



## 2021 年 5 月

---

2021 年 5 月にリリースされた、シスコのクラウドベースの機械学習によるグローバル脅威アラートに関するアップデートです。

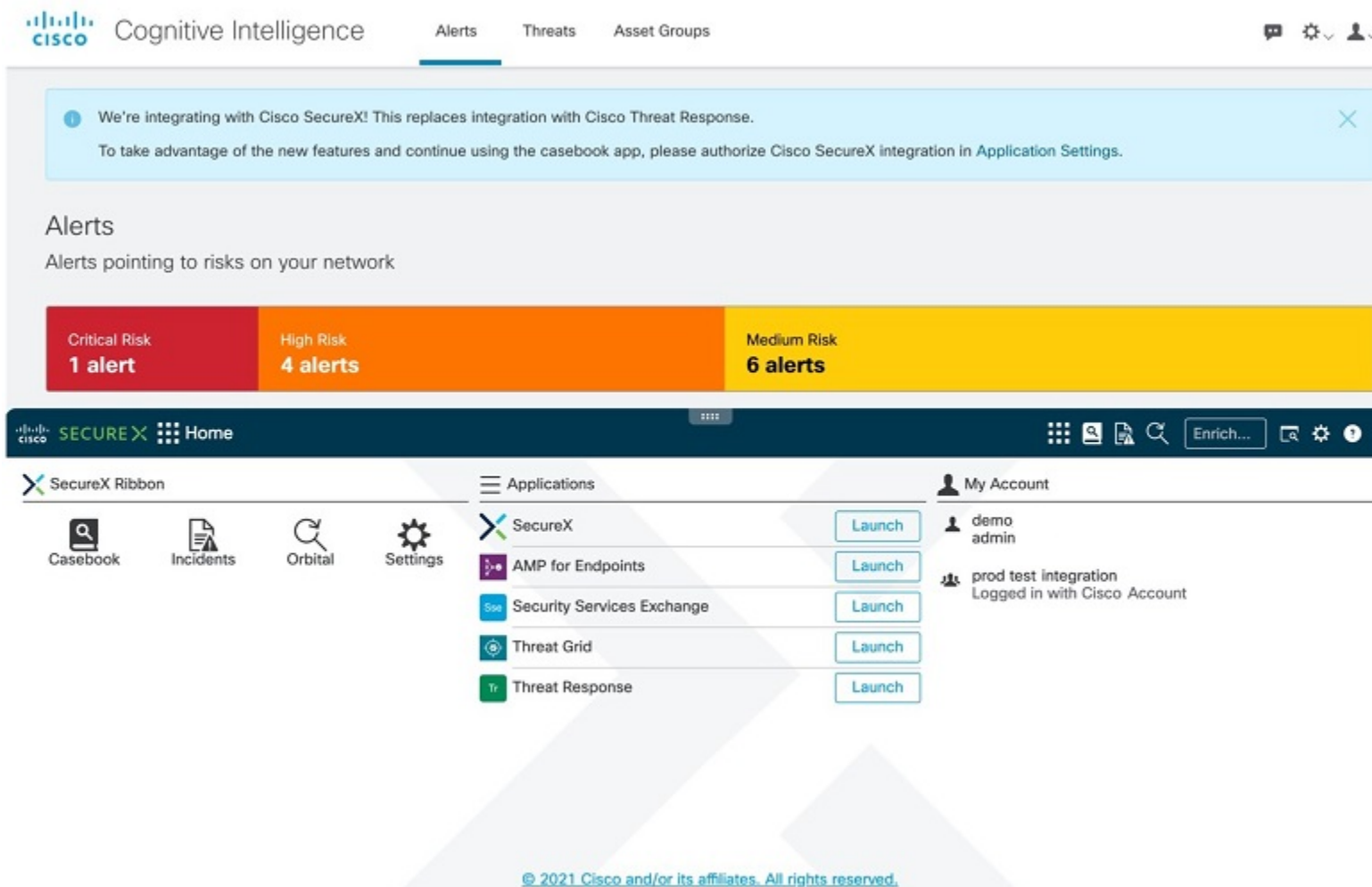
- [SecureX リボンのサポート \(1 ページ\)](#)
- [更新された日次レポート電子メール \(4 ページ\)](#)

