威胁猎人研究团队 · 业务安全与身份对抗情报

失守的采集层：虚拟摄像头即服务如何击穿生物识别 eKYC 与视频核验

基于三类真实虚拟摄像头工具链的静态二进制逆向与受控沙箱分析——覆盖宿主应用 Hook、iOS 相机守护进程 IOSurface 共享内存注入与零恶意特征 WebRTC 欺诈 SaaS，并系统剖析 ISO/IEC 30107-3 PAD 评测下的 0/9 合规盲区。

> **核心论断：**现代身份欺诈团伙已不再执着于在镜头前对抗活体算法。通过在软件采集管线内部直接替换视频帧，攻击者将物理摄像头完整性移出业务链路——下游活体与核验模型并未失效，**它只是在诚实地评估一份被伪造的输入。**

形态一 · 应用层 Hook

62 处 Hook + 五层伪造

精确重建 BGRA/420v/420f 帧并复用 PTS 与 EXIF，同步伪造设备指纹、WiFi、GPS、代理与截屏审计。

形态二 · 系统守护进程

mediaserverd + 重光照

iOS 17/18 零拷贝 IOSurface 守护进程结合 Vision 人脸 ROI 物理重光照、合成 IMU 与音频桥接。

形态三 · WebRTC SaaS

9 项常规权限 · 零恶意告警

干净的会议 APK 与 Web 端由服务端 `virtualCam` 开关驱动，批量 30 天席位用于真人语音视频仿冒。

1. 执行摘要

过去十年间，金融机构、支付网络、数字钱包与持牌平台普遍将生物识别活体检测与远程视频核验视为身份安全的最后一道防线。这套信任模型隐含着一个极少被审计的前提：**进入核验链路的人脸视频帧，确实采集自终端设备的物理摄像头传感器。**

威胁猎人研究团队对三类真实流转的虚拟摄像头工具链开展静态二进制逆向与受控沙箱分析后证实，这一前提已经失效。现代欺诈团伙不再执着于在镜头前用高清照片、翻拍屏幕或硅胶面具对抗活体算法，而是将物理摄像头直接移出业务流程——将预录视频或远端实时视频流注入软件采集管线。下游活体与核验模型并未“出错”，**它只是在诚实地评估一份被伪造的输入。**

3 大注入层	62 处 Hook	0 / 9	9 项权限
采集层劫持技术栈	**单模块全面接管**	**PAD → ISO 24745**	**零恶意特征 SaaS**
覆盖宿主应用 Hook、iOS 相机守护进程 IOSurface IPC 与零恶意特征 WebRTC 媒体轨。	单个免费 iOS 动态库即可挂钩 62 处 AVFoundation 与 5 层设备身份/代理/截屏接口。	常规 PAD 评测交付物中，直接满足 ISO/IEC 24745 采集到服务端完整性证明的数量为零。	视频诈骗 APK 无需 Root、悬浮窗或无障碍权限，作恶能力完全由服务端配置控制。

研究范围与证据边界

本报告综合三类一手技术证据：（1）对两套灰黑产 iOS 虚拟摄像头工具链（`FakeTools` v5.5 与基于 `LordVCAM 3.0.47` 引擎的 RootHide 分销变体）开展完整静态二进制反汇编，覆盖 Mach-O 符号、Objective-C 选择器、嵌入式 GLSL 着色器与安装脚本；（2）对一套 Android/Web 双端视频仿冒套件（`Tianqiong` v1.3.2）进行静态反编译与受控沙箱实测；（3）面向 `ISO/IEC 30107-3:2023`、`19795-1:2021` 与 `24745:2022` 的逐项标准差距映射。全部客户标识、内部运营信息及存活恶意端点均已脱敏；超出静态与沙箱边界的特定商业活体 SDK 实测通过率不做外推。

