如何修复来自CTR的邮件

目录

简介

本文档介绍如何从思科威胁响应(CTR)修复邮件。

背景信息

CTR调查已更新，以支持按需邮件补救。管理员可以搜索来自O365和OnPrem Exchange用户邮箱的特定电子邮件，并通过邮件安全设备(ESA)或安全管理设备(SMA)进行补救。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- CTR帐户
- 思科安全服务交换
- ESA AsycnOs 14.0.1-033

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

注意：O365、Exchange 2016和2019混合部署和2013内部部署仅支持搜索和邮件补救。

配置

1. 在ESA中配置帐户设置
2. 配置链接的配置文件并将域映射到帐户配置文件
3. 将CTR与ESA或SMA集成

确认

您可以使用以下步骤调查CTR门户中的可观察项，并选择用于补救的消息：

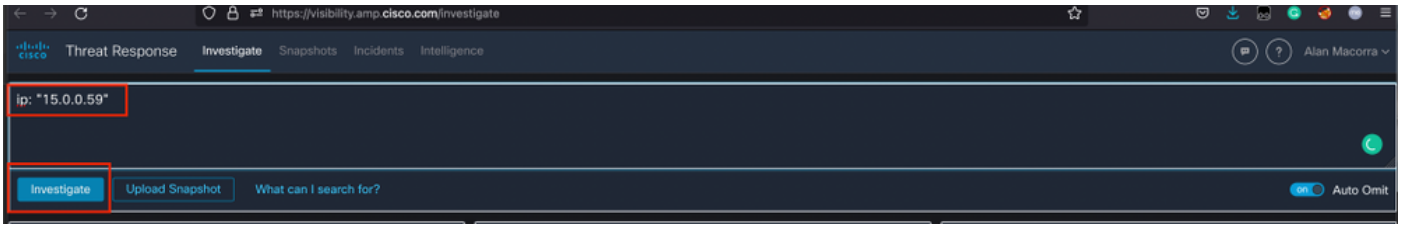
步骤1.根据对可用服务器的访问权限访问CTR门户并调查

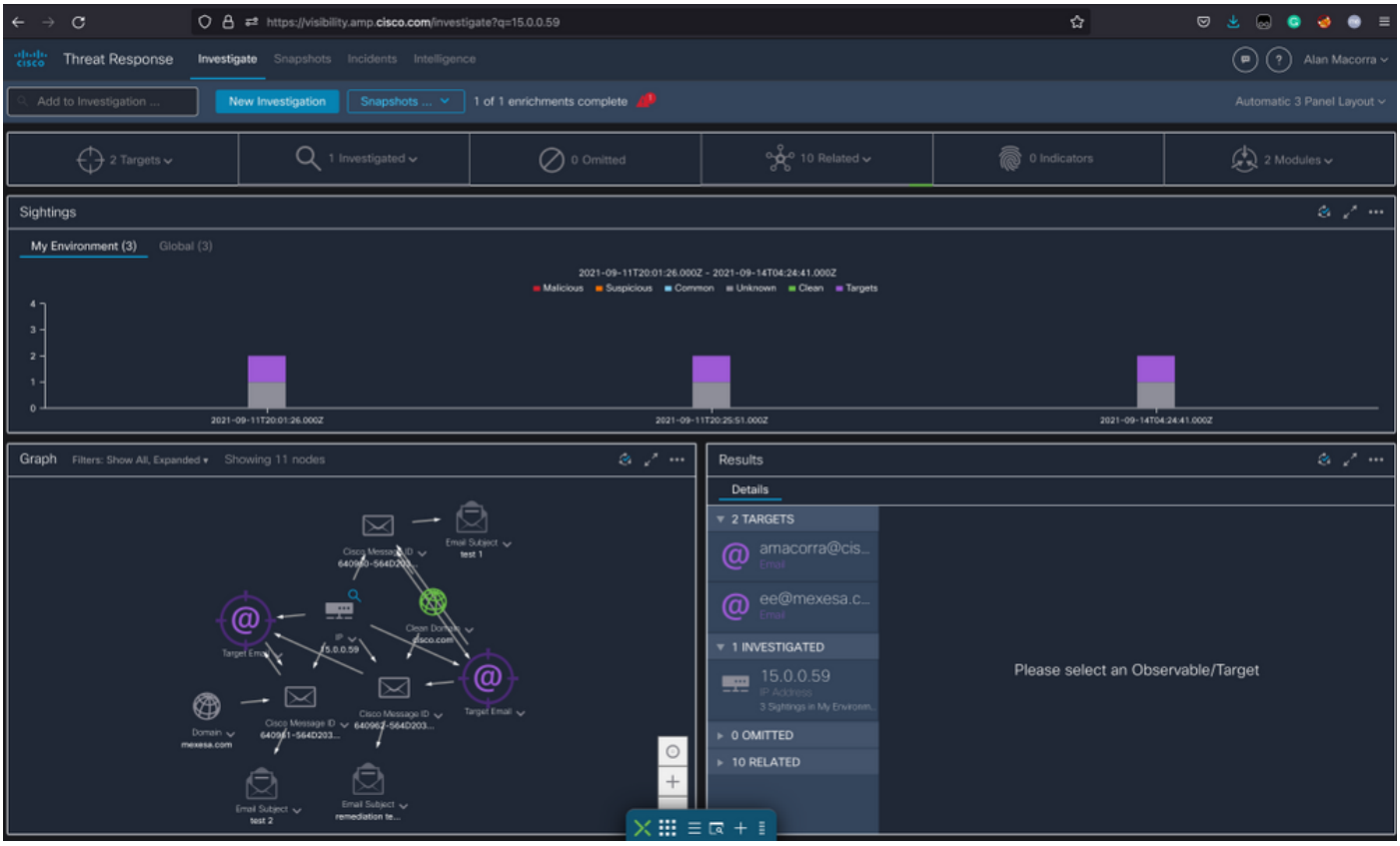
- 美国https://visibility.amp.cisco.com/investigate
- APJC https://visibility.apjc.amp.cisco.com/investigate
- 欧盟https://visibility.eu.amp.cisco.com/investigate

