# 2021년 8월

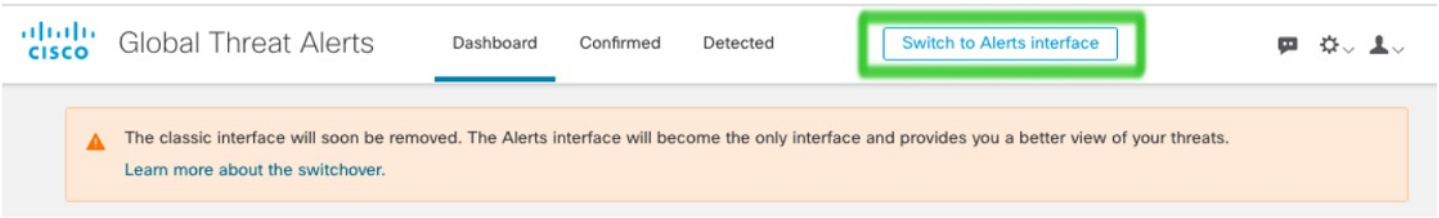
2021년 8월에 릴리스된, Cisco 클라우드 기반 머신 러닝 전역 위협 알림에 대한 업데이트:



## 클래식 인터페이스 해제됨

6월에는 클래식 인터페이스에서 알림 인터페이스로의 전환을 권장했습니다.

그림 *1:*




이제 기존 기본 인터페이스가 사용 중지되었고, 신규 알림 인터페이스가 유일한 인터페이스가 되어 네트워크상의 위협에 대한 향상된 보기를 제공합니다.

## 스캔 및 차단된 통신 처리 개선

오탐 수를 줄이기 위해 이제 전역 위협 알림에서 수평 스캔 통신에 의해 트리거된 위협 탐지를 억제할 수 있습니다. 또한 감염 초기 단계에서 프록시 차단 통신의 위협 탐지를 억제할 수도 있습니다.

케이스 시각화를 개선하기 위해, 엔드포인트에서 감염이 지속되고 아웃바운드 통신의 일부가 프록시(또는 기타 아웃바운드 제어 프로세스)에 의해 차단되는 경우 전역 위협 알림은 위협 탐지의 일부로서 표시되는 특정 보안 이벤트를 설명합니다.

이 예에서는 (트로이 목마가 있는 것으로 알려진) 호스트와의 통신 시도가 프록시 센서에 의해 차단됩니다. 보안 이벤트는 이 소프트웨어가 사용자의 프라이버시 또는 시스템의 보안을 침해할 수 있으므로 바람직하지 않은 것으로 간주됨을 알려줍니다.

그림 *2:* 예*:* 프록시에 의해 통신 시도가 차단되었음을 알려주는 보안 이벤트