# 2022년 8월

2022년 8월에 릴리스된, Cisco 클라우드 기반 머신 러닝 전역 위협 알림에 대한 업데이트:

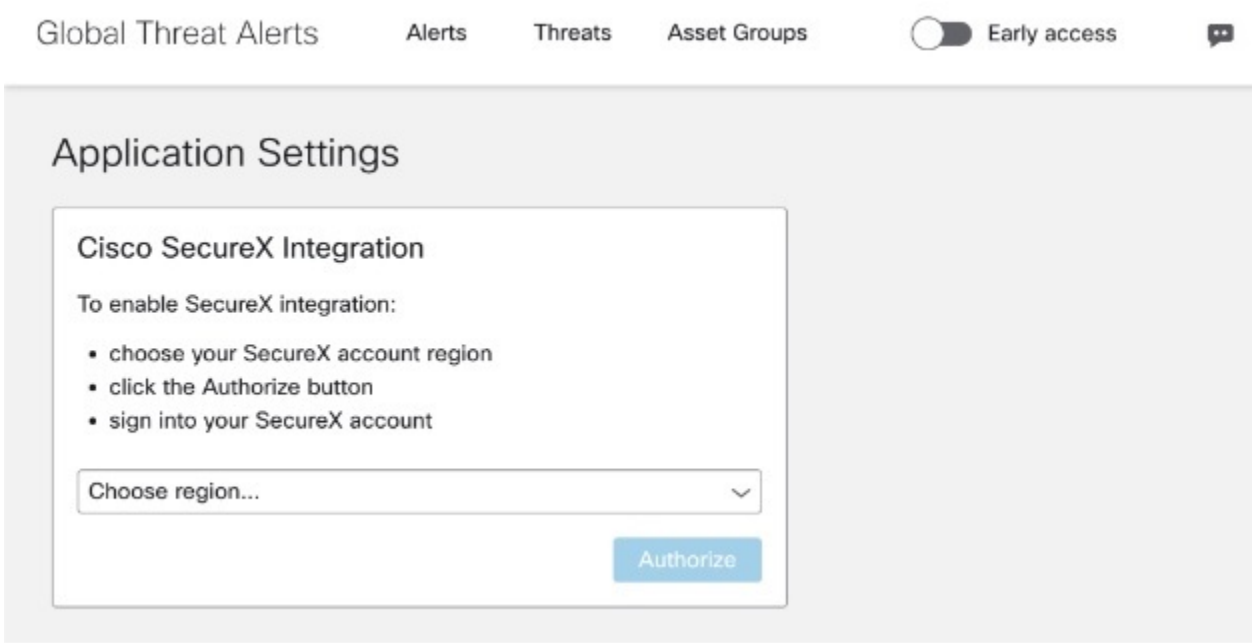


## 개선된 알림 워크플로

얼리 액세스의 알림을 사용하여 작업하는 방법과 전역 위협 알림의 알림을 SecureX 인시던트 관리자로 승격하는 방법을 개선했습니다.

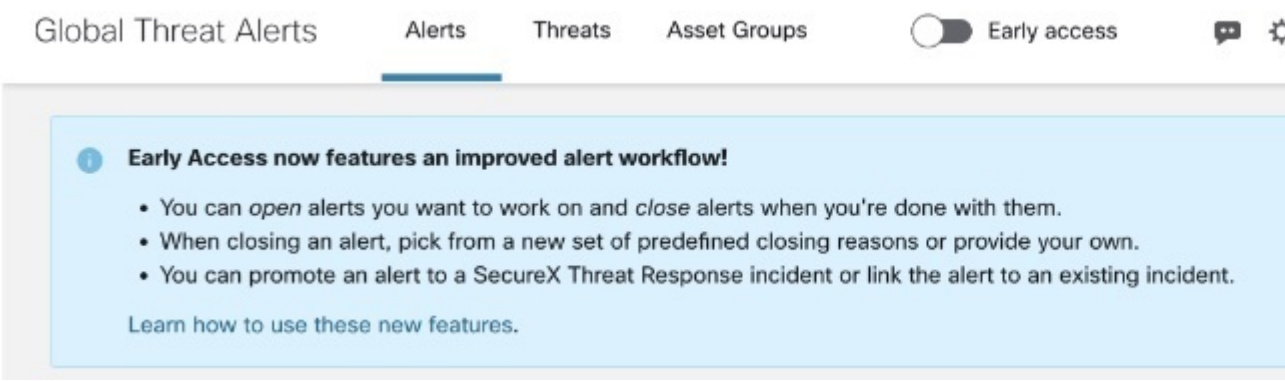
SecureX 인시던트 관리자와의 통합에 따른 이점을 활용하려면 전역 위협 알림 콘솔의 **Application Settings(**애플리케이션 설정**)**에서 SecureX 통합을 활성화해야 합니다.

