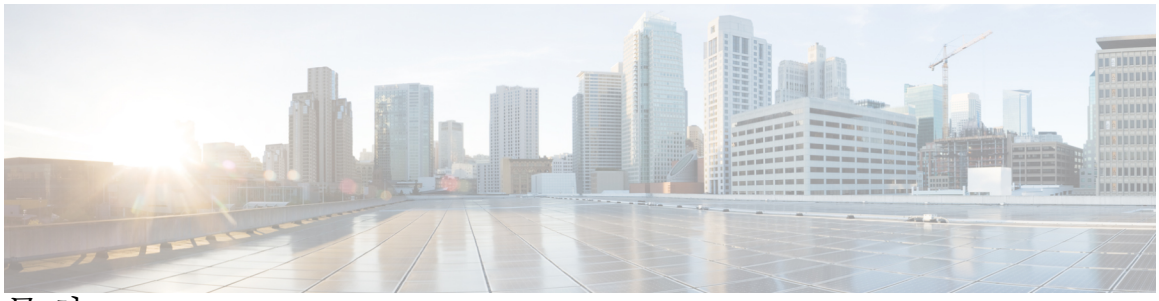
Secure Network Analytics의 전역 위협 알림

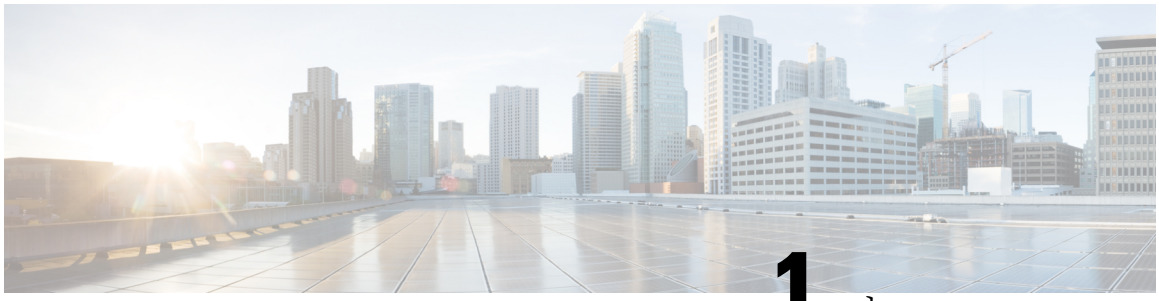
초판: 2021년 7월 1일

최종 변경: 2022년 8월 9일

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



목 차



1 장

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.

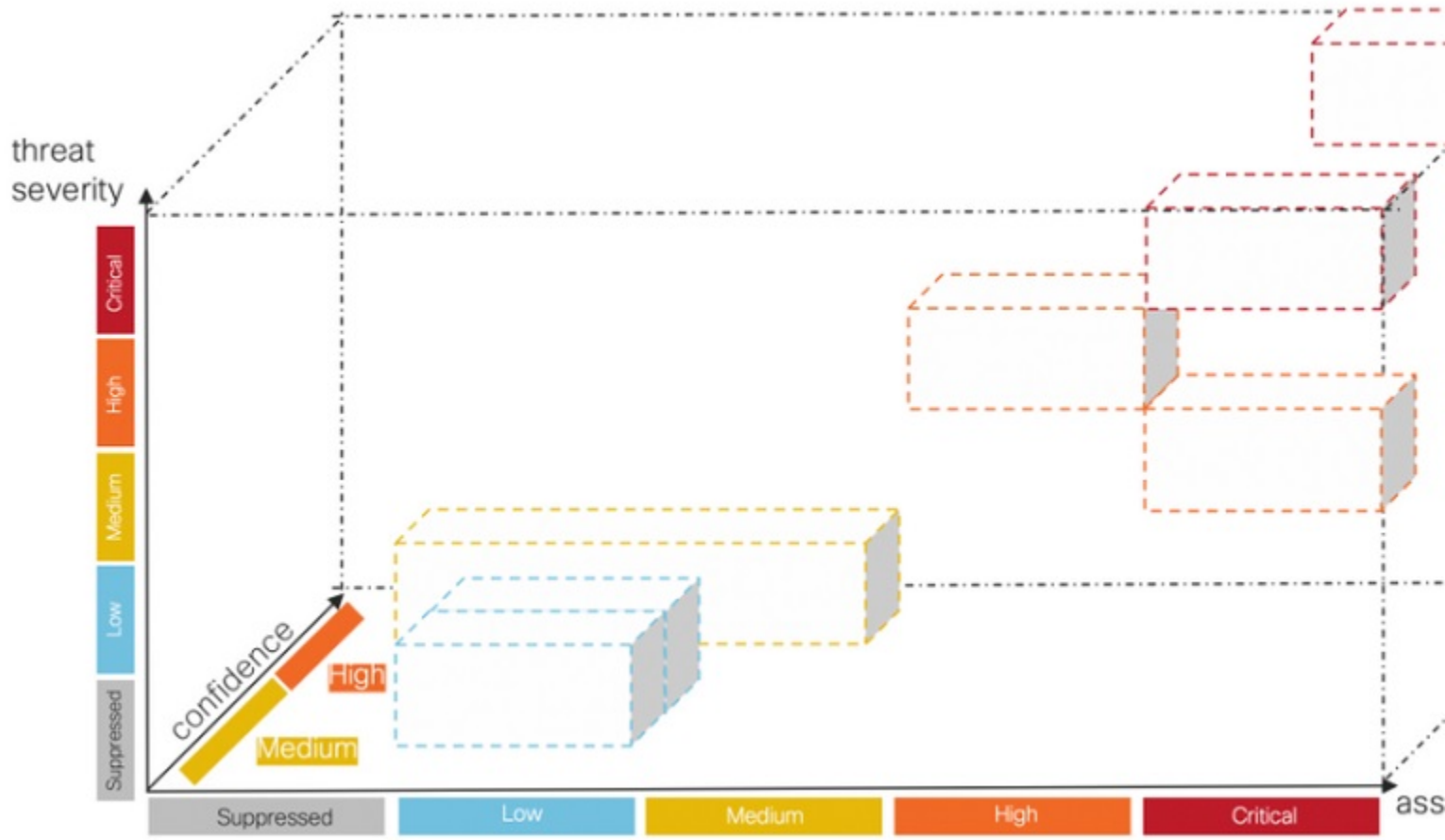
전역 위협 알림은 기계 학습 및 통계적 네트워크 모델링을 통해 정상적인 활동의 기준선을 마련하여 네트워크 내에서 일어나는 비정상적인 트래픽을 식별합니다. 디바이스 동작 및 웹 트래픽을 분석하여 명령 및 제어 통신과 데이터 유출을 찾아냅니다.

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.

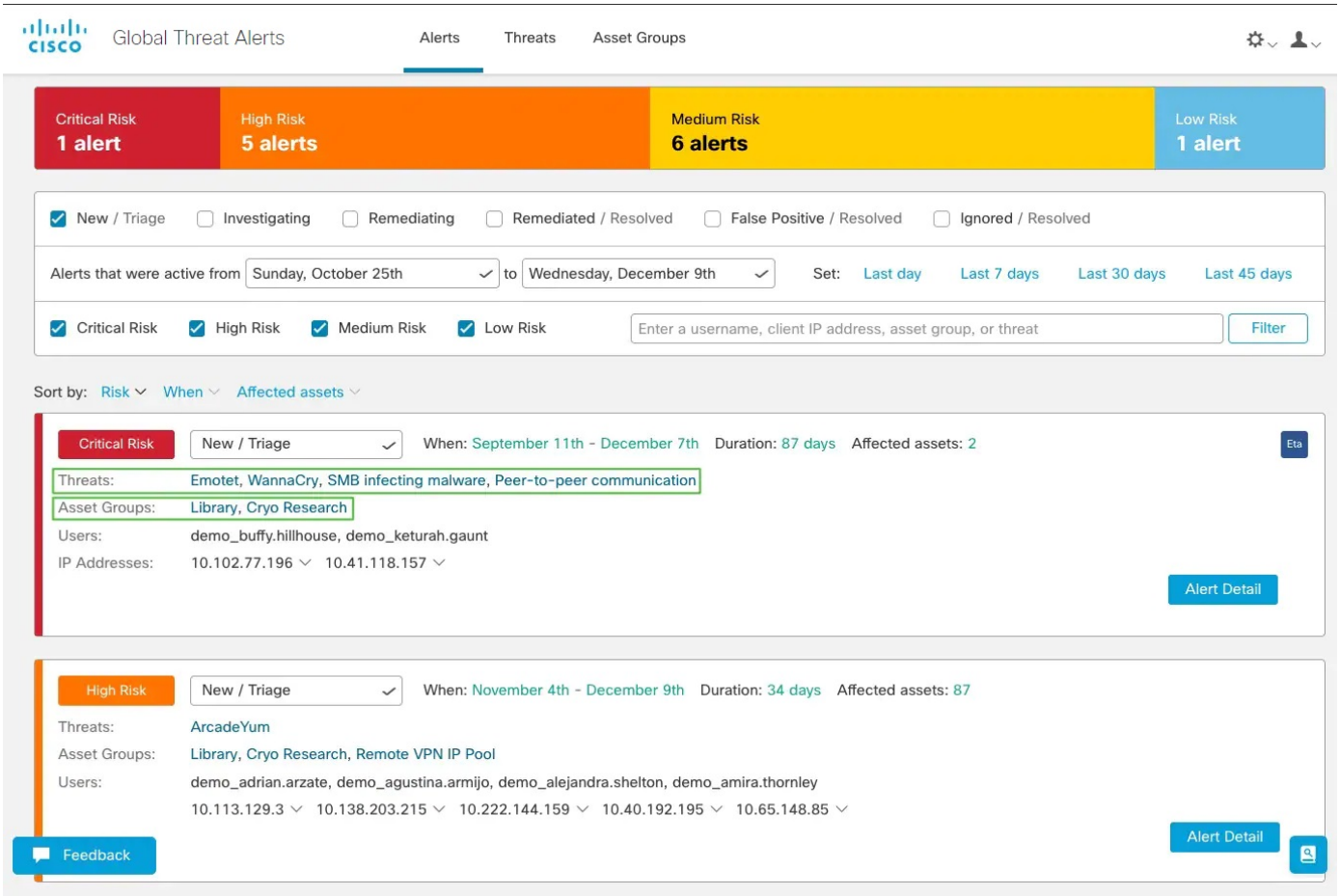
Cisco의 퓨전 알고리즘은 이러한 탐지를 사용하여 유사한 위협 및 예측의 클러스터를 식별하여 위험 수준을 계산합니다. 그런 다음 Cisco의 웹 포털에서 이를 위험 수준에 따라 우선순위가 지정된 목록에 보안 알림으로 표시합니다. 각 알림은 네트워크상의 위협을 가리키며 조사 및 후속 치료를 위한 자연스러운 작업 단위를 나타냅니다.

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.

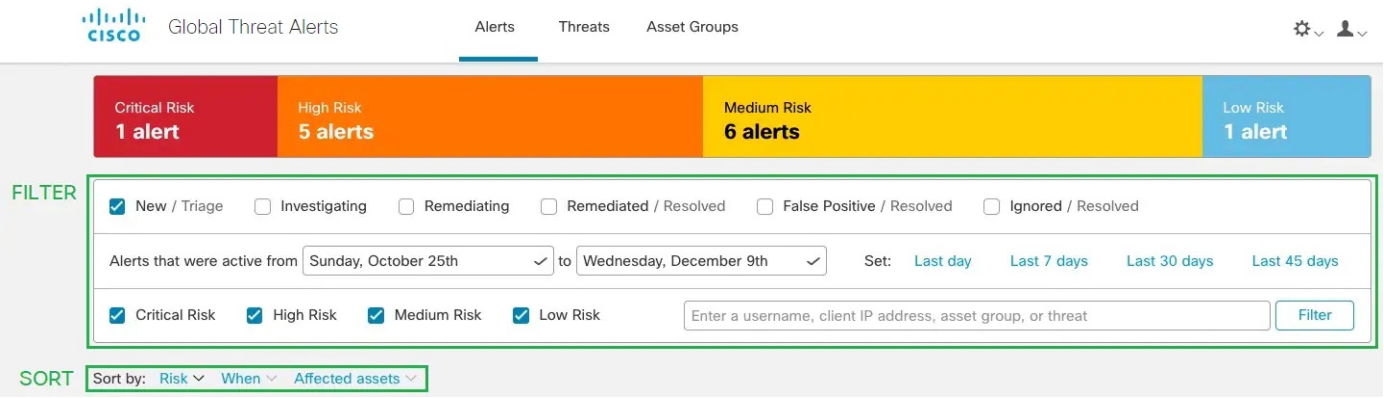
- 중대

- 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.