步骤2.使用支持的可观察信息来调查似乎是恶意或威胁的已传送邮件。可按以下标准搜索可观察项，如图所示：

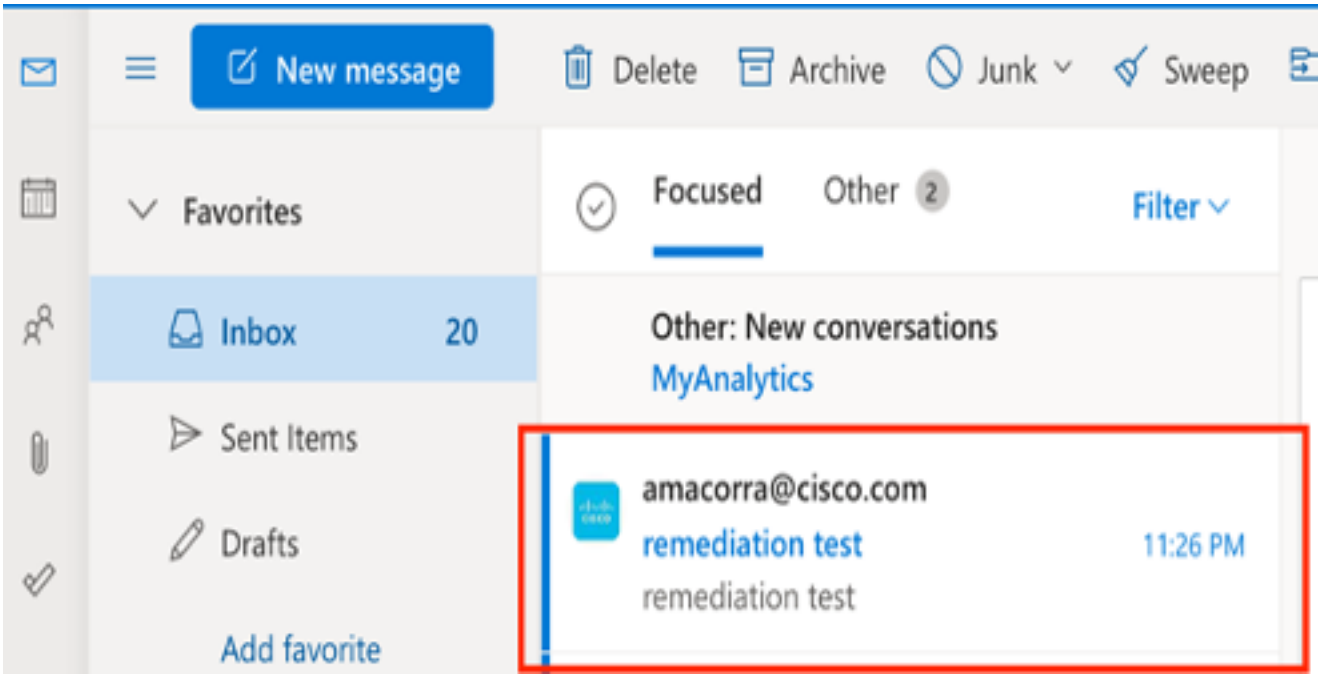
IP address	ip:"4.2.2.2"	Email subject	email_subject:"Invoice Due"
Domain	domain:"cisco.com"	Cisco Message ID (MID)	cisco_mid:"12345"
Sender email address	email:"noreply@cisco.com"	SHA256 filehash	sha256:"sha256filehash"
Email message header	email_messageid:"123-abc-456@cisco.com"	Email attachment file name	file_name:"invoice.pdf"