2. 从物理呈现攻击到软件采集层注入

传统生物识别防伪聚焦于**呈现攻击（Presentation Attacks, PAs）**：攻击者在真实物理镜头前展示照片、平板翻拍视频或 3D 面具。由于光线仍须穿过光学镜头与硬件 ISP 处理管线，呈现攻击检测（PAD）算法可依据摩尔纹、屏幕边框反光、景深平面化与微纹理畸变等线索实施拦截。

数字注入攻击彻底绕开了物理世界。攻击者在操作系统相机服务、宿主应用进程或 WebRTC 媒体管线内部拦截帧缓冲，直接注入具备完全合规像素格式（`BGRA`、`420v`、`420f`）、原样复用时间戳（`PTS` / `DTS`）与硬件 EXIF/TIFF 元数据的伪造画面。更严峻的是，摄像头劫持常与五层设备伪造、合成运动传感与路网吸附 GPS 打包出现，导致设备指纹与风控引擎同步失明；而**商户入网、远程视频尽调、大额步进核验与客服视频连线**等异步/半实时链路，正成为最薄弱的突破口。



图 1：基于威胁猎人二进制逆向与受控沙箱分析还原的三层虚拟摄像头注入架构，对比 ISO/IEC 30107-3 PAD 评测所覆盖的物理镜头采集管线。

评估维度	形态一：宿主应用 Hook（`FakeTools` v5.5）	形态二：OS 守护进程引擎（`LordVCAM` 3.0.47 变体）	形态三：零恶意 WebRTC SaaS（`Tianqiong` v1.3.2）
注入层级	宿主应用 ObjC 运行时（`AVFoundation` 代理）	系统相机进程（`mediaserverd`）+ `avfsupportd` `IOSurface` IPC（iOS 17/18）	应用层 WebRTC（`UriVideoCapturer`）+ 浏览器 `canvas.captureStream(30)`
平台与权限	iOS；强依赖越狱 + `MobileSubstrate`	iOS（适配至 iOS 17/18）；依赖越狱（`RootHide` / `Dopamine`）	Android（`minSdk 30`）+ 移动 Web；**无需 Root 或越狱**
视频源机制	`AVAssetReader` 解码本地预录 MP4（`temp.mp4`）	本地 `.mov` 循环槽位**或**远端 PC 经 WebSocket（`:8765`）推流 H.264/YUV	Android `OpenDocument` 选择任意本地视频（静音循环 `1280×720@24fps`）
活体与传感器对抗	像素/PTS/EXIF 对齐 + 5 层设备/GPS/WiFi/代理/截屏伪造	Vision 人脸 ROI GLSL 重光照 + `CMDeviceMotion` 合成 + 音频桥接 + 真帧混合	循环视频仿冒配合真人实时语音 + 房间锁定/等候室隔离
商业化模式	免费未签名插件，向加密通讯群组与下载站导流	按量/周期订阅（巴西 PIX + USDT/BTC/LTC）+ 安全隔区硬件绑定 + 贴牌换皮层	批量开通 30 天租赁席位，由服务端 `virtualCam` 开关远程启停
核心防御破绽	强依赖越狱；线性预录视频无法响应随机交互挑战	人脸 ROI 外围 2 - 5 px 光照梯度断层；合成 IMU 缺少自然手抖微噪；守护进程/IPC 痕迹	循环视频口型漂移与背景静止异常；Punycode 域名与 WebRTC 轨道特征

3. 三类真实样本的二进制逆向与机制拆解

3.1 形态一：宿主应用内运行时挂钩（`FakeTools` / “虚拟工具箱 5.5”）

对一款在越狱社区免费流通、未加密且未剥离符号的 `16.40 MB` arm64 Mach-O 动态库（`com.xuuz.faketools`，自称虚拟工具箱 5.5）开展静态反汇编，共还原出 **15,321 个符号**、**91 个类**与 **2,034 个方法**，内嵌面向 `iPhoneOS17.0` SDK 编译的 OpenSSL 与 FFmpegKit。经 `CydiaSubstrate` 注入宿主应用后，单一初始化器即部署 **62 处全局 `_MSHookMessageEx` Objective-C 挂钩**：