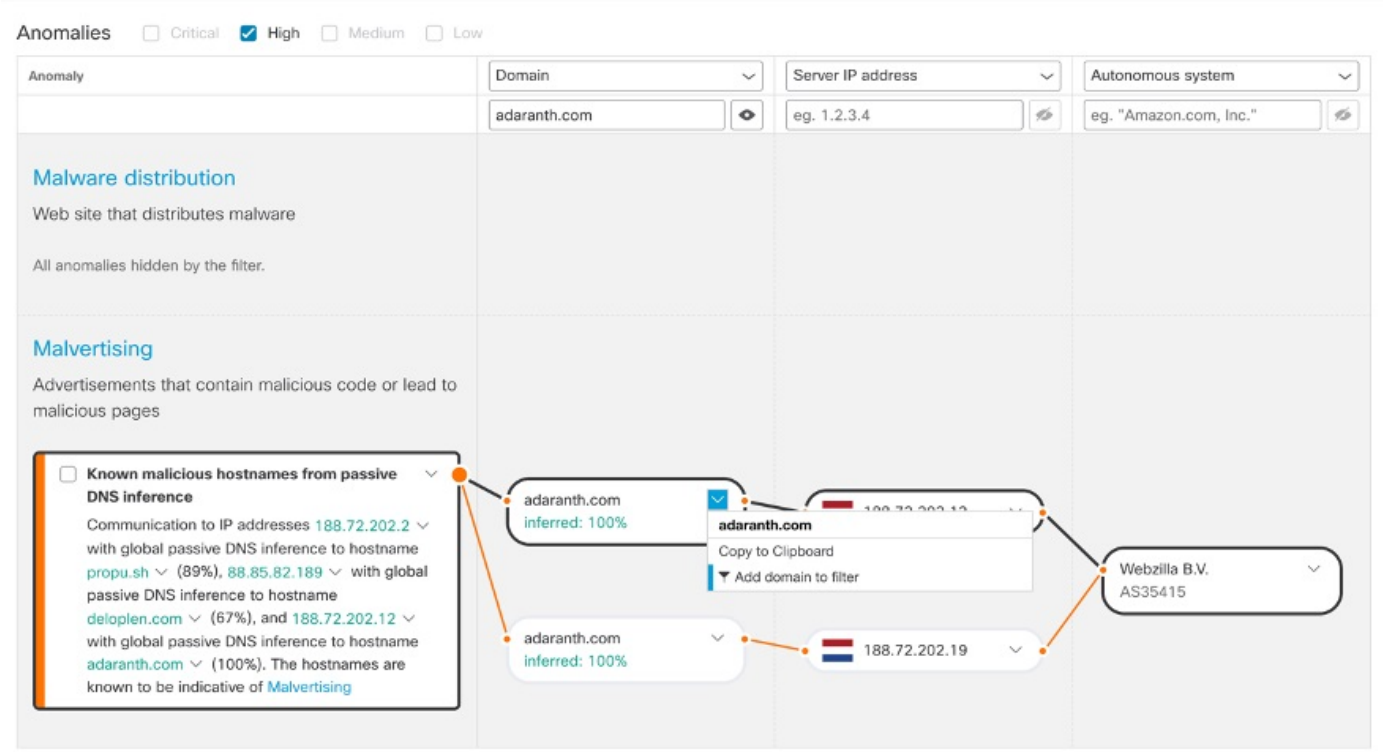
참고 상태가 **New/Triage(**신규/분류**)**가 아니게 되면 쉽게 조사할 수 있도록 알림 카드가 변경되지 않고 안정적으로 유지됩니다.

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:*

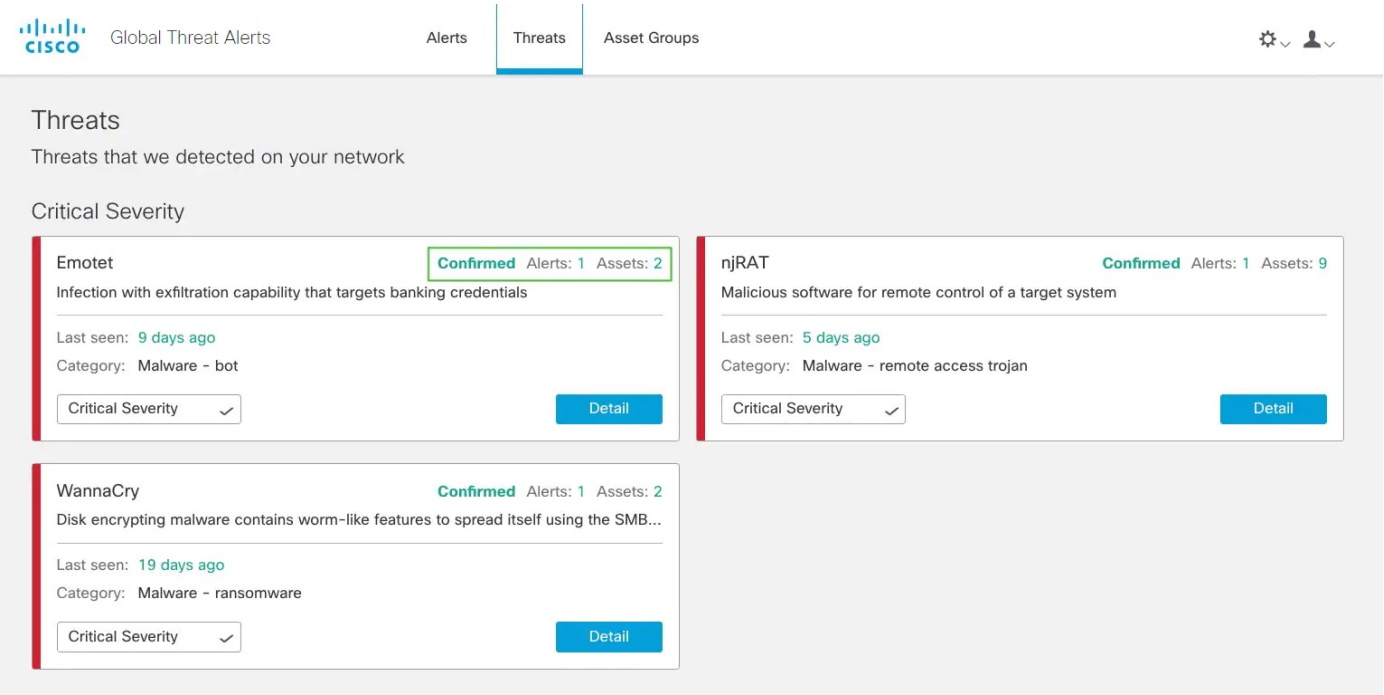


팁 조사 다음 단계를 쉽게 수행할 수 있도록 드롭다운 화살표를 클릭하고 이 IoC를 클립보드에 복사합니다.

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:*



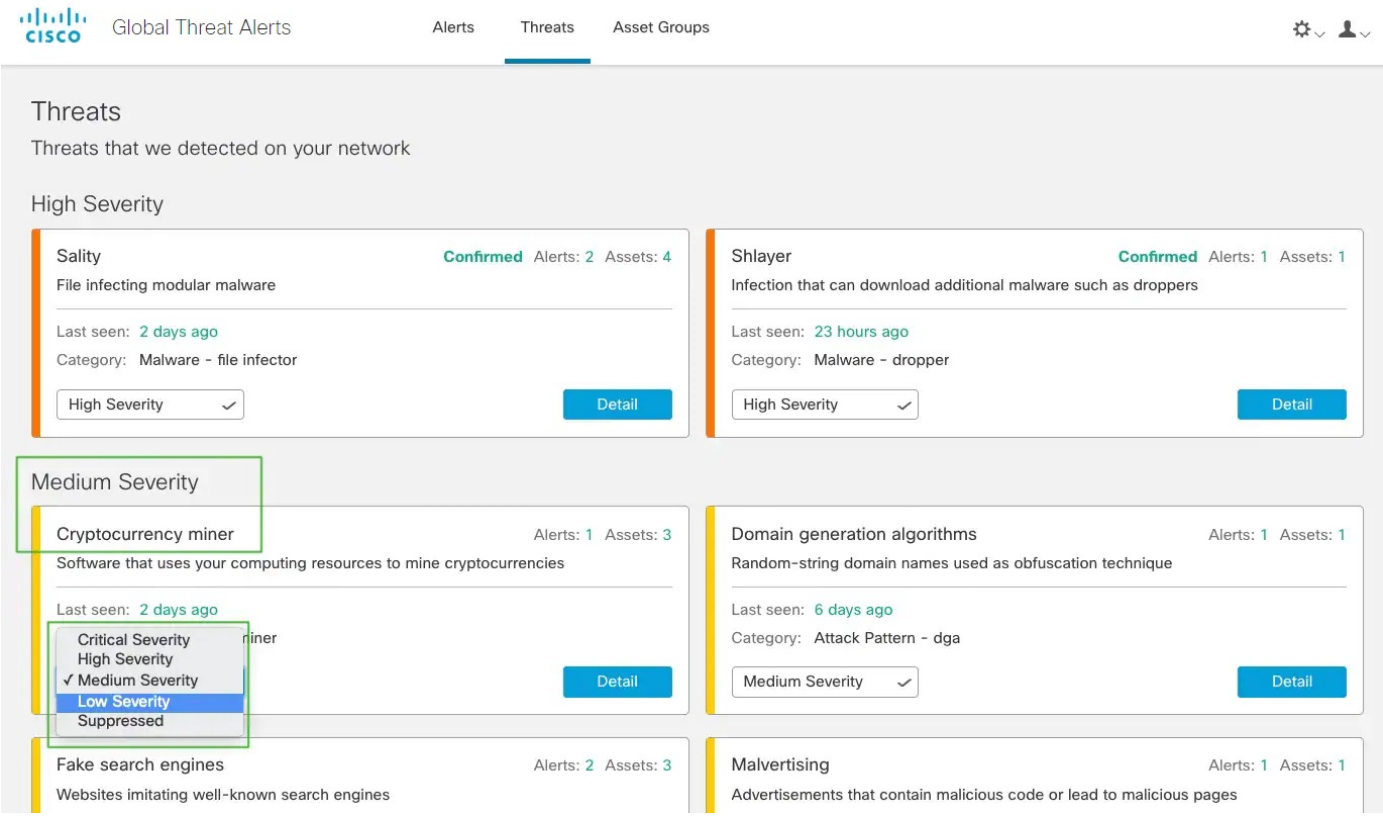
단계 **2** 특정 유형의 위협이 여러 알림과 관련될 수 있습니다. 카드에는 이러한 특정 유형의 위협과 관련된 알림 수 및 이러한 위협의 영향을 받는 자산 수를 나타내는 카운터가 표시됩니다.

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

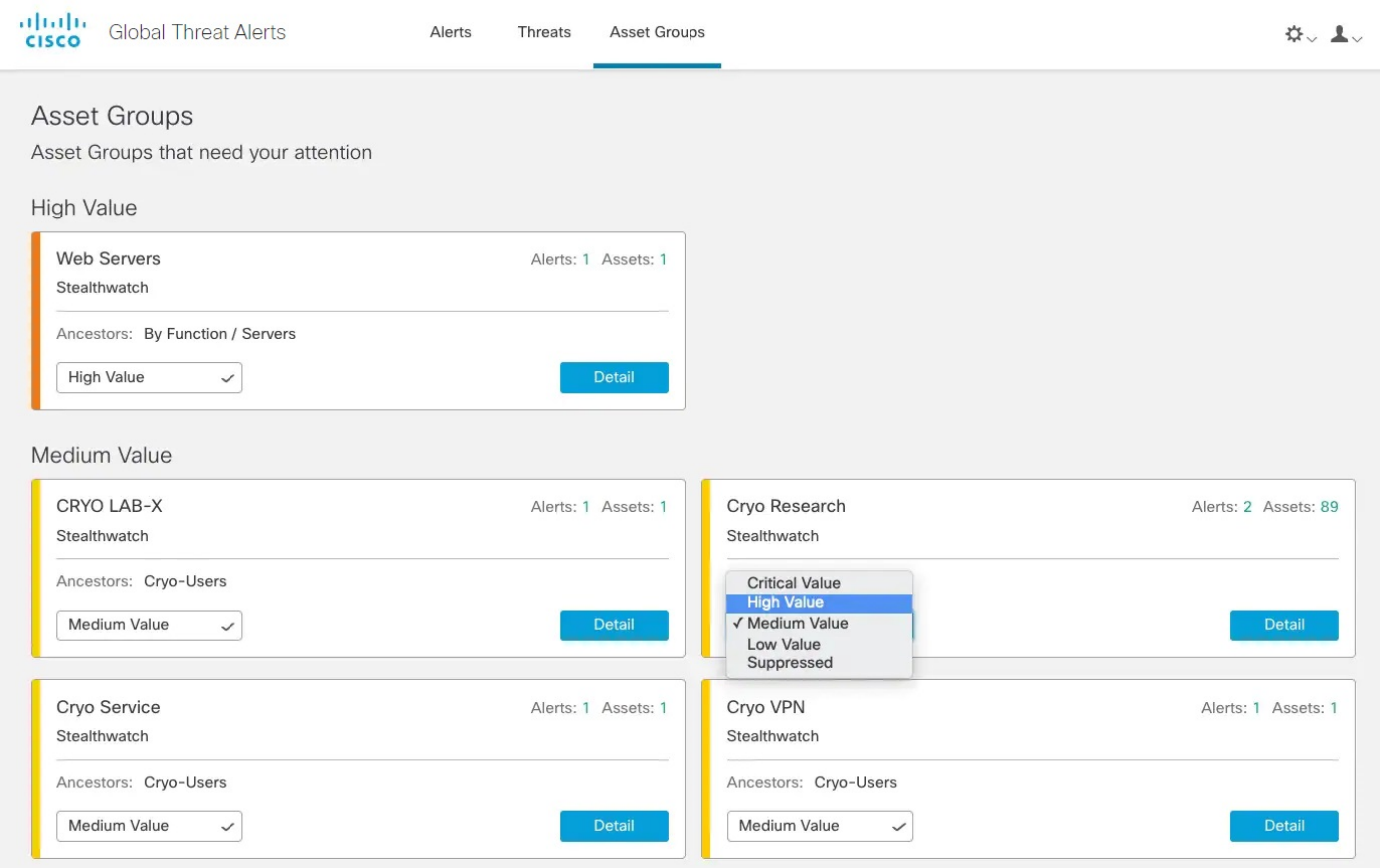
단계 **1** **Assets(**자산**)** 탭을 클릭하여 트래픽이 전역 위협 알림으로 전송된 모든 자산 그룹을 확인하십시오. 각 카드는 전역 위협 알림이 하나 이상의 알림을 보고하는 자산 그룹을 나타냅니다.