2.1下图所示的IP调查和调查示例：

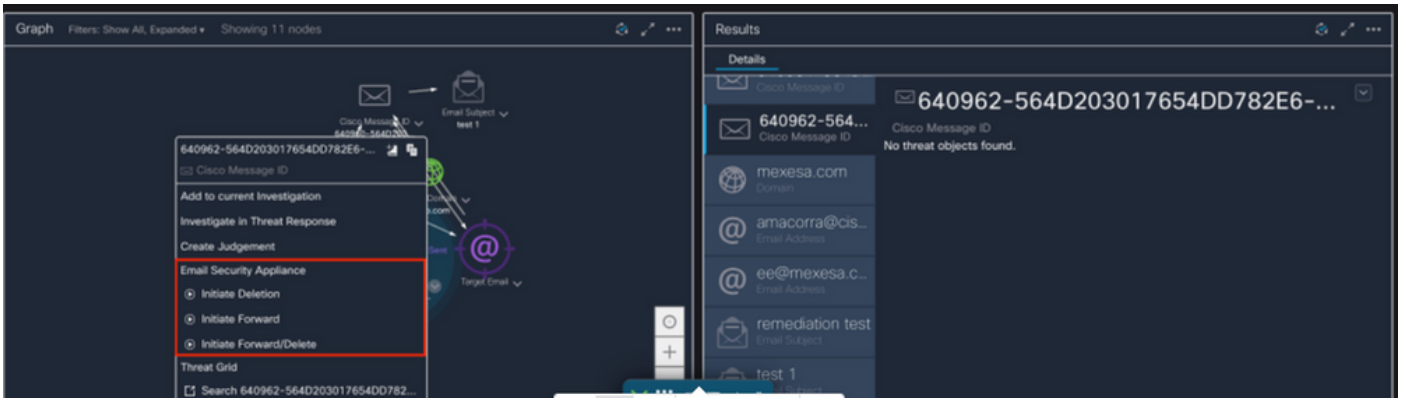




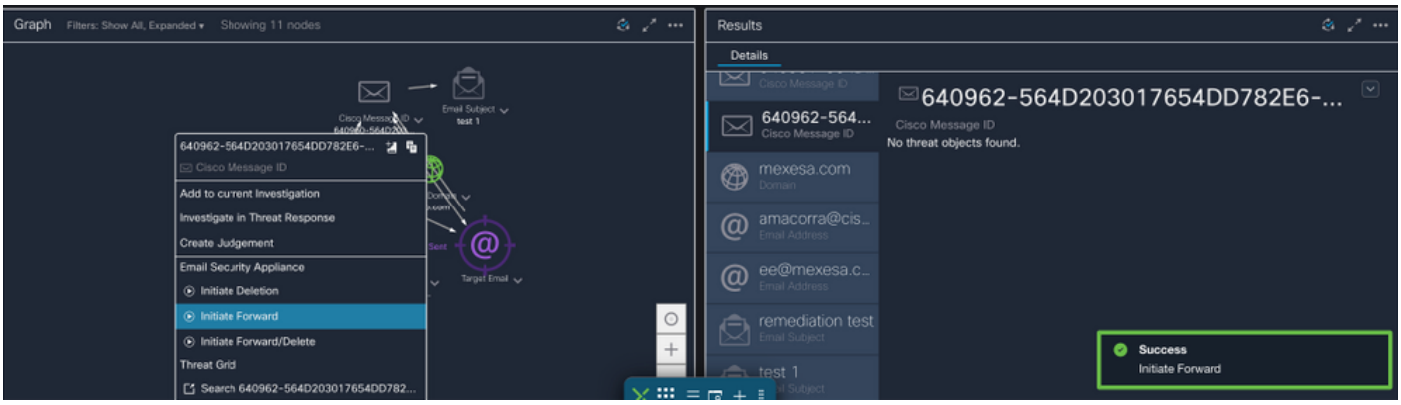
2.2如图所示，在修复邮件之前，您收到的收件箱内容如下：