- **全通道相机接管：**同步挂钩 `AVCaptureVideoPreviewLayer`、`AVCaptureSession`、`AVCaptureStillImageOutput`、`AVCapturePhotoOutput` 与 `AVCaptureVideoDataOutput`（动态拦截所有代理对象的 `captureOutput:didOutputSampleBuffer:`），预览、拍照与录像一次全替换。
- **像素、时序与元数据完全对齐：**在 `GetFrame::getCurrentFrame::` 中通过 `AVAssetReader` 读取 `Documents/temp.mp4`，按宿主请求的像素格式输出 `BGRA` / `420v` / `420f`，重建复用原始 `duration` / `PTS` / `DTS` 的 `CMSampleBuffer`，并将真实帧的 `__Exif_` 与 `__TIFF_` 附件原样拷贝至伪造帧。

捆绑伪造与对抗能力	二进制中证实的技术实现	对企业风控控制的冲击
五层设备身份伪造	依次挂钩 `uname`、`sysctl` / `sysctlbyname`、`MGCopyAnswer`（`HWModelStr`）、`UIDevice` 与 `NSBundle`	批量伪造机型（如 `iPhone16,2`）、系统/应用版本、`IDFV` 与 `IDFA`，击穿设备指纹连续性与黑名单关联
网络与地理伪装	挂钩 `CNCopyCurrentNetworkInfo`（`SSID` / `BSSID`）、`CLLocation` 与 `CFNetworkCopySystemProxySettings`	强制代理检测返回 `HTTPEnable=false` 并伪造 WiFi/GPS，使端侧 VPN 与地域检测失效
截屏与录屏审计屏蔽	强制 `UIScreen.isCaptured` 返回 `0`，并吞没 `UIApplication._handleScreenshot`	在敏感核验与支付步骤中屏蔽端侧截屏与录屏风控告警
行为自动化与时钟变速	私有 `IOHIDEvent` 触控注入（`PTFakeMetaTouch`）、按文案自动点击及 4 档 `mach_absolute_time` 变速	支撑自动化领券/下单，并扰动端侧行为时序风控模型
运行时 UI 与 URL 改写	读取本地映射表（`tihuan.plist`）挂钩 `UILabel` / `UITextView` 与 `NSURLSession`	动态篡改界面文案、重定向接口地址或改写外发请求头

防御边界：形态一强依赖越狱与 Substrate 注入，且仅支持线性预录视频回放。服务端下发的随机动作挑战与硬件级 `App Attest` 挑战-响应校验，即可以极低成本阻断该类工具。

3.2 形态二：操作系统相机守护进程注入与 GLSL 重光照（`LordVCAM` 3.0.47 变体）

形态二彻底下沉至宿主应用边界之下。对一份压缩包大小 `929.12 KB` 的 RootHide 软件包（`.deb`，包标识 `com.apple.avservicesd.roothide`，分销渠道以“三色相机”等名称推广，基于 `LordVCAM 3.0.47` 引擎）的静态逆向揭示出一套适配至 iOS 17/18 的**三组件模块化架构**：

