将邮件网关与思科高级网络钓鱼防护集成

本章包含以下部分：

思科高级网络钓鱼保护概述

思科高级网络钓鱼防护提供企业邮件危害 (BEC) 和网络钓鱼检测功能。它通过使用高级机器学习技术和新增的智能来对发件人地址执行信誉检查，从而检测基于身份欺骗的威胁。这类智能技术会不断调整优化，以便实时了解发件人的相关信息，从而带来增强保护。

邮件网关上的高级网络钓鱼防护引擎会根据发往贵组织的历史邮件流量来检查所有合法发件人的独特行为。思科高级网络钓鱼防护的云服务接口提供风险分析，以区分正常邮件和潜在的恶意邮件。

思科高级网络钓鱼防护云服务依靠作为传感器引擎的邮件网关，来接收入站发送到组织中的邮件元数据的副本。此传感器引擎从邮件网关收集元数据（例如邮件信头），然后将它们中继到思科高级网络钓鱼防护云服务进行分析。在经过分析后，根据高级网络钓鱼防护云服务上预配置的策略，从收件人邮箱中自动补救潜在的恶意邮件。

将邮件网关用作传感器引擎有助于组织：

- 识别、调查和补救从收件人邮箱的邮件信头中观察到的威胁。
- 查看组织中多个邮件网关的邮件元数据报告数据。

不支持思科安全邮件网络钓鱼防御系统：

自 2022 年 12 月 14 日起，安全邮件云网关 14.3 及更高版本将不再支持思科安全邮件网络钓鱼防御（以前称为思科高级网络钓鱼防护）功能。有关更多详细信息，请点击此处。如需进一步帮助，请联系思科技术援助部门。

注释 上述声明不适用于拥有有效许可证且正在主动使用思科安全邮件网络钓鱼防御功能的现有用户。

思科高级网络钓鱼防护的优势

以下是在邮件网关上部署思科高级网络钓鱼防护的优势：

- 基于传感器的解决方案可以快速部署，以确保您的用户完全免受破坏性漏洞攻击。
- 提供另一层防御，以更有效地保护您的邮件环境。
- 实时获得发件人的相关信息，了解并对邮件身份和行为关系进行身份验证，以防止BEC攻击。
- 自动删除收件人收件箱中的恶意邮件，并调用身份欺骗技术，以防止电汇欺诈或其他高级攻击。
- 详细了解邮件攻击活动，包括保护的邮件总数和阻止的攻击。
- 防止出现以下情况：
  - 使用受感染帐户和社交工程的攻击。
  - 网络钓鱼、勒索软件、零日攻击和欺诈。
  - 不使用恶意负载或 URL 的 BEC。

工作流程

1. 激活许可证以访问思科高级网络钓鱼防护云服务。
2. 将邮件网关设置为思科高级网络钓鱼防护云服务上的传感器引擎。这样会通过云或现场将邮件网关作为轻量级传感器进行部署。
3. 向思科高级网络钓鱼防护云服务注册邮件网关上的传感器引擎。
4. 邮件网关上的传感器引擎将被视为正常的邮件元数据转发到思科高级网络钓鱼防护云服务。
5. 思科高级网络钓鱼防护云服务确定邮件元数据是否为恶意。
6. 思科高级网络钓鱼防护云服务上的预配置策略在配置了“实施”传感器时，会阻止或重定向邮件以进行进一步的事件调查。

如何将邮件网关与思科高级网络钓鱼防护云服务相集成

请按以下顺序执行步骤：

过程

	命令或操作	目的
步骤 1	查看前提条件。	前提条件，第 3 页
步骤 2	从思科高级网络钓鱼防护云服务获取调配密钥。	从思科高级网络钓鱼防护云服务获取调配密钥，第 4 页
步骤 3	向思科高级网络钓鱼防护云服务作为传感器引擎注册您的邮件网关。	在邮件网关上注册思科高级网络钓鱼防护传感器，第 4 页
步骤 4	在邮件网关上启用高级网络钓鱼防护。	在邮件网关上启用高级网络钓鱼防护，第 5 页
步骤 5	从思科高级网络钓鱼防护云服务获取 API 访问密钥。	从思科高级网络钓鱼防护云服务获取 API 访问密钥，第 6 页
步骤 6	配置传入邮件策略以便启用邮件元数据的转发。	配置传入邮件策略以启用邮件元数据转发，第 7 页
步骤 7	监控转发到思科高级网络钓鱼防护云服务的邮件元数据。	监控思科高级网络钓鱼防护云服务上的邮件元数据，第 9 页

