BANKING & INSURANCE

Threat Intelligence In The Financial Industry

APPLICATIONS

KYC COMPLIANCE, CUSTOMER ONBOARDING

PROTECT CUSTOMER DATA

REDUCE FINANCIAL FRAUD

PREVENT BRAND IMPERSONATIONS

Risks The Financial Industry Faces

Banks and Financial institutions (FIs) handle some of the most valuable and comprehensive information to cyber criminals, from account details, credit card data, sensitive personally identifiable information (PII) and access to capital.

FIs are often the target for brand impersonations, financial frauds, money laundering, hacking and terrorism facilitation. It is also one of the most regulated industries, making it pertinent to adopt threat intelligence solutions as part of maintaining a strong security posture.

Advancements in the banking industry such as e-banking, mobile banking and adoption of crypto are expected to increase security vulnerabilities.

Customer Onboarding

NexVision helps FIs to do customer on-boarding screenings quickly and accurately. We screen for politically exposed persons, corruption, averse media, links to terrorism, criminal records worldwide and evidence of money-laundering. Our screening algorithm is automated - this facilities workflow and alerts FIs to high-risk persons and companies allowing it to assess and monitor their risks continually according to the latest FinCen rulings and KYC (Know your customer) requirements.

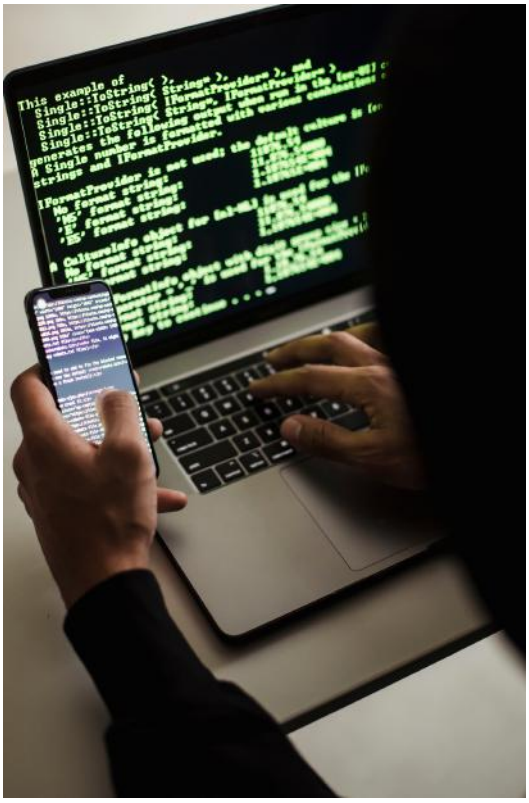
Protect Customer Data And Reduces Financial Fraud

NexVision scans the clear, deep and dark web as well as social media for data leaks of BINs, leaked account numbers, SWIFT codes, and various financial scams to identify and mitigate fraud campaigns at the source.

In the case of credit card fraud, chargebacks given by the banks and FIs reduce profitability. Even a one-time data leak will lead to erosion of trust between the client and your organization and drives them away to your competitors who have stronger security and risk-mitigation plans.

NexVision functions as a real-time and predictive intelligence monitoring tool - it can give you alerts of leaked personal information like credit card details, even before they have been used, preventing financial losses from fraud.

NexVision also secures and sends automatic alerts on key assets such as your executives, key personnel, sensitive systems, products, supply chain, cloud provider and cyber data such as IP ranges and domain names to reveal vulnerabilities.



Market Manipulation and Insider Dealing

Market manipulation occurs when a person deliberately spreads false information about facts material to the audit, or omits certain information subject to mandatory reporting requirements, thus influencing the market price by deception. These are prevalent in the financial services and banking industry.

Insider dealings also occur when related members of the financial institution act upon insider data to obtain financial gain.

NexVision uncover suspicious financial activity and sends alerts - reducing investigation time by up to 90%. For example, leaked and shared financial details and statements can be recovered in real-time and its paper trail can be detected. Parameters can be expanded to key employees and their family members etc.

Contact us for a demo to see how NexVision works for you:

NEXVISION
REAL-TIME DARK WEB THREAT INTELLIGENCE

UK/Europe/North America Contact:
Kemp House 152 - 160 , City Road City Road, London, England EC1V 2NX.
(+44) 203 6953536

APAC Contact:
Level 11, Marina Bay Financial Centre Tower 1, 8 Marina Boulevard, Singapore 018981
(+65) 6841 0094
E-mail: info@nexvisionlab.com

Prevent Brand Impersonations

It is becoming increasingly common for threat actors to pose as bank employees and contact customers to provide personal details like pin numbers, or to make dubious transactions. New and more sophisticated social engineering schemes and fraud tactics are developed daily. FIs have to utilize reliable threat intelligence to defend against the onslaught of threats that damage its brand and hurts its bottom line. NexVision scans through social media, private and public chat rooms as well as the clear and dark web to identify instances of impersonation and fraud, and sends you alerts, including details of the attacker and even the region where they are from, allowing you to alert your customers and protect yourself in real-time.