2021 年 6 月

2021 年 6 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。

自動化サポート用の新しい REST API

グローバル脅威アラートのダッシュボードに表示されるすべてのデータが、新しい REST API を介して使用できるようになりました。これを使用して、単一のアラートの内容をダウンロードしたり、すべてのアラートをネットワーク内のサードパーティ SIEM にストリーミングすることで、データ収集プロセス全体を自動化したりすることもできます。

API は読み取り専用ではないため、グローバル脅威アラート環境の設定を変更できます。たとえば、重要なアセットグループの特定のビジネス価値を高めたり、脅威に割り当てられた重大度を変更したりできます。

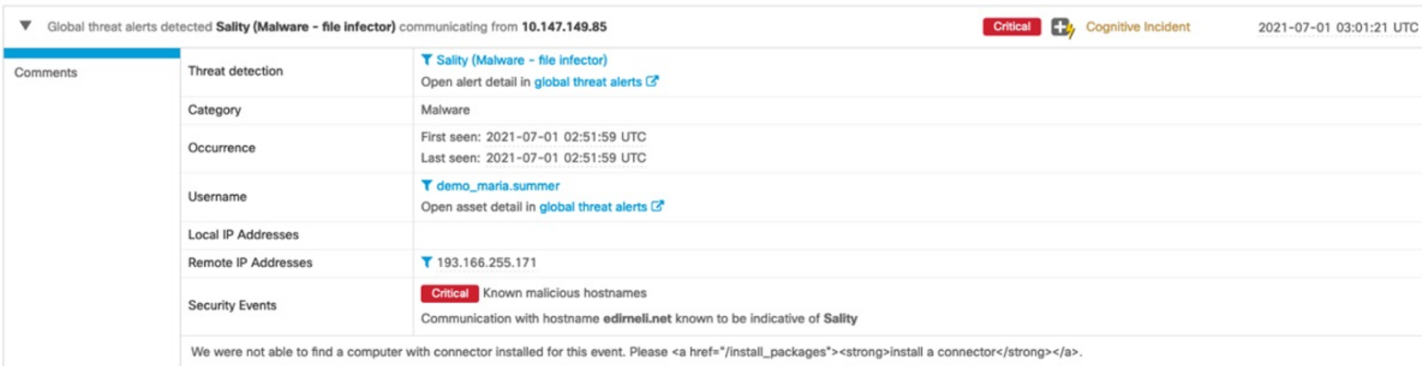
API の機能については、https://api.cta.eu.amp.cisco.com を参照してください。API の機能をより詳細に説明する仕様や使用例、追加の統合のためのサンプルスクリプトを確認することができます。

新しい REST API の詳細については、「global threat alerts REST API is now released!」[英語] を参照してください。

Secure Endpoint 統合の更新

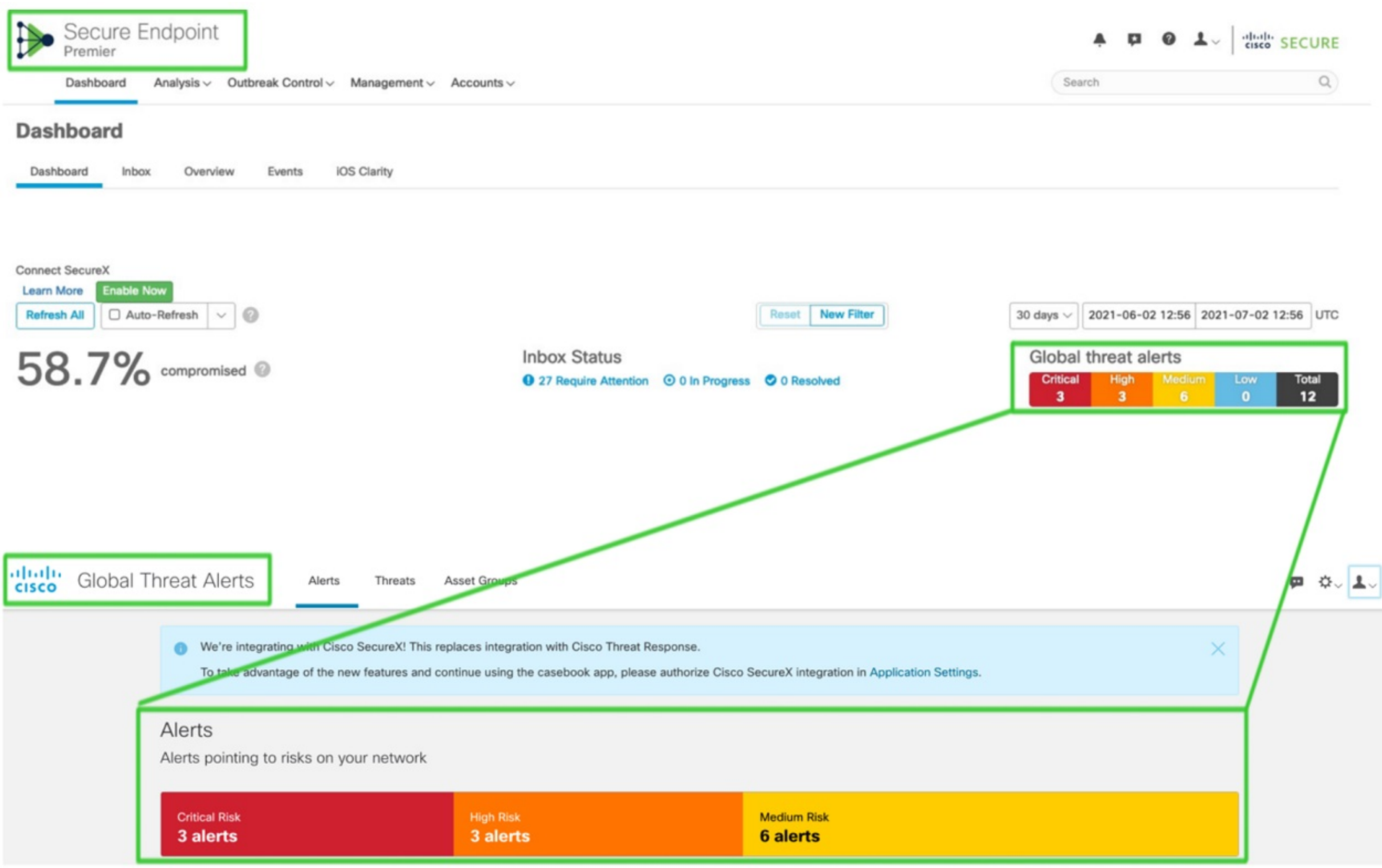
グローバル脅威アラートからの検出内容を Secure Endpoint で表示する方法が更新されました。現在、検出内容はコンソールにイベントとして表示され、アラートインターフェイスに直接リンクされています。その結果、アラートインターフェイスでの脅威の重大度が変更されると、その変更がこれらのイベントで反映されます。

