2021 年 6 月

2021 年 6 月发布的思科基于云的机器学习全局威胁警报更新。

- 用于自动化支持的新 REST API ， 第 1 页
- Secure Endpoint 集成更新， 第 1 页
- STIX/TAXII API 更新， 第 3 页

用于自动化支持的新 REST API

现在，您可以通过新的 REST API 使用全局威胁警报控制面板中的所有可见数据。您可以使用它下载单个警报的内容，甚至通过将所有警报流式传输到网络中的第三方 SIEM，以自动化整个数据收集过程。

API 不是只读的；您可以更改全局威胁警报环境的配置。例如，您可以增加关键资产组的特定商业价值或更改分配给威胁的严重性。

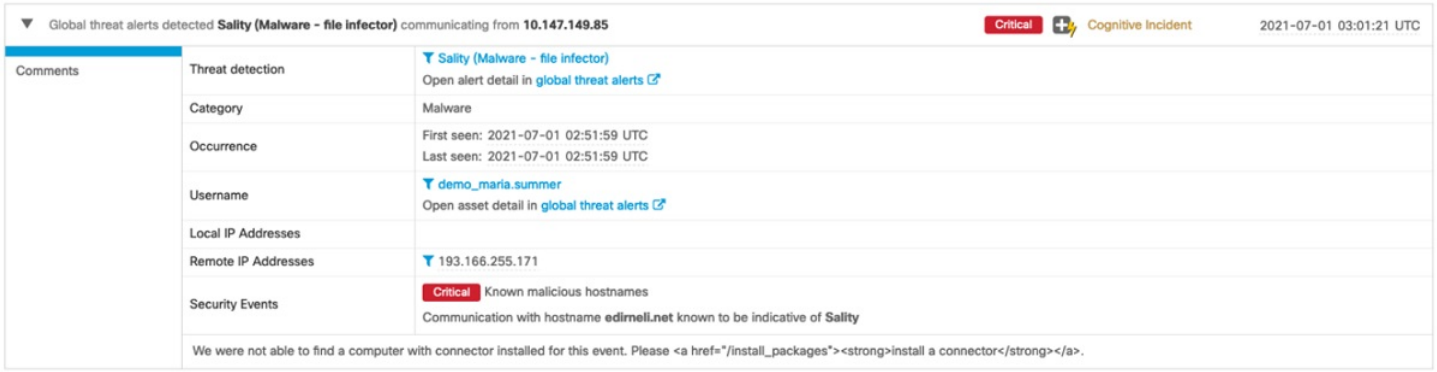
要查看 API 可能性，请参阅https://api.cta.eu.amp.cisco.com。在那里，您可以找到更详细地描述 API 可能性的规范和使用案例，以及用于额外集成的示例脚本。