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:*

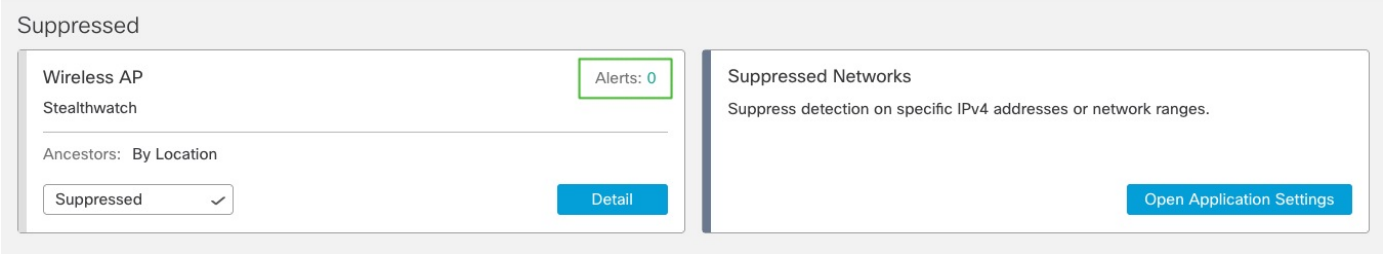


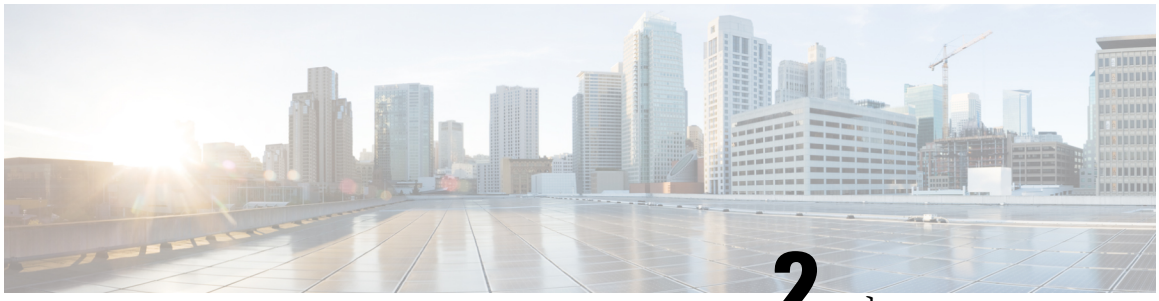
참고 **New/Triage(**신규/분류**)** 상태가 아닌 다른 모든 알림은 위협 심각도 변경의 영향을 받지 않습니다. 이러한 알림은 쉽게 조사할 수 있도록 변경되지 않고 안정적으로 유지됩니다.

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



2 장

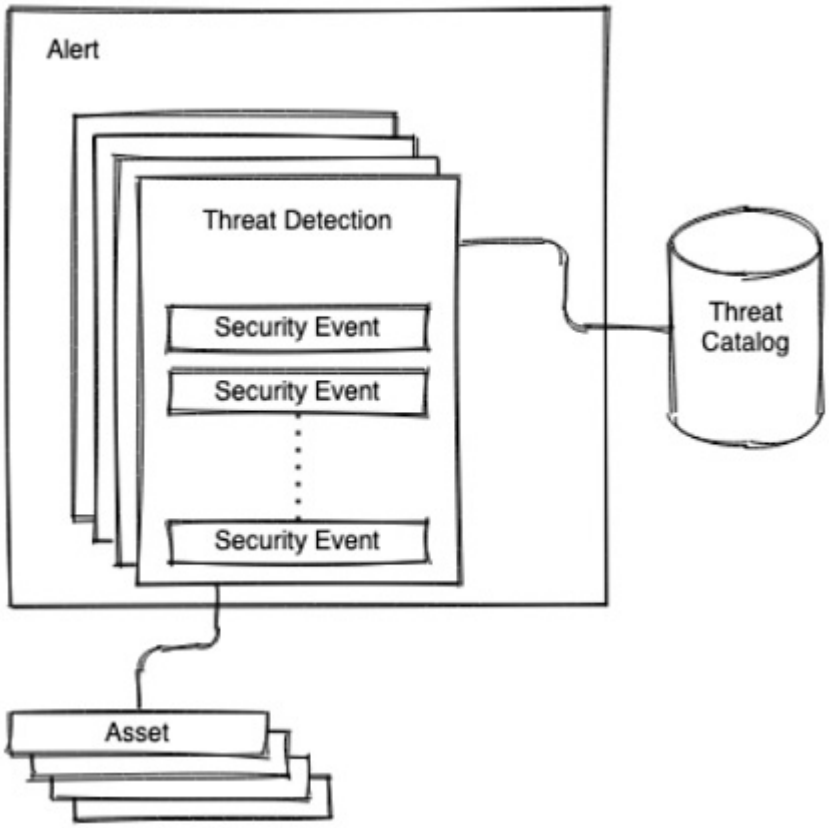
용어집

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 *9:*



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.

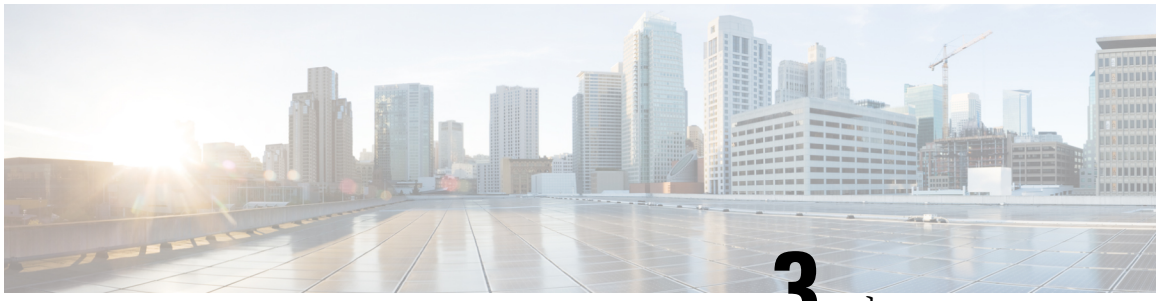
위협 카탈로그

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.



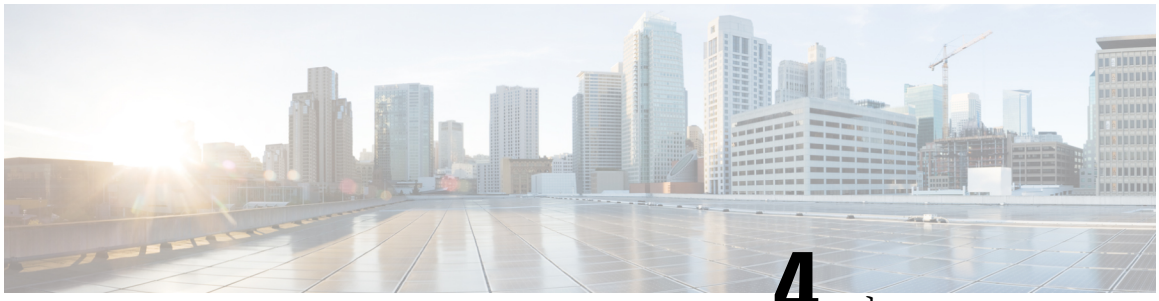
3 장

설정

설정

전역 설정을 구성하려면 페이지 오른쪽 위에 있는 톱니바퀴 아이콘 드롭다운 메뉴를 클릭합니다.

- **Email Notifications(**이메일 알림**)** - 24시간마다 새로운 위협 및 업데이트된 위협의 요약을 전송할 이메일 주소를 입력합니다.
- **CTA STIX/TAXII API** - 전역 위협 알림에서 탐지한 인시던트 관련 정보를 추가 분석, 인시던트 대응 및 데이터 보관을 위해 CTA STIX/TAXII API를 사용하여 SIEM 클라이언트로 가져옵니다. STIX/TAXII 서비스를 참조하십시오.
- **Device Accounts(**디바이스 계정**)** - 하나 이상의 소스 프록시 디바이스에 있는 로그 파일의 텔레메트리 데이터를 전역 위협 알림 시스템으로 업로드하여 분석합니다. 이 서비스에 액세스하려면 외부 텔레메트리 기능을 활성화하고 회사에 프로비저닝해야 합니다. 외부 텔레메트리 기능이 없다면 Cisco Security 어카운트 팀에 문의하십시오. 프록시 디바이스 업로드를 참조하십시오.
- 애플리케이션 설정
  - **Suppressed Networks(**억제된 네트워크**)** - 무시할 IPv4 주소 및 네트워크 범위를 나열하여 알림을 숨깁니다. 게스트 네트워크 또는 네트워크의 다른 덜 중요한 부분에서 오는 알림과 같은 불필요한 알림을 필터링하고 억제하는 데 유용합니다. 인시던트 목록에서 숨길 호스트, 서브넷 또는 IPv4 주소 범위(예: 10.100.10.1, 10.100.10.0/24, 10.100.10.1-10.100.10.254)에 대한 IPv4 주소를 입력합니다.
  - **Cisco SecureX Integration(Cisco SecureX** 통합**)** - SecureX 계정의 지역을 선택하고 **Authorize(**권한 부여**)**를 클릭한 다음 SecureX 계정에 로그인하여 SecureX와의 통합을 활성화합니다.
- **Release Notes(**릴리스 노트**)** - 기능 업데이트, 변경 사항 및 수정 사항을 요약합니다(이 가이드의 뒷부분에 표시됨).



4 장

STIX/TAXII 서비스

새로운 기능

2022년 하반기부터는 전역 위협 알림이 STIX/TAXII API를 지원하지 않습니다.

(자동화 지원을 위한 새 REST API) 새 REST API를 대신 사용하는 것이 좋습니다.

- 이 API에 액세스하려면 https://api.cta.eu.amp.cisco.com에 있는 설명서를 따르십시오.
- 자세한 내용은 전역 위협 알림 REST API가 릴리스되었습니다!를 참조하십시오.
- 도움이 필요하다면 cognitive-api-support@cisco.com으로 문의하십시오.

개요

전역 위협 알림을 사용하면 추가 상관관계 분석 및 보관을 위해 탐지된 인시던트에 관한 정보를 클라이언트로 가져올 수 있습니다. 모든 알림을 네트워크의 서드파티 SIEM으로 스트리밍하여 전체 데이터 수집 프로세스를 자동화할 수도 있습니다. 이 서비스는 보안 정보 및 이벤트 관리(SIEM) 시스템과의 통합을 위한 MITRE의 TAXII(Trusted Automated eXchange of Indicator Information) 표준을 지원합니다. TAXII 표준은 시스템 간에 사이버 위협 정보를 공유하는 데 사용하는 전송 메커니즘을 지정합니다.

TAXII에 대한 자세한 내용은 다음을 참조하십시오.

TAXII MITRE 조직

TAXII 프로젝트 GitHub

각 인시던트의 정보는 STIX(Structured Threat Information eXpression) 언어 형식으로 표시됩니다. STIX는 일관된 방식으로 공유, 저장 및 분석할 수 있도록 사이버 위협 정보를 설명하는 데 사용하는 구조적 언어입니다. STIX 형식을 사용하면 전역 위협 알림에서 위반 탐지 결과를 계층적 형식으로 표현할 수 있습니다. TAXII 서비스는 전역 위협 알림이 탐지한 인시던트를 STIX 언어 하위 집합을 사용하여 설명합니다. 현재 지원되는 개체는 다음과 같습니다.

- 캠페인-확인된 위협 범주(사용 가능한 경우)
- 인시던트-비정상적인 활동
- TTP-Tactics(전술), Techniques(기술), Procedures(절차)
- 관찰 가능 항목 - 웹 요청
- 지표 - 관찰 가능 조건을 식별하는 패턴

STIX에 관한 자세한 내용은 다음을 참조하십시오.

https://stix.mitre.org/

폴링 서비스

폴링 서비스는 표준화된 TAXII 전송 메커니즘을 사용하여 전역 위협 알림의 인시던트 정보를 TAXII 표준을 지원하는 클라이언트로 전송합니다. TAXII 클라이언트는 인시던트 정보를 가져오기 위해 TAXII 폴링 서비스에 폴링 요청을 전송합니다. HTTP 기본 인증은 권한 있는 사용자만 액세스할 수 있게 하는 데 사용합니다. 그러면 TAXII 폴링 서비스는 전역 위협 알림의 인시던트 정보를 TAXII 클라이언트로 전송하여 응답합니다. HTTPS 프로토콜은 모든 데이터 전송을 보호하는 데 사용합니다.

SIEM 또는 기타 보안 워크플로 시스템은 STIX/TAXII를 기본적으로 지원해야 합니다. TAXII 폴링 서비스를 주기적으로 폴링하도록 서드파티 TAXII 클라이언트를 구성하십시오.

- 계정 정보를 가져오려면 STIX/TAXII 서비스를 요청하십시오.
  1. 페이지 오른쪽 상단에 있는 전역 설정 톱니바퀴 아이콘을 클릭합니다.
  2. **CTA STIX/TAXII API**를 클릭합니다.
  3. **Add account(**계정 추가**)** 버튼을 클릭합니다.
  4. 계정을 식별하기 위한 이름을 입력하고 **Add account(**계정 추가**)** 버튼을 클릭합니다.
- 프로비저닝 프로세스가 완료되면 계정 정보가 표시됩니다. 창을 닫기 전에 이 계정 정보를 안전한 곳에 복사하십시오.

