Cisco XDR

Cisco XDR は、シスコのセキュリティ製品を統合プラットフォームに接続します。Secure Email Threat Defense は、Cisco XDR および Cisco XDR リボンと統合されています。

- XDR を使用すると、その他のシスコのセキュリティ製品からのデータと一緒に Secure Email Threat Defense の情報を確認し、アクションを実行できます。
- XDR リボンを使用すると、シスコのセキュリティ製品間を移動したり、ケースブックにアクセスしたり、オブザーバブルを検索したり、インシデントを表示したりできます。

このドキュメントに記載されていない XDR の詳細については、Cisco XDR のマニュアル（https://docs.xdr.security.cisco.com/）を参照してください。

XDR

Secure Email Threat Defense には、Cisco XDR ダッシュボードで表示できる次のタイルがあります。

- [宛先別メッセージ（Messages by direction）]：電子メールトラフィックの合計が宛先別に表示されます。電子メールは、[送信（Outgoing）]、[内部（Internal）]、および [受信（Incoming）] に分けられます。
- [脅威（Threats）]：BEC、詐欺、フィッシング、または悪意のあると判定されたメッセージのスナップショットが表示されます。
- [スパム（Spam）]：スパムと判定されたメッセージのスナップショットが表示されます。
- [グレイメール（Graymail）]：グレイメールと判定されたメッセージのスナップショットが表示されます。

XDR ダッシュボードの詳細については、Cisco XDR のマニュアル（https://docs.xdr.security.cisco.com/）を参照してください。

の Cisco XDR の承認 Secure Email Threat Defense

Secure Email Threat Defense の Cisco XDR を承認するには、Cisco XDR のアカウントを持ち、Cisco XDR 組織の一員となる必要があります。詳細については、Cisco XDR のマニュアル（https://docs.xdr.security.cisco.com/）を参照してください。

注：Secure Email Threat Defense アカウントは、一度に 1 つの Cisco XDR 組織とのみ統合できます。

Secure Email Threat Defense のネットワーク管理者および管理者ユーザーは、Secure Email Threat Defense インスタンス向けに Cisco XDR モジュールを承認できます。

1. [管理（Administration）] > [ビジネス（Business）] の順に選択します。
2. [初期設定（Preferences）] > [Extended Detection and Response] で、[XDR 統合の承認（Authorize XDR Integration）] をクリックします。
3. 承認フローを完了します。

XDR 設定が成功したことを示すバナーが表示されます。

XDR ダッシュボードに Secure Email Threat Defense のタイルを追加できるようになりました。その実行方法については、Cisco XDR のマニュアル（https://docs.xdr.security.cisco.com/Content/Control-Center/configure-dashboards.htm）を参照してください。

の XDR 承認の取り消し Secure Email Threat Defense

注: スーパー管理者または管理者ユーザーがこのタスクを実行できます。Secure Email Threat Defense インスタンス向けに XDR を承認したユーザーでなくてもこのタスクを実行できます。

XDR の承認を取り消すには、次の手順に従います。

1. [管理（Administration）] > [ビジネス（Business）] の順に選択します。
2. [初期設定（Preferences）] > [Extended Detection and Response] で、[承認を取り消す（Revoke Authorization）] をクリックします。

XDR 設定が正常に更新されたことを示すバナーが表示されます。

XDR リボン

XDR リボンはページの下部に配置されており、ご使用環境内で Secure Email Threat Defense とその他のシスコのセキュリティ製品間を移動しても保持されます。すべての Secure Email Threat Defense ユーザーは、XDR リボンの使用を承認できます。リボンを使用して、シスコのセキュリティ アプリケーション間を移動したり、ケースブックにアクセスしたり、オブザーバブルを検索したり、インシデントを表示したりします。

XDR リボンの詳細については、Cisco XDR のマニュアル（https://docs.xdr.security.cisco.com/Content/Ribbon/ribbon.htm）を参照してください。

ピボットメニュー

リボンを承認すると、Secure Email Threat Defense のメッセージレポート内に XDR ピボットメニューが追加されます。これらのメニューは、購入したシスコのセキュリティ製品に応じて、各オブザーバブルに関する追加情報にアクセスするための中心地点となります。

