SecureX との統合

Cisco SecureX 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、SecureX および SecureX リボンと統合されています。

- SecureX を使用すると、他のシスコセキュリティ製品からのデータと一緒に Secure Email Threat Defense の情報を確認することができます。
- SecureX 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。

本書に記載されていない SecureX の詳細については、SecureX のドキュメントを参照してください：
https://docs.securex.security.cisco.com/

SecureX

Secure Email Threat Defense には、SecureX 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）]、[混合（Mixed）]、[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。
- [悪意ありおよびフィッシング（Malicious & Phishing）]：悪意のある、またはフィッシングで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。

  注：このタイルは廃止され、今後のリリースで削除されます。[悪意ありおよびフィッシング（Malicious and Phishing）] タイルを削除し、新しい [脅威（Threats）] タイルを SecureX ダッシュボードに追加する必要があります。

SecureX ダッシュボードの詳細については、SecureX のドキュメントを参照してください：
https://docs.securex.security.cisco.com/

SecureX の承認 Secure Email Threat Defense

Secure Email Threat Defense に対して SecureX を承認する前に、SecureX アカウントを取得し、SecureX 組織の一員になっている必要があります。詳細については、SecureX のドキュメントを参照してください：
https://docs.securex.security.cisco.com/SecureX-Help/Content/introduction.html

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

Secure Email Threat Defense のスーパー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 SecureX モジュールを承認できます。

1. [設定（Settings）]（歯車アイコン）> [管理（Administration）] > [ビジネス（Business）] を選択します。
2. [初期設定（Preferences）] > [SecureX] で、[SecureX 統合の承認（Authorize SecureX Integration）] をクリックします。
3. 承認フローを完了します。

SecureX 設定が成功したことを示すバナーが表示されます。

SecureX 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。その手順については、SecureX のドキュメントを参照してください：
https://docs.securex.security.cisco.com/SecureX-Help/Content/configure-tiles.html

SecureX の承認を取り消す 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 SecureX 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。

SecureX の承認を取り消すには、次の手順に従います。

1. [設定(Settings)](歯車アイコン)> [管理(Administration)] > [ビジネス(Business)] を選択します。
2. [初期設定(Preferences)] > [SecureX] で、[承認を取り消す(Revoke Authorization)] をクリックします。

SecureX 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。

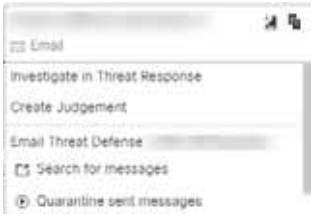
SecureX のリボン

SecureX 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 と他のシスコ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、SecureX 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。

SecureX リボンの詳細については、SecureX のドキュメントを参照してください：
https://docs.securex.security.cisco.com/SecureX-Help/Content/ribbon.html

ピボットメニュー

リボンを承認すると、Secure Email Threat Defense の展開メッセージビュー内に SecureX 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 SecureX の統合により、ピボットメニューを使用して 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
- 送信者 IP(Sender IP)
- SHA 256
- 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、SecureX を使用して、または SecureX 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、現在 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。

SecureX のピボットメニューの詳細については、SecureX のドキュメントを参照してください:
https://docs.securex.security.cisco.com/SecureX-Help/Content/pivot-menus.html

SecureX リボンの承認

SecureX 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、SecureX 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、SecureX の承認 Secure Email Threat Defense(53 ページ)の指示に従うか、他のモジュールを SecureX に統合します。

SecureX リボン内からの承認

リボン内から SecureX リボンを承認するには、次の手順を実行します。

1. SecureX リボンで [SecureX を取得(Get SecureX)] 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。

SecureX リボンが認証されました。SecureX 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 SecureX 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)] > [SecureX リボン(SecureX Ribbon)] で、[SecureX リボンの承認(Authorize SecureX 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。

SecureX リボンが認証されました。SecureX 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。

SecureX リボンの承認を取り消す

SecureX 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。

Secure X リボン内から承認を取り消す

リボン内から SecureX リボンの承認を取り消すには、次の手順を実行します。

1. SecureX 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。

SecureX リボンが Secure Email Threat Defense 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 SecureX 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)] > [SecureX リボン(SecureX Ribbon)] で、[承認を取り消す(Revoke Authorization)] をクリックします。

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