June 2021

Updates released in June of 2021 to Cisco cloud-based machine learning global threat alerts:

New REST API for Automation Support

All visible data in the global threat alerts dashboard is now available to you through a new REST API. You can use it to download the content of a single alert, and even automate the whole data-collection process by streaming all your alerts to a third-party SIEM in your network.

The API is not read-only; you're able to change the configuration of your global threat alerts environment. For example, you can increase the specific business value of a critical asset group or change the severity assigned to a threat.

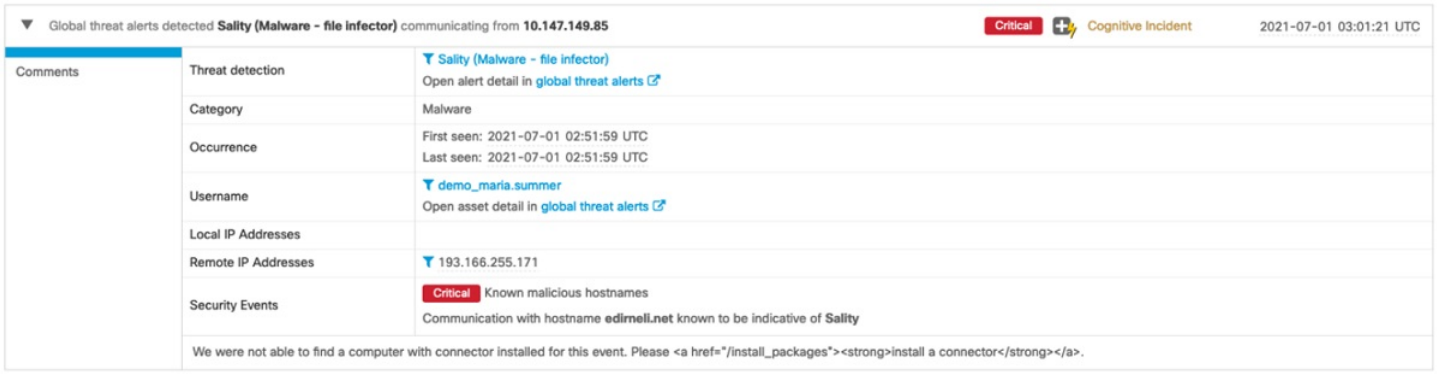
To see the API possibilities, refer to https://api.cta.eu.amp.cisco.com. There you can find the specification and use cases which describe the API possibilities in more detail and example scripts for additional integration.

To read more about the new REST API, see global threat alerts REST API is now released!