- **核心引擎（`AVServicesd.dylib`，`3.4 MB`，提取 `13,419` 条字符串）**：注入 `mediaserverd`、`UIKit` 与 `WebKit.GPU`，负责系统级 `CMSampleBuffer` 替换、iOS Vision 人脸定位、Metal/CoreImage 物理重光照、运动合成、音频桥接与虚拟 GPS。
- **iOS 17/18 持久化生产守护进程（`avfsupportd`，`977 KB`）**：作为 `KeepAlive` LaunchDaemon 伪装成 `com.apple.*` 服务（IPC 缓存 `/var/tmp/com.apple.avfcache`）。解码本地或 PC WebSocket（`:8765`）推流的 H.264/YUV 帧，零拷贝写入 **`IOSurface` 共享 GPU 内存**，经 `CFNotification`（`com.apple.avfcache.framepulse`）触发消费并执行过期帧丢弃（`WK REJECT: frame STALE`）。
- **白标贴牌换皮层（`lordvcamroothide.dylib`，`168 KB`）**：经 `MSHookMessageEx` 拦截授权与计费界面的 `baseURL` 内存槽位，将计费与品牌流量导向区域分销商后端，支撑“一套核心引擎、多品牌贴牌分销”。

```
// 提取自 AVServicesd.dylib — 嵌入式 Metal/CoreImage CIColorKernel k0（脱敏核心片段）
kernel vec4 k0(__sample base, vec4 face, vec4 light, vec3 lightDir, float strength, float range, float
feather, ...) {
  vec2 uv = (destCoord() - face.xy) / max(face.zw, vec2(1.0));
  // 椭圆面颊轮廓遮罩（避免矩形边框穿帮）
  float faceShape = 1.0 - pow(abs(centered.x/halfW), 2.35) - pow(abs(centered.y/halfH), 2.20);
  float mask      = ccSmooth(-0.15 - 0.55 * feather, 0.05, faceShape);
  // 线性空间兰伯特漫反射 + 镜面高光 + Reinhard 色调映射回转 sRGB
  vec3 diffuse    = bl * (ll * w);
  vec3 specular   = ll * ccSmooth(0.72, 1.0, Llum) * w * 0.60;
  vec3 outL       = bl + diffuse + specular;
  outL            = outL / (vec3(1.0) + max(vec3(0.0), outL - vec3(1.0)));
  return vec4(clamp(ccSRGB(outL), 0.0, 1.0), base.a);
}
```

在重光照画面之上，引擎同步叠加四项多模态对抗模块：**`AVSMotionSynthesizer`**（合成与转头/点头同步的 `CMDeviceMotion` 加速度计与陀螺仪数据）、**`AVSAudioBridge`**（将视频音轨桥接至麦克风应对数字朗读挑战）、**`blendFrame:withFrame:alpha:`**（叠加真实物理帧保留细微微表情）以及 **`forceMapMatching` 道路吸附虚拟 GPS**（自动将伪造经纬度吸附到真实路网，规避落点异常）。



图 2： `LordVCAM 3.0.47` 端到端系统级活体对抗管线及威胁猎人逆向暴露的两类高置信度服务端物理取证断层：人脸 ROI 外围 2 - 5 px 光照边界阶跃与合成 IMU 微颤噪声缺失。

3.3 形态三：零恶意特征的 WebRTC 视频仿冒 SaaS（`Tianqiong` v1.3.2）

形态三揭示了传统移动杀毒与权限评分失效的根本原因：**作恶能力被干净利落地设计为业务功能，客户端二进制本身不含任何传统恶意代码特征。**

对 Android 会议应用（`com.tianqiong.thadmin`，v1.3.2，`29.2 MB` 未加密 DEX，内置原生 WebRTC `libjingle_peerconnection_so.so`）及配套移动端 Web 客户端的静态反编译与沙箱实测证实：

- **与合法会议软件几乎无异：**仅申请 **9 项常规权限**（网络、相机、麦克风、蓝牙音频、前台通话服务、通知），仅声明 **4 个组件**（`LoginActivity`、`WorkActivity`、`CallActivity`、`CallService`），无无障碍滥用、无录屏权限、无短信/通讯录读取、无加壳混淆。
- **双端产品化虚拟摄像头：**Android 端通过 `UriVideoCapturer` 实现标准 `org.webrtc.VideoCapturer`，调用系统 `OpenDocument` 选择本地视频，经 `MediaPlayer` 静音循环（`setLooping(true)`、`setVolume(0,0)`），关闭真实摄像头并以 `1280×720@24fps` 注入 `VideoTrack("th-vcam")`；Web 端则通过离屏 `<video loop muted>` 绘制至 `canvas.captureStream(30)` 完成同等换轨。
- **服务端权益门控与 30 天席位租赁：**“虚拟画面”入口由后端 `/auth/me` 返回的 `virtualCam` 字段动态控制；后台支持批量开通 30 天到期回收的操作员席位。受害者仅需 7 位房间号即可在手机浏览器免注册入会，同时房间密码、锁房、等候室审批与踢人机制阻断家属或反诈干预。
- **模块化诈骗工具链拆分：**后台元数据指向独立并行的同屏产品，印证团伙将“视频仿冒 + 实时同屏 + 真人语音”拆分为多个低权限单功能应用，规避端侧权限异常阈值。