그림 ***1:*** 애플리케이션 설정에서 ***SecureX*** 통합 승인



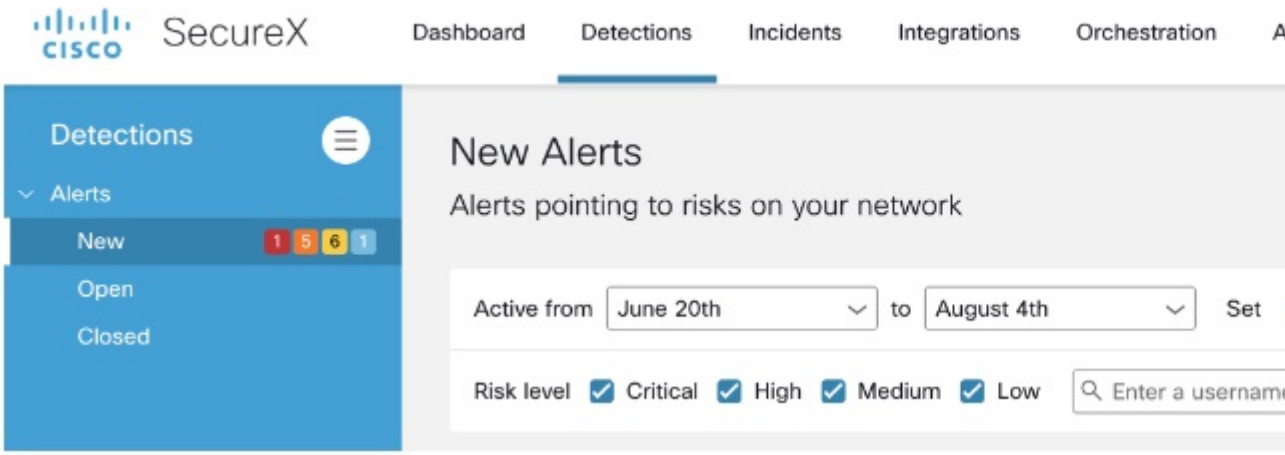
전역 위협 알림 콘솔의 헤더에서 **Early access(**얼리 액세스**)**를 클릭하여 활성화합니다.