Secure Endpoint Integration Update

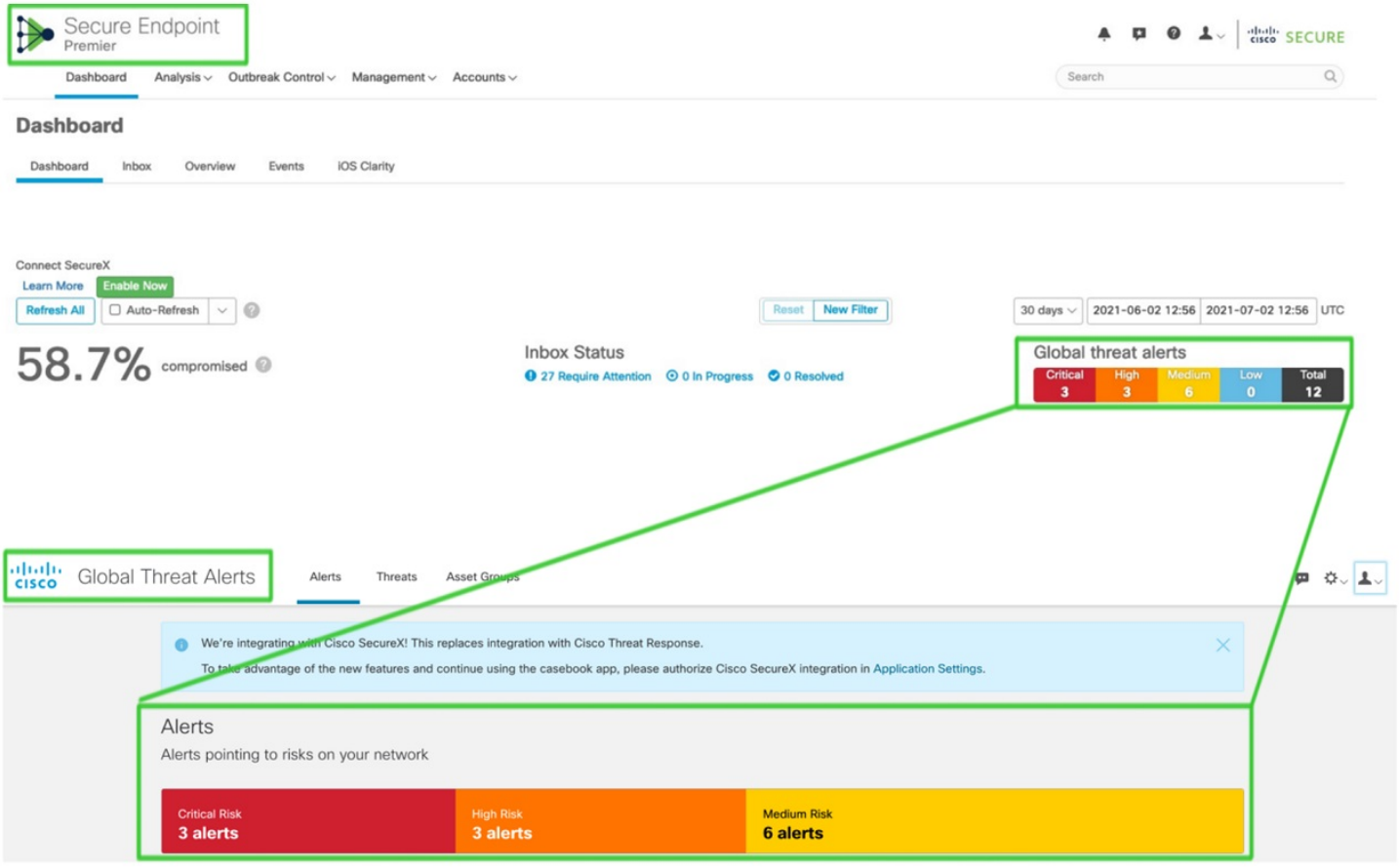
We've updated the way that detections from global threat alerts are presented in Secure Endpoint. Now, the detections are visible as events in the console, and they're directly linked with the alerts interface. As a result, threat severity changes in the alerts interface are reflected in those events.

Figure 1: Global Threat Alerts detections are now presented as events in the Secure Endpoint console



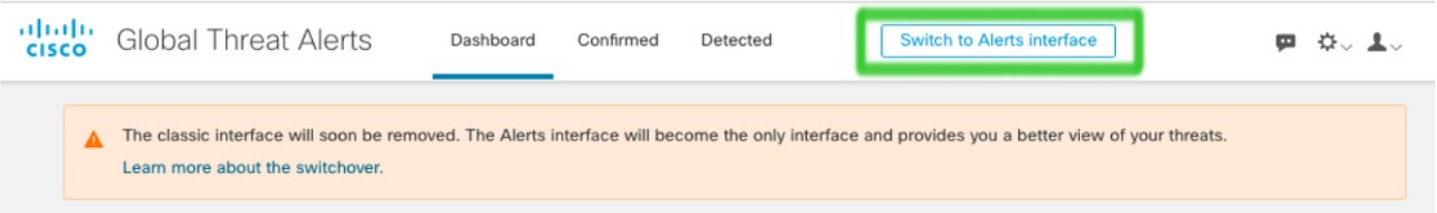
When an alert's state or risk changes in the global threat alerts interface, it's reflected in the alerts overview in the Secure Endpoint console:

Figure 2:



To avoid a compatibility issue, the classic interface will be decommissioned soon, so we recommend that you switch from the classic interface to the alerts interface. On the global threat alerts dashboard, click the **Switch to Alerts interface** button:

Figure 3:



STIX/TAXII API Update

Detection links and threat vocabulary provided by the STIX/TAXII API feeds are now compatible with the alerts interface in the global threat alerts dashboard.

Figure 4:

```
<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>
```

As a result of changes in the threat wording and taxonomy, we recommend that you check for incompatibility issues and broken dependencies in the tools and SIEM fed by the STIX/TAXII API.