电子邮件 MDR (PhishGuard)

提供托管式检测和响应，以实现最佳的网络钓鱼韧性

增强您的电子邮件安全运营，以快速、高效地检测并解决网络钓鱼威胁

更好的保护，更少的开销

随着针对性的网络钓鱼攻击和商业电子邮件泄露 (BEC) 不断增加，运营团队不堪重负，难以跟上不断演变的网络钓鱼威胁。以被动方式应对网络钓鱼通常会因检测和响应时间延长而导致风险和成本增加。PhishGuard 缓解了网络钓鱼预防和电子邮件安全管理中更具挑战性和耗时的方面，包括：

- 针对欺诈 (BEC) 和内部威胁的**自定义通知和响应**
- **评估和解决**网络钓鱼提交
- **隔离和撤回**已识别的威胁
- 电子邮件环境中的**威胁搜寻**
- 针对指定指标的**自定义检测**

用于实时监控和通知的专用技术资源

技术专家迅速调查并通知网络钓鱼相关活动，释放运营能力，提前一步防范网络钓鱼攻击。我们的专家可以帮助改进检测和解决指标，同时提供对新兴网络钓鱼活动和策略的见解。

主要优势

主动预防

消除遭受 BEC 攻击的风险，众所周知，这些攻击代价高昂，很难被发现，并且可能对您的品牌和资产负债表产生负面影响。

快速审查与响应

减轻评估和解决最终用户提交的网络钓鱼问题的负担，这些提交可能会堆积起来，形成一个缓慢、耗时的过程。

更广的可见性和更深的洞察力

深入了解针对各行业的网络钓鱼策略，确保您做好准备，在这些活动以您的行业为目标时足以应对。

通过定期审查和报告获得更好的可见性

除了增强您的电子邮件安全营运外，PhishGuard 还让客户能够要求其专属分析师定期审查。审查包括分析师生成的报告，其中提供有关发现结果和指标的概述。

服务交付项目

托管电子邮件安全运营

- 评估和解决网络钓鱼提交
- 审查所有可疑判定
- 撤回恶意邮件
- 重新分类并释放安全邮件

主动欺诈防御

- 监控 BEC 活动
- 报告攻击活动详细信息和 IOC
- 创建和撤回新发现的指标
- 出现活动 BEC 时发出通知并执行操作

内部威胁防御

- 跟踪 HUMINT 相关通信
- 识别包含 IP 的通信
- 检测到活动的内部威胁时发出通知
- 审查/报告事件和严重程度

托管威胁搜寻

- 审查可疑判定
- 审查几近恶意的判定
- 对任何新判定采取行动
- 提交以增强检测能力

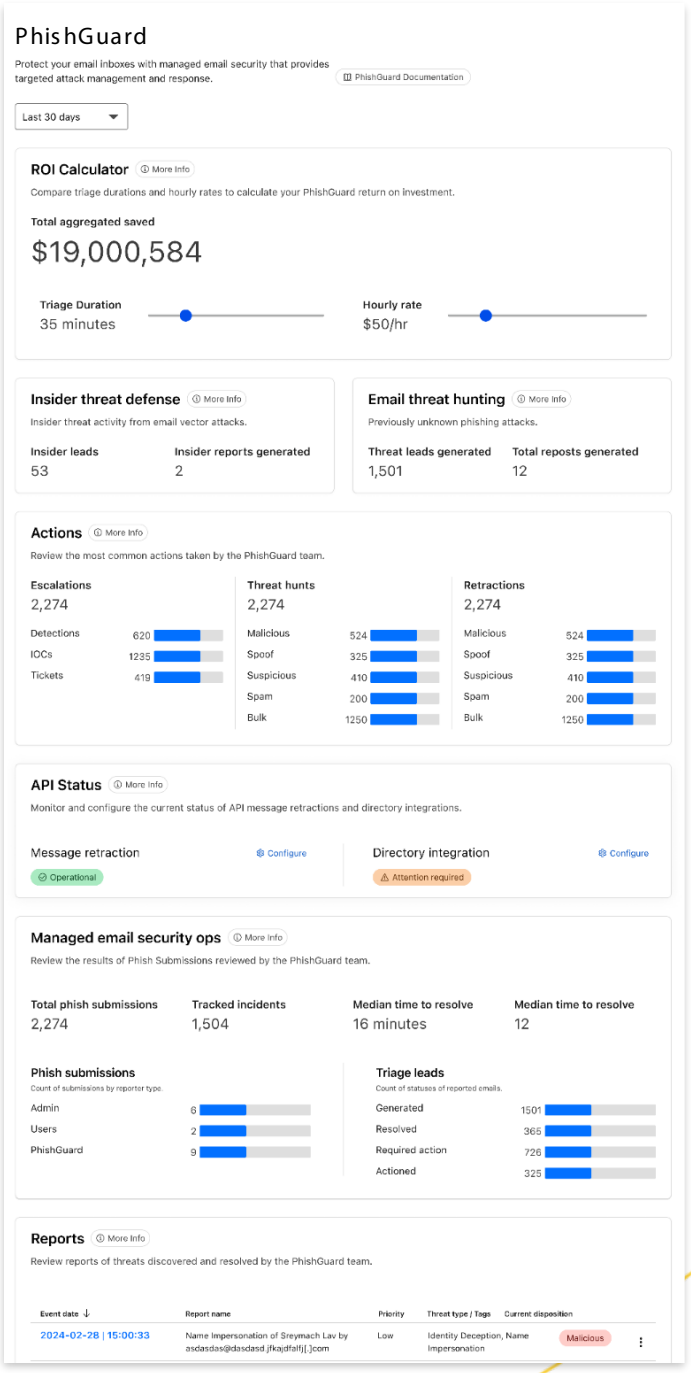

图 1：仪表板指标

