용어집

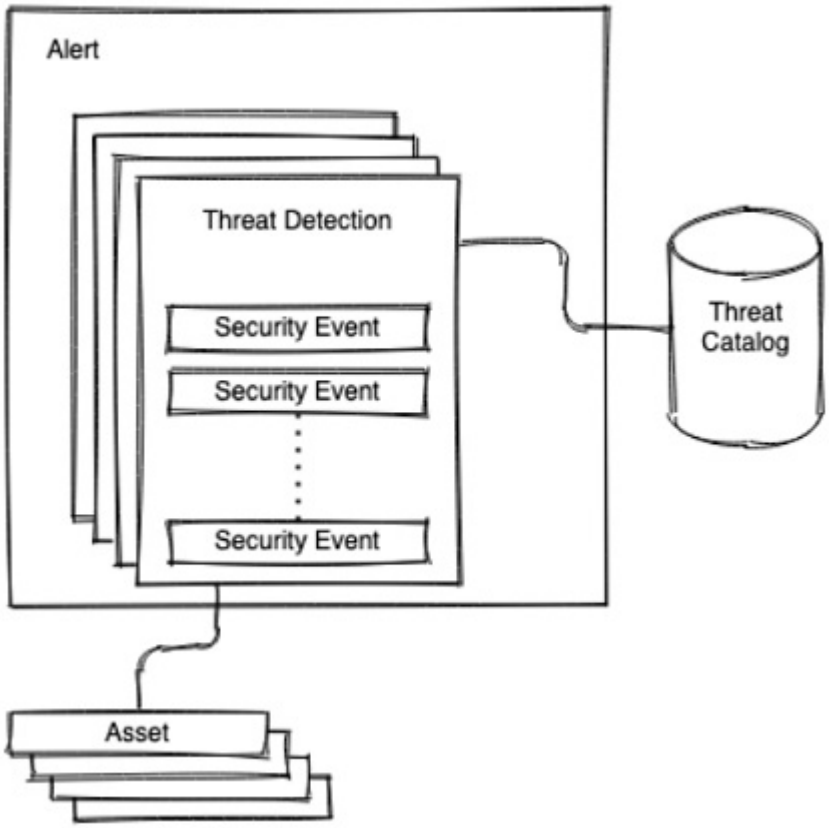
- 경고, 1 페이지
- 보안 이벤트, 2 페이지
- 위협 카탈로그, 2 페이지
- 위협 탐지, 3 페이지

경고

알림은 위협 탐지를 조사하라는 메시지를 표시하는 역할을 합니다.

전역 위협 알림에서 알림은 하나 이상의 위협 탐지에 집중합니다. 이러한 위협 탐지는 하나 이상의 자산에서 발생합니다. Cisco의 퓨전 알고리즘은 이러한 탐지를 사용하여 유사한 위협 및 관련 예측의 클러스터를 식별하여 위험 수준을 계산합니다. 그런 다음 Cisco의 웹 포털에서 이를 위험 수준에 따라 우선순위가 지정된 목록에 보안 알림으로 표시합니다. 각 알림은 네트워크상의 위협을 가리키며 조사 및 후속 치료를 위한 자연스러운 작업 단위를 나타냅니다.

그림 *1:*



보안 이벤트

보안 이벤트는 악의적이거나 의심스러운 동작을 나타낼 수 있는 중요한 보안 이벤트입니다. 위협 탐지 엔진은 보안 이벤트를 처리합니다. 의심스럽거나 악의적인 동작을 탐지하는 데 중요한 역할을 하는 보안 이벤트를 유해성 판정 이벤트라고 합니다. 위협 탐지 시 영향을 받는 자산에서 관측된 보안 이벤트를 상황별 이벤트라고 합니다. 각 보안 이벤트에는 보안 이벤트가 중요한 이유에 대한 설명이 포함되어 있습니다. 이 설명을 보안 주석이라고 합니다.

위협 카탈로그

위협 카탈로그는 가능한 위협 탐지를 구성하고 악성코드, 툴 및 공격 패턴이라는 3가지 기본 범주로 순서를 지정합니다. (존재하는 경우) MITRE에 대한 매핑도 포함됩니다.

위협 탐지

위협 탐지는 자산에 영향을 미치는 의심스럽거나 악의적인 행동을 탐지하는 것입니다. 전역 위협 알림 위협 카탈로그에서는 다양한 유형의 위협 탐지가 인식됩니다.

위협 탐지 엔진은 보안 이벤트 같은 다양한 소스를 이용해 작동합니다. 이러한 소스의 상관관계를 만들어, 특정 신뢰도 수준의 위협이 존재함을 나타내거나 분석적으로 확인할 수 있는 비정상적인 패턴 및 추세를 찾아냅니다.