2021년 6월

2021년 6월에 릴리스된, Cisco 클라우드 기반 머신 러닝 전역 위협 알림에 대한 업데이트:

자동화 지원을 위한 새 **REST API**

이제 새로운 REST API를 통해 전역 위협 알림 대시보드에 표시되는 모든 데이터를 확인할 수 있습니다. 이 대시보드를 사용하여 단일 알림의 콘텐츠를 다운로드하고, 나아가 모든 알림을 네트워크의 서드파티 SIEM으로 스트리밍하여 전체 데이터 수집 프로세스를 자동화할 수도 있습니다.

API는 읽기 전용이 아닙니다. 사용자는 전역 위협 알림 환경의 컨피그레이션을 변경할 수 있습니다 예를 들어 중요 자산 그룹의 특정 비즈니스 가치를 높이거나 위협에 할당된 심각도를 변경할 수 있습니다.

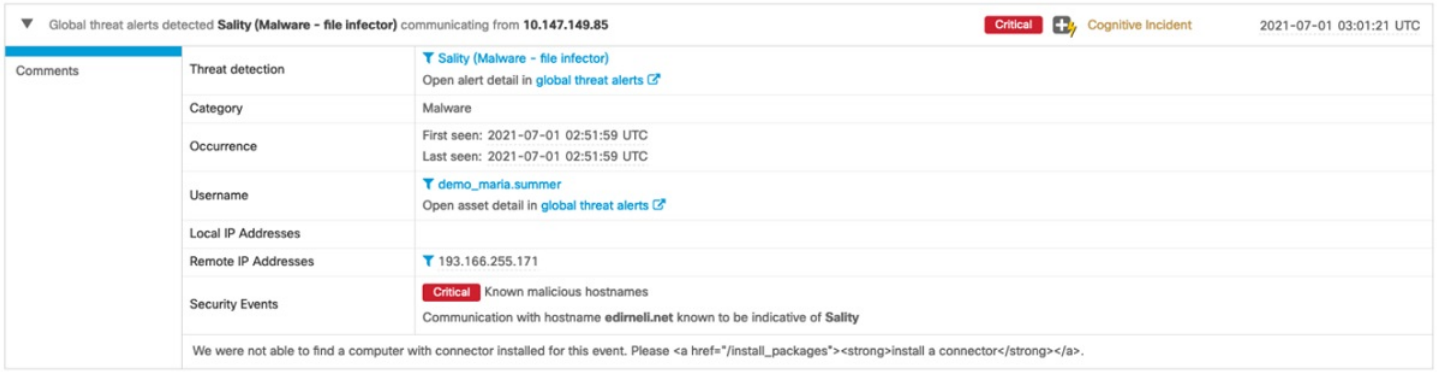
API 가능성을 확인하려면 https://api.cta.eu.amp.cisco.com을 참조하십시오. API 가능성을 자세히 설명하는 사양 및 사용 사례와 추가 통합을 위한 예제 스크립트를 확인할 수 있습니다.

새 REST API에 관한 자세한 내용은 전역 위협 알림 REST API가 릴리스되었습니다!를 참조하십시오.