2.3单击“思科消息ID”，从菜单选项中选择任何受支持的补救操作，如图所示：



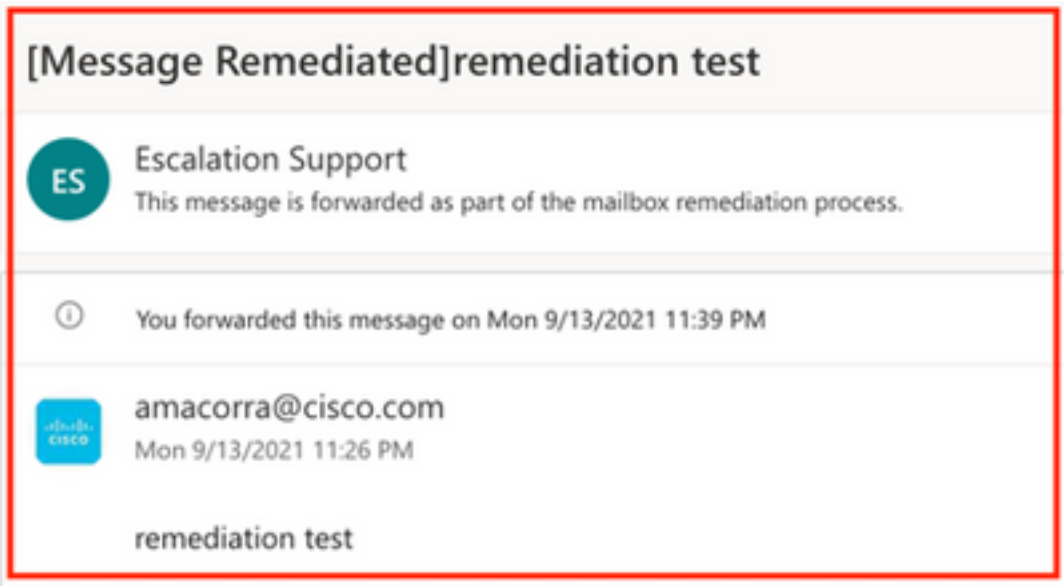
2.4在本例中，选择“Initiate Forward”，并在右下角显示“Success”弹出窗口，如图所示：