要了解有关新 REST API 的更多信息，请参阅全局威胁警报 REST API 现已发布！

Secure Endpoint 集成更新

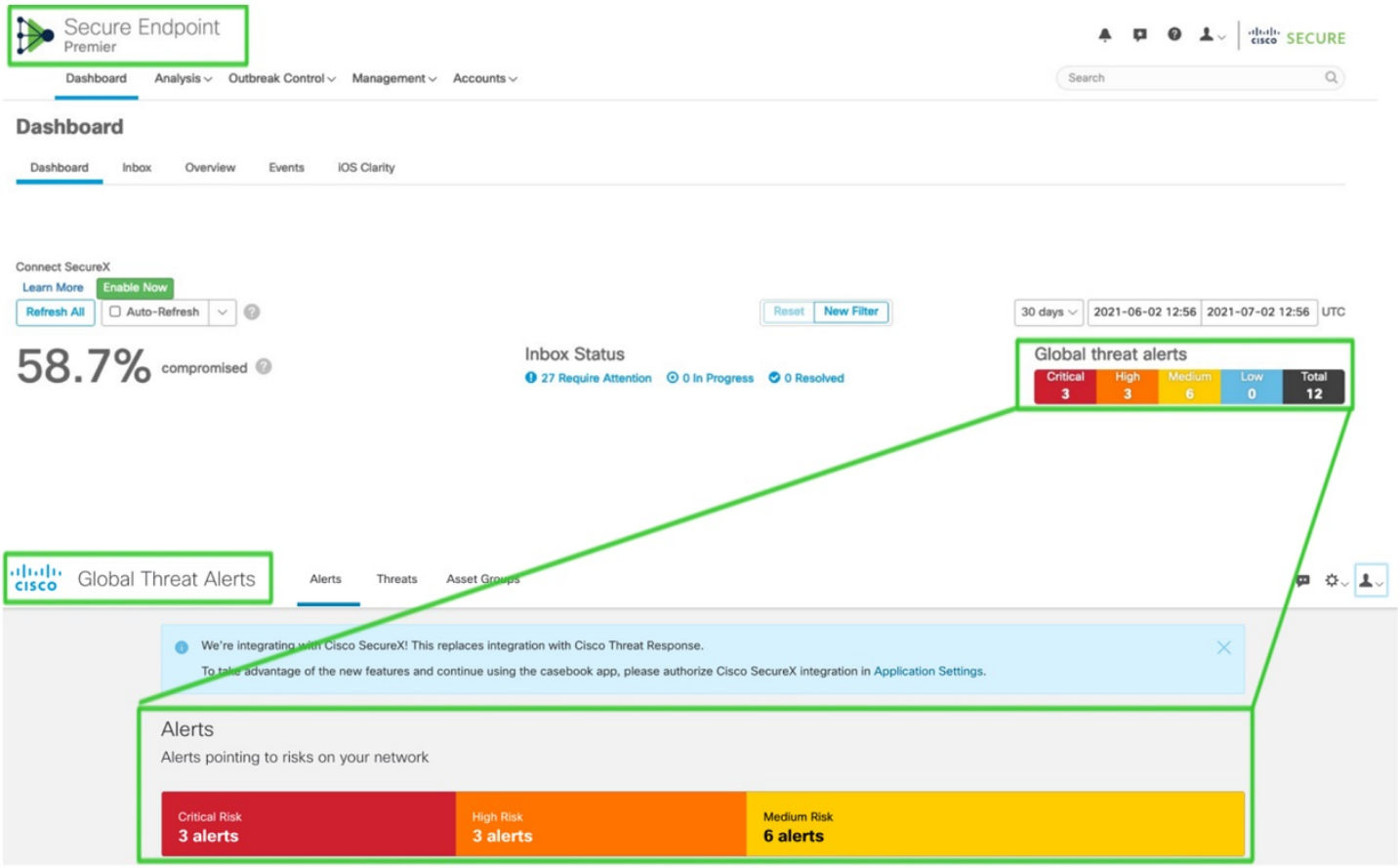
我们更新了在安全终端中显示全局威胁警报的检测方式。现在，检测在控制台中显示为事件，并且与警报接口直接关联。因此，警报接口中的威胁严重性变化会反映在这些事件中。

图 *1:* 全局威胁警报检测现在在安全终端控制台中显示为事件



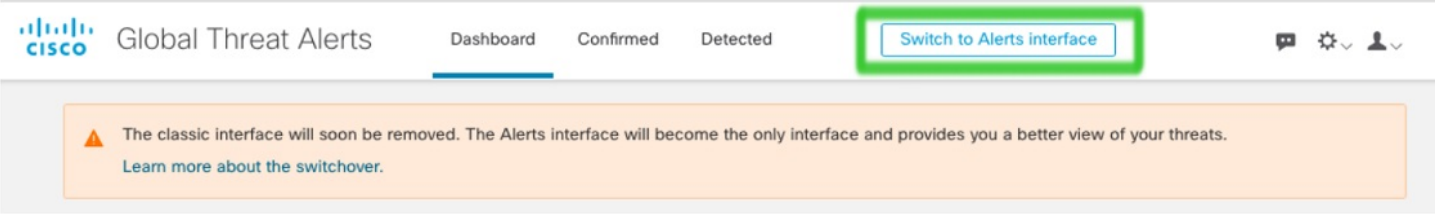
当全局威胁警报界面中的警报状态或风险发生变化时，它会反映在安全终端控制台的警报概述中：

图 *2:*



为避免出现兼容性问题，传统接口将很快停用，因此我们建议您从传统接口切换到警报接口。在全局威胁警报控制面板上，点击切换到警报接口按钮：

图 *3:*



STIX/TAXII API 更新

STIX/TAXII API 源提供的检测链接和威胁词汇现在与全局威胁警报控制面板中的警报接口兼容。

图 *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>
```

由于威胁措辞和分类发生了变化，我们建议您检查 STIX / TAXII API 提供的工具和 SIEM 中是否存在不兼容问题以及依赖关系是否中断。