## SecureX リボンのサポート

SecureX は、中央管理型コンソールであると同時に、可視性の統合、自動化の実現、インシデント対応ワークフローの迅速化、脅威ハンティングの改善を行う一連の分散機能でもあります。これらの分散機能は、SecureX リボンでアプリケーションおよびツールの形式で表示されます。

SecureX リボンがページ下部にあるグローバル脅威アラートでも使用できるようになり、環境内のダッシュボードと他のセキュリティ製品間を移動しても保持されます。これは、事例集やインシデントと調査結果を関連付けるのに役立ちます。

図 1: ページの下部にある SecureX リボン



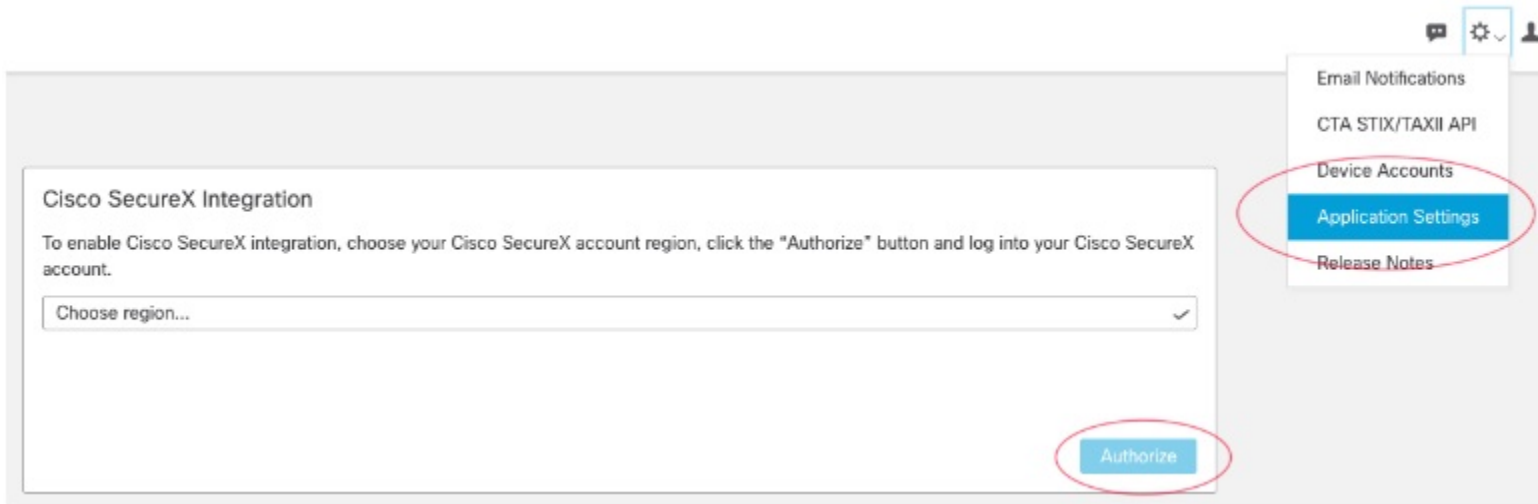
リボンを使用して、事例集、設定、およびその他のアプリケーションにアクセスできます。また、インシデントを表示し、監視対象を検索してエンリッチメントを追加することもできます。

図 2: 例 : SecureX リボンを使用して事例集にアクセスする

The screenshot displays the Cisco SecureX interface. At the top, there are navigation tabs for Alerts, Threats (selected), and Asset Groups. The main section is titled 'Threats' and shows 'Threats that we detected on your network'. Under 'Critical Severity', two threat cards are visible: 'Gamarue' (Confirmed, Alerts: 1, Assets: 1) and 'QuasarRAT' (Confirmed, Alerts: 1, Assets: 1). Below this, the 'Casebook' view is shown for a case titled 'B connected to http://.../com/'. The Casebook interface includes a search bar, a list of cases (Owned By Me, Owned By Others), and a detailed view of the selected case. The detailed view shows the title, creation date (May 19, 2021, 2:25:24 AM), owner, and linked incidents. A list of observables is also displayed, including AMP GUID, Domains, Hostname, IP Addresses, MAC Address, SHA-256, and URLs, each with associated counts and status indicators.

