将邮件网关与思科安全感知云服务集成

本章包含以下部分：

概述

通过思科安全感知云服务，您可以有效地部署网络钓鱼模拟和/或感知培训，以便测量和报告结果。它让安全运营团队能够专注于实时威胁，而不是最终用户缓解。

思科安全感知云服务提供重复点击者报告 - 重复单击邮件中任何 URL 或附件的用户。这些用户通过思科安全感知云服务定义的网络钓鱼模拟活动来加以识别。

有关思科安全感知云服务的详细信息，请参阅https://secat.cisco.com。

您可以将邮件网关与思科安全感知云服务集成，以便：

- 提高最终用户对实际网络钓鱼攻击的意识。
- 允许邮件管理员为被识别为重复点击者的用户配置严格的策略。

如何将邮件网关与思科安全感知云服务相集成

请按顺序执行下列步骤：

步骤	相应操作	更多信息
第 1 步	[在思科安全感知上]根据您所在的区域为组织创建思科安全感知云服务帐户。	创建思科安全感知云服务帐户，第 3 页
第 2 步	将防火墙设置配置为允许您的邮件网关访问思科安全感知云服务。	配置防火墙设置以访问思科安全感知云服务， 第 3 页
第 3 步	创建新的发件人组，以允许邮件网关中来自思科安全感知云服务的模拟网络钓鱼邮件。	创建发件人组以在邮件网关中允许模拟的网络钓鱼邮件， 第 4 页
第 4 步	[在思科安全感知上]在思科安全感知云服务中创建新用户，以便识别重复点击者。 :	请参阅《CSA 管理员指南》，网址为： • https://secat.cisco.com/portal/Support [适用于美洲用户] • https://secat-eu.cisco.com/portal/Support [适用于欧盟 (EU) 用户]
第 5 步	[在思科安全感知上]在思科安全感知云服务中创建模拟网络钓鱼邮件，并将其发送给您组织中的最终用户。此过程用于跟踪重复单击邮件中任何附件或 URL 的最终用户。	请参阅《CSA 管理员指南》，网址为： • https://secat.cisco.com/portal/Support [适用于美洲用户] • https://secat-eu.cisco.com/portal/Support [适用于欧盟 (EU) 用户]
第 6 步	从思科安全感知云服务获取身份验证令牌。	从思科安全感知云服务获取身份验证令牌， 第 5 页
第 7 步	在邮件网关上启用思科安全感知云服务。	在邮件网关上启用思科安全感知云服务， 第 5 页
第 8 步	创建自定义传入邮件策略，为归类为重复点击者的最终用户配置积极的邮件策略。	为归类为重复点击者的最终用户创建自定义传入邮件策略， 第 6 页

创建思科安全感知云服务帐户

根据您所在的地区，使用以下URL之一为您的组织创建具有管理访问权限的思科安全感知云服务帐户：

- https://secat.cisco.com [适用于美洲用户]
- https://secat-eu.cisco.com [适用于欧盟 (EU) 用户]

后续操作

配置防火墙设置，将您的邮件网关连接到思科安全感知云服务。有关详细信息，请参阅配置防火墙设置以访问思科安全感知云服务 ， 第 3 页

配置防火墙设置以访问思科安全感知云服务

您必须在防火墙上为以下主机名或 IP 地址打开 HTTPS（输出）443 端口（请参阅下表），才能将邮件网关连接到思科安全感知云服务。

服务	美洲地区		欧盟	
	主机名	IP 地址	主机名	IP 地址
思科安全感知云服务	secat.cisco.com	52.242.31.199	secat-eu.cisco.com	40.127.163.97
过程通知（出站）	-	167.89.98.161	-	40.127.163.97
登录和反馈页面（出站）	-	52.242.31.199	-	
邮件附件（出站）	-		-	

注释 上表所列的 IP 地址可能会变化。有关 IP 地址的最新列表，请参阅思科安全感知云服务上的“IP 允许列表指南”，网址为 https://secat.cisco.com/portal/Support/IpWhitelistingGuide