Secure Endpoint 통합 업데이트

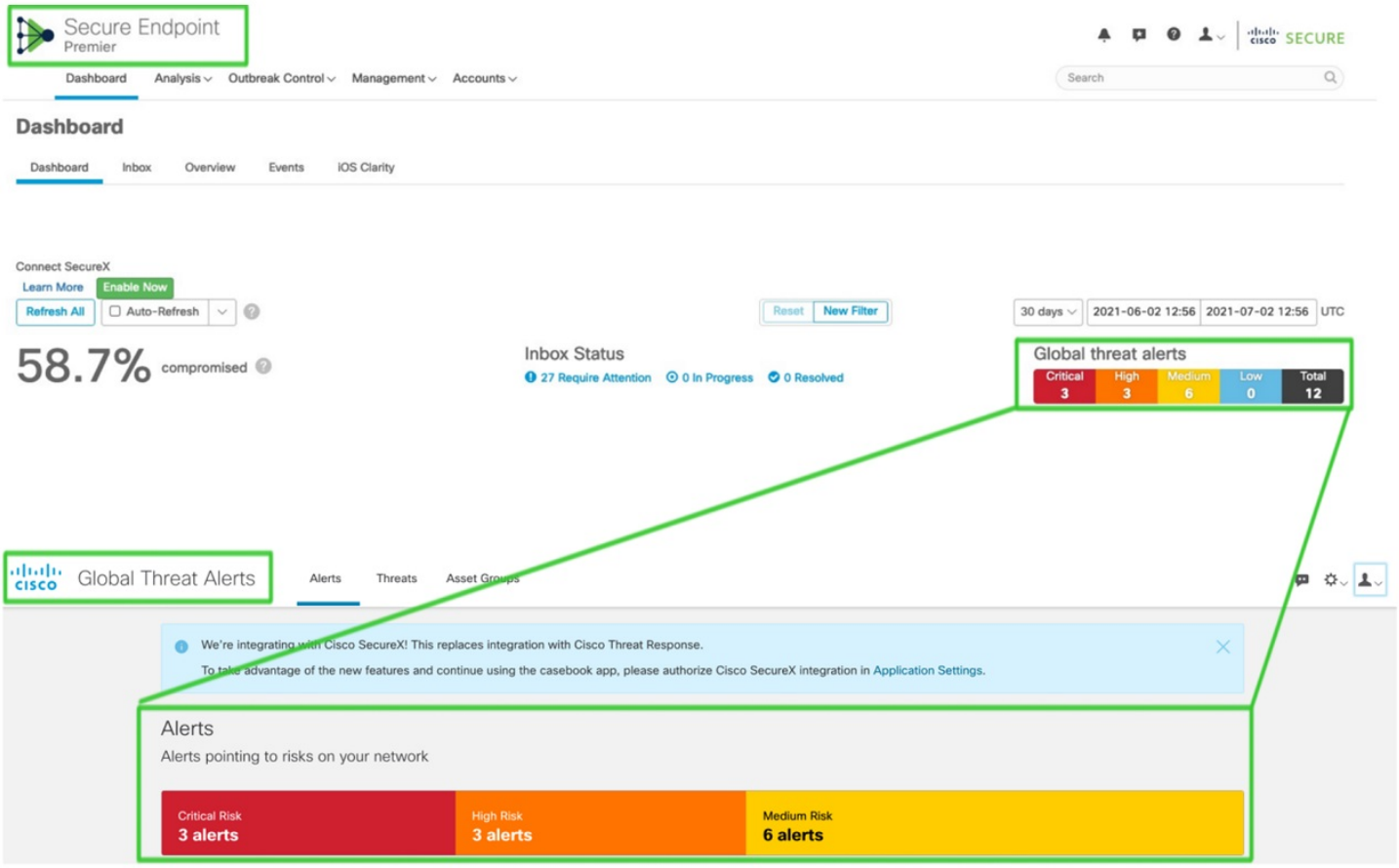
전역 위협 알림의 탐지 항목이 Secure Endpoint에 표시되는 방식을 업데이트했습니다. 이제 탐지 항목은 콘솔에서 이벤트로 표시되며, 알림 인터페이스에 바로 연결됩니다. 따라서 알림 인터페이스의 위협 심각도 변경 사항은 이러한 이벤트에 반영됩니다.

그림 *1:* 이제 전역 위협 알림 탐지가 ***Secure Endpoint*** 콘솔에서 이벤트로 표시됩니다*.*



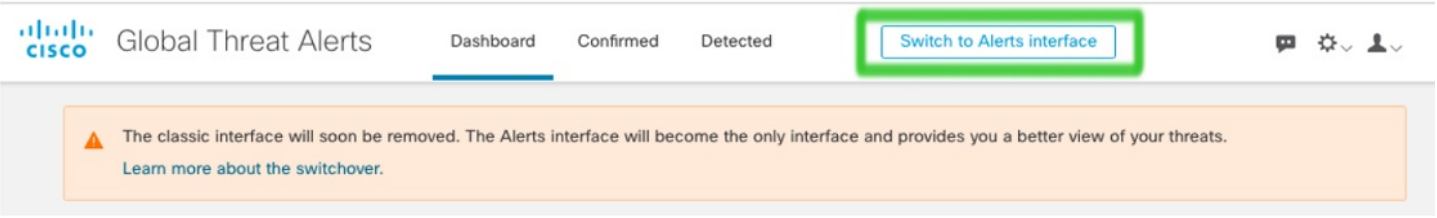
전역 위협 알림 인터페이스에서 알림의 상태 또는 위험이 변경되면, Secure Endpoint 콘솔의 알림 개요에 반영됩니다.

그림 *2:*



호환성 문제를 방지하기 위해 클래식 인터페이스는 곧 사용이 중단되므로, 클래식 인터페이스에서 알림 인터페이스로 전환하는 것이 좋습니다. 전역 위협 알림 대시보드에서 **Switch to Alerts interface(**알림 인터페이스로 전환**)** 버튼을 클릭합니다.

그림 *3:*



STIX/TAXII API 업데이트

이제 STIX/TAXII API 피드에서 제공하는 탐지 링크 및 위협 용어가 전역 위협 알림 대시보드의 알림 인터페이스와 호환됩니다.

그림 *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>
```

위협 문구 및 분류가 변경되었으므로 STIX/TAXII API에서 제공하는 툴 및 SIEM에서 비호환성 문제와 손상된 종속성을 확인하는 것이 좋습니다.