그림 ***2:*** 새 기능을 활성화하기 위해 얼리 액세스로 전환



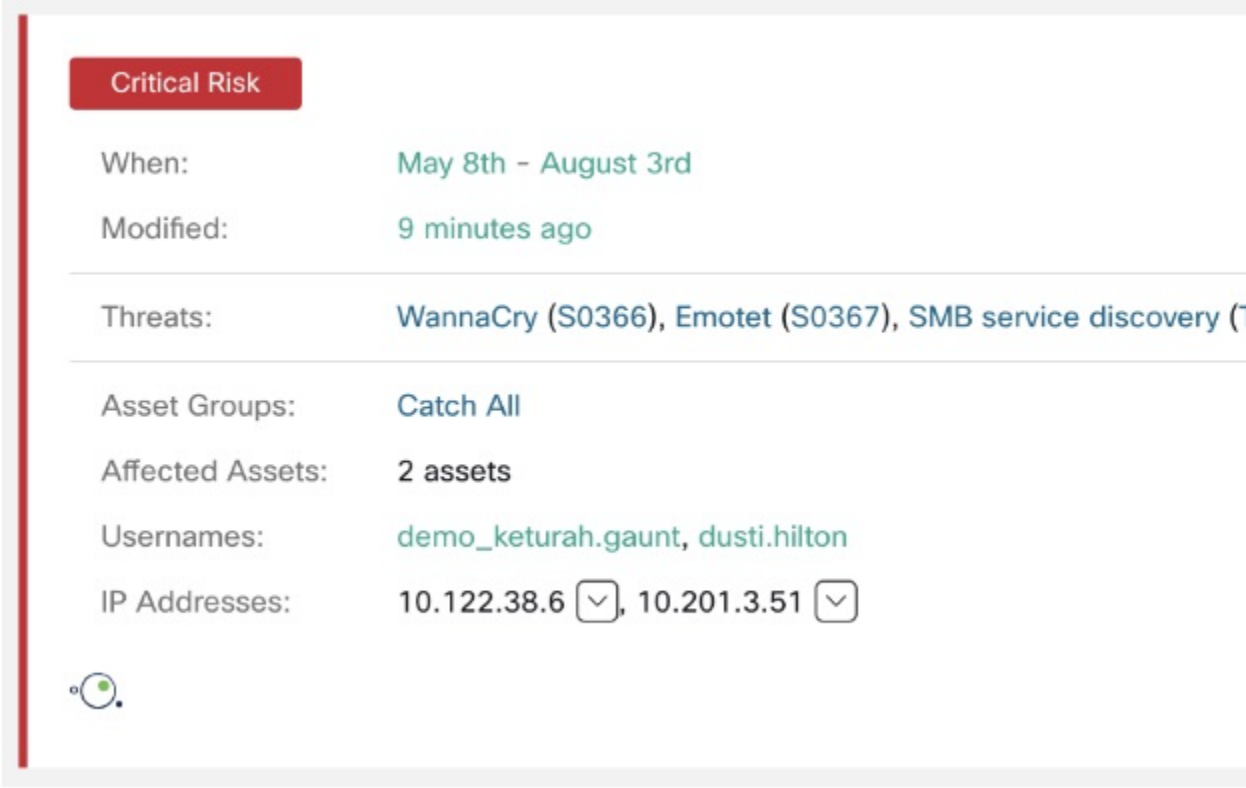

**Early access(**얼리 액세스**)**가 활성화되면 알림은 **New(**신규**)**, **Open(**열림**)** 또는 **Closed(**닫힘**)**로 분류됩니다.

그림 ***3:*** 신규**,** 열림 및 닫힘 상태 범주의 알림




**Open(**열기**)** 또는 **Close(**닫기**)** 버튼을 사용하여 신규 알림 상태를 변경할 수 있습니다.

그림 *4:* 알림 열기 또는 닫기

