대시보드

전역 위협 알림(구 Cognitive Intelligence) 기능을 사용하면 이미 진행 중이거나 네트워크에 침투하려 하는 정교하고 은밀한 공격을 신속하게 탐지하고 대응할 수 있습니다. 이 기능은 의심스럽거나 악성인 웹 기반 트래픽을 자동으로 식별하고 조사합니다. 확인된 위협과 잠재적 위협을 모두 식별하므로, 신속하게 감염을 해결하고 공격의 범위 및 피해 규모를 줄일 수 있습니다. 여러 조직에 확산된 알려진 위협 캠페인 또는 지금까지 본 적이 없는 특별한 위협을 모두 다룹니다.

클라우드 기반 서비스인 전역 위협 알림은 기존 웹 보안 솔루션에서 생성한 정보를 추가 하드웨어 또는 소프트웨어 없이 분석합니다. 보안 제어 장치를 통과한 악성 활동에 초점을 맞춥니다.

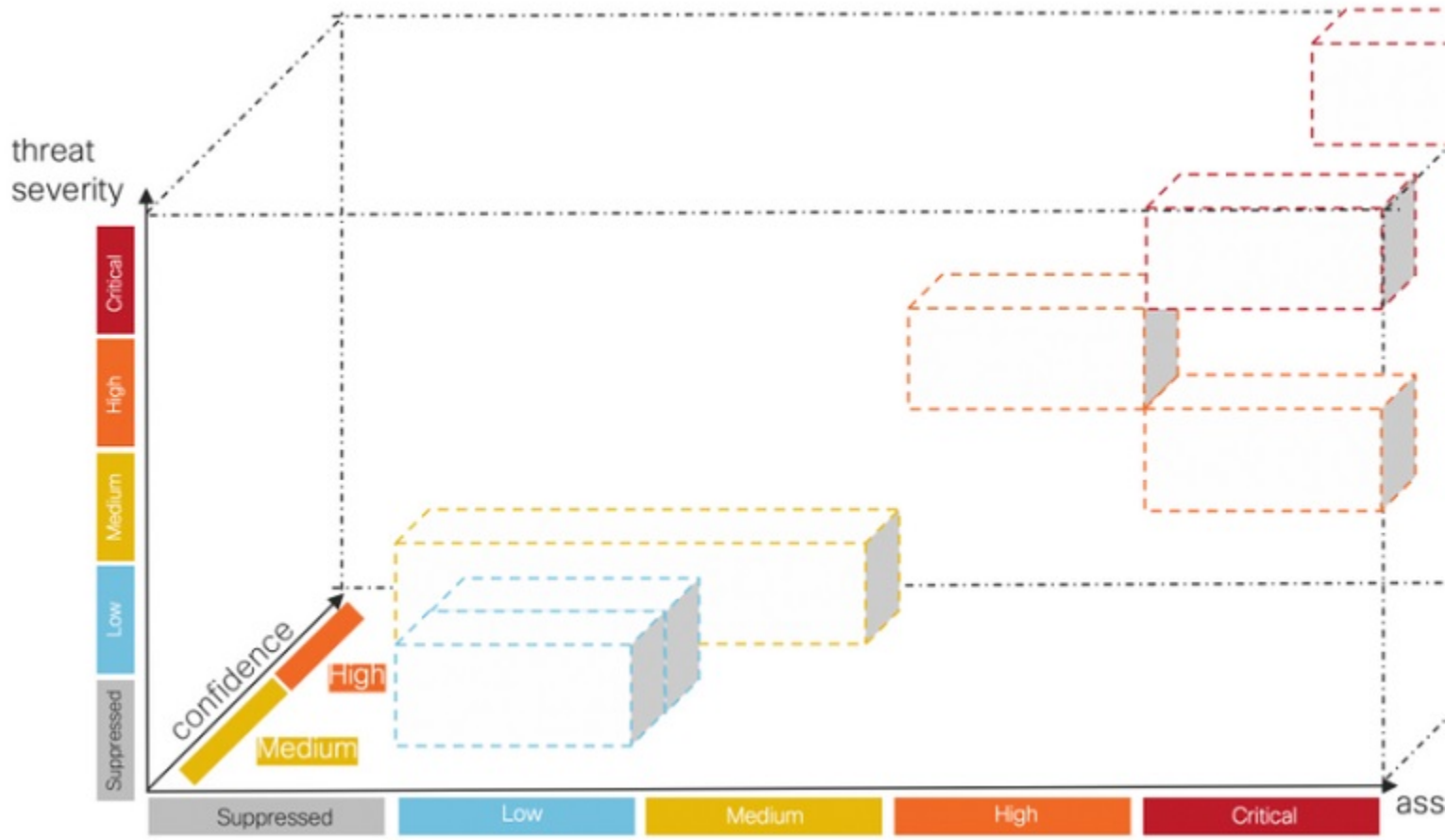
전역 위협 알림은 기계 학습 및 통계적 네트워크 모델링을 통해 정상적인 활동의 기준선을 마련하여 네트워크 내에서 일어나는 비정상적인 트래픽을 식별합니다. 디바이스 동작 및 웹 트래픽을 분석하여 명령 및 제어 통신과 데이터 유출을 찾아냅니다.