참고 보안 유지를 위해 비밀번호는 한 번만 표시됩니다. 비밀번호를 분실했다면 기존 비밀번호를 취소하고 새 비밀번호를 만들어야 합니다.

- 고유한 속성을 서드파티 TAXII 클라이언트에 복사합니다.

- pollEndpoint 또는 피드 서비스
  URL=`https://taxii.cloudsec.sco.cisco.com/skym-taxii-ws/PollService`
- 사용자 이름
- 비밀번호
- 컬렉션 이름 또는 피드 이름

참고 2018년 8월 Cognitive Intelligence(구 Cognitive Threat Analytics 또는 CTA)가 Amazon Web Services의 새 위치로 마이그레이션하기 시작했으며, 그 결과 서비스에 액세스하고 서비스를 사용하는 데 필요한 새 IP 주소 및 추가 URL이 생성되었습니다. 서비스에 대한 액세스를 유지하려면 아웃바운드 방화벽 규칙을 업데이트해야 할 수 있습니다. 2018년 11월의 전환이 끝나면 이전 데이터 수집 서비스 IP 주소로 데이터를 전송할 수 없습니다. 필요한 변경 사항 및 기타 중요 정보에 관한 구체적인 세부 정보는 Field Notice(현장 알림)에서 확인할 수 있습니다.

참고 Cisco에서는 서드파티 제품 또는 SIEM 디바이스 구성 관련 기술 지원을 제공하지 않습니다. 문제가 있다면 벤더별 지원팀에 문의하십시오.

Cisco에서 TAXII 클라이언트 예시를 다운로드하여 사용하는 방법도 있습니다. SIEM 또는 기타 보안 시스템이 STIX/TAXII를 기본적으로 지원하지 않는 경우, Cisco는 SIEM 옆에 있는 Linux 또는 Windows VM 환경에 구축할 수 있는 경량 Java TAXII Log Adapter를 제공합니다. 제공된 링크를 클릭하여 설정 지침을 확인합니다. 이 어댑터는 TAXII API를 사용하여 새로운 인텔리전스의 정기 폴링을 수행하고 STIX 메시지에 데이터를 전달합니다. 그런 다음 어댑터가 STIX 메시지를 일반 SIEM 시스템에서 허용되는 다른 형식으로 변환합니다.

폴링 서비스의 안정성, 성능 및 가용성을 지원하려면 다음 조건이 충족되어야 합니다.

- 단일 TAXII 클라이언트의 폴링 요청은 10분마다 한 번만 허용됩니다. 그렇지 않으면 이 오류를 나타내는 상태 메시지가 반환됩니다.
- 각 폴링 요청은 최대 3일 동안의 인시던트 정보를 검색할 수 있습니다.
- 인시던트 정보는 검색을 위해 최대 30일 동안 저장됩니다.

폴링 요청

다음은 TAXII 클라이언트가 TAXII 폴링 서비스에 보내는 폴링 요청의 예입니다.

메서드는 POST입니다.

HTTP 요청 헤더:

```
x-taxii-content-type: urn:taxii.mitre.org:message:xml:1.1
x-taxii-protocol: urn:taxii.mitre.org:protocol:http:1.1
x-taxii-services: urn:taxii.mitre.org:services:1.1
```

```
x-taxii-accept: urn:taxii.mitre.org:message:xml:1.1
content-type: application/xml
accept: application/xml
authorization: Basic ...
```

요청 본문:

```
<taxii_11:Poll_Request xmlns:taxii_11="http://taxii.mitre.org/messages/taxii_xml_binding-1.1"

                            message_id=" " collection_name=" ">

<taxii_11:Exclusive_Begin_Timestamp>2015-01-16T00:00:00+00:00</taxii_11:Exclusive_Begin_Timestamp>


<taxii_11:Inclusive_End_Timestamp>2015-01-17T00:00:00+00:00</taxii_11:Inclusive_End_Timestamp>

 <taxii_11:Poll_Parameters allow_asynch="false"/>
  <taxii_11:Response_Type>FULL</taxii_11:Response_Type>
 </taxii_11:Poll_Parameters>
</taxii_11:Poll_Request>
```

지원되는 요청 매개변수	설명
Poll_Request	
message_id	TAXII 사양에 따라 각 요청에 대해 임의로 생성된 문자열입니다. 모든 요청에 대해 고유한 문자열을 재생성합니다.
collection_name	전역 위협 알림 서비스에서 추출하거나 가져올 컬렉션의 이름입니다. 이 속성은 프로비저닝 프로세스가 완료된 후 Cisco에서 제공합니다.
exclude_Begin_Timestamp	기간에 따라 이 값을 조정합니다.
Inclusive_End_Timestamp	기간에 따라 이 값을 조정합니다.
Poll_Parameters	
allow_async	이 특성은 항상 false로 설정합니다.

참고 **Exclusive_Begin_Timestamp**와 **Inclusive_End_Timestamp** 사이에 허용되는 최대 기간은 3일입니다. 기간이 더 길면 반환되는 결과는 **Inclusive_End_Timestamp** 이전 3일로 제한됩니다.

폴링 응답

다음은 TAXII 폴링 서비스가 TAXII 클라이언트에 보내는 폴링 응답의 예입니다.

HTTP 응답 헤더:

```
x-taxii-content-type: urn:taxii.mitre.org:message:xml:1.1
x-taxii-protocol: urn:taxii.mitre.org:protocol:http:1.1
x-taxii-services: urn:taxii.mitre.org:services:1.1
```

응답 본문:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<t:Poll_Response xmlns:t="http://taxii.mitre.org/messages/taxii_xml_binding-1.1"
                 xmlns:c="http://cybox.mitre.org/cybox-2"
                 xmlns:cc="http://cybox.mitre.org/common-2"
                 xmlns:co="http://cybox.mitre.org/objects#CustomObject-1"
                 xmlns:coa="http://stix.mitre.org/CourseOfAction-1"
                 xmlns:sc="http://stix.mitre.org/common-1"
                 xmlns:ind="http://stix.mitre.org/Indicator-2"
                 xmlns:ttp="http://stix.mitre.org/TTP-1"
                 xmlns:inc="http://stix.mitre.org/Incident-1"
                 xmlns:s="http://stix.mitre.org/stix-1"
                 collection_name=" " more="true"
                  result_id=" " result_part_number="1"
                  in_response_to="generatedMessageID" message_id="responseMessageID">
    <t:Exclusive_Begin_Timestamp>2015-01-17T15:11:00.648Z</t:Exclusive_Begin_Timestamp>
    <t:Inclusive_End_Timestamp>2015-01-20T15:11:00.649Z</t:Inclusive_End_Timestamp>
    <t:Content_Block>
      <t:Content_Binding binding_id="STIX_XML_1.1"/>
      <t:Content>
        <s:STIX_Package xmlns:cta="http://cisco.com/td/cta"
               id="cta:package-1412045744-66911c07-c9b8-4389-8888-00e438f58c2e"
               timestamp="2015-01-20T15:11:02.766Z" version="1.1.1">
          <s:STIX_Header>
            <s:Package_Intent>Incident</s:Package_Intent>
              <s:Information_Source>
                <sc:Identity id="cta:customer-1234567890"/>
                <sc:Tools>
                   <cc:Tool id="cta:tool-cta">
                       <cc:Name>Cognitive Threat Analytics</cc:Name>
                       <cc:Vendor>Cisco</cc:Vendor>
                   </cc:Tool>
                   <cc:Tool id="cta:tool-amp">
                       <cc:Name>Advanced Malware Protection</cc:Name>
                       <cc:Vendor>Cisco</cc:Vendor>
                   </cc:Tool>
                </sc:Tools>
             </s:Information_Source>
          </s:STIX_Header>
          <s:Incidents>
            <s:Incident xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                    xsi:type="inc:IncidentType"
                    id="cta:incident-1412045744_f8bae03fb2ff7d6185907ae3240d_ITMAL1">
             <inc:Title>malware|using automatically generated domain (DGA)</inc:Title>
             <inc:Victim>
                 <sc:Name>JohnDoe</sc:Name>
             </inc:Victim>
              <inc:Related_Indicators>
               <inc:Related_Indicator>
                <sc:Indicator xsi:type="ind:IndicatorType"
               id="cta:indicator-1412045744_1421623800000_f8bae03fb2ff7d6185907ae3240d_0">

                  <ind:Observable>
                   <c:Observable_Composition operator="AND">
                     <c:Observable>
                      <c:Object>
                       <c:Properties xsi:type="co:CustomObjectType">
                        <cc:Custom_Properties>
                         <cc:Property name="timestamp">1421623882432</cc:Property>
```

```
                                <cc:Property name="xElapsedTime">1810</cc:Property>
                                <cc:Property name="scHttpStatus">0</cc:Property>
                                <cc:Property name="csContentBytes">622</cc:Property>
                                <cc:Property name="scContentBytes">907</cc:Property>
                                <cc:Property name="csUrl"></cc:Property>
                                <cc:Property name="sIP">195.22.26.231</cc:Property>
                                <cc:Property name="cIP">33.196.39.11</cc:Property>
                                <cc:Property name="cUsername">JohnDoe</cc:Property>
                                <cc:Property name="sReputation">-580</cc:Property>
                                <cc:Property name="sCategory">unclassified</cc:Property>
                               </cc:Custom_Properties>
                              </c:Properties>
                             </c:Object>
                            </c:Observable>
                            <c:Observable>
                             <c:Object>
                              <c:Properties xsi:type="co:CustomObjectType">
                               <cc:Custom_Properties>
                                <cc:Property name="timestamp">1421623896635</cc:Property>
                                <cc:Property name="xElapsedTime">1942</cc:Property>
                                <cc:Property name="scHttpStatus">0</cc:Property>
                                <cc:Property name="csContentBytes">361</cc:Property>
                                <cc:Property name="scContentBytes">582</cc:Property>
                                <cc:Property name="csUrl"></cc:Property>
                                <cc:Property name="sIP">195.22.26.231</cc:Property>
                                <cc:Property name="cIP">33.196.39.11</cc:Property>
                                <cc:Property name="cUsername">JohnDoe</cc:Property>
                                <cc:Property name="sReputation">-580</cc:Property>
                                <cc:Property name="sCategory">unclassified</cc:Property>
                               </cc:Custom_Properties>
                              </c:Properties>
                             </c:Object>
                            </c:Observable>
                           </c:Observable_Composition>
                          </ind:Observable>
                          <ind:Indicated_TTP>
                           <sc:TTP xsi:type="ttp:TTPType">
                            <ttp:Title>communication to automatically generated domain
(DGA)</ttp:Title>
                           </sc:TTP>
                          </ind:Indicated_TTP>
                         </sc:Indicator>
                        </inc:Related_Indicator>
                       </inc:Related_Indicators>
                       <inc:Discovery_Method>Log Review</inc:Discovery_Method>
                       <inc:COA_Requested>
                        <inc:Course_Of_Actionxsi:type="coa:CourseOfActionType">
                         <coa:Stage>Remedy</coa:Stage>
                         <coa:Type>Eradication</coa:Type>
                         <coa:Parameter_Observablescybox_major_version="2"cybox_minor_version="1">
                          <c:Observable_Package_Source>
                           <cc:Time>
                            <cc:Produced_Time>2016-08-15T17:02:02.616Z</cc:Produced_Time>
                           </cc:Time>
                          </c:Observable_Package_Source>
                          <c:Observable>
                           <c:Object>
                            <c:Propertiesxsi:type="user:UserAccountObjectType">
                             <user:Username>JohnDoe</user:Username>
                            </c:Properties>
                           </c:Object>
                          </c:Observable>
                          <c:Observable>
                           <c:Object>
```

