NICE · ACTIMIZE

IFM-X 暗网智能：从根本上减少诈骗犯罪的主动智能

人工智能与专有技术的无敌组合大幅降低欺诈损失与金融犯罪，以此提供有据可依的投资回报率。

立即可操作、自定义和不断刷新的情报，并监控泄露后和欺诈前的情景。

全面多语言覆盖暗网、深网、恶意软件网络、僵尸网络、私人信息平台以及地下诈骗者基础设施和社区。

反诈骗操作变被动为主动

- 通过三个精选的高分化专有数据源，**全面覆盖**客户账户侵权、被盗的支付卡和骡子账户。
- 在反诈骗和调查相关领域**显著降低运营成本**。
- **易于使用的设计简化整合**现有反诈骗流程与控制措施，以及无需下游处理或分析的安全系统。
- 在各种互动和交易过程中进行**最终检测并响应可疑活动**，却不会给客户带来不便。
- 根据当前的和新的攻击途径，**建立并优化反诈骗模式。**
- **利用共享情报**扩大并赋能金融犯罪、反洗钱、反诈骗和信息安全团队。

实时情报。直接反诈骗。

实时情报。直接反诈骗。
金融机构可以利用暗网智能打击所有支付渠道中难以发现的账户侵权和一系列金融犯罪。实时检测账户侵权意图并立即挽救被盗的账户，防止侵权和随之出现的客户冲突。此外，金融机构还可以识别诈骗者正在利用被盗账户的最新战术，采取强有力的对策。

零客户冲突打击支付卡诈骗
金融机构可以补发新卡或标记被盗的支付卡，在诈骗导致不必要的客户冲突之前预测诈骗的发生，先发制人。针对已被网络罪犯盗取或在暗网市场交易的危险支付卡，提供连续生成的数据馈送，在有卡和无卡环境下欺诈损失均能实时降低。被盗用的支付卡源可以进一步帮助金融机构开展常规购买点分析，以精准识别暴露支付卡数据的商户违规情况，保护其卡组合。

利用暗网监控封锁骡子活动
对骡子账户的广泛数据驱动可见性使金融机构得以检测涉及骡子的非法金融交易事件，并提前采取行动。暗网智能提供可操作的数据源，详细列出各金融机构的骡子账户，包括姓名、电子邮件地址、银行账号和电话号码。

部署该威胁智能可以探知某骡子账户是否与客户账户匹配，骡子账户关联第三方金融机构与否，并对照骡子数据筛查新账户申请。

准备好了吗？欢迎联系我们：info@niceactimize.com >