전역 위협 알림은 관찰하고 학습하며 적응하는 방식으로 계속 보안 침입을 식별하여 공격의 재발 또는 지속적인 감염의 위험을 줄입니다. 여러 Cisco Security 제품과 통합된 직관적인 웹 기반 포털을 통해 정보를 제공하므로, 침입의 심각도와 범위를 평가하고 위협의 목적과 작동 방식을 이해하여 즉각적인 조치를 취할 수 있습니다.

개요

Cisco의 분석 엔진은 머신 러닝을 수신 데이터 스트림에 적용하고 탐지 항목을 3차원 공간에 투사합니다.

그림 *1:*



- 위협 심각도 차원**.** 위협의 심각도는 어느 정도입니까? 확인된 위협 및 위협의 심각도입니다. 조직의 위험 프로파일을 개별 위협 유형에 더 잘 일치시킬 수 있도록, 개별 위협의 사전 정의된 심각도를 조정할 수 있습니다.
- 자산-가지 차원**.** 자산의 가치는 어느 정도입니까? 네트워크에 연결된 디바이스의 중요도가 차이가 난다면, 개별 자산 그룹의 비즈니스 가치를 조정하여 더 중요한 디바이스에 탐지 우선순위를 지정할 수 있습니다.
- 신뢰도 차원**.** 판정을 얼마나 신뢰합니까? 고객 환경에서 관찰된 개별 위협에 대해 알고리즘이 내리는 판정의 신뢰도입니다. 판정을 확신할 수 있을 정도록 충분한 행동 지표가 충분히 관찰될 때도 있습니다. 증상은 비슷하지만 실제 증거는 명확하지 않을 때도 있습니다. 결과적으로 오차가 발생할 가능성이 증가합니다.