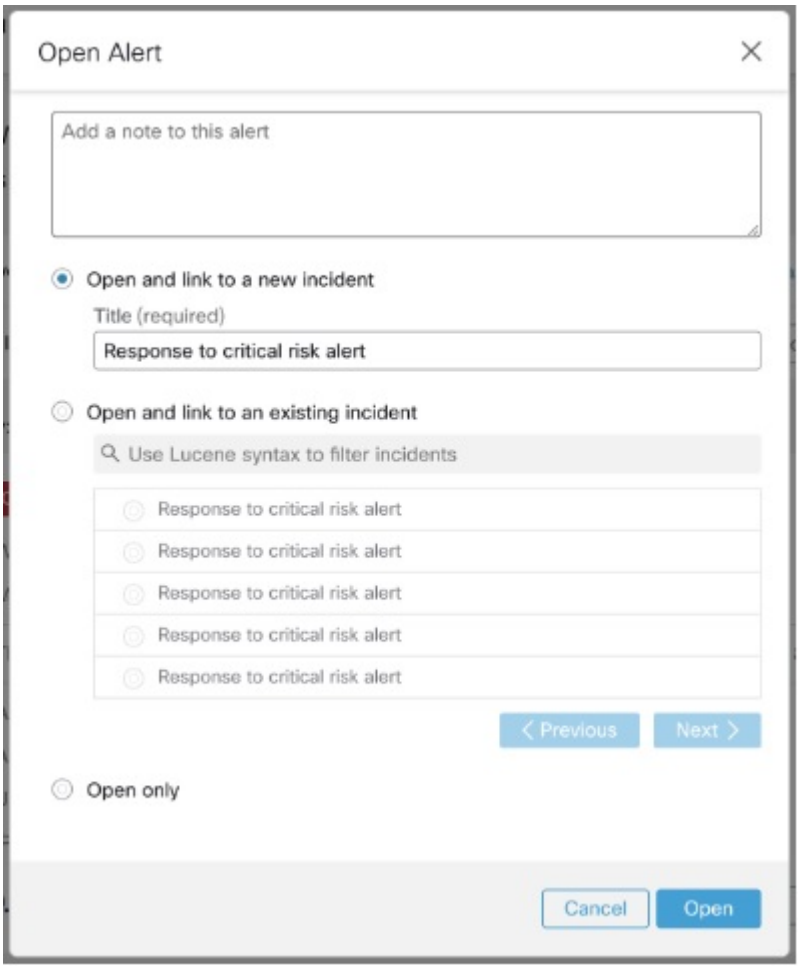



글로벌 위협 알림은 확장된 탐지 및 효율적인 알림 분류 같은 핵심 역량에 계속 집중하지만, 이제 클릭 한 번으로 탐지를 SecureX의 인시던트 대응 워크플로로 승격하는 SecureX 에코시스템을 이용해 더욱 긴밀하게 통합됩니다.

알림이 열리면 다음을 수행할 수 있습니다.

- Open and link the alert to a new incident(알림을 열고 새 인시던트에 연결)
- Open and link the alert to an existing incident(알림을 열고 기존 인시던트에 연결)
- Open only(열기만 하기)