后续操作

创建新的发件人组，以允许邮件网关中来自思科安全感知云服务的模拟网络钓鱼邮件。有关详细信息，请参阅创建发件人组以在邮件网关中允许模拟的网络钓鱼邮件 ， 第 4 页

创建发件人组以在邮件网关中允许模拟的网络钓鱼邮件

您必须创建新的发件人组，以允许邮件网关中来自思科安全感知云服务的模拟网络钓鱼邮件。

开始之前

确保已将防火墙设置配置为允许您的邮件网关访问思科安全感知云服务。有关详细信息，请参阅配置防火墙设置以访问思科安全感知云服务，第 3 页

过程

步骤 1 单击**邮件策略 (Mail Policies) > HAT 概览 (HAT Overview)**。

步骤 2 单击**添加发件人组 (Add Sender Group)**。

步骤 3 输入发件人组的名称。

步骤 4 选择 **1** 作为优先级顺序。

步骤 5 选择 **CYBERSEC_AWARENESS_ALLOWED** 作为策略。

步骤 6 选中**不使用 SBRS (SBRS to Not in Use)** 复选框以禁用 IP 信誉过滤。

步骤 7 单击**提交并添加发件人 (Submit and Add Senders)**。

步骤 8 添加以下任何思科安全感知云服务 IP 地址，以根据您所在的区域配置为发件人 IP 地址：

- 美洲 - 207.200.3.14 或 173.244.184.143
- 欧盟 (EU) - 77.32.150.153

注释　思科安全感知云服务 IP 地址用于防止您的邮件网关将模拟网络钓鱼邮件解释为实际网络钓鱼。

步骤 9 提交并确认更改。

下一步做什么

1. 在思科安全感知云服务中创建新用户，以识别重复点击者。
2. 在思科安全感知云服务中创建模拟网络钓鱼邮件，并将其发送给您组织中的最终用户。

   有关如何完成上述两项任务的详细信息，请参阅《CSA 管理员指南》，网址为：

   - https://secat.cisco.com/portal/Support [适用于美洲用户]
   - https://secat-eu.cisco.com/portal/Support [适用于欧盟 (EU) 用户]

3. 从思科安全感知云服务获取身份验证令牌，以便从思科安全感知云服务下载重复点击者列表。有关详细信息，请参阅从思科安全感知云服务获取身份验证令牌，第 5 页

从思科安全感知云服务获取身份验证令牌

您必须从思科安全感知云服务获取身份验证令牌，并使用该令牌从思科安全感知云服务下载重复点击者列表。

开始之前

确保您在思科安全感知云服务中拥有一个具有管理员访问权限的帐户。有关详细信息，请参阅创建思科安全感知云服务帐户，第 3 页。如果您无法访问思科安全感知云服务，请联系思科支持部门获取帮助。

过程

步骤 1 登录思科安全感知云服务。

步骤 2 转到**环境 (Environment) > 设置 (Settings)**

步骤 3 单击**报告 API (Report API)** 选项卡。

步骤 4 选中**启用报告 API (Enable Report API)** 复选框。

步骤 5 复制身份验证令牌。

使用此身份验证令牌从思科安全感知云服务下载重复点击者列表。

下一步做什么

在邮件网关上启用思科安全感知云服务。有关详细信息，请参阅在邮件网关上启用思科安全感知云服务，第 5 页

在邮件网关上启用思科安全感知云服务

开始之前

确保您有：

- 有效的思科安全感知云服务帐户，且具有管理员访问权限。
- 从思科安全感知云服务获取了有效的身份验证令牌。有关详细信息，请参阅从思科安全感知云服务获取身份验证令牌，第 5 页，

过程

步骤 1 转到**安全服务 (Security Services) > 思科安全感知 (Cisco Secure Awareness)**。

步骤 2 单击**启用 (Enable)**。

步骤 3 选中**启用思科安全感知 (Enable Cisco Secure Awareness)** 复选框。

步骤 4 选择将您的邮件网关连接到思科安全感知云服务所需的服务器。

步骤 5 输入从思科安全感知云服务获取的身份验证令牌。

步骤 6 [可选]输入轮询间隔以便从思科安全感知云服务下载重复点击者列表。

步骤 7 提交并确认更改。

下一步做什么

- 启用思科安全感知云服务后，邮件网关会从思科安全感知云服务自动下载重复点击者列表。您可以通过导航到邮件网关 Web 界面中的**安全服务 (Security Services)** > **思科安全感知 (Cisco Secure Awareness)** > **重复点击者列表设置 (Repeat Clickers List Settings)** 部分，在“重复点击者”(Repeat Clickers) 列表中查看重复点击者用户数。有关“重复点击者”(Repeat Clickers) 列表的详细信息，请登录思科安全感知云服务，然后导航至“分析”(Analytics) > “标准报告”(Standard Reports) > “网络钓鱼模拟”(Phishing Simulations) > “重复点击者”(Repeat Clickers) 部分。
- 创建自定义传入邮件策略，为归类为重复点击者的最终用户配置积极的邮件策略。有关详细信息，请参阅为归类为重复点击者的最终用户创建自定义传入邮件策略，第 6 页