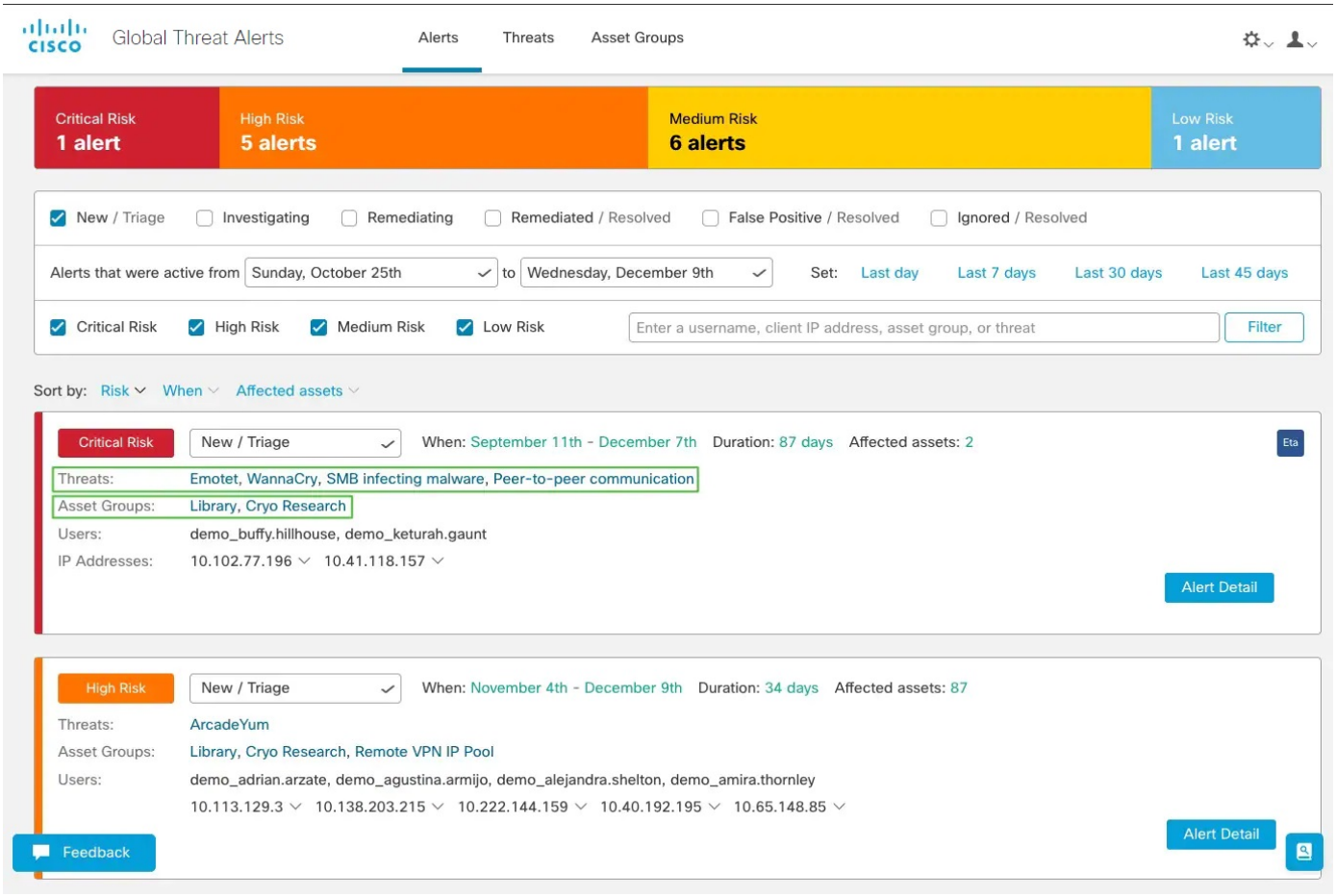
Cisco의 퓨전 알고리즘은 이러한 탐지를 사용하여 유사한 위협 및 예측의 클러스터를 식별하여 위험 수준을 계산합니다. 그런 다음 Cisco의 웹 포털에서 이를 위험 수준에 따라 우선순위가 지정된 목록에 보안 알림으로 표시합니다. 각 알림은 네트워크상의 위협을 가리키며 조사 및 후속 치료를 위한 자연스러운 작업 단위를 나타냅니다.

알림 조사

단계 **1** 네트워크의 모든 활성 알림을 보려면 **Alerts(**알림**)** 탭을 클릭합니다. 각 알림은 자체 카드에 표시됩니다.

a) 각 알림 카드는 비즈니스 가치가 유사한 네트워크상의 자산 집합에 동시에 영향을 미치는 하나 이상의 위협을 집계합니다.

그림 ***2:***



- **Threats(**위협**)**. 함께 발생하는 서로 다른 위협입니다.
- 자산 그룹. 이러한 위협은 비즈니스 가치가 유사한 자산 그룹에 속한 엔드포인트에서 발생합니다.

b) 위험 수준은 자산 그룹의 위협 심각도 수준과 비즈니스 가치를 기반으로 합니다. 위험 수준이 높을수록 네트워크상의 중요한 자산에 심각한 영향을 미치는 위협이 발생할 위험이 높습니다.

단계 **2** 위험도가 높은 알림 카드는 목록 상단에 배치됩니다. 위험 수준을 기준으로 알림에 응답하고 위험 수준이 높은 알림을 먼저 조사하여 분석의 우선순위를 지정하십시오.