4. 地下商业化分工：从免费引流到多币种 SaaS

三类样本共同勾勒出分工成熟的地下 B2B 供给体系，其商业化模式已高度逼近正规 SaaS 产业：

市场分层	代表样本	变现机制与防破解保护	对防御方的战略启示
一层：免费引流漏斗	`FakeTools` v5.5（iOS 越狱插件）	无授权校验，依托加密通讯群组与下载站免费分发，沉淀操作员社群并向付费工具导流	显著拉低初级团伙门槛；可通过 Substrate 检测与 `App Attest` 低成本阻断
二层：多币种订阅 + 贴牌分销	`LordVCAM` 3.0.47 引擎 + 换皮模块	反用 **iOS 安全隔区 ECDSA-P256**（`AVSAttestationProvider`）一机一码与按量计费；支持**巴西 PIX + USDT/BTC/LTC**；`168 KB` 换皮钩子改写计费 `baseURL`	单一品牌封堵收效甚微；跨贴牌变体追踪核心 IPC/GLSL 指纹与上游鉴权更具杠杆效应
三层：交钥匙席位租赁 SaaS	`Tianqiong` v1.3.2（Android + Web）	批量开通 30 天席位、单账号 `virtualCam` 动态开关，搭配一次性 Punycode 国际化域名与短周期免费 TLS 证书	端侧查杀无效；必须结合网络/IDN 情报、随机活体挑战与面向客户的防诈宣导

5. eKYC 合规盲区：ISO/IEC 30107-3、19795-1 与 24745 差距审计

银行与金融科技风控治理中普遍存在误判：“供应商已通过 ISO/IEC 30107-3 Level 2 PAD 活体认证，因此能防住虚拟摄像头。” 威胁猎人跨标准映射审计表明，仅凭 PAD 证书无法覆盖软件采集层注入。

关键标准边界：同一段视频，属于截然不同的治理范畴

攻击者在**真实物理镜头前**用屏幕播放人脸视频，属于 **ISO/IEC 30107-3** 管辖的呈现攻击（PA）；当完全相同的视频被数字注入 `AVFoundation`、`mediaserverd`、`IOSurface` 或 WebRTC 时，它已绕过物理传感器，成为必须依据 **ISO/IEC 24745** 评测的**样本替换与重放威胁**。两类测试结论绝不可混为一谈。

对照维度	ISO/IEC 30107-3:2023	ISO/IEC 19795-1:2021	ISO/IEC 24745:2022
覆盖范围	采集传感器前方的物理呈现攻击	正常业务运行下的端到端核验准确率	生物特征在采集、传输与存储全链路的保护
必备证据	按 PAI 介质分列 `APCER`、独立报告 `BPCER` 及无响应统计	`FTA`、真人 `FRR`、冒充 `FAR`、置信区间，并在重试时保留首次结果	架构级证明机密性、完整性、抗样本替换与服务端防重放控制
虚拟摄像头盲区	**不覆盖** OS 守护进程或软件管线内的数字注入	PAD 攻击通过计数不可并入正常业务 `FAR`	仅凭客户端 PAD 认证证书几乎无法证明采集链路完整性



图 3： 威胁猎人对 9 类常规 PAD 评测交付物（受试者样本量、采集执行日志、呈现攻击用例、误识指标/分母、报告元数据、统计方法、效率日志、设备环境配置与测试人员职责）向 `ISO/IEC 19795-1:2021` 与 `ISO/IEC 24745:2022` 复用的审计结论。