为归类为重复点击者的最终用户创建自定义传入邮件策略

您必须创建自定义传入邮件策略，为归类为重复点击者的最终用户配置积极的邮件策略。

过程

步骤 1 转到**邮件策略 (Mail Policies)** > **传入邮件策略 (Incoming Mail Policies)**。

步骤 2 单击**添加策略 (Add Policy)**。

步骤 3 输入策略的名称。

步骤 4 选中**添加用户 (Add User)**。

步骤 5 选择**以下收件人 (Following Recipients)**。

步骤 6 选中**包括重复点击者列表 (Include Repeat Clicker List)** 复选框以包括被思科安全感知云服务归类为重复点击者的收件人列表。

步骤 7 单击**确定 (OK)**。

步骤 8 单击**提交 (Submit)**。

步骤 9 为邮件策略配置所需的服务引擎（例如，防病毒、灰色邮件等）。

步骤 10 确认您的更改。

思科安全感知云服务和集群

如果使用集中管理，则可以启用集群、组和计算机级别的思科安全感知云服务。如果您在单机模式下启用了带有思科安全感知云服务的邮件网关，则可以选择加入使用思科安全感知云服务注册的集群。

注释 当您在计算机级别禁用思科安全感知云服务时，它只会对登录的邮件网关禁用，而集群中的其他计算机仍可连接到思科安全感知云服务。

查看日志

思科安全感知云服务信息会被发布到邮件日志。大多数信息处于“信息”或“调试”级别。

思科安全感知日志条目示例：

- 在本例中，日志显示由于令牌无效，从思科安全感知云服务下载重复点击者列表失败。

```
Tue Oct 13 10:12:59 2020 Warning: CSA:
The download of the Repeat Clickers list from
the Cisco Secure Awareness cloud service failed because
of an invalid token.
```

  解决方案：确保您从思科安全感知云服务获取有效的身份验证令牌。

- 在本例中，日志显示由于连接错误，从思科安全感知云服务下载重复点击者列表失败。

```
Wed Oct 14 10:59:36 2020 Warning: CSA:
The download of the Repeat Clickers list from
the Cisco Secure Awareness cloud service failed because
of a connection error.
```

  解决方案：验证用于将邮件网关连接到思科安全感知云服务的防火墙配置设置。

- 在本例中，日志显示由于内部服务器错误，从思科安全感知云服务下载重复点击者列表失败。

```
Wed Oct 14 10:59:36 2020 Warning: CSA:
The download of the Repeat Clickers list from
the Cisco Secure Awareness cloud service failed because
of an internal server error.
```

  解决方案：请联系思科支持部门以获取技术帮助。

- 在本例中，日志显示由于 SSL 证书验证失败，从思科安全感知云服务下载重复点击者列表失败。

```
Wed Oct 14 11:02:46 2020 Warning: CSA:
 The download of the Repeat Clickers list from
the Cisco Secure Awareness cloud service failed because
the SSL certificate verification failed.
```

  解决方案：在邮件网关的自定义证书颁发机构列表中添加代理服务器所需的 CA 证书。

- 在本例中，日志显示由于代理身份验证失败，从思科安全感知云服务下载重复点击者列表失败。

```
Wed Oct 14 11:09:48 2020 Warning: CSA:
The download of the Repeat Clickers list from
the Cisco Secure Awareness cloud service failed
because the proxy authentication failed.
```

解决方案：检查代理服务器是否在邮件网关中配置了正确的身份验证凭证。

- 在本例中，日志显示由于未在思科安全感知云服务上启用报告 API，对思科安全感知云服务的请求失败。

```
Mon Aug 17 15:35:42 2020 Warning: CSA:
The download of the Repeat Clickers list failed.
A request to the CSA cloud service failed because
the Report API was not enabled on the CSA cloud service
```

解决方案：在思科安全感知云服务的“环境 (Environmental) > 设置 (Settings) > 报告 API (Report API)”选项卡中选中“启用报告 API”(Enable Report API) 复选框。