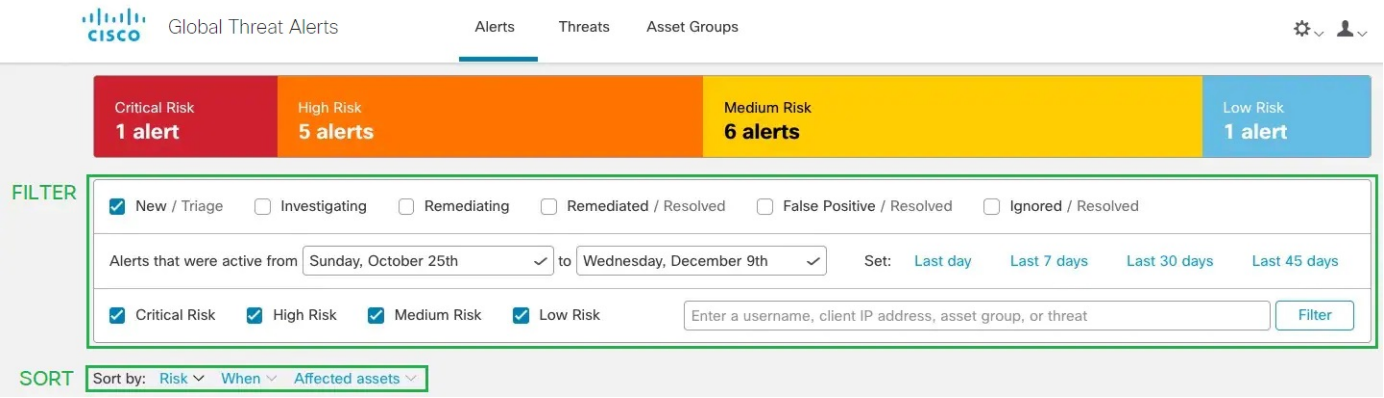
- 중대

- 높음
- 보통
- 낮음

참고 알림 카드는 새 위협이 그룹에 추가되거나 자산 그룹 비즈니스 값 또는 위협 심각도가 변경되는 상황 등에서 동적으로 변경될 수 있습니다.

단계 **3** 상태, 기간, 위험 수준, 사용자 이름, IP 주소, 자산 그룹 및/또는 위협을 선택하여 표시할 알림을 **Filter(**필터링**)**할 수 있습니다. 연령, 위험 수준 또는 영향 받는 자산의 수를 기준으로 **Sort by(**정렬**)**할 수도 있습니다.

그림 ***3:***



단계 **4** **New/Triage(**신규/분류**)**에서 알림 상태를 변경하여 알림 조사를 시작합니다.

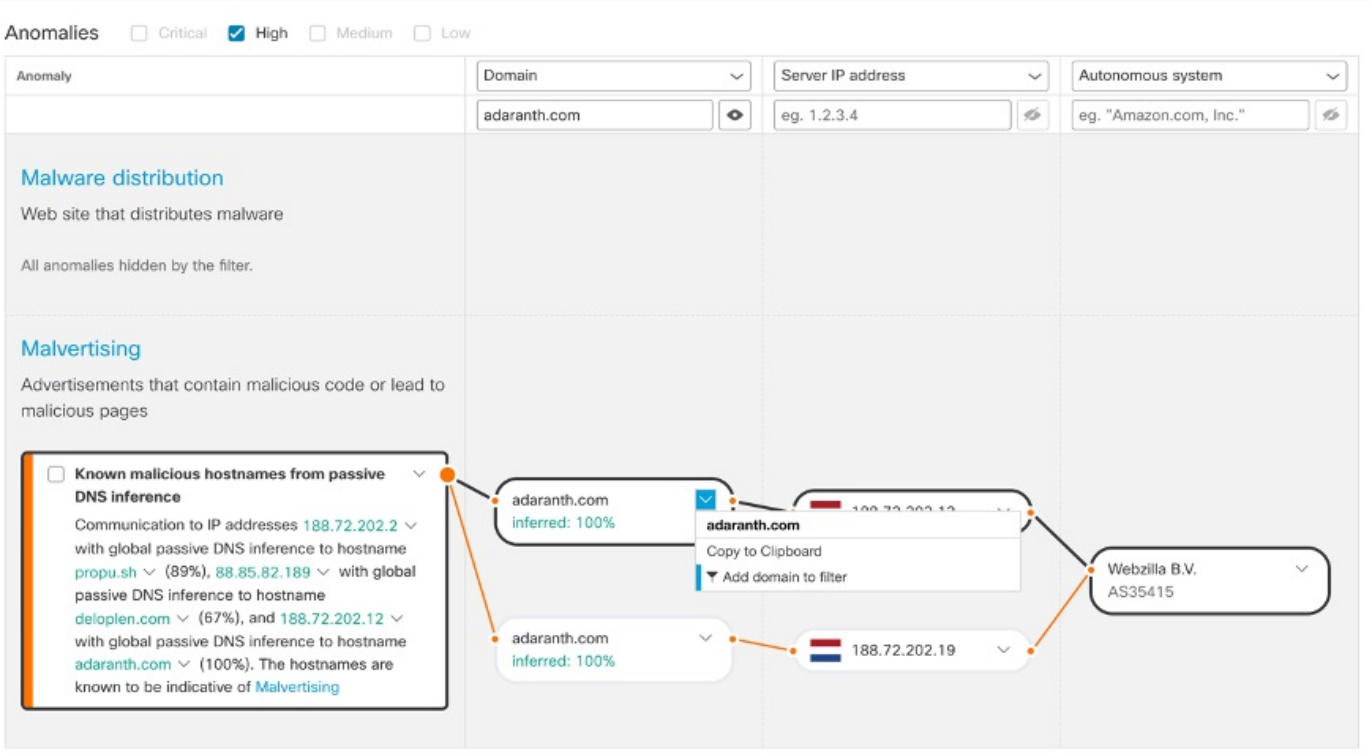
참고 상태가 **New/Triage(**신규/분류**)**가 아니게 되면 쉽게 조사할 수 있도록 알림 카드가 변경되지 않고 안정적으로 유지됩니다.

