Arkose Labs

TOP FRAUD TRENDS AND INSIGHTS FROM CISOs

From preparing for returning to offices to assessing the changing threat landscape, measuring the impact of fraud on their businesses and prioritizing budgets, CISOs have a lot on their plates.

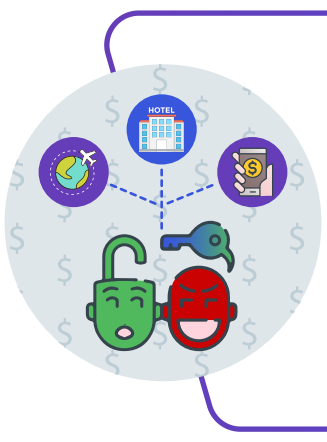
CISOs from companies in financial services, ecommerce, travel, media, gaming and more joined Arkose Labs for a roundtable to discuss pain points and strategies to tackle them. Here are some of the key takeaways from the discussion:

RETURN TO OFFICE PLAN

Many teams will continue to work entirely virtually, with a hybrid approach adopted for others. However, SOC and threat intel departments are likely to stay onsite, since they require careful planning and coordination.

OVERCOMING INTERNAL SILOS

CISOs are accountable for any attacks targeting their business. However, when fraud is involved, the responsibilities are shared with finance and other departments, often with little to no communication between the two.



INDUSTRY TRENDS

Fraudsters are increasingly targeting financial services and fintech firms and using social engineering in a more sophisticated way to gain access to these accounts. Going forward, travel and hospitality will be increasingly targeted for promo abuse as travel resumes.

BIGGEST THREATS

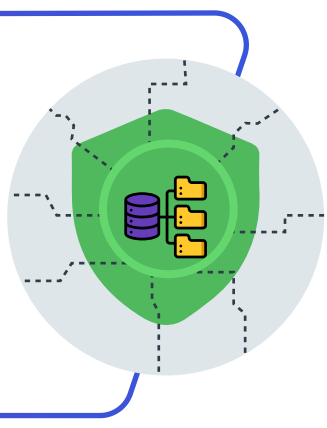
The past year saw many attacks from nation-states, which will likely continue. Other top threats cited include account takeover attacks, mobile device management, vishing, password spraying, denial of service, and misuse of computing power.

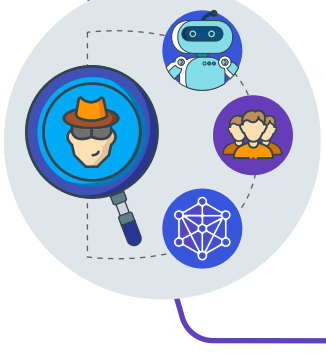
SYNTHETIC IDENTITY CONCERNS

Synthetic IDs remain difficult to detect because there are no systems in place to validate the different elements of information as belonging to one single person. Only the SSN and date of birth are static, while address, phone numbers and names can be changed.

PROTECTING LEGACY DEVICES

Many older devices are often not enabled with modern security controls and can be easily compromised by fraudsters. There is much evaluation that needs to be done around managing legacy endpoints to ensure they are secure.



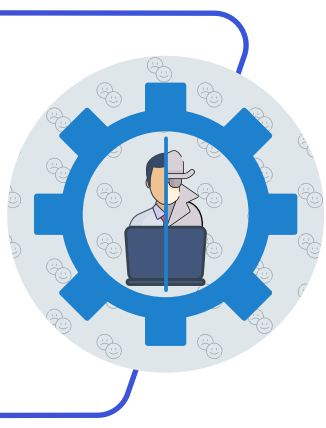


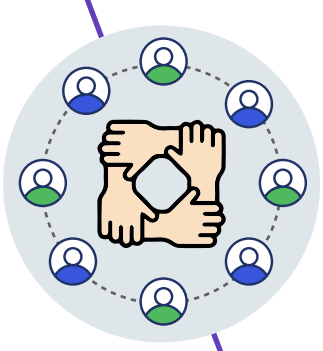
DETECTING FINANCIAL FRAUD

Financial institutions should use portfolio scoring to detect fraud across assets, as well as implementing machine learning to learn the context of certain transactions and detect anomalous patterns.

MAINTAINING CUSTOMER HAPPINESS

Businesses must enhance trust and safety for authentic users. They must strike a balance between using low friction authentication for an enhanced user experience and protection against fraud.





IMPORTANCE OF COLLABORATION

Businesses across geographies have varying appetites to share data and information. Unlike fraudsters who share knowledge and expertise, merchants and vendors do not often share data amongst each other. More collaboration in some areas is needed.

REGISTER

Register for our upcoming events.
https://www.arkoselabs.com/events/