此外，采购治理中普遍存在**标准版本漂移**：内部新编方案已对标 `ISO/IEC 30107-3:2023`，但供应商准入仍沿用旧版 `ISO/IEC 30107-3:2017` 历史报告，导致攻击类别口径与证据边界脱节。

为何 9 类 PAD 交付物中可直接满足 ISO/IEC 24745 的数量为 0

全部 9 类常规交付物中，**4 项**（受试者数量、误识率、统计方法与耗时日志）完全不涉及机密性、载荷完整性或防重放能力；其余 **5 项**也仅能在补充“服务端采集到存储数据流验真”与“抗数字注入/防重放边界控制”证据后作为辅助材料部分复用。

6. 纵深防御框架：将信任锚点从客户端迁移至服务端

当攻击者既能挂钩宿主进程、又能替换 `mediaserverd` 系统帧、还能交付零恶意特征 WebRTC 应用时，**任何单一端侧校验都不再适合作为唯一信任锚点。**建议金融机构、eKYC 供应商与平台风控团队按优先级落实五层服务端锚定防御体系：

优先级	控制层级	关键工程与风控落地措施	对抗目标能力
P0 · 立即落地	**封堵异步核验时效缺口**	将实时采集到提交的严格超时校验扩展至**商户入网、远程视频尽调与大额步进审核**，不再仅覆盖零售实时开户场景。	预录视频上传与非实时画面替换
P0 · 立即落地	**硬件级设备证明与运行时完整性**	在高敏 eKYC/支付动作前强制执行服务端验签的 **iOS App Attest / DeviceCheck**（安全隔区挑战-响应）与 **Android Play Integrity**；同步检测越狱/Substrate/RootHide、`mediaserverd` 非系统 dylib 及伪造 `com.apple.*` IPC 痕迹。	五层设备伪造（`FakeTools`）与越狱守护进程引擎（`LordVCAM`）
P0 · 立即落地	**服务端随机交互挑战**	以绑定单次会话 Nonce 的服务端随机动作序列与随机朗读口令，替代固定或可预测的活体指令，阻断静态预录循环。	线性预录视频回放（`FakeTools`、`Tianqiong`）
P1 · 高优先级	**服务端物理光照与 ROI 取证**	部署**人脸 ROI 外围 2 - 5 px 环带亮度与色温梯度连续性检测**，捕捉局部 GLSL 重光照拼接断层；分析连续帧传感器底噪分布、二次压缩伪影与运动模糊连续性。	局部 GLSL 人脸重光照（`LordVCAM`）与解码视频流注入
P1 · 高优先级	**传感器与网络上下文交叉校验**	随视频同步回传原始加速度计/陀螺仪遥测，识别合成运动轨迹中缺失的自然手持微颤；通过服务端 IP/ASN 校验代理与地域属性，不轻信客户端 API 或 GPS。	`AVSMotionSynthesizer`、代理屏蔽与路网吸附 GPS
P1 · 高优先级	**行为频次与远程视频风控**	实施单证件关联设备上限、eKYC 通过后短时大额交易冷静期、背景/设备聚类与视频通话异常标记（背景冻结、口型延迟、拒绝切换镜头），并强化客户宣导——“视频里看到活人面孔”不再等同于身份真实。	PC 实时推流真人代操与零恶意视频诈骗 SaaS（`Tianqiong`）
P2 · 治理演进	**ISO/IEC 24745 准入与外部情报**	在 eKYC 供应商准入中要求独立提交 `ISO/IEC 24745` 采集到存储完整性与防重放验证证据；持续追踪虚拟摄像头核心引擎、贴牌变体与一次性 Punycode 会议基础设施。	合规盲区与白标贴牌工具链扩散