단계 **5** 탐지된 각 위협 및 영향 받는 자산에 대한 추가 콘텐츠를 보려면 **Alert Detail(**알림 세부 정보**)**을 클릭합니다.

- 트리거되고 이 위협의 식별로 이어진 보안 이벤트
- 자산이 통신한 IP 주소와 도메인
- 이 악성 동작을 나타내는 특정 IoC
- 머신 러닝 알고리즘이 이 탐지에 할당한 신뢰도 수준

단계 **6** 한 사용자에 대한 특정한 이벤트 중 하나를 선택하면 보안 이벤트 보기로 전환되며, 여기서는 악성 탐지를 트리거한 특정 이벤트의 자세한 컨텍스트를 볼 수 있습니다.

그림 *4:*

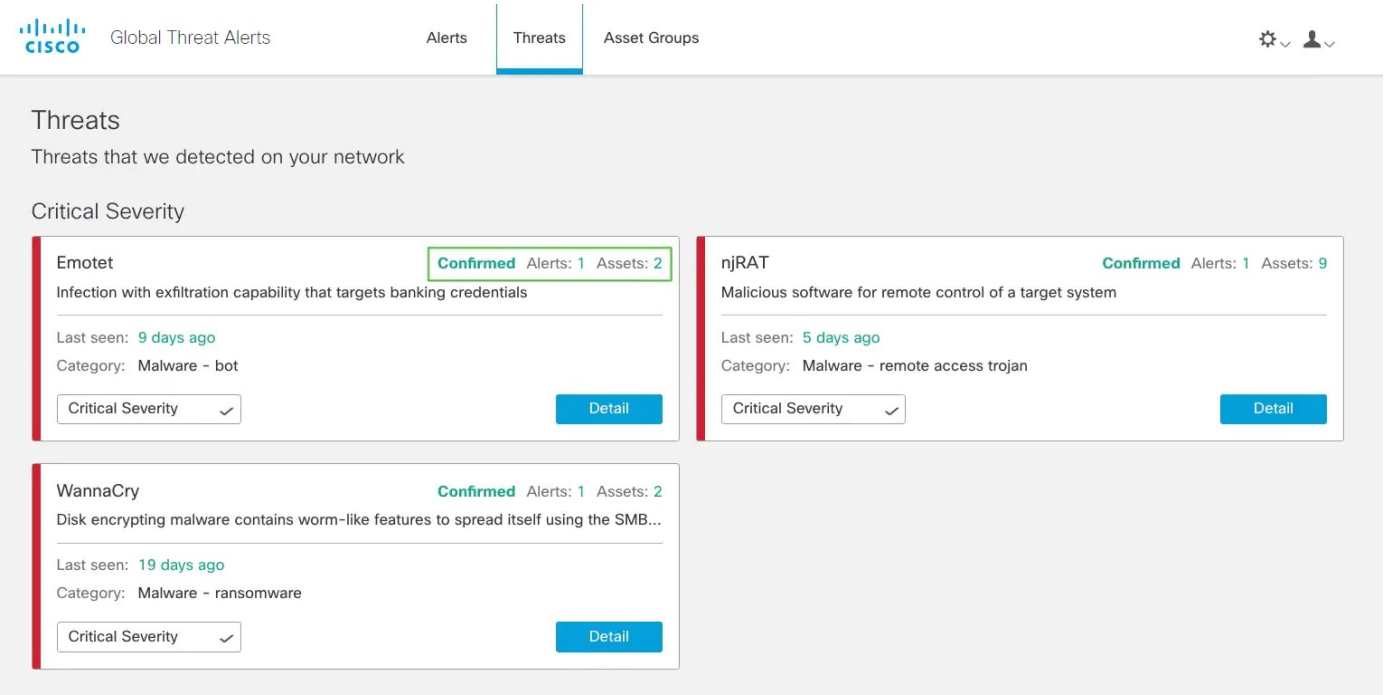


팁 조사 다음 단계를 쉽게 수행할 수 있도록 드롭다운 화살표를 클릭하고 이 IoC를 클립보드에 복사합니다.