그림 *5:* 인시던트에 연결 옵션을 이용해 알림 열기

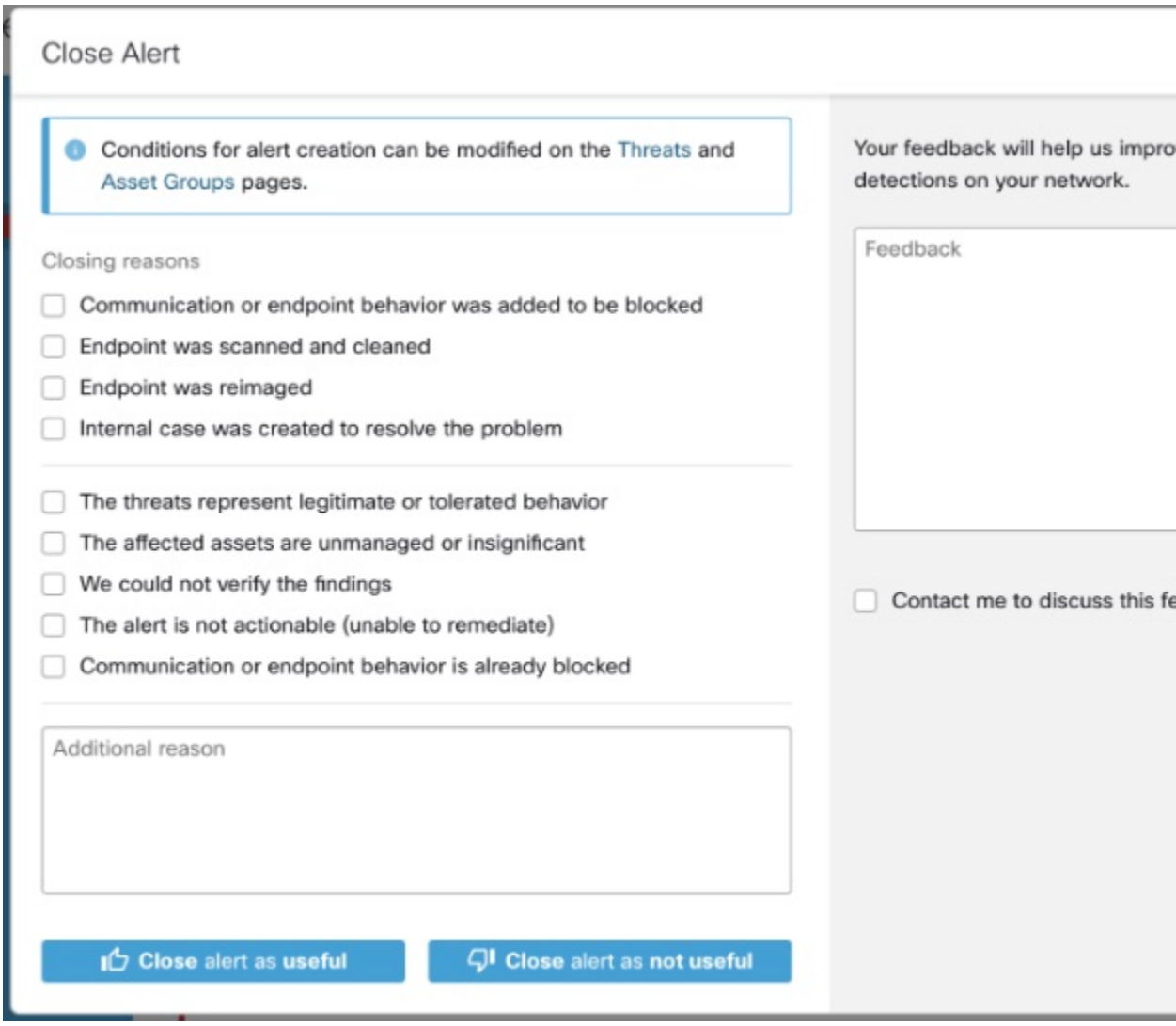



SecureX 인시던트 관리자에 있는 인시던트에는 **Summary(**요약**)** 및 원래 알림의 모든 보안 **Events(**이벤트**)**와 **Observables(**관찰 가능 항목**)**을 포함한 세부 정보가 포함됩니다. 조사, 강화 및 오케스트레이션 같은 SecureX 기능을 사용하여 추가로 조사하고 대응할 수 있습니다.

알림을 인시던트로 승격하는 것이 바람직하지 않다면 **Open only(**열기만 하기**)**를 선택하고 전역 위협 알림 콘솔에서만 작업만 추적할 수 있습니다.

두 경우 모두 작업이 끝나면 알림을 닫을 수 있습니다. 알림을 닫을 때는 사전 정의된 새로운 종료 사유 집합에서 사유를 선택하거나 직접 입력합니다.