前提条件

- 激活思科高级网络钓鱼防护云服务的帐户，第 3 页
- 安装思科高级网络钓鱼防护云服务中的传感器，第 3 页

激活思科高级网络钓鱼防护云服务的帐户

确保您：

- 获取了从以下 URL 访问思科高级网络钓鱼防护云服务的许可证 - https://www.cisco.com/c/en/us/buy.html。
- 已使用您通过邮件通知收到的激活链接激活您的帐户，以便使用思科高级网络钓鱼防护云服务进行调配。

安装思科高级网络钓鱼防护云服务中的传感器

确保已根据组织要求将邮件网关设置为传感器引擎。有关详细信息，请参阅《思科高级网络钓鱼防护用户指南》。

从思科高级网络钓鱼防护云服务获取调配密钥

开始之前

确保您具有管理员访问权限，可以访问思科高级网络钓鱼防护云服务。有关详细信息，请参阅 前提条件，第 3 页。如果您无法访问思科高级网络钓鱼防护云服务，请联系思科 TAC 寻求帮助。

过程

步骤 1 登录思科高级网络钓鱼防护云服务。

步骤 2 选择“管理”**(Manage)** >“传感器”**(Sensors)**。

步骤 3 选择“安装”**(Installation)** >“下载传感器安装程序”**(Download Sensor Installer)**。

步骤 4 从下拉列表中选择根据组织要求配置的传感器安装脚本。例如：思科 SEG。

有关详细信息，请参阅 安装思科高级网络钓鱼防护云服务中的传感器，第 3 页。

步骤 5 复制 6 字调配密钥。

使用该调配密钥将思科邮件安全网关配置为传感器。

注释 要将邮件网关注册为传感器，您必须在生成后 7 天内使用调配密钥。

下一步做什么

向思科高级网络钓鱼防护云服务注册您的邮件网关。有关详细信息，请参阅在邮件网关上注册思科高级网络钓鱼防护传感器，第 4 页。

在邮件网关上注册思科高级网络钓鱼防护传感器

开始之前

确保您：

- 向高级网络钓鱼防护云服务注册邮件网关的有效调配密钥。有关详细信息，请参阅 从思科高级网络钓鱼防护云服务获取调配密钥，第 4 页。
- 在防火墙上为 FQDN 打开 HTTPS（入和出）443 端口，以便向思科高级网络钓鱼防护云服务注册您的邮件网关。

过程

步骤 1 使用 CLI 登录邮件网关。

步骤 2 运行 `eaasconfig` 命令并按照以下示例中的说明进行操作：

```
mail1.example.com> eaasconfig

Choose the operation you want to perform:
- REGISTER - To Register the appliance with APP portal
[]> register

Available list of APP region(s) for the registration
1. AMERICA

Select the EAAS region to connect
[]> 1

Enter passphrase obtained from APP portal: xxxxxx

Registration is in progress. Please wait.
Successfully registered the device with APP portal.

Would you like enable APP [Y]>

mail1.example.com> commit

Please enter some comments describing your changes:
[]>

Do you want to save the current configuration for rollback? [Y]>

Changes committed: Fri Feb 14 07:49:57 2023 GMT
mail1.example.com>
```

在向传感器注册邮件网关后，思科高级网络钓鱼防护云服务会生成通用唯一 ID (UUID)。

注释 成功注册后，思科高级网络钓鱼防护云服务会在云服务中识别邮件网关的主机名。

下一步做什么

在邮件网关上启用思科高级网络钓鱼防护引擎。有关详细信息，请参阅在邮件网关上启用高级网络钓鱼防护，第 5 页。

在邮件网关上启用高级网络钓鱼防护

开始之前

确保在思科高级网络钓鱼防护云服务上将您的邮件网关作为传感器进行了注册。有关详细信息，请参阅 在邮件网关上注册思科高级网络钓鱼防护传感器，第 4 页。

过程

步骤 1 登录邮件网关。

步骤 2 转到**安全服务 (Security Services) > 高级网络钓鱼防护 (Advanced Phishing Protection)**。

注释 仅当您使用 CLI 将邮件网关注册为思科高级网络钓鱼防护云服务的传感器时，才能查看“高级网络钓鱼防护”(Advanced Phishing Protection) 子菜单。