위협 조사

단계 **1** **Threats(**위협**)** 탭을 클릭하면 네트워크에서 보고되고 심각도에 따라 우선순위가 지정된 위협 목록을 확인할 수 있습니다. 각 카드는 알림에서 그룹화되는 서로 다른 위협을 나타냅니다.

그림 *5:*



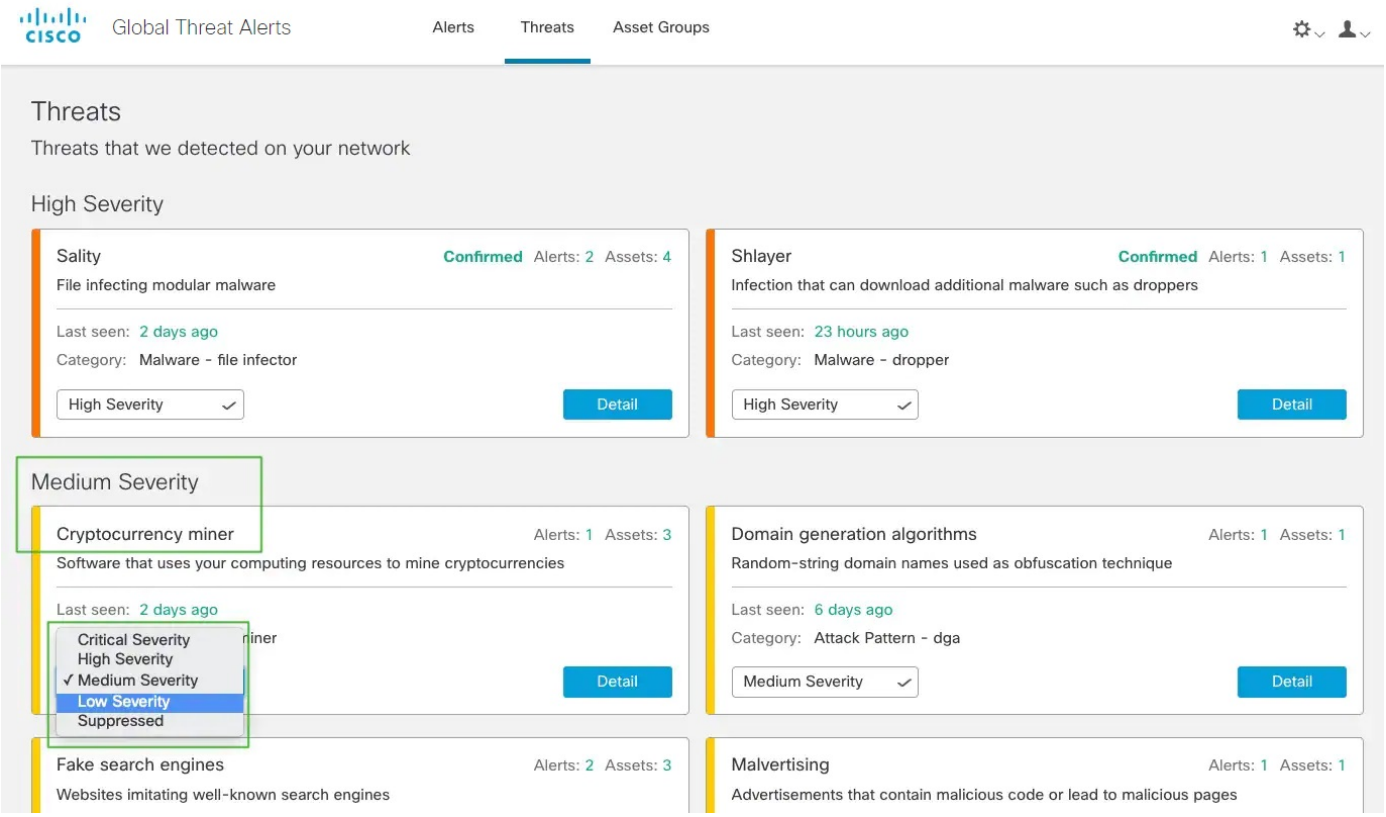
단계 **2** 특정 유형의 위협이 여러 알림과 관련될 수 있습니다. 카드에는 이러한 특정 유형의 위협과 관련된 알림 수 및 이러한 위협의 영향을 받는 자산 수를 나타내는 카운터가 표시됩니다.