7. 附录：脱敏检测锚点与 eKYC 治理自查清单

7.1 脱敏结构与行为取证检测信号

以下全部特征均为面向移动风险 SDK、EDR 与服务端分析的脱敏工程检测锚点，已剔除全部客户标识与存活恶意基础设施。

工具形态	面向移动风险 SDK / EDR / 服务端分析的脱敏检测信号
宿主应用内 Hook（`FakeTools` 类）	存在 `CydiaSubstrate` / `MobileSubstrate` 运行时库或 `/var/jb` 路径；`AVCaptureVideoDataOutput` 与 `UIDevice` 出现 `_MSHookMessageEx` 符号挂钩；`NSUserDefaults` 偏好域命中 `com.xuuz.faketools`；`IOHIDEvent` 模拟触控间隔方差趋近于零；`mach_absolute_time` 重绑定导致的单调 `PTS` 与系统挂钟漂移。
系统守护进程引擎（`LordVCAM` 类）	`mediaserverd` 加载非系统签名 dylib；异常 LaunchDaemon（`avfsupportd`）或伪造 `com.apple.*` IPC 缓存目录（`/var/tmp/com.apple.avfcache`）；`CFNotification` 特定通知模式（`com.apple.avfcache.framepulse`）；炫彩打光帧中**人脸 ROI 外围 2 - 5 px 边界亮度/色温阶跃断层**；原始 `CMDeviceMotion` 流缺失自然手部微颤噪声。
零恶意 WebRTC SaaS（`Tianqiong` 类）	自定义 `org.webrtc.VideoCapturer` 绑定静音循环 `MediaPlayer`（`UriVideoCapturer`、`th-vcam` 及服务端 `virtualCam` 权益字段）；浏览器会话组合离屏 `<video loop muted>` 与 `canvas.captureStream()`；新签发短周期 TLS 证书的 Punycode 国际化域名配合 `?room=<数字>` 邀请路径；与并行同屏域名共享前端构建资产的运营关联。

7.2 eKYC 风险治理自查清单（ISO/IEC 30107-3 与 24745）

- ☐ **拆分 PAD 与数字注入评测：**确认供应商报告将 `ISO/IEC 24745` 数字注入/重放防护与 `ISO/IEC 30107-3:2023` 物理呈现攻击检测独立测试、独立记账。
- ☐ **消除标准版本漂移：**确保内部测试规范与外部实验室认证证书均对齐 `ISO/IEC 30107-3:2023`，淘汰滞后的 `2017` 旧版报告。
- ☐ **保留首次尝试遥测数据：**核实 `ISO/IEC 19795-1` 指标清晰拆分真人与冒充者尝试，并在允许重试时完整留存首次失败记录。
- ☐ **审计非实时与半实时核验路径：**将严格采集新鲜度窗口与随机挑战扩展至商户入网、大额步进校验与远程视频尽调。
- ☐ **将信任锚点迁至服务端：**组合硬件级设备证明（`App Attest` / `Play Integrity`）、服务端人脸 ROI 边界光照取证、IMU 交叉校验与核验后行为频次风控。

关于威胁猎人（Threat Hunter）

威胁猎人是一家专注于业务反欺诈与网络威胁情报的安全科技企业。依托持续运转的地下黑灰产外部情报视野——从外部欺诈供应链源头而非孤立的内部日志出发——威胁猎人帮助银行、支付网络、电商平台与数字企业更早发现欺诈基础设施、账号接管、支付滥用与场外数字风险，并以清晰上下文驱动处置。

洞察外部风险，赋能业务决策 · www.threathunter.cn/research

公开发布与合规声明：本报告由威胁猎人研究团队基于静态二进制分析、受控沙箱测试及 ISO/IEC 标准映射整理编制。文中提及的合法操作系统接口、移动开发框架及支付通道均系被威胁行为体滥用或作为攻击目标，与欺诈活动无任何关联。全部客户标识、个人隐私数据及存活恶意端点均已按公开发布合规标准完成脱敏处理。