```
                    <c:Propertiesxsi:type="addr:AddressObjectType"category="ipv4-addr">
                     <addr:Address_Value>33.196.39.11</addr:Address_Value>
                    </c:Properties>
                   </c:Object>
                  </c:Observable>
                 </coa:Parameter_Observables>
                </inc:Course_Of_Action>
               </inc:COA_Requested>
               <inc:Confidence>
                <sc:Value>Low</sc:Value>
               </inc:Confidence>
               <inc:Information_Source>
                   <sc:Tools>
                       <cc:Tool idref="cta:tool-cta"/>
                   </sc:Tools>
               </inc:Information_Source>
            </s:Incident>
          </s:Incidents>
         </s:STIX_Package>
        </t:Content>
    </t:Content_Block>
</t:Poll_Response>
```

참고 `Poll_Reponse`에 추가 위협 항목이 없다면, `more`과 `result_id`라는 두 속성이 존재하지 않습니다. `more=true`가 존재한다면, `Poll_Fulfillment`를 사용하여 응답의 다음 페이지를 요청할 수 있습니다.

지원되는 응답 개체	필드 설명
Poll_Response	
collection_name	전역 위협 알림 서비스에서 추출하거나 가져올 컬렉션의 이름입니다. 이 속성은 프로비저닝 프로세스가 완료된 후 Cisco에서 제공합니다.
result_id	이 값을 폴링 이행 요청에 복사합니다.
exclude_Begin_Timestamp	이 폴링 응답이 적용되는 시간 범위의 시작 지점(지점 제외)입니다. 이 필드가 없다면 설문조가 응답이 이 TAXII 데이터 피드에 대한 가장 빠른 시간을 포함한다는 뜻입니다.
Inclusive_End_Timestamp	이 폴링 응답이 적용되는 시간 범위의 종료 지점(지점 포함)입니다.
Content_Block	반환된 콘텐츠입니다.
Content_Binding	
콘텐츠	
STIX_Package	STIX 언어 관련 정보입니다.

지원되는 응답 개체	필드 설명
STIX_Header	이 STIX 콘텐츠 패키지에 관한 정보입니다.
인시던트	하나 이상의 인시던트입니다.
사고	단일 인시던트 관련 정보입니다.
직함	이 인시던트를 설명하는 제목입니다.
피해자	이 인시던트의 피해자에 관한 정보입니다.
Related_Indicators	이 인시던트와 관련된 지표를 식별합니다.
Related_Indicator	이 인시던트와 관련된 단일 지표를 식별합니다.
지표	특정 관찰 가능 조건과 패턴의 의미에 대한 상황별 정보, 조치 방법 및 시점 등에 관한 정보를 식별하는 패턴으로 구성된 지표입니다.
관찰 가능 항목	이 지표와 관련된 관찰 가능 항목입니다.
Observable_Composition	다른 관찰 가능 항목의 논리적 조합을 작성하여 고차 복합 관찰 가능 항목을 지정할 수 있게 합니다.
관찰 가능 항목	단일 관찰 가능 항목을 나타냅니다.
객체	특정 개체의 특성(예: 파일, 레지스트리 키, 프로세스)을 식별합니다.
속성	개체에 대한 작업의 결과로 열거된 속성입니다.
Custom_Properties	기존 Properties(속성) 스키마에 정의되어 있지 않은 사용자 지정 개체 속성 집합을 지정할 수 있게 합니다.
속성	개체에 대한 작업의 결과로 열거된 단일 속성입니다.
Indicatord_TTP	이 지표가 나타내는 관련 TTP(Tactics, Techniques, and Procedures)를 지정합니다.
Discovery_Method	코드를 검색하는 데 사용하는 방법 및/또는 툴에 관한 정보입니다.
COA_Requested	이 인시던트에 권장되는 조치입니다.
신뢰	이 인시던트의 특성에 대한 신뢰도 수준 관련 정보입니다.

지원되는 응답 개체	필드 설명
Information_Source	이 인시던트의 소스 관련 정보입니다.
툴	
Tool(툴)	이 인시던트를 탐지한 툴(CTA 또는 AMP)입니다.

오류가 발생하면 오류 메시지가 반환됩니다. 예를 들면 다음과 같습니다.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<t:Status_Message
          xmlns:t="http://taxii.mitre.org/messages/taxii_xml_binding-1"
          xmlns:c="http://cybox.mitre.org/cybox-2"
          xmlns:cc="http://cybox.mitre.org/common-2"
          xmlns:co="http://cybox.mitre.org/objects#CustomObject-1"
          xmlns:sc="http://stix.mitre.org/common-1"
          xmlns:ind="http://stix.mitre.org/Indicator-2"
          xmlns:ttp="http://stix.mitre.org/TTP-1"
          xmlns:inc="http://stix.mitre.org/Incident-1"
          xmlns:s="http://stix.mitre.org/stix-1"
                status_type="FAILURE" in_response_to="23537"
                message_id="16ed0b75-2af6-4537-b71c-da00e0a0c419">
   <t:Message>An error occurred during request processing.</t:Message>
</t:Status_Message>
```

TAXII status_type	오류 설명
	사용자가 인증되지 않음, HTTP 응답 상태 코드 404
DENIED	사용자에게 권한이 부여되지 않음, HTTP 응답 상태 코드 401
BAD_MESSAGE	잘못된 요청 메시지입니다. `Message` 매개변수를 참조하십시오.
FAILURE	지정되지 않은 오류입니다. `Message` 매개변수를 참조하십시오.

폴링 이행

다음은 TAXII 클라이언트가 TAXII 폴링 서비스에 보내는 폴링 수행 요청의 예입니다.

메서드는 POST입니다.

HTTP 요청 헤더:

```
x-taxii-content-type: urn:taxii.mitre.org:message:xml:1.1
x-taxii-protocol: urn:taxii.mitre.org:protocol:http:1.1
x-taxii-services: urn:taxii.mitre.org:services:1.1
x-taxii-accept: urn:taxii.mitre.org:message:xml:1.1
content-type: application/xml
accept: application/xml
authorization: Basic ...
```

요청 본문:

```
<taxii_11:Poll_Fulfillment
xmlns:taxii_11="http://taxii.mitre.org/messages/taxii_xml_binding-1.1"
                           message_id=" " collection_name=" "
                           result_id=" " result_part_number="2" />

<taxii_11:Exclusive_Begin_Timestamp>2015-01-16T00:00:00+00:00</taxii_11:Exclusive_Begin_Timestamp>


<taxii_11:Inclusive_End_Timestamp>2015-01-17T00:00:00+00:00</taxii_11:Inclusive_End_Timestamp>

 <taxii_11:Poll_Parameters allow_asynch="false"/>
  <taxii_11:Response_Type>FULL</taxii_11:Response_Type>
 </taxii_11:Poll_Parameters>
</taxii_11:Poll_Request>
```

지원되는 요청 매개변수	설명
Poll_Request	
message_id	TAXII 사양에 따라 각 요청에 대해 임의로 생성된 문자열입니다. 모든 요청에 대해 고유한 문자열을 재생성합니다.
collection_name	전역 위협 알림 서비스에서 추출하거나 가져올 컬렉션의 이름입니다. 이 속성은 프로비저닝 프로세스가 완료된 후 Cisco에서 제공합니다.
result_id	폴링 응답에서 이 값을 붙여넣습니다.
result_part_number	폴링 응답의 값에서 1 높은 값을 이 값으로 만듭니다.
exclude_Begin_Timestamp	기간에 따라 이 값을 조정합니다.
Inclusive_End_Timestamp	기간에 따라 이 값을 조정합니다.
Poll_Parameters	
allow_async	이 특성은 항상 false로 설정합니다.

참고 **Exclusive_Begin_Timestamp**와 **Inclusive_End_Timestamp** 사이에 허용되는 최대 기간은 3일입니다. 기간이 더 길면 반환되는 결과는 **Inclusive_End_Timestamp** 이전 3일로 제한됩니다.

일반 쿼리

이 섹션에서는 추가 조사를 위해 결과의 우선 순위를 지정하는 데 도움이 되는, Cisco STIX/TAXII API에서 사용하는 몇 가지 일반적인 쿼리에 대해 설명합니다. 예제 쿼리에서 사용하는 구문은 SPLUNK

통합을 기반으로 하며, 상징적입니다. 구체적인 필드와 값은 로컬 통합에 따라 달라질 수 있지만, 쿼리의 의미는 SIEM 시스템 및 통합 전반에 광범위하게 적용됩니다.

팁 SPLUNK에서 다른 데이터를 수집한다면, 전역 위협 알림 데이터를 통해서만 검색될 수 있도록 호스트, 인덱스 또는 소스 이름을 쿼리 앞에 추가하십시오.

확인된 위협의 영향을 받는 사용자

이 쿼리는 확인된 위협이 있는 모든 사용자를 반환하며, 데스크톱 치료를 위해 인시던트 대응 팀에 보고될 수 있습니다. 인시던트의 위험성이 높다면 영향 받는 디바이스의 이미지 재설치를 고려해야 합니다. 이 쿼리는 영향을 받는 사용자 이름 및 캠페인 이름이 포함된 표를 생성합니다. 비어 있지 않은 캠페인 이름을 검색한 다음 사용자 이름+캠페인 쌍을 중복 제거합니다.

```
campaign!="" | table cUsername campaign | dedup cUsername campaign | sort + cUsername
```

또는 캠페인 이름에 다중 값 필드를 사용합니다.

```
campaign!="" | transaction cUsername | table cUsername campaign | sort + cUsername
```

특정 기간 내에 확인된 위협의 영향을 받는 사용자

이 쿼리에는 first-seen 및 last-seen 열도 포함됩니다. 비어 있지 않은 캠페인을 검색하고, 사용자 이름+캠페인 쌍으로 집계하고, 웹 플로우 타임스탬프의 최소값과 최대값을 계산합니다. 결과는 에포크-밀리초 단위로 표시되며 필요하다면 달력 시간으로 변환할 수 있습니다.

```
campaign!="" | stats min(timestamp) max(timestamp) by cUsername campaign
```

strftime 함수를 사용하여 에포크 변환을 포함할 수도 있습니다. 이 예에서는 타임스탬프를 1000으로 나눠 밀리초를 제거합니다.

```
campaign!="" | stats min(timestamp) as oldest max(timestamp) as newest by cUsername campaign
 |
  eval oldest_time=strftime(oldest/1000,"%m/%d/%y %H:%M:%S") |
  eval newest_time=strftime(newest/1000,"%m/%d/%y %H:%M:%S") |
  table cUsername, campaign, oldest_time, newest_time
```

높은 위험 및 높은 신뢰도 인시던트의 영향을 받는 사용자

이 쿼리는 확인된 캠페인 보유 여부에 관계없이 높은 위험 및 높은 신뢰도 사용자의 우선순위 목록 테이블을 생성합니다. 높은 위험, 높은 신뢰도 및 중복 사용자 이름을 검색합니다. 모든 인시던트의 위험과 신뢰도 수준이 모두 높으니, 영향 받는 디바이스의 이미지 재설치를 고려해야 합니다.

```
confidence="High" risk="High" | dedup cUsername | table cUsername campaign
```

캠페인의 영향을 받는 사용자

이 쿼리는 시간 경과에 따른 감염된 사용자 수를 캠페인별로 분류한 차트를 생성합니다. 비어 있지 않은 캠페인을 검색하여 1일 기간으로 비운 다음, 해당 빈에 있는 고유한 사용자 이름 수를 계산합니다.

```
campaign!="" | timechart dc(cUsername) span=1d by campaign
```

참고 SPLUNK에서는 시간 차트 바로 가기를 사용할 수 있습니다.

C&C(Command and Control) 서버

이 쿼리는 Confirmed(확인됨) 범주에 속하는 모든 탐지된 C&C(명령 및 제어) 서버의 목록을 생성합니다. 서버 IP 주소 및 캠페인을 표시하는 비어 있지 않은 캠페인을 검색한 다음 서버 IP 주소를 중복 제거합니다. 결과에는 C&C 통신을 유지하기 위해 감염된 디바이스에서 사용 중인 C&C IP 수신 주소가 나열됩니다. 각 C&C IP 주소와 관련된 위협 캠페인도 표시됩니다. 다른 시스템을 쿼리하여 추가 정보를 얻고, IOC(보안 침해 지표)를 제공하고, 감염된 엔드포인트에서 악성 프로세스 및 애플리케이션을 식별하는 데 사용할 수 있습니다.

```
campaign!="" | table sIP campaign | dedup sIP
```

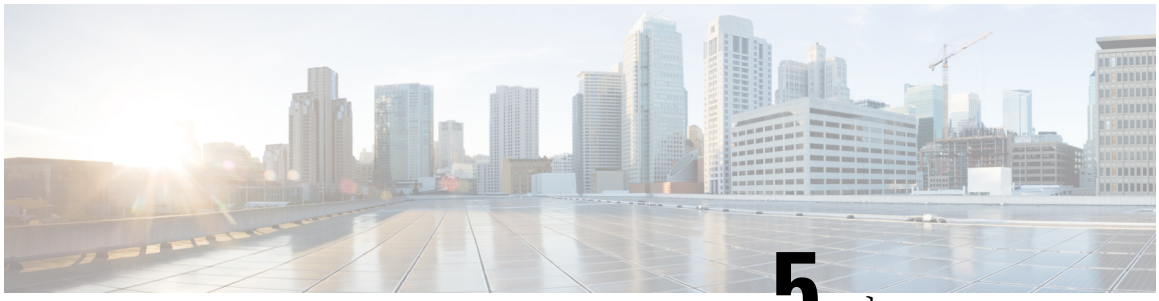
Cisco ISE와의 통합

Cisco ISE(71Introduction)는 네트워크 리소스에 대한 보안 액세스를 제공하는 보안 정책 관리 플랫폼입니다. Cisco ISE는 정책 결정 지점 역할을 하고, 기업이 규정을 준수하고, 인프라 보안을 개선하고, 서비스 작업을 효율화할 수 있도록 합니다. Cisco ISE를 사용하는 기업은 네트워크, 사용자 및 디바이스에서 실시간 상황별 정보를 수집할 수 있습니다. 그런 다음 이 정보를 사용하여 네트워크의 다양한 요소에 ID를 연결하여 사전 대응적 거버넌스 결정을 내릴 수 있습니다.

전역 위협 알림은 Cisco ISE와 통합되어 네트워크 수준의 격리를 제공합니다. 이 격리는 민감한 데이터가 더 이상 추출되지 감염된 디바이스를 않도록 네트워크에서 차단하는 기능을 제공합니다. 글로벌 위협 알림과 Cisco ISE의 통합은 STIX/TAXII를 사용합니다. 시스템이 감염의 원인을 개별 사용자에게 돌릴 수 있는 중요도가 높은 위험을 발견한 경우, Cisco ISE는 Cisco Rapid Threat Containment 프레임워크의 일부인 TC-NAC(Threat Centric Network Access Control) Quarantine을 제안하는 Requested Course of Action(요청된 조치)을 수신합니다. 감염과 관련된 위험에 따라, Requested Course of Action(요청된 조치)은 모니터링, 박멸, 내부 차단 또는 이러한 요소의 조합일 수 있습니다. 내부 차단은 TC-NAC의 차단 정책에서 사용하는 행동 방침입니다. 자세한 내용은 Cisco Rapid Threat Containment를 참고하십시오.

Cisco ISE와 전역 위협 알림 STIX/TAXII 서비스에서 제공하는 데이터 피드를 사용하여 고유한 솔루션을 개발할 수 있습니다. 데이터 피드에는 감염된 디바이스 및 수행할 작업을 식별하는 방법에 대한 정보가 포함되어 있습니다. 전역 위협 알림 STIX/TAXII 피드의 권장 사항을 기준으로 Cisco ISE에서 격리 정책을 정의할 수 있습니다. Cisco ISE에서 전역 위협 알림 어댑터를 구성하는 방법에 대한 자세한 내용은 Cisco ISE 관리자 가이드, 릴리스 2.2를 참조하십시오.

