思科高级网络钓鱼保护：前期活动

发布日期：2018 年 6 月 22 日

确定项目团队的主要成员

- **执行发起人**：关键问题/项目障碍的问题升级联系人
- **项目负责人**：负责引导项目取得成功
- **项目经理**：您组织的主要联系人和接洽点。这些人员还负责按照协商一致的时间表推进项目，以及与其他内部团队和部门沟通合作。
- **部署工程师**：此人将作为部署专家，以及项目的主要技术联系人。
- **主题专家**：作为技术主管，针对设计和集成提供意见；确保决策与组织的业务战略保持一致。
  - 消息传送架构师
  - 安全架构师

发起首次客户成功通话之前必须完成的步骤

- 查看用户指南
- 观看 eLearning 门户上的培训视频
  - 创建新用户 - https://cl.ly/qrPd
  - 域标记功能的优点 - https://cl.ly/2A1m2w391L1Z
  - 收件箱策略/白名单 - https://cl.ly/1V2w1u463k3e
  - 如何重新配置邮件收件人，使其按照已触发的策略接收邮件 - https://cl.ly/1v381o3F0K0A
- 为需要使用平台或接收电子邮件报告的团队成员创建用户。

初次数据收集

- 确定您的邮件架构：创建一份显示端到端邮件流的图表，以确定适合您的环境的最佳传感器部署位置
  - 选择下列架构设计中的一种

内联传感器	内联传感器是一种内联配置，传感器将作为 MTA 工作，即：负责接收邮件，并将其投递至下一跳地址（通常是另一个内部 MTA）。采用内联配置的客户可以使用下一跳 MTA 根据传感器添加的报头对传入邮件进行相应操作。
双重投递传感器	传感器基本上作为 SMTP“邮件汇聚器”工作，它会通过 SMTP 接收邮件的副本，并以流传输方式提取邮件的元数据。邮件正文和附件将被丢弃。传感器上不会保留任何 SMTP 邮件。双重投递配置通常用于托管邮件架构，例如 Office365 和 G 套件。

  - 确定传感器是采用托管部署，还是在您的组织本地部署。
  - 确定当前是否执行 DKIM 和 SPF 检查。如果未执行，我们建议启用 DKIM 和 SPF。

需要注意的是，如果没有这些验证结果，则会延迟数据建模的调整，并导致数据建模不完整。

- 审查传感器安装要求
  - 安装传感器 - 第 1 章：https://agari.zendesk.com/hc/en-us/articles/360000659691-Agari-Enterprise-Protect-Admin-Guide。
- 确定所要保护的主要用户或关键组。
- 记录您的问题，并提供多个理想时间，就本前期活动的结果与您安排通话。