate behavioral biometrics along with anomaly detection, predictive analytics, and AI-driven threat hunting?*

3 | REAL-TIME Fraud Detection, Risk Analysis, and Response

Real-time capabilities like transaction monitoring, instant alerts for suspicious activities, and automated account locking are crucial for minimizing the impact of fraud and protecting sensitive information.

- ☐ *Does the solution provide real-time fraud signal analysis leveraging a global network of telemetry?*
- ☐ *Can it handle a vast array of data signals and deliver accurate real-time decisioning?*

4 | HIGH-FIDELITY Risk Signals and Reporting

Precise, actionable risk signals allow for early and proactive fraud detection. High-fidelity data ensures that CISOs can accurately assess the totality of potential risk, and make faster, more informed decisions.

- ☐ *Are the risk signals generated by the solution scalable and accurate over time, considering both static and behavioral data?*
- ☐ *How effectively does the solution differentiate between genuine user behavior and fraudulent activities?*
- ☐ *Does the solution provide customizable dashboards, real-time reporting, visualization tools, and historical data analysis?*

5 | INTEGRATION, Automation, and Compliance

Solutions that seamlessly integrate with your existing security infrastructure enhance efficiency and effectiveness. Automation capabilities streamline threat detection and response, and robust compliance features give CISOs confidence that all regulatory requirements are being met.

- ☐ *Can the solution integrate seamlessly with existing systems and automate fraud detection processes to reduce manual intervention?*
- ☐ *Does it offer cross-channel monitoring, as well as API integrations that align with your existing security infrastructure?*
- ☐ *Can you access audit trails, compliance checklists, automated compliance reporting, and risk scoring reports in order to maintain compliance?*

Dive deeper into the fraud solutions landscape with our Evaluation Guide, and learn more about AI-powered fraud prevention at sift.com.