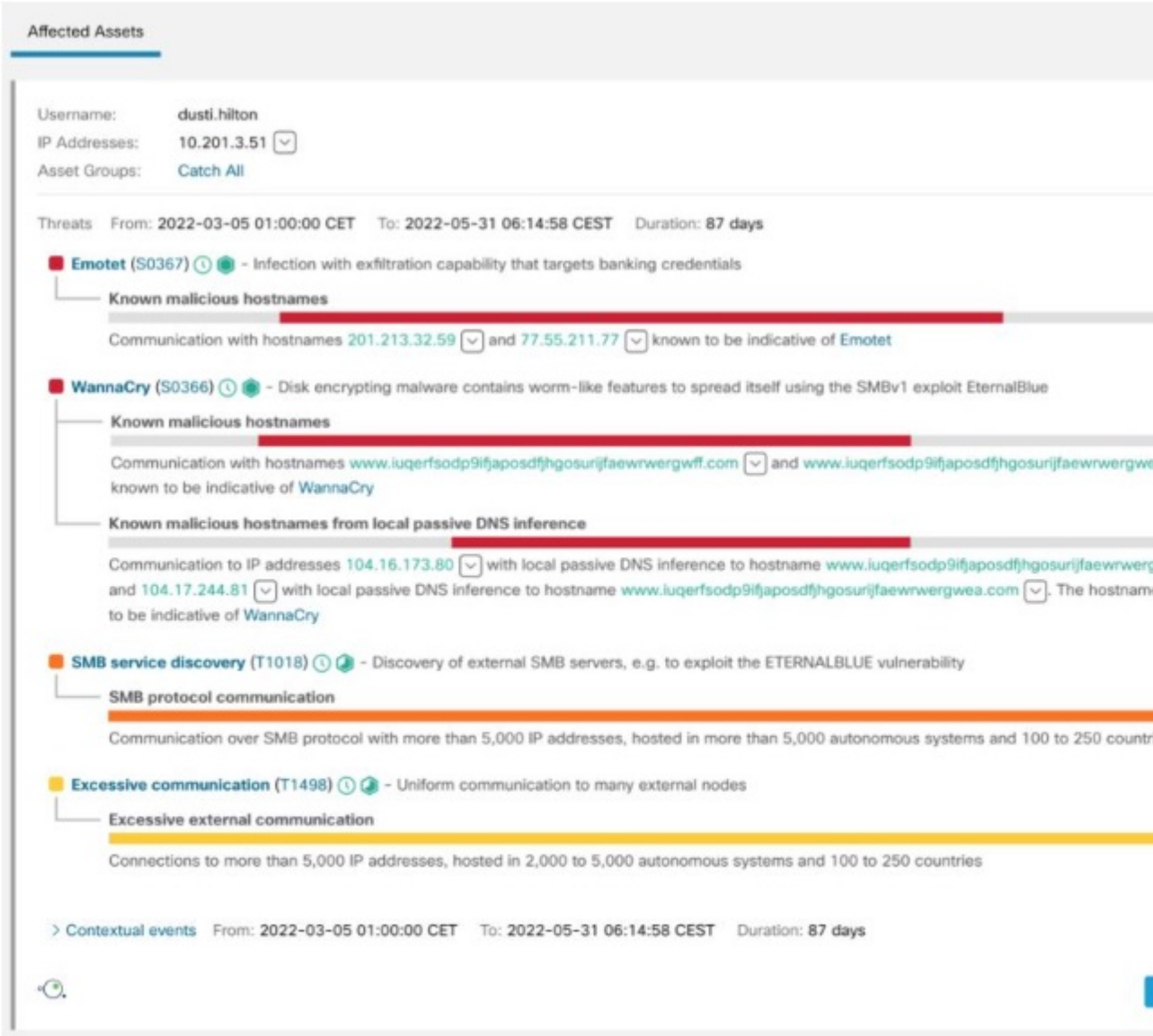
2022년 5월

2022년 5월에 릴리스된, Cisco 클라우드 기반 머신 러닝 전역 위협 알림에 대한 업데이트:

향상된 알림 세부 정보 보기

Affected Assets(영향 받는 자산**)**에 대한 추가 정보를 표시하도록 **Alert Detail(**알림 세부 정보**)** 페이지를 개선했습니다. 영향 받는 각 자산에는 모든 유해한 보안 이벤트를 포함한, 해당 자산에 대해 수행된 모든 위협 탐지를 나열하는 새로운 **Threats(**위협**)** 섹션이 포함됩니다.

그림 *1:*



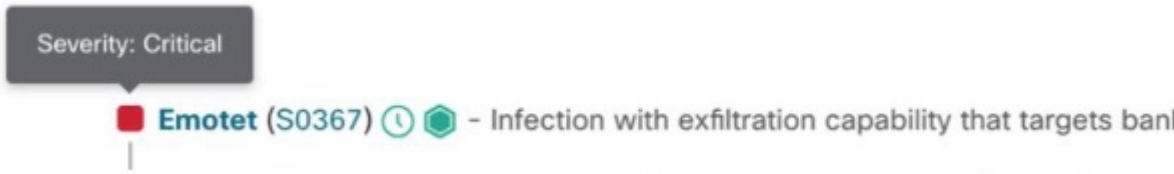
Threats(위협) 섹션의 상단에는 특정 자산에서 탐지된 모든 위협 및 해당 보안 이벤트의 총 관찰 기간이 표시됩니다.

그림 *2:*

각 위협 탐지에는 이름, MITRE 링크, 설명 및 다음이 표시됩니다.