참고 전역 위협 알림은 웹 프록시 로그에 클라이언트 IP 또는 사용자 이름으로 나열되는 사용자 ID를 이용해 작동합니다. 특히 IP 주소의 경우 프록시 로그를 통해 사용 가능한 IP 주소가 내부 기업 네트워크에서 (다른 디바이스를 위한) 다른 IP 주소와 충돌하는 IP 주소일 수 있습니다. 예를 들어 인터넷에 바로 연결되는 스플릿 터널이 있는 AnyConnect를 통해 연결된 로밍 사용자는 집에서 로컬 IP 주소(예: 10.0.0.x 주소)를 얻게 되는데, 이 주소가 내부 기업 네트워크에서 사용하는 중복된 프라이빗 범위에 있는 IP 주소와 충동할 수 있습니다. Rapid Threat Containment(신속한 위협 억제) 정책을 정의할 때는 일치하지 않는 디바이스에 격리 작업이 적용되지 않게 하는 논리적 네트워크 아키텍처를 고려해야 합니다.



5 장

프록시 디바이스 업로드

프록시 디바이스 업로드

Cisco Secure Web Appliance(구 Web Security Appliance 또는 WSA)와 Blue Coat ProxySG 같은 프록시 디바이스의 로그 파일에 있는 텔레메트리 데이터를 분석을 위해 전역 위협 알림 시스템에 업로드합니다.

단계 **1** 페이지 오른쪽 상단에 있는 톱니바퀴 아이콘을 클릭하고 **Device Accounts(**디바이스 계정**)**를 선택하여 설정 마법사를 엽니다.

참고 기존 디바이스 계정이 이미 하나 이상 있다면 설정을 건너뛰고 Device Accounts(디바이스 계정) 페이지가 표시됩니다.

단계 **2** 설정 마법사를 시작하여 디바이스 계정을 추가할 준비가 되면 **Let's Get Started(**시작하기**)**를 클릭합니다.

단계 **3** 드롭다운에서 자동 또는 수동 업로드를 선택하여 텔레메트리 데이터를 디바이스에서 업로드하는 방법을 선택합니다. 전역 위협 알림 시스템은 한 번에 하나의 업로드 방법만 지원합니다. 업로드 방법을 결합할 수는 없습니다.

참고 자동 업로드에서 수동 업로드로 전환하려면 먼저 모든 프록시 디바이스를 자동 업로드 구성에서 제거해야 합니다.

단계 **4** 자동 업로드 방법을 선택했다면, 로그 파일을 전송하는 데 사용할 프로토콜로 **SCP** 또는 **HTTPS**를 선택합니다.

a) 이 디바이스의 이름을 입력하고 **Add Account(**계정 추가**)**를 클릭합니다.

b) SCP를 선택한 경우:

- 정보(호스트, 포트, 디렉터리, 사용자 이름)를 복사하여 Cisco WSA 컨피그레이션에 붙여넣습니다. 보안 유지를 위해 정보는 한 번만 표시됩니다.
- Cisco WSA를 구성하는 자세한 방법은 로그 파일을 Cisco 전역 위협 알림에 업로드하도록 Cisco Secure Web Appliance 구성을 참고하십시오.
- Cisco WSA Management Console에서 공개 SSH 키를 반환하면, 공개 SSH 키를 복사하여 디바이스 계정에 붙여넣습니다.

프록시 디바이스 업로드

- 마침을 클릭합니다.
- 원한다면 Device Accounts(디바이스 계정) 페이지로 이동하고 디바이스를 클릭하여 나중에 공개 SSH 키를 입력해도 됩니다.

c) HTTPS를 선택한 경우:

- 정보(호스트, 포트, 경로, 사용자 이름, 비밀번호)를 복사하여 Blue Coat ProxySG 컨피그레이션에 붙여넣습니다.
- Blue Coat ProxySG를 구성하는 자세한 방법은 로그 파일을 Cisco 전역 위협 알림에 업로드하도록 Blue Coat ProxySG 구성을 참고하십시오.
- 마침을 클릭합니다.

단계 **5** 수동 업로드 방법을 선택한 경우:

a) 로그 파일의 형식을 검증합니다. 다음 준비 지침을 따릅니다.

- Cisco WSA 및 Blue Coat 프록시에서 생성한 W3C 로그 파일이 지원됩니다.
- 모든 로그 파일은 GZip(*.gz) 형식으로 압축해야 합니다.
- 각 로그 파일은 1GB보다 작아야 합니다. 1GB보다 큰 로그 파일은 복수의 작은 파일로 분할해야 합니다. 개별 시간 간격이 중복되지 않으며 모든 파일에 동일한 올바른 헤더가 포함되어 있는지 확인합니다.
- 로그 파일이 적용되는 총 시간 간격은 2일을 초과해야 합니다.
- 각 로그 파일은 중복되지 않는 특정 시간 간격을 대상으로 해야 합니다.
- 각 로그 파일은 로그 항목을 시간 오름차순으로 포함해야 합니다. 즉 이전 항목이 새 항목 앞에 와야 합니다.
- 로그 파일은 알파벳순/숫자순으로 정렬하고 시간 순으로 업로드해야 합니다. 즉 이전 파일을 새 파일보다 먼저 업로드해야 합니다. 단일 업로드에서 업로드 구성 요소가 파일을 자동으로 정렬합니다. 여러 번 업로드한다면, 항상 최신 데이터를 업로드해야 합니다. 프록시 로그 파일에서 기본적으로 사용하는 명명 규칙이 유지된다면, 파일 이름이 이미 올바르게 정렬되었다는 뜻입니다.
- 이전에 업로드한 데이터보다 오래된 데이터는 처리되지 않습니다.
- 업로드할 수 있으려면 로그 파일의 콘텐츠가 특정 기준을 충족해야 합니다.
  - 업로드하기 전에 로그 파일을 확인할 수 있는 Log Validation Tool이 제공됩니다.
  - 로그 파일의 처음 20개 행을 복사하고 Log Validation Tool에 붙여넣어 오류를 확인합니다.
  - 모든 오류가 표시되며, 사용자가 오류를 수정하는 동안 툴이 자동으로 오류를 계속 확인합니다.

b) **Add files(**파일 추가**)**를 클릭하여 업로드할 로그 파일을 선택하거나 로그 파일을 업로드 상자에 끌어다 놓습니다.

참고 업로드 상자에 추가된 모든 파일을 지우려면 **Clear files(**파일 지우기**)**를 클릭합니다.

c) **Start upload(**업로드 시작**)**를 클릭하면 선택된 로그 파일이 분석을 위해 전역 위협 알림 시스템에 업로드됩니다. 전역 위협 알림 시스템에 결과가 표시될 때까지 기다립니다.

참고 데이터 삭제 위험을 최소화하기 위해 전역 위협 알림 시스템은 5시간이 지나야 업로드된 데이터 처리를 시작합니다. 따라서 처리를 시작하기 전에 모든 업로드를 완료하고 모든 요소가 올바른지 확인할 수 있습니다.

주의 수동에서 자동으로 전환하면 모든 업로드가 즉시 중단되고 업로드된 데이터의 처리가 중단됩니다. 업로드된 데이터가 모두 삭제됩니다.

참고 페이지를 닫거나 다른 페이지로 이동하면 현재 파일 업로드가 모두 중단됩니다.

참고 자동 업로드를 사용하려면 먼저 모든 수동 업로드를 중단해야 합니다. 모든 데이터가 처리되기 전에 전환하면 전환에서 일부 분석 데이터가 손실될 수 있습니다. 시스템에서 데이터를 삭제하지 않도록, 마지막 수동 업로드로부터 24시간이 지난 후에 전환을 수행하십시오.

다음에 수행할 작업

Device Accounts(디바이스 계정) 페이지에 프록시 디바이스와 관련 정보가 나열됩니다. Status(상태) 열에는 각 디바이스의 상태가 표시됩니다.

- New(신규) - SCP에 대한 컨피그레이션이 완료되지 않았습니다. 공개 SSH 키가 누락되었을 수 있습니다.
- Provisioning(프로비저닝) - 계정을 프로비저닝하는 중이며, 아직 준비되지 않았습니다.
- Ready(준비) - 계정이 생성되었습니다.
- Error(오류) - 상태 위에 커서를 올리면 오류를 설명하는 팝업 메시지가 표시됩니다.

이 개요 페이지에서는 다른 디바이스 계정을 추가하거나, 임의의 디바이스를 클릭하여 제거하거나, 공개 SSH 키를 입력하거나, 문제를 해결할 수 있습니다.

여러 디바이스 또는 업로드 프로세스 간에 계정을 공유할 수 있지만, 파일 이름 충돌 가능성을 최소화하고 업로드 문제 해결을 간소화할 수 있도록 각 디바이스에 별도의 계정을 사용하는 것이 좋습니다.

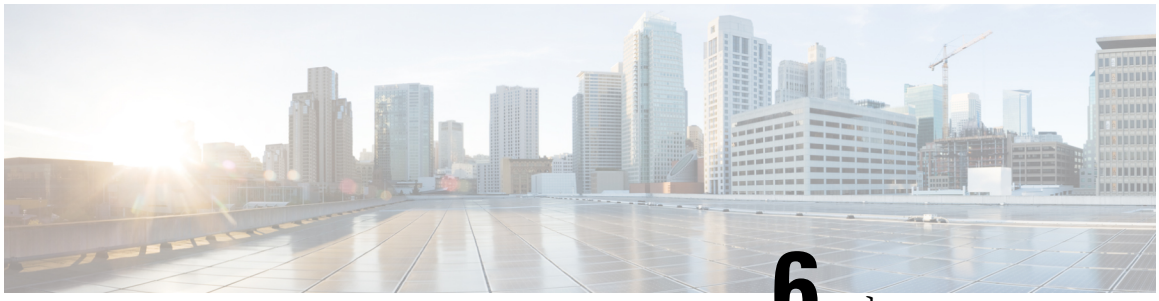
디바이스 계정이 준비되면 **Confirmed(**확인됨**)** 또는 **Detected(**탐지됨**)** 페이지를 클릭하여 네트워크 상의 의심스러운 활동에 관한 정보를 확인합니다.

참고 데이터는 일반적으로 프로비저닝이 완료된 후 2~3일 이내에 사용할 수 있습니다.

프록시 디바이스 업로드

부

릴리스 정보



6 장

2022년 8월

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

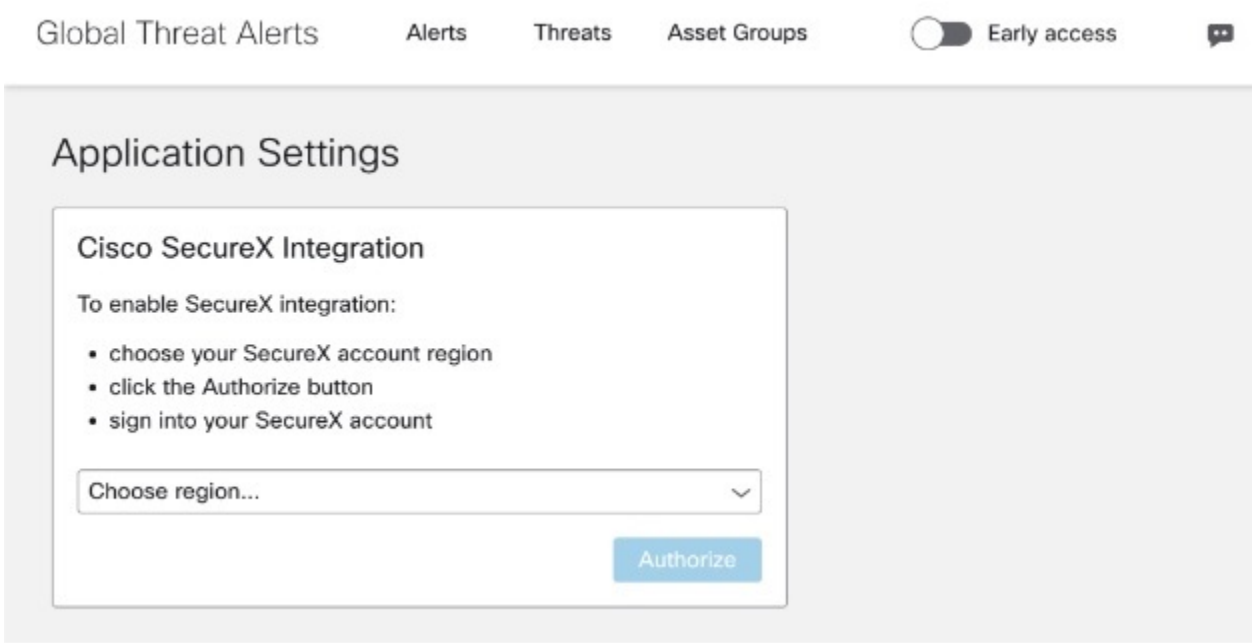
- 개선된 알림 워크플로, 37 페이지
- 추가 위협 탐지, 42 페이지

개선된 알림 워크플로

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

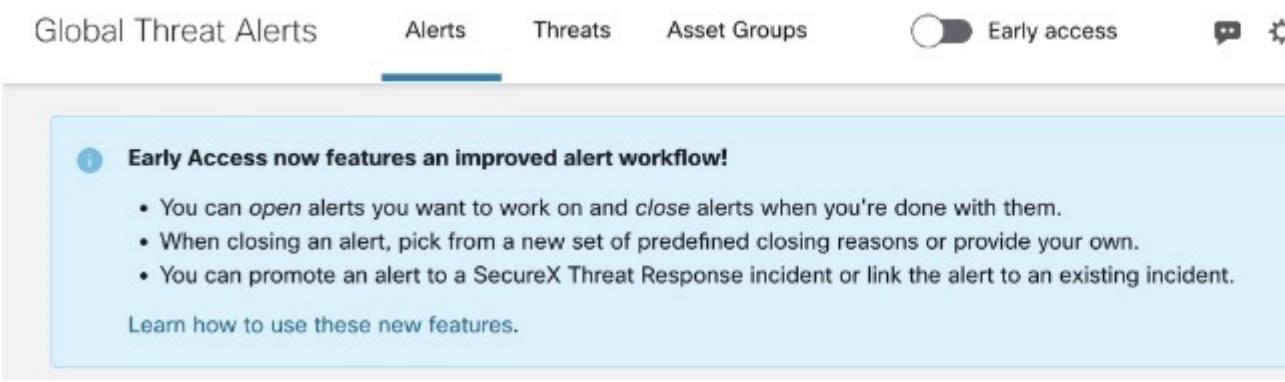
SecureX 인시던트 관리자와의 통합에 따른 이점을 활용하려면 전역 위협 알림 콘솔의 **Application Settings(**애플리케이션 설정**)**에서 SecureX 통합을 활성화해야 합니다.