단계 **3** **Confirmed(**확인됨**)**라는 레이블이 붙은 위협 카드는 위협 및 위협의 심각도에 대한 신뢰도가 높음을 의미합니다. 우리는 특정 악의적인 행동과 관련된 트래픽에서 하나 이상의 IoC(보안 침해 지표)를 확인했습니다. 이 IoC는 위협 연구팀에서 확인했습니다. **Confirmed(**확인됨**)** 위협의 설명은 이 알림이 비즈니스에 미치는 영향을 자세히 설명합니다.

단계 **4** 네트워크별 조건 및 비즈니스 요구 사항에 따라 위협의 심각도를 조정할 수 있습니다.

- 결과적으로 이 위협 유형이 포함된 모든 **New/Triage(**신규/분류**)** 알림은 위험 레벨이 재계산되어, 새 심각도에 자산 가치 및 신뢰도 수준이 적용됩니다.
- 이후의 모든 위험 수준 변경 사항은 **New/Triage(**신규/분류**)** 알림의 상대적 순서에 영향을 미칩니다.
- 예를 들어 위협의 심각도를 낮추면 관련 알림 위험 수준이 증가하며, 연결된 알림 카드가 **Alerts(**알림**)** 탭의 목록에서 하위에 표시됩니다.
- 드롭다운 목록을 클릭하여 위협의 심각도를 조정하십시오.

그림 *6:*



참고 **New/Triage(**신규/분류**)** 상태가 아닌 다른 모든 알림은 위협 심각도 변경의 영향을 받지 않습니다. 이러한 알림은 쉽게 조사할 수 있도록 변경되지 않고 안정적으로 유지됩니다.

자산 그룹

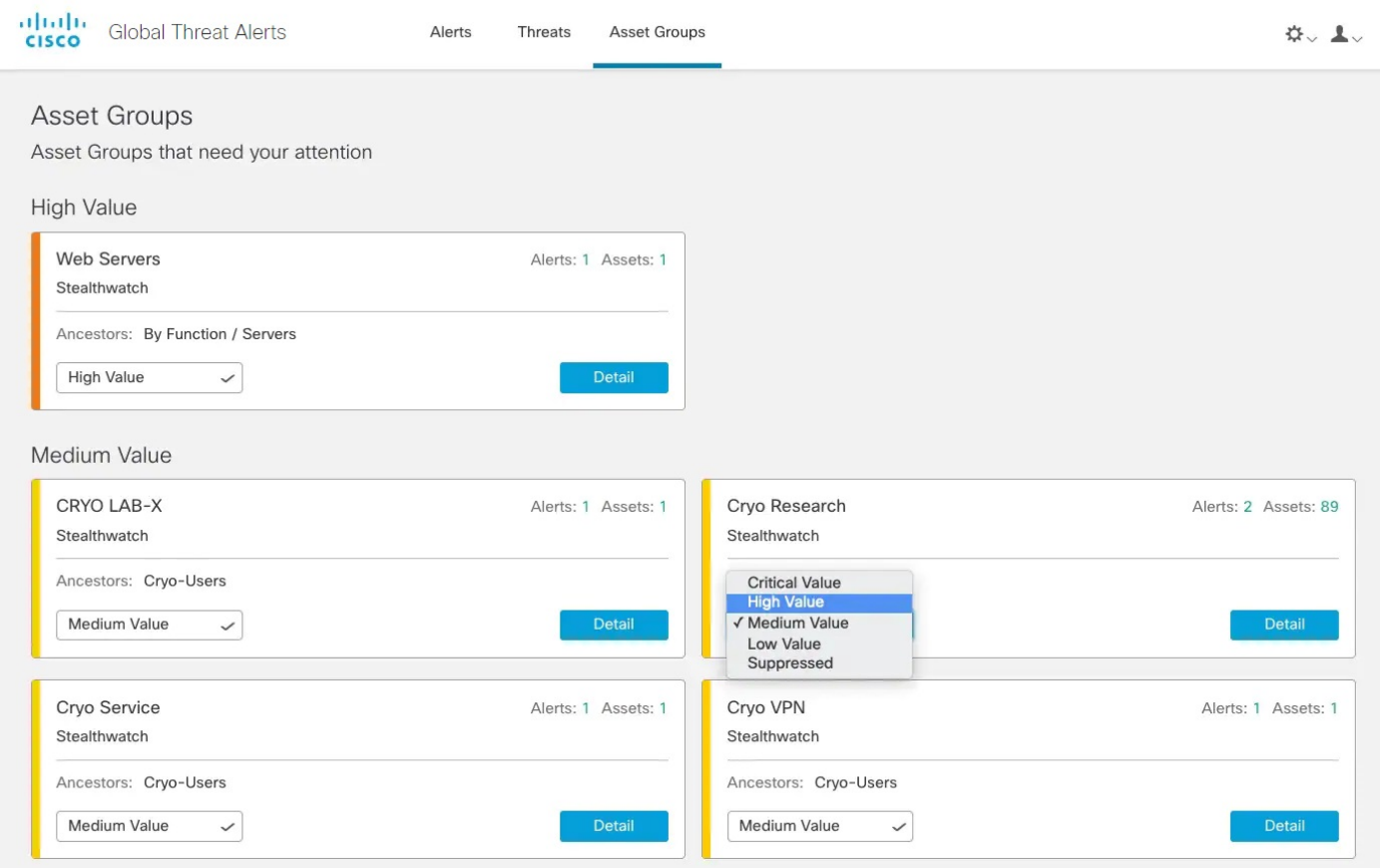
단계 **1** **Assets(**자산**)** 탭을 클릭하여 트래픽이 전역 위협 알림으로 전송된 모든 자산 그룹을 확인하십시오. 각 카드는 전역 위협 알림이 하나 이상의 알림을 보고하는 자산 그룹을 나타냅니다.