步骤 3 点击**启用 (Enable)**。

步骤 4 确认您的更改。

下一步做什么

启用将邮件元数据转发到思科高级网络钓鱼防护云服务。有关详细信息，请参阅配置传入邮件策略以启用邮件元数据转发，第 7 页。

从思科高级网络钓鱼防护云服务获取 API 访问密钥

您可以使用 API 访问密钥在邮件网关中执行以下任务：

- 向用户发送有关应用程序许可证到期详细信息的邮件通知警报。
- 在控制面板小组件中查看从组织级别的所有邮件网关发送到思科高级网络钓鱼防护云服务的邮件总数。控制面板小组件在新 Web 界面的“高级网络钓鱼防护”(Advanced Phishing Protection) 报告页面上提供。

开始之前

确保您：

- 已在思科高级网络钓鱼防护云服务上作为传感器注册邮件网关。有关详细信息，请参阅在邮件网关上注册思科高级网络钓鱼防护传感器，第 4 页。
- 已在邮件网关上启用高级网络钓鱼防护。有关详细信息，请参阅在邮件网关上启用高级网络钓鱼防护，第 5 页。

过程

步骤 1 登录思科高级网络钓鱼防护云服务。

步骤 2 选择“**管理**”**(Manage)** > “**用户**”**(Users)**。

步骤 3 点击所需的用户名。

步骤 4 点击**生成 API 密钥**(Generate API Secret) 链接以生成 API 访问密钥。

步骤 5 在您的系统上本地复制 **API 访问 UID (API Access UID)** 和 **API 访问密钥 (API Access Secret)**。

注释 如果您不复制 API 访问密钥并关闭思科高级网络钓鱼防护云服务，则需要执行该程序的步骤 **1-3**，然后点击**重新生成 API 密钥 (Regenerate API Secret)** 链接以获取新的 API 访问密钥。

步骤 6 登录到邮件网关的旧 Web 界面。

步骤 7 转到**安全服务 (Security Services)** > **高级网络钓鱼防护 (Advanced Phishing Protection)**。

步骤 8 点击“高级网络钓鱼防护 API 访问”(Advanced Phishing Protection API Access) 部分下的**编辑设置 (Edit Settings)**。

步骤 9 在“API 访问 UID”(API Access UID) 字段中输入 **API 访问 UID** 密钥。

步骤 10 在“API 访问密钥”(API Access key) 字段中输入**API 访问密钥**。

步骤 11 点击**提交 (Submit)**。

下一步做什么

启用将邮件元数据转发到思科高级网络钓鱼防护云服务。有关详细信息，请参阅配置传入邮件策略以启用邮件元数据转发 ， 第 7 页。

配置传入邮件策略以启用邮件元数据转发

您可以配置邮件策略，以便将邮件元数据转发到思科高级网络钓鱼防护云服务。

如果您在邮件网关上启用思科高级网络钓鱼防护，则以下邮件信头将与思科高级网络钓鱼防护云服务共享：

- Authentication-Results
- Authentication-Results-original
- DMARC-result
- DKIM-domain
- DKIM-result
- DKIM-selector
- DKIM-signatures
- From-header
- Full-Header-From
- HELO_domain
- Last-Hop-IP-Address
- List-ID
- Mail-From
- Mailing-list
- 邮件 ID
- Rcpt-To
- Received-Header
- Received-SPF
- Received-Timestamps

- 回复收件人
- SPF-result
- Subject-header
- To-header
- Originator-Return-Address
- X-Mailer
- X-Original-Authentication-Results
- X-Original-From
- X-Original-To
- X-Original-Sender
- X-Originating-IP
- X-OriginatorOrg
- X-Received

开始之前

确保您：

- 已在思科高级网络钓鱼防护云服务上作为传感器注册邮件网关。有关详细信息，请参阅在邮件网关上注册思科高级网络钓鱼防护传感器，第 4 页。
- 已在邮件网关上启用高级网络钓鱼防护。有关详细信息，请参阅在邮件网关上启用高级网络钓鱼防护，第 5 页。