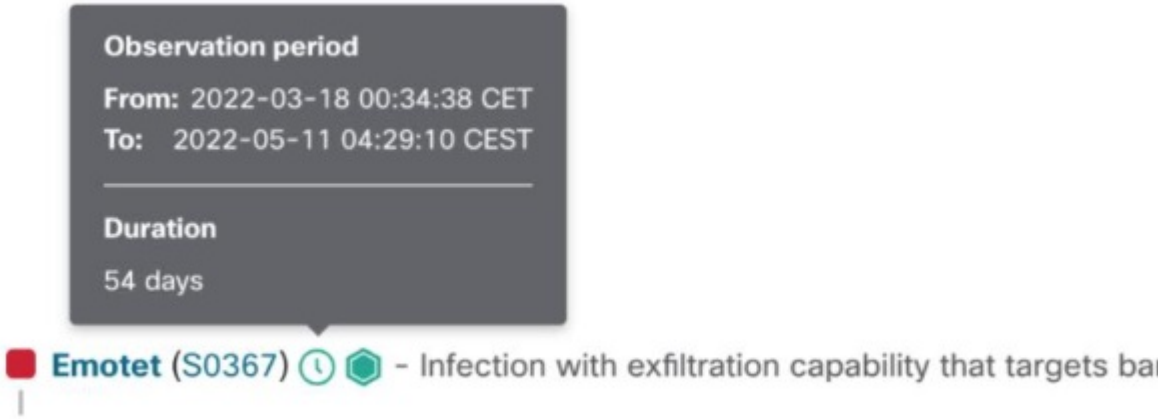
- 심각도

그림 *3:*



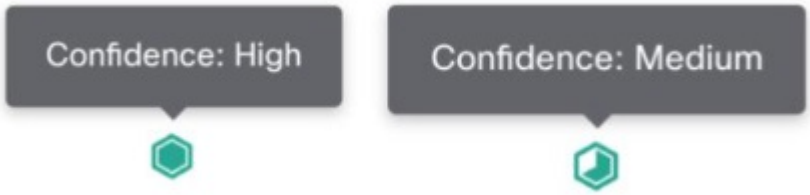
- 관찰 기간

그림 *4:*



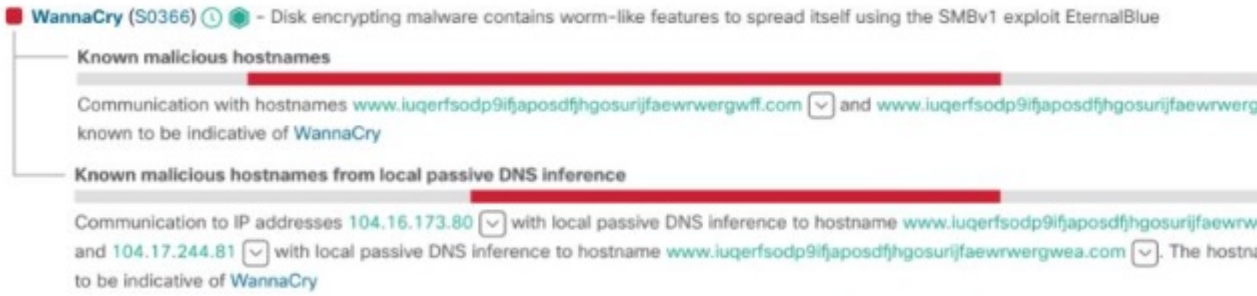
- 신뢰

그림 *5:*



각 위협 탐지는 하위 보안 이벤트를 바탕으로 합니다. 대부분의 이벤트에는 이벤트 생성을 유발한 증거를 제공하는 다양한 보안 주석이 포함되어 있습니다.

그림 *6:*

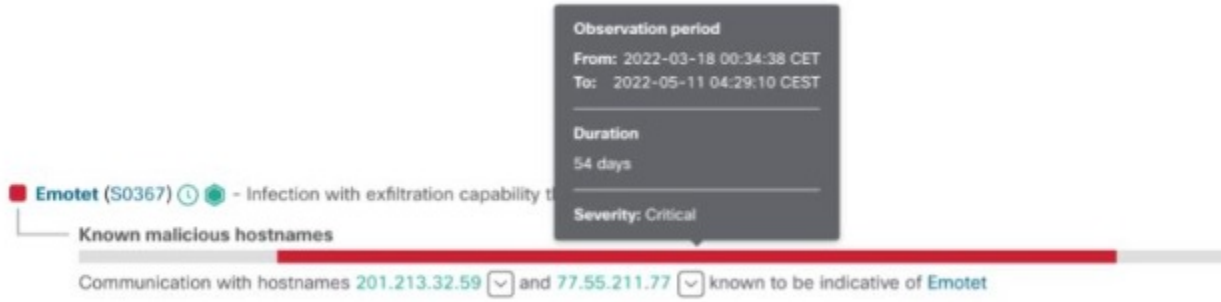


이벤트 주석에는 다른 Cisco Security 제품으로 전환하고 관찰 가능 항목에 대한 추가 정보 및 인텔리전스를 가져올 수 있는 드롭다운 메뉴가 포함되기도 합니다.

그림 *7:*

각 보안 이벤트에는 **Threats(**위협**)** 총 관찰 기간의 맥락에서 동작의 시점과 발생을 보여주는 타임라인이 포함되어 있습니다.

그림 *8:*



새로운 **Contextual events(**상황별 이벤트**)** 섹션을 확장하면 더 많은 이벤트를 표시하여 자산에서 발생한 상황에 대한 추가 맥락을 확인할 수 있습니다.

그림 *9:*