그림 ***10:*** 애플리케이션 설정에서 ***SecureX*** 통합 승인



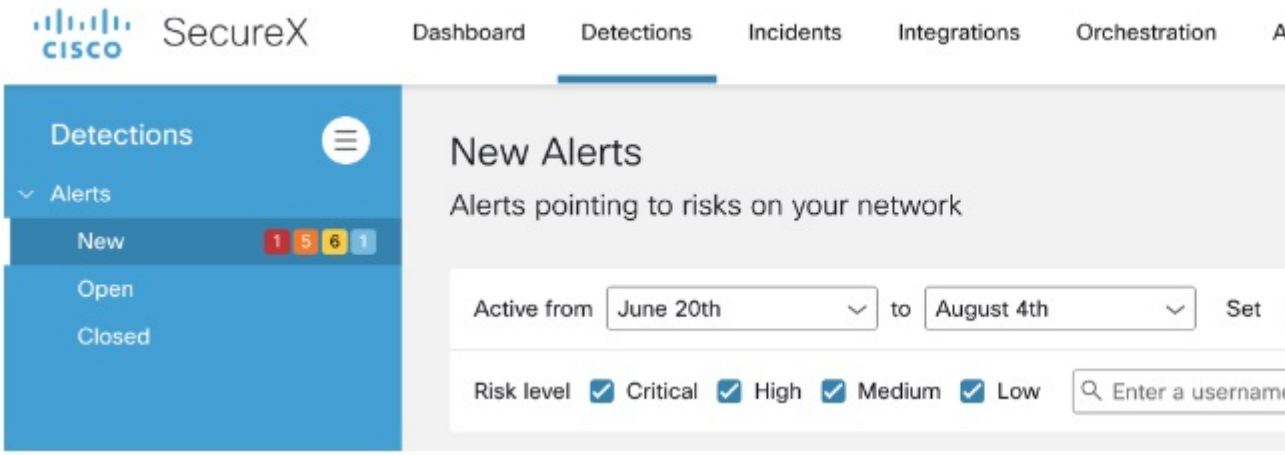
전역 위협 알림 콘솔의 헤더에서 **Early access(**얼리 액세스**)**를 클릭하여 활성화합니다.

그림 ***11:*** 새 기능을 활성화하기 위해 얼리 액세스로 전환



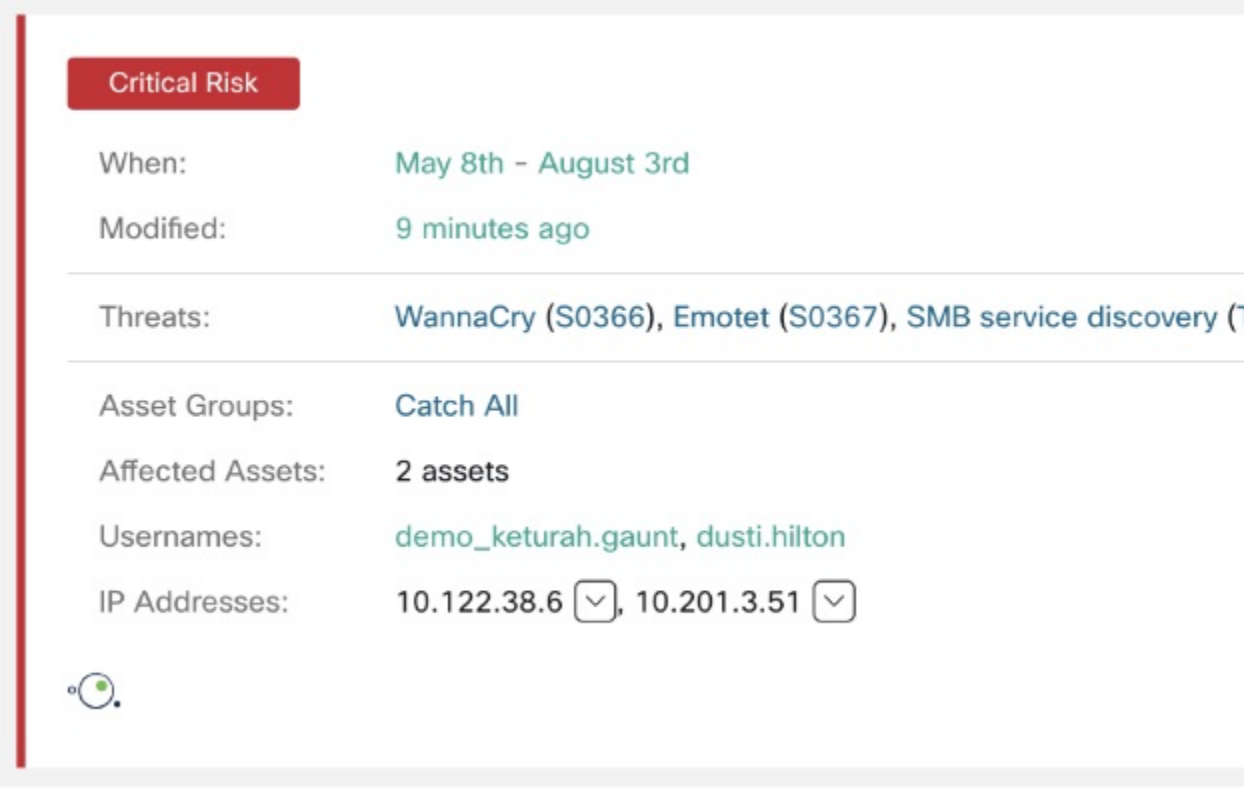
Early access(얼리 액세스**)**가 활성화되면 알림은 **New(**신규**)**, **Open(**열림**)** 또는 **Closed(**닫힘**)**로 분류됩니다.

그림 ***12:*** 신규, 열림 및 닫힘 상태 범주의 알림



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

그림 **13:** 알림 열기 또는 닫기

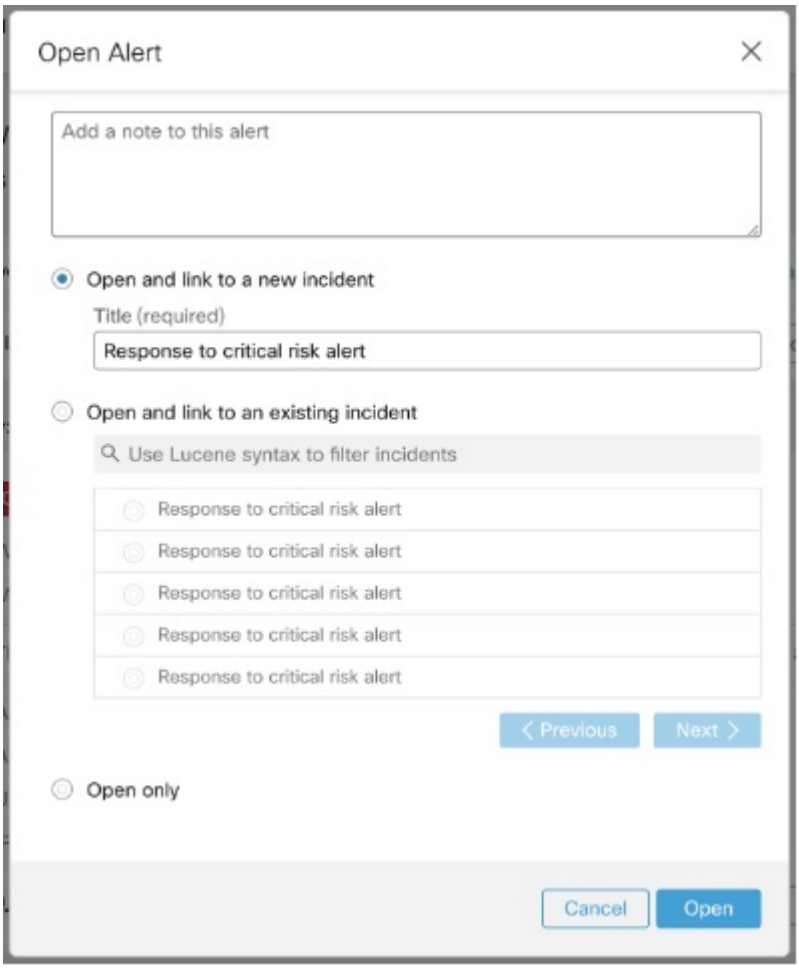


글로벌 위협 알림은 확장된 탐지 및 효율적인 알림 분류 같은 핵심 역량에 계속 집중하지만, 이제 클릭 한 번으로 탐지를 SecureX의 인시던트 대응 워크플로로 승격하는 SecureX 에코시스템을 이용해 더욱 긴밀하게 통합됩니다.

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 ***14:*** 인시던트에 연결 옵션을 이용해 알림 열기

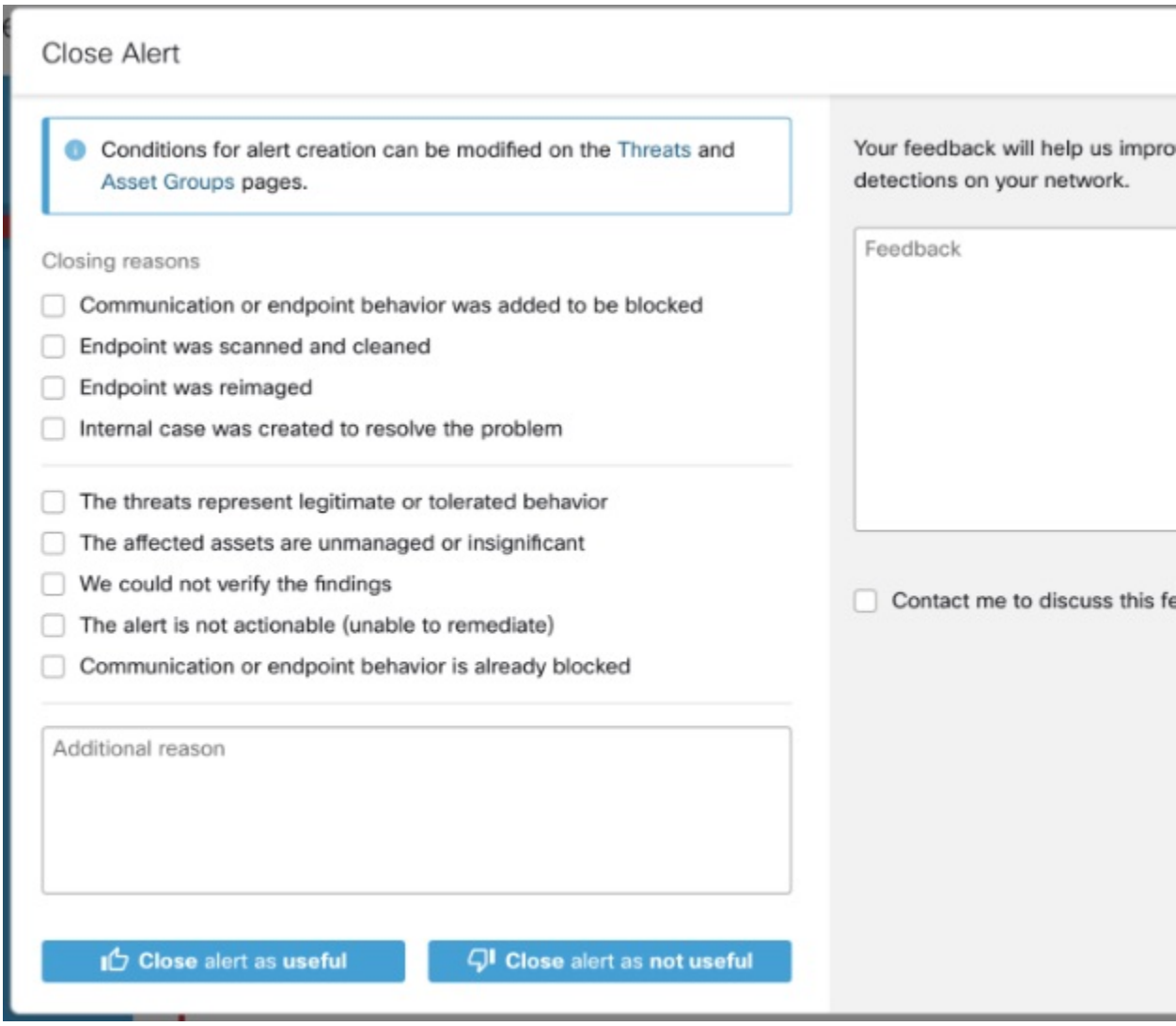


SecureX 인시던트 관리자에 있는 인시던트에는 **Summary(**요약**)** 및 원래 알림의 모든 보안 **Events(**이벤트**)**와 **Observables(**관찰 가능 항목**)**을 포함한 세부 정보가 포함됩니다. 조사, 강화 및 오케스트레이션 같은 SecureX 기능을 사용하여 추가로 조사하고 대응할 수 있습니다.

