Cisco XDR

思科 XDR 将思科安全产品连接到了一个集成平台。思科安全邮件威胁防御 与思科 XDR 和思科 XDR 功能区集成。

- XDR 让您可以在其他思科安全产品的数据旁边查看 思科安全邮件威胁防御 信息并对其采取行动。
- XDR 功能区让您可以在思科安全产品之间导航、访问案例集、搜索可观察对象以及查看事件。

有关本文档中未提供的 XDR 详细信息，请参阅思科 XDR 文档：
https://docs.xdr.security.cisco.com/

XDR

思科安全邮件威胁防御 提供可在思科 XDR 控制面板中查看的以下磁贴：

- 按方向分类的邮件：按方向显示总邮件流量。邮件被分为传出邮件、内部邮件和传入邮件。
- 威胁：显示被确定为 BEC、诈骗、网络钓鱼或恶意的邮件的快照。
- 垃圾邮件：显示被确定为垃圾邮件的邮件的快照。
- 灰色邮件：显示被确定为灰色邮件的邮件的快照。

有关 XDR 控制面板的信息，请参阅思科 XDR 文档：https://docs.xdr.security.cisco.com/

授权思科 XDR 思科安全邮件威胁防御

您必须拥有思科XDR帐户并且是思科XDR组织的成员，然后才能为思科安全邮件威胁防御授权思科XDR。有关详细信息，请参阅思科 XDR 文档：
https://docs.xdr.security.cisco.com/

注意：一个 思科安全邮件威胁防御 帐户一次只能与一个思科 XDR 组织集成。

思科安全邮件威胁防御 超级管理员和管理员用户可以为其 思科安全邮件威胁防御 实例授权思科 XDR 模块：

1. 选择**管理 (Administration) > 企业 (Business)**。
2. 在**首选项(Preferences)-扩展检测和响应(Extended Detection and Response)**下，点击**授权XDR集成(Authorize XDR Integration)**。
3. 完成授权流程。

系统将显示一个横幅，说明 XDR 配置成功。

现在，您可以将 思科安全邮件威胁防御 磁贴添加到 XDR 控制面板。有关如何执行此操作的信息，请参阅思科 XDR 文档：
https://docs.xdr.security.cisco.com/Content/Control-Center/configure-dashboards.htm

撤销 XDR 授权 思科安全邮件威胁防御

注意：任何超级管理员或管理员用户均可执行此任务。它不必由为 思科安全邮件威胁防御 实例授权 XDR 的用户执行。

要撤销 XDR 授权，请执行以下操作：

1. 选择**管理 (Administration)** > **企业 (Business)**。
2. 在**首选项 (Preferences)**、**扩展检测和响应 (Extended Detection and Response)** 下，点击**撤销授权 (Revoke Authorization)**。

系统将显示一个横幅，说明 XDR 配置已成功更新。

XDR 功能区

XDR 功能区位于页面下方，当您在 思科安全邮件威胁防御 和环境中的其他思科安全产品之间移动时，此功能仍然存在。任何思科安全邮件威胁防御用户都可以授权使用XDR功能区。使用功能区在思科安全应用之间导航、访问案例集、搜索可观察对象以及查看事件。

有关 XDR 功能区的信息，请参阅思科 XDR 文档：
https://docs.xdr.security.cisco.com/Content/Ribbon/ribbon.htm

深入调查菜单

如果授权功能区，XDR透视菜单将被添加到思科安全邮件威胁防御邮件报告中。通过这些菜单，您可以集中访问每个可观察对象的其他信息，具体取决于您购买的思科安全产品。

同样，通过思科安全邮件威胁防御与XDR的集成，您可以使用透视菜单来从XDR访问思科安全邮件威胁防御。您可以从中透视的可观察对象包括：

- 邮箱地址
- 邮件 ID
- 电子邮件主题
- 文件名
- 发件人 IP
- SHA 256
- URL

使用透视菜单执行以下操作：

- 直接从透视菜单隔离具有特定可观察对象的邮件。思科安全邮件威胁防御会将这些邮件指示为由 XDR 用户手动补救。
  - **注意**：透视菜单中的隔离区限制为 100 封邮件。
- 将您隔离的邮件移回收件箱。思科安全邮件威胁防御会将这些邮件指示为由 XDR 用户手动补救。
  - **注意：**从隔离区移至收件箱的邮件数量限制为 100 封。

有关 XDR 透视菜单的更多信息，请参阅 XDR 文档：
https://docs.xdr.security.cisco.com/Content/pivot-menu.htm

授权 XDR 功能区

XDR 功能区在用户级别进行授权。您可以从功能区中或从“用户首选项”(User Preferences) 菜单中授权功能区。

注意：需要先激活 XDR 帐户，然后才能授权功能区。您可以按照授权思科 XDR 思科安全邮件威胁防御，第 55 页中的说明或通过在 XDR 中集成任何其他模块来执行此操作。

从 XDR 功能区中授权

要从功能区中授权 XDR 功能区，请执行以下操作：

1. 点击 XDR 功能区中的**获取 XDR (Get XDR)**。
2. 在“授予应用访问权限”(Grant Application Access) 对话框中，点击**授权安全邮件威胁防御功能区 (Authorize Secure Email Threat Defense Ribbon)**。

您的 XDR 功能区现已获得授权。系统将显示一个横幅，说明 XDR 配置已成功更新。

从思科安全邮件威胁防御用户设置授权

要从“用户设置”(User Settings) 菜单授权 XDR 功能区，请执行以下操作：

1. 选择**用户**（配置文件图标）> **用户设置 (User Settings)**。
2. 在**首选项 (Preferences)** > **XDR 功能区 (XDR Ribbon)** 下，点击**授权 XDR 功能区 (Authorize XDR Ribbon)**。
3. 在“授予应用访问权限”(Grant Application Access) 对话框中，点击**授权思科安全邮件威胁防御功能区 (Authorize Cisco Secure Email Threat Defense Ribbon)**。

您的 XDR 功能区现已获得授权。系统将显示一个横幅，说明 XDR 配置已成功更新。

撤销 XDR 功能区授权

XDR 功能区在用户级别进行授权。您可以从功能区中或从“用户首选项”(User Preferences) 菜单中撤销授权。

从 XDR 功能区中撤销授权

要从功能区中撤销 XDR 功能区授权，请执行以下操作：

1. 在 XDR 功能区中选择**设置 (Settings)** > **授权 (Authorization)** > **撤销 (Revoke)**。
2. 在“撤销”(Revoke) 对话框中，点击**确认 (Confirm)**。

您的 思科安全邮件威胁防御 用户帐户已不再获得 XDR 功能区的授权。

从思科安全邮件威胁防御用户设置撤销授权

要从“用户设置”(User Settings) 菜单撤销 XDR 功能区授权，请执行以下操作：

1. 选择**用户**（配置文件图标）> **用户设置 (User Settings)**。
2. 在**首选项 (Preferences)** > **XDR 功能区 (XDR Ribbon)** 下，点击**撤销授权 (Revoke Authorization)**。

您的 思科安全邮件威胁防御 用户帐户已不再获得 XDR 功能区的授权。系统将显示一个横幅，说明 XDR 配置已成功更新。

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。