- 在本例中，日志显示思科安全感知功能在特定日期到期。

```
2020-10-15 08:00:11,968 INFO csa The Cisco Secure
Awareness feature expires on 2029-12-28T23:59:59Z. You need to
contact your Cisco Account Manager to renew the license.
```

解决方案：请联系思科客户经理以续订许可证。

- 在本例中，日志显示思科安全感知功能的许可证已过期，并且您的电子邮件网关上已禁用该功能。

```
2020-10-27 13:33:21,714 CRITICAL csa The Cisco Secure
Awareness feature license has expired, and the feature is
disabled on your email gateway. Contact your Cisco Account Manager
to renew the license.
```

解决方案：请联系思科客户经理以续订许可证。

- 在本例中，日志显示下载的重复点击者列表为空。

```
Tue Oct 13 10:10:18 2020 Info: CSA: The downloaded
Repeat Clickers list is empty.
```

解决方案：在思科安全感知云服务中创建模拟网络钓鱼邮件，并将其发送给组织中的收件人。

- 在本例中，日志显示由于已达到最大下载尝试次数，从思科安全感知云服务下载重复点击者列表失败。

```
Fri Oct 16 05:22:08 2020 Warning: CSA: The download
of the Repeat Clickers list from the Cisco Secure Awareness
cloud service failed because you have reached the maximum
number of attempts.
```

解决方案：请联系思科支持，以增加从思科安全感知云服务下载重复点击者列表的尝试次数。

查看警报

下表包含为思科安全感知云服务生成的系统警报的列表，包括对警报和警报严重性的说明。

组件/警报名称	邮件和描述	参数
MAIL.CSA.DOWNLOAD _FAILURE	警报文本：从思科安全感知云服务下载重复点击者列表失败。$reason. (The download of the Repeat Clickers list from the Cisco Secure Awareness cloud service failed. $reason.） 警报级别：WARNING。 说明：从思科安全感知云服务下载重复点击者列表失败时发送警报。	参数：reason reason - 未能从思科安全感知云服务下载重复点击者列表的原因。 例如：“无效令牌”、“已达到最大尝试次数”等。
MAIL.CSA.EMPTY_ EMAIL_LIST	警报文本：下载的重复点击者列表为空。(The downloaded Repeat Clickers list is empty.) 警报级别：INFO。 说明：当下载的重复点击者列表为空时发送警报。此警报表示思科安全感知云服务中未列出重复点击者。	不适用。
MAIL.CSA.LICENSE_ EXPIRING	警报文本：思科安全感知功能许可证将于 $expiry 到期。您必须联系思科客户经理以续订许可证。(The Cisco Secure Awareness feature license expires on $expiry. You must contact your Cisco Account Manager to renew the license.) 地区：$region 服务器：$server 警报级别：INFO 说明：警报在到期前 7 天、3 天和 1 天时发送。	参数：expiry, region, server expiry – 思科安全感知许可证的到期日期。 region – 思科安全感知许可证即将到期的区域。区域可以是 AMERICAS、EUROPE 等。 server – 服务器 URL 的名称，例如 https://secat.cisco.com。

组件/警报名称	邮件和描述	参数
MAIL.CSA.LICENSE_ 已过期	警报文本：思科安全感知功能的许可证已过期，并且您的电子邮件网关上已禁用该功能。请联系思科客户经理以续订许可证。(The Cisco Secure Awareness feature license has expired, and the feature is disabled on your email gateway. Contact your Cisco Account Manager to renew the license.) 地区：$region 服务器：$server 警报级别：Critical 说明：在思科安全感知许可证到期时发送警报。	参数：region, server region – 思科安全感知许可证的区域已过期。区域可以是 AMERICAS、EUROPE 等。 server – 服务器 URL 的名称，例如 https://secat.cisco.com。
MAIL.CSA.LICENSE_ RETRIVAL_FAILURE	警报文本：从思科安全感知云服务检索许可证到期详细信息失败 $reason (The retrieval of the license expiry details from the Cisco Secure Awareness cloud service failed $reason) 警报级别：WARNING 说明：在思科安全感知云服务检索许可证到期详细信息失败时发送警报，连续三次。每天都会尝试检索许可证到期详细信息，直到成功检索许可证到期详细信息。	参数：reason reason - 未能从思科安全感知云服务检索许可证到期详细信息的原因。 例如：“无效令牌”和“已达到最大尝试次数”。