단계 **2** 자산 그룹이 조직에 얼마나 중요한지 결정하십시오. 자산 그룹의 비즈니스 가치를 조정할 수 있습니다.

- 결과적으로 이 자산 그룹에 영향을 미치는 모든 **New/Triage(**신규/분류**)** 알림은 위험 레벨이 재계산되어, 새 자산 값에 심각도 및 신뢰도 수준이 적용됩니다.
- 이후의 모든 위험 수준 변경 사항은 **New/Triage(**신규/분류**)** 알림의 상대적 순서에 영향을 미칩니다.
- 예를 들어 자산 그룹의 비즈니스 가치를 높이면 관련 알림 위험 수준이 증가하며, 연결된 알림 카드가 **Alerts(**알림**)** 탭의 목록에서 상위에 표시됩니다.

- 드롭다운 목록을 클릭하여 자산 그룹의 비즈니스 가치를 조정합니다.

그림 *7:*

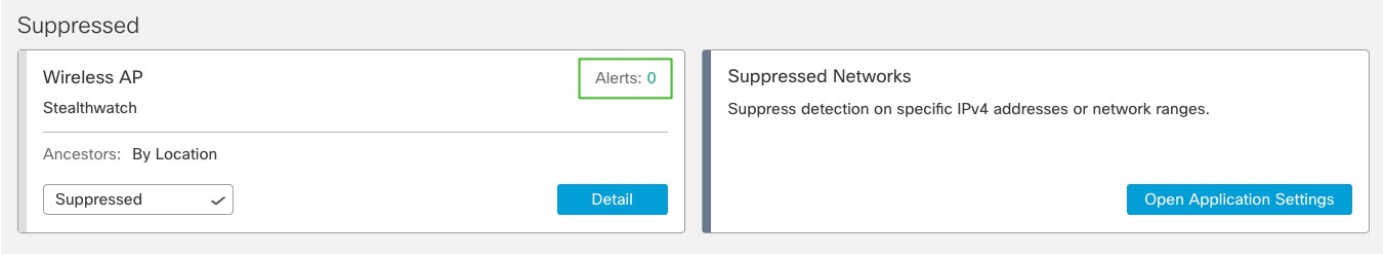


참고 **New/Triage(**신규/분류**)** 상태가 아닌 다른 모든 알림은 위협 심각도 변경의 영향을 받지 않습니다. 이러한 알림은 쉽게 조사할 수 있도록 변경되지 않고 안정적으로 유지됩니다.

단계 **3** 비즈니스 값을 **Suppressed(**억제**)**로 변경하여 자산 그룹을 억제할 수 있습니다. **Suppressed Networks(**억제된 네트워크**)** 카드에서 **Open Application Settings(**애플리케이션 설정 열기**)**를 클릭하여 억제할 특정 IPv4 자산 또는 전체 서브넷을 정의할 수 있습니다.

참고 억제된 그룹에 속한 자산에서 탐지된 위협은 더 이상 알림을 생성하지 않습니다. 억제된 자산 그룹은 **Assets(**자산**)** 탭에 계속 표시됩니다.

그림 *8:* 억제된 네트워크


Suppressed
Wireless AP
Alerts: 0
Stealthwatch
Ancestors: By Location
Suppressed
Detail
Suppressed Networks
Suppress detection on specific IPv4 addresses or network ranges.
Open Application Settings