この機能を有効にするには、ユーザーが SecureX アカウントを持ち、アプリケーション設定で統合を承認する必要があります。

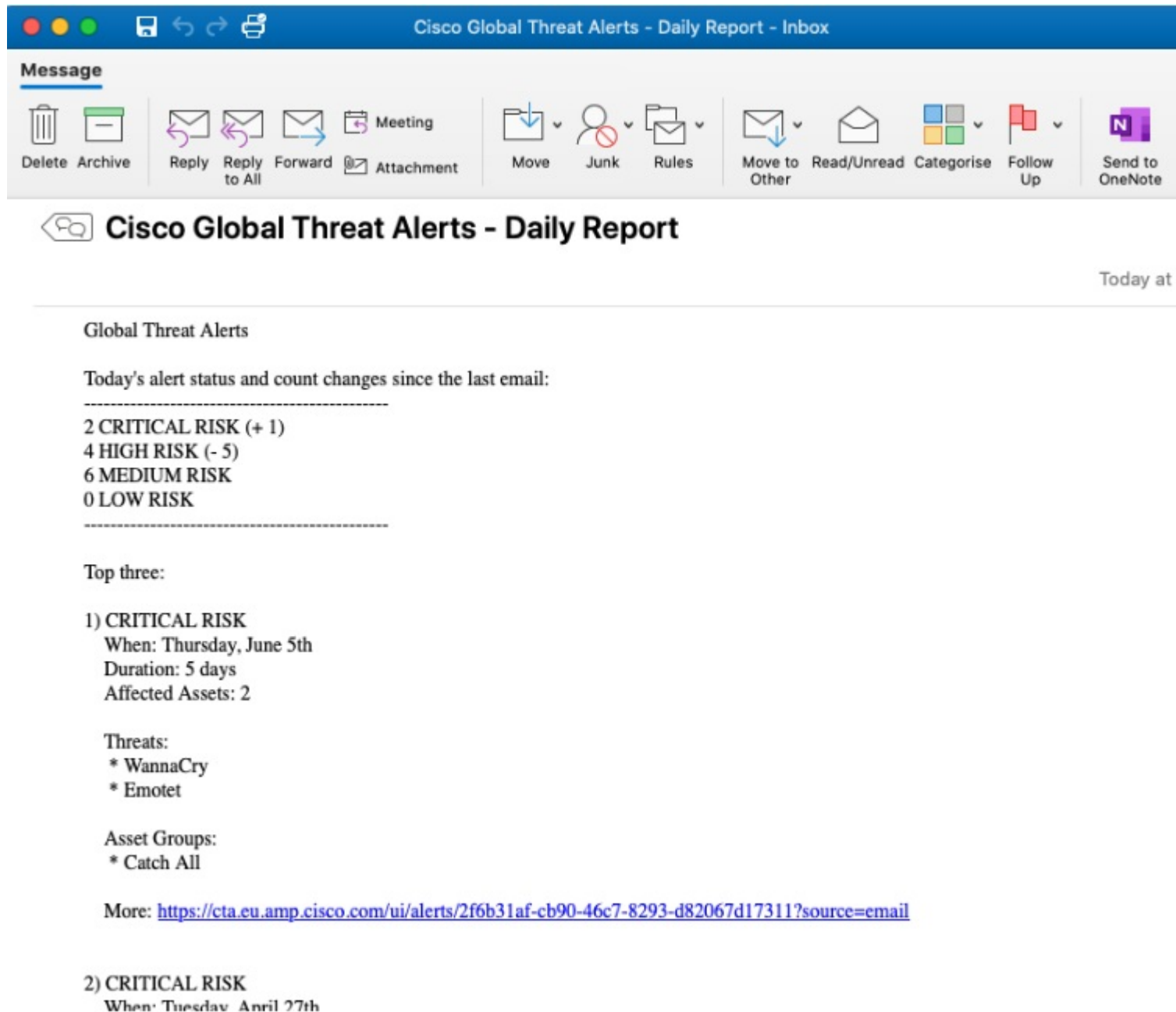
図 3: [アプリケーション設定 (Application Settings)] に移動し、SecureX との統合を承認します。



## 更新された日次レポート電子メール

電子メール通知サービスが更新され、アラートダッシュボードと互換性のあるコンテンツが電子メールで送信されるようになりました。日次レポートの電子メールでは、アラートの現在のステータスと、報告されたアラート数の最近の変化が通知されます。

図 4: 例: 更新された日次レポートの電子メール



このサービスを有効にするには、グローバル設定メニューから [電子メール通知 (Email Notifications)] を選択し、日次レポートを受信する電子メールアドレスを入力します。



## 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。