図 *1* : グローバル脅威アラートの検出内容は、*Secure Endpoint* コンソールでイベントとして表示されるようになりました。



グローバル脅威アラートインターフェイスでアラートの状態またはリスクが変更されると、その変更が Secure Endpoint コンソールのアラートの概要で反映されます。

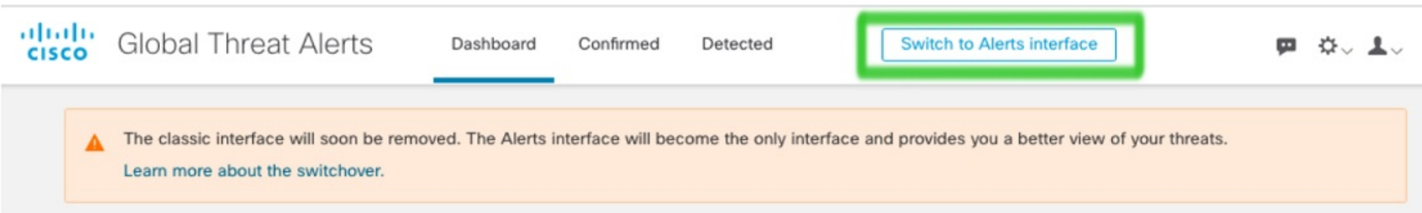
図 *2* :



互換性の問題を回避するため、従来のインターフェイスは間もなく廃止されます。そのため、従来のインターフェイスからアラートインターフェイスに切り替えることをお勧めします。グ

ローバル脅威アラートダッシュボードで、[アラートインターフェイスに切り替え（Switch to Alerts interface）] ボタンをクリックします。

図 *3:*



STIX/TAXII API の更新

STIX/TAXII API フィードによって提供される検出リンクと脅威に関する用語が、グローバル脅威アラートダッシュボードのアラートインターフェイスと互換性を持つようになりました。

図 *4:*


```xml
<s:Incident xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
            xsi:type="inc:IncidentType"
            URL="https://cta.eu.amp.cisco.com/ui/assets/demo_3399f455c51cf4879ce08796f0dee9613832f2bd165127f4f7e5fabcc825979c"
            id="cta:incident-demo_a304ea5e63d526a9077406ada15697554bbb1d3ea7d2b49f1773c0ee104ede1d">
   <inc:Title>njRAT</inc:Title>
   <inc:Victim>
      <sc:Name>demo_sook.putnam</sc:Name>
   </inc:Victim>
   <inc:Impact_Assessment>
      <inc:Impact_Qualification>Catastrophic</inc:Impact_Qualification>
   </inc:Impact_Assessment>
   <inc:Related_Indicators>
      <inc:Related_Indicator>
         <sc:Indicator xsi:type="ind:IndicatorType"
                       id="cta:indicator-demo_6a0d469ac3f4383b00f6b221fe4c7d88fa70161089a75fa8b6c8058985dc981e">
            <ind:Observable>
               <c:Observable_Composition operator="AND">
                  <c:Observable>
                     <c:Object>
```


脅威に関する表現と分類が変更されたため、STIX/TAXII API によって提供されるツールと SIEM で、非互換性の問題や依存関係の破損がないか確認することをお勧めします。

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。