同様に、Cisco Secure Email Threat Defense と XDR の統合により、ピボットメニューを使用して XDR から Cisco Secure Email Threat Defense にアクセスできます。ピボットできる観測対象は次のとおりです。

- [電子メールアドレス（Email Address）]
- [電子メールメッセージ ID（Email Message ID）]
- [電子メールの件名（Email Subject）]
- [ファイル名（File Name）]
- [送信者 IP（Sender IP）]
- [SHA 256（SHA 256）]
- [URL（URL）]

ピボットメニューを使用して、次の操作を実行します:

- 特定の監視可能なメッセージをピボットメニューから直接隔離します。この方法で隔離されたアイテムは、XDR を使用して、または XDR ユーザーによって手動で修復されたことを Cisco Secure Email Threat Defense で示します。
  - **注:** ピボットメニューからの隔離は 100 メッセージまでに制限されています。
- Cisco Secure Email Threat Defense で検索を開始します。

XDR のピボットメニューの詳細については、XDR のマニュアル（https://docs.securex.security.cisco.com/SecureX-Help/Content/pivot-menus.html）を参照してください

XDR リボンの承認

XDR リボンはユーザーレベルで承認されます。リボン内または [ユーザー設定(User Preferences)] メニューからリボンを承認できます。

注: リボンを承認する前に、XDR アカウントをアクティブ化する必要があります。これを行うには、の Cisco XDR の承認 Secure Email Threat Defense（55 ページ）の指示に従うか、他のモジュールを XDR に統合します。

XDR リボン内からの承認

リボン内から XDR リボンを承認するには、次の手順を実行します。

1. XDR リボンで [XDR の取得(Get XDR)] をクリックします。
2. [アプリケーションアクセスの許可(Grant Application Access)] ダイアログで、[Secure Email Threat Defense リボンを承認(Authorize Secure Email Threat Defense Ribbon)] をクリックします。

XDR リボンが承認されました。XDR 設定が正常に更新されたことを示すバナーが表示されます。

Secure Email Threat Defense のユーザー設定からの承認

[ユーザー設定(User Settings)] メニューから XDR リボンを承認するには、次の手順を実行します。

1. [ユーザー(User)](プロフィールアイコン)> [ユーザー設定(User Settings)] を選択します。
2. [初期設定(Preferences)] > [XDR リボン(XDR Ribbon)] で、[XDR リボンの承認(Authorize XDR Ribbon)] をクリックします。
3. [アプリケーションアクセスの許可(Grant Application Access)] ダイアログで、[Cisco Secure Email Threat Defense リボンを承認(Authorize Cisco Secure Email Threat Defense)] をクリックします。

XDR リボンが承認されました。XDR 設定が正常に更新されたことを示すバナーが表示されます。

XDR リボンの承認の取り消し

XDR リボンはユーザーレベルで承認されます。リボン内または [ユーザー設定(User Preferences)] メニューから承認を取り消すことができます。

XDR リボン内からの承認の取り消し

リボン内から XDR リボンの承認を取り消すには、次の手順を実行します。

1. XDR リボンで [設定(Settings)] > [承認(Authorization)] > [取り消し(Revoke)] を選択します。
2. [取り消し(Revoke)] ダイアログで、[確認(Confirm)] をクリックします。

XDR リボンが Secure Email Threat Defense ユーザーアカウントに対して承認されなくなりました。

Secure Email Threat Defense のユーザー設定からの承認の取り消し

[ユーザー設定(User Settings)] メニューから XDR リボンの承認を取り消すには、次の手順を実行します。

1. [ユーザー(User)](プロフィールアイコン)> [ユーザー設定(User Settings)] を選択します。
2. [初期設定(Preferences)] > [XDR リボン(XDR Ribbon)] で、[承認を取り消す(Revoke Authorization)] をクリックします。

XDR リボンが Secure Email Threat Defense ユーザーアカウントに対して承認されなくなりました。XDR 設定が正常に更新されたことを示すバナーが表示されます。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。