过程

步骤 1 登录邮件安全网关。

步骤 2 转到**邮件策略 (Mail Policies)** > **传入邮件策略 (Incoming Mail Policies)**。

步骤 3 点击 APP 过滤器下方的链接。

步骤 4 从下拉列表中选择**启用高级网络钓鱼防护（自定义设置）(Enable Advanced Phishing Protection [Customize Settings])**。

步骤 5 选中**启用转发 (Enable Forwarding)** 复选框。

步骤 6 点击**提交 (Submit)** 并确认更改。

监控思科高级网络钓鱼防护云服务上的邮件元数据

您可以监控邮件安全网关转发到思科高级网络钓鱼防护云服务的邮件的元数据。云服务的“分析”(Analyze) > “邮件”(Messages) 页面提供了有关邮件来源以及与邮件和发件人相关的风险的见解。

思科高级网络钓鱼防护云服务上的邮件元数据会根据以下标准来获得信任分数：

- 邮件身份验证
- 域信誉
- 发件人合法性

高级网络钓鱼防护和集群

如果使用集中管理，则可以启用集群、组和计算机级别的高级网络钓鱼防护。如果您在单机模式下注册了带有思科高级网络钓鱼防护云服务的邮件网关，则可以选择加入使用思科高级网络钓鱼防护云服务注册的集群。

注释 如果在计算机级别禁用了高级网络钓鱼防护，则也会在组和集群级别禁用相同的功能。

“高级网络钓鱼防护报告”(Advanced Phishing Protection Reports) 页面

监控 (Monitor) > 高级网络钓鱼防护 (Advanced Phishing Protection) 报告页面会显示以下内容：

- 已成功转发到思科高级网络钓鱼防护云服务的邮件总数。
- 未转发到思科高级网络钓鱼防护云服务的邮件总数。

注释 如果邮件元数据转发失败，则必须验证“高级网络钓鱼防护”(Advanced Phishing Protection) 功能的配置。有关详细信息，请参阅 如何将邮件网关与思科高级网络钓鱼防护云服务相集成，第 2 页。

您可以在“高级网络钓鱼防护”(Advanced Phishing Protection) 报告页面上查看以下内容：

- 尝试转发到思科高级网络钓鱼防护云服务的邮件总数，以图形格式显示。
- 已转发到思科高级网络钓鱼防护云服务的邮件摘要（图形格式）。

要查看转发到思科高级网络钓鱼防护云服务的邮件元数据的详细信息，请点击链接并登录到思科高级网络钓鱼防护云服务。有关详细信息，请参阅监控思科高级网络钓鱼防护云服务上的邮件元数据，第 9 页。

监控思科高级网络钓鱼防护云服务上的邮件元数据

您可以监控邮件安全网关转发到思科高级网络钓鱼防护云服务的邮件的元数据。云服务的“分析”(Analyze) > “邮件”(Messages) 页面提供了有关邮件来源以及与邮件和发件人相关的风险的见解。

思科高级网络钓鱼防护云服务上的邮件元数据会根据以下标准来获得信任分数：

- 邮件身份验证
- 域信誉
- 发件人合法性

显示提交至思科高级网络钓鱼防护云服务的邮件

您可以查看转发到思科高级网络钓鱼防护云服务的邮件元数据（与成功和失败相对应）。

开始之前

请确保在邮件网关上启用邮件跟踪功能。要启用邮件跟踪 (Message Tracking)，请转到 Web 界面中的**安全服务 (Security Services) > 集中服务 (Centralized Services) > 邮件跟踪 (Message Tracking)**页面。

过程

步骤 1 登录邮件安全网关。

步骤 2 转到**监控 (Monitor) > 邮件跟踪 (Message Tracking)**。

步骤 3 点击**高级 (Advanced)**。

步骤 4 选中“邮件事件”Message Event) 下的**高级网络钓鱼防护转发 (Advanced Phishing Protection Forwarding)**。

步骤 5 （可选）选择**选择成功 (Select Success)**，以便查看已经成功转发到思科高级网络钓鱼防护云服务的邮件。

步骤 6 （可选）选择**失败 (Failed)**，以便查看未转发到思科高级网络钓鱼防护云服务的邮件。

步骤 7 点击**搜索 (Search)**。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。