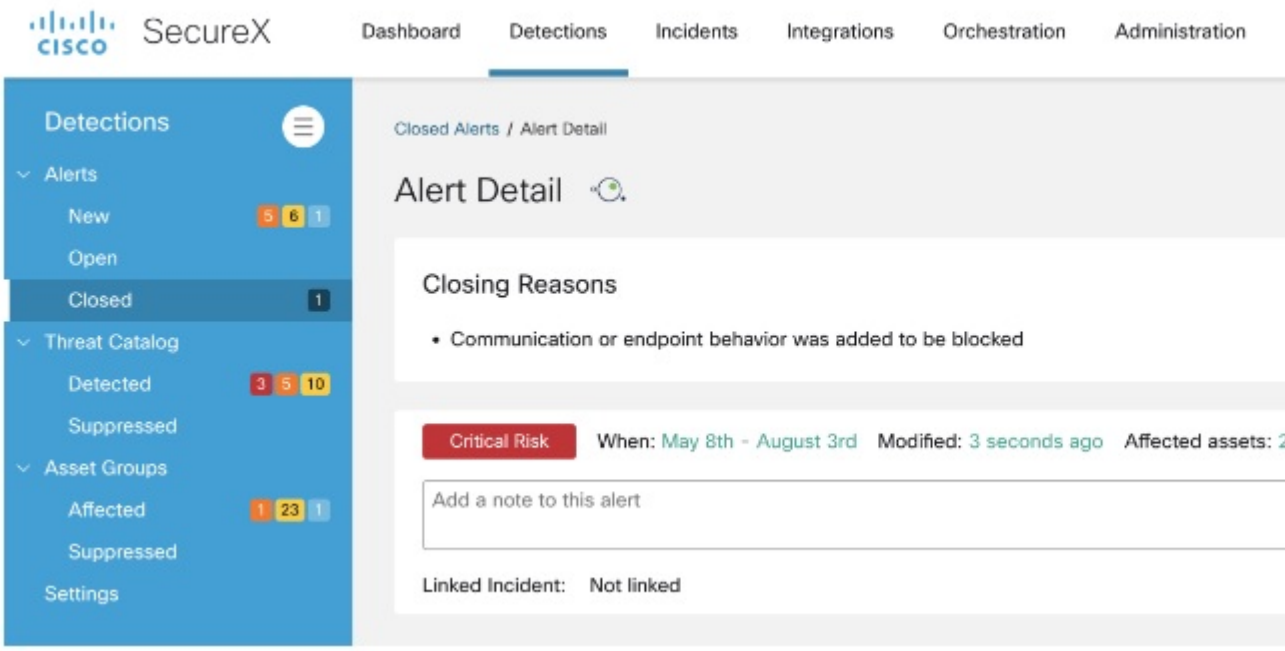
그림 *6:* 종료 사유를 선택하여 알림 종료




알림을 닫을 때는 유용하거나 유용하지 않은 알림으로 닫을 수 있습니다. 알림에 대한 추가 피드백을 Cisco 팀에 제공할 수도 있습니다. 귀하의 소중한 피드백은 향후 탐지를 개선하는 데 도움이 됩니다.

종료 사유는 나중에 참조할 수 있도록 알림의 일부로 기록됩니다.

그림 ***7: Alert Detail(***알림 세부 정보***)*** 페이지에 표시되는 종료 사유




닫힌 알림은 열 수 있습니다. 알림을 다시 열면 모든 종료 이유가 제거됩니다. 이전에 연결된 SecureX 인시던트에 대한 참조도 제거됩니다. 그러나 이전과 동일한 SecureX 인시던트에 알림을 다시 연결하도록 선택할 수도 있습니다.

# 추가 위협 탐지

새로운 위협 탐지인 SocGholish가 포트폴리오에 추가되었습니다. 기존 위협 탐지 관련 지표도 업데이트했습니다.

### SocGholish

FakeUpdates라고도 하는 SocGholish는 합법적인 소프트웨어 업데이트를 사칭하는 다운로더 악성코드입니다. Javascript(T1059.007)를 기반으로 하며 의도하지 않은 다운로드(T1608.004)를 통해 확산됩니다. 엔드포인트(T1005)와 네트워크 데이터(예: 사용자 권한(T1069), 도메인 트러스트(T1482), 도메인 계정 정보(T1087.002), 실행 중인 서비스(T1007), 자격 증명을 포함하는 파일(T1083))를 수집할 수 있습니다. 다른 악성코드 제품군에 의한 추가 감염을 유발하기도 합니다.

사용자 환경에서 SocGholish가 탐지되었는지 확인하려면 SocGholish Threat Detail(SocGholish 위협 세부 정보)을 클릭하여 전역 위협 알림에서 관련 세부 정보를 확인하십시오.

그림 *8:*


SocGholish
Javascript based malware mimicing legitimate software updates
High Severity
5+ affected assets in 5+ companies
SocGholish, also known as FakeUpdates, is a downloader malware that mimics legitimate software updates. It is based on Javascri
drive-by downloads (T1608.004). It is capable of collecting endpoint (T1005) and network data such as user permissions (T1069),
account information (T1087.002), services running (T1007), files containing credentials (T1083), etc. It also leads to further infectio
Category: Malware - downloader