2.5在ESA中，您可以在“mail_logs”下看到以下日志，这些日志显示“CTR”补救已启动、已选操作和最终状态。

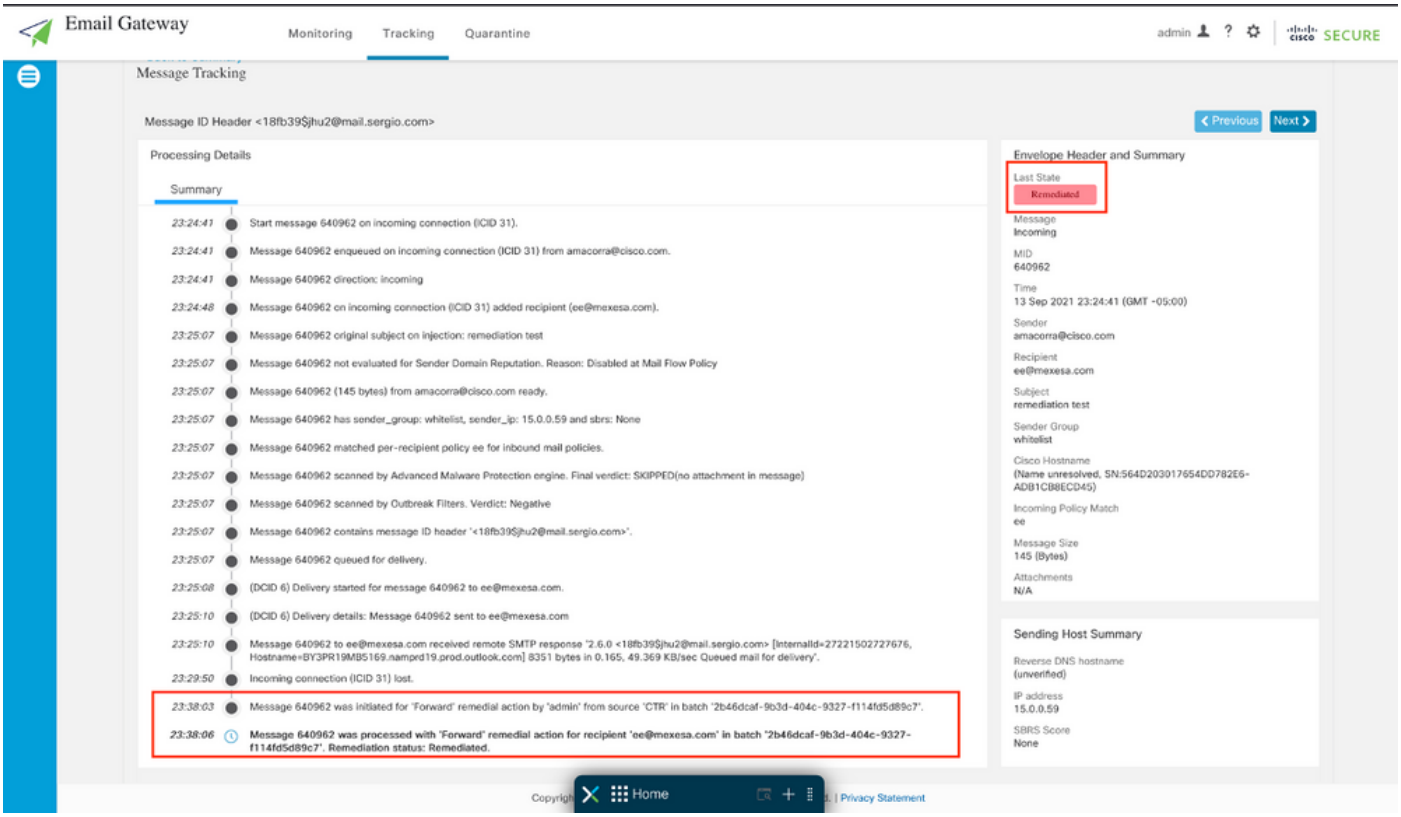
```
Mon Sep 13 23:38:03 2021 Info: Message 640962 was initiated for 'Forward' remedial action by
'admin' from source 'CTR' in batch '2b46dcaf-9b3d-404c-9327-f114fd5d89c7'.

Mon Sep 13 23:38:06 2021 Info: Message 640962 was processed with 'Forward' remedial action for
recipient 'ee@mexesa.com' in batch '2b46dcaf-9b3d-404c-9327-f114fd5d89c7'. Remediation status:
Remediated.
```

2.6语句“[Message Remediated]”在消息主题中出现前置，如图所示：



2.7在配置ESA/SMA模块时键入的电子邮件地址是在选择“转发”或“转发/删除”选项时接收修正电子邮件的地址，如图所示：

2.8最后，如果您查看ESA/SMA新接口的消息跟踪详细信息，可以看到在“mail_logs”和“Last State”中获取的日志与“Remediated”相同，如图所示：



注意：若在ESA/SMA中配置搜索和补救功能，则可以从CTR和ESA/SMA补救相同的消息。这允许您将同一邮件转发到与集成模块中配置的邮件地址不同的邮件地址。