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.

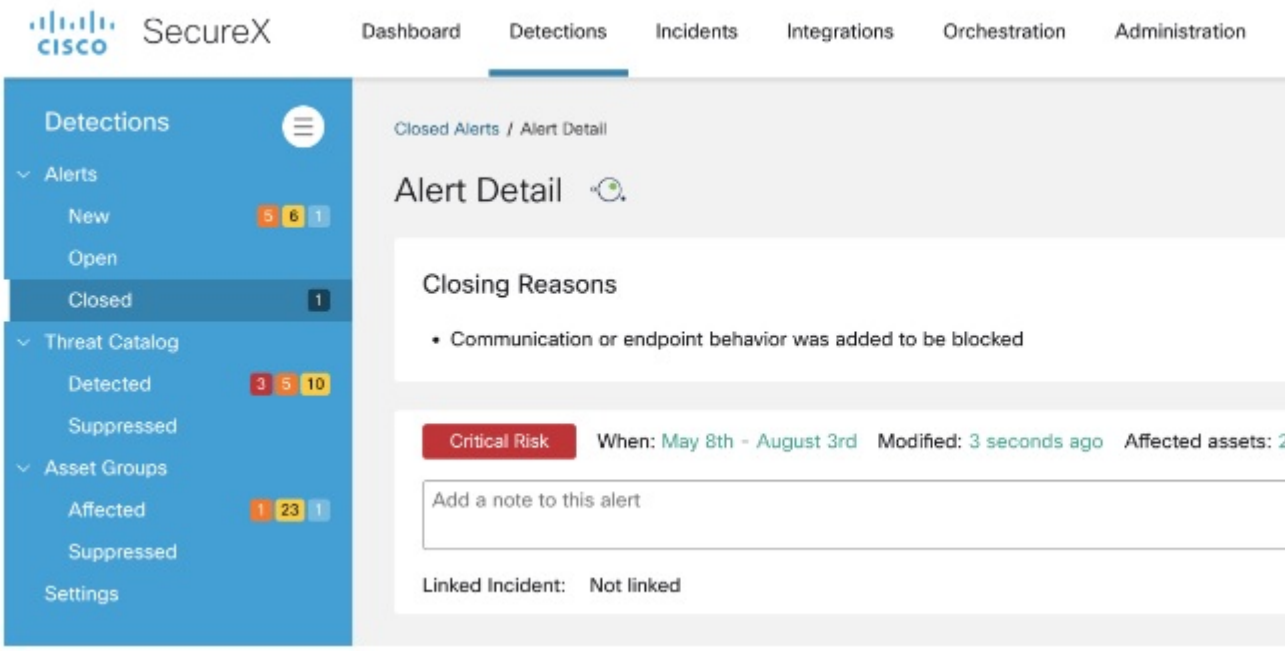
그림 ***15:*** 종료 사유를 선택하여 알림 종료



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 ***16: 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.

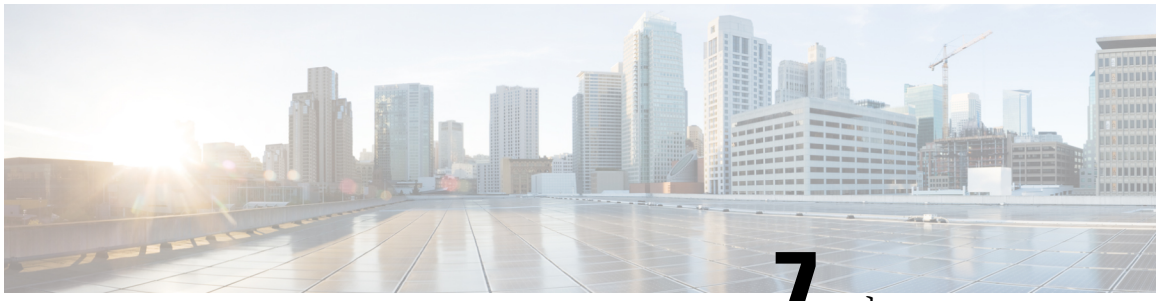
SocGholish

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 *17:*


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



7 장

2022년 7월

2022년 7월에 릴리스된, Cisco 클라우드 기반 머신 러닝 전역 위협 알림에 대한 업데이트:

- CCI로 마이그레이션된 SSO, 45 페이지
- 추가 위협 탐지, 45 페이지

CCI로 마이그레이션된 SSO

고객 경험을 개선하기 위해 SSO(Single Sign-On)가 CCI(Cisco Customer Identity) 포털로 마이그레이션되었습니다. **Cisco SSO**를 클릭하고 **id.cisco.com**에 이메일과 비밀번호를 입력하여 로그인합니다.

추가 위협 탐지

다음과 같은 새로운 위협 탐지가 포트폴리오에 추가되었습니다.

- Conti
- REvil

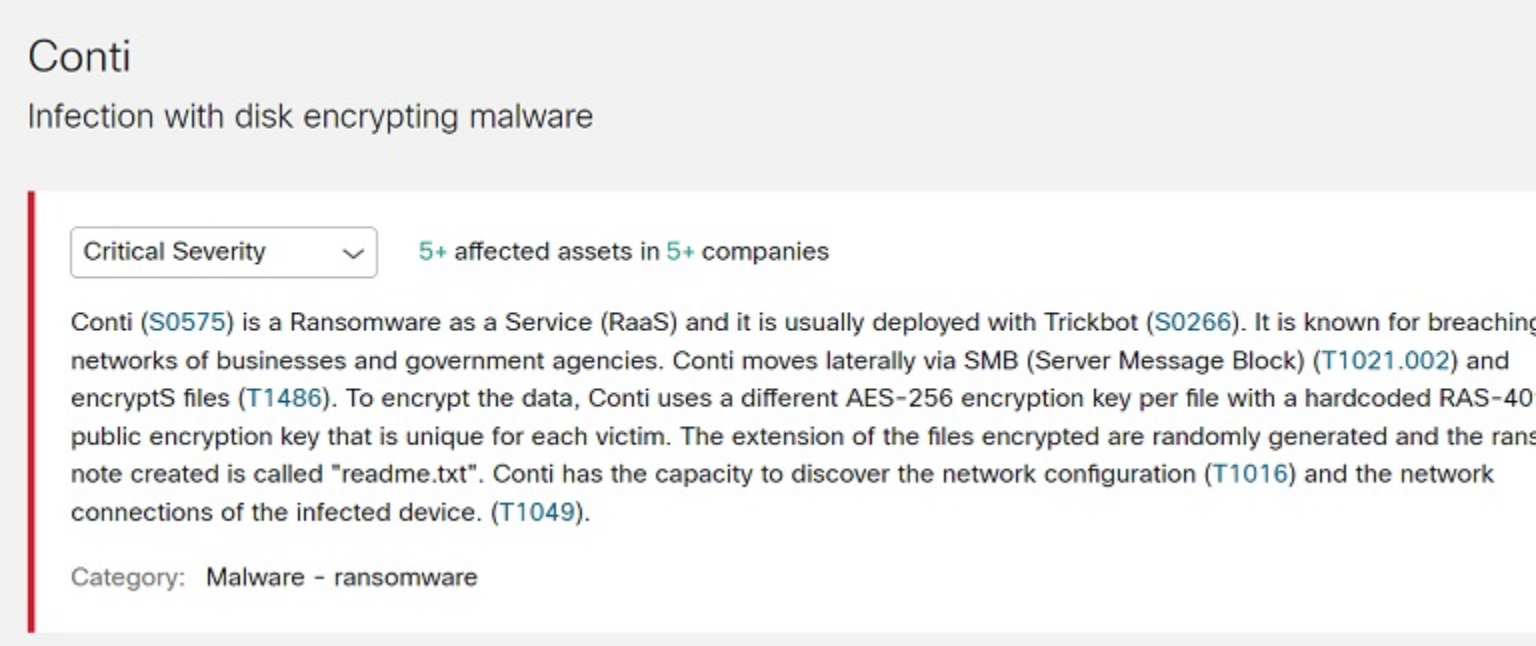
기존 위협 탐지 관련 지표도 업데이트했습니다.

Conti

Conti(S0575)는 대부분 Trickbot(S0266)을 이용해 구축되는 RaaS(Ransomware as a Service)입니다. 기업 및 정부 기관의 네트워크의 보안을 침해합니다. Conti는 SMB(Server Message Block)(T1021.002)를 이용해 수평으로 이동하고 파일을 암호화합니다(T1486). 데이터를 암호화하기 위해 Conti는 파일별로 서로 다른 AES-256 암호화 키를 사용하며, 피해자별로 고유한 하드코딩된 RAS-4096 공개 암호화 키를 사용합니다. 암호화된 파일의 확장자는 무작위로 생성되며, 생성된 몸값 요구 메시지의 이름은 "readme.txt"입니다. Conti는 감염된 디바이스(T1049)의 네트워크 컨피그레이션(T1016)과 네트워크 연결을 검색할 수 있습니다.

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

그림 ***18:***

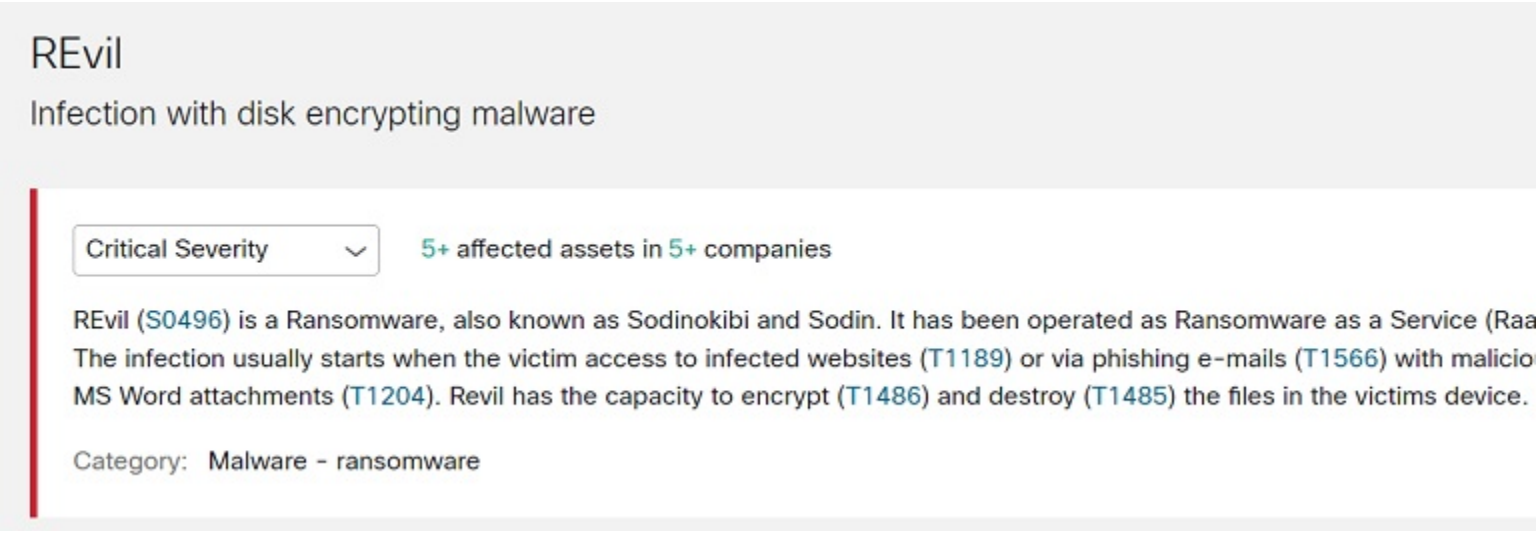


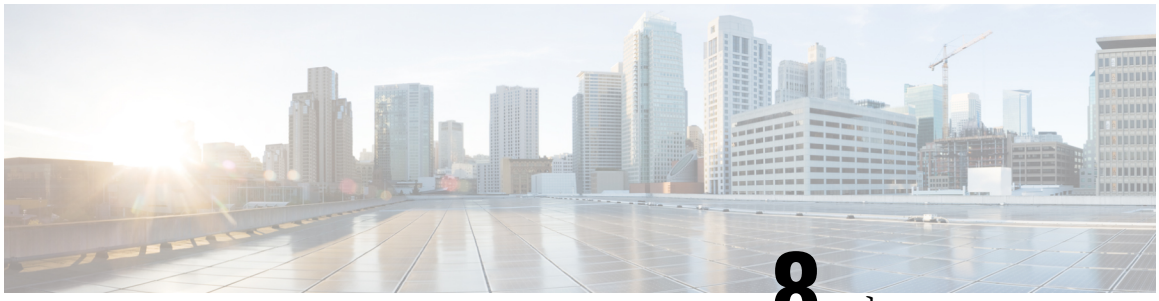
REvil

REvil(S0496)은 Sodinokib 및 Sodin이라고도 하는 RaaS(Ransomware as a Service)입니다. 감염은 주로 피해자가 감염된 웹사이트(T1189) 또는 악성 MS Word 첨부 파일(T1204)이 있는는 피싱 이메일(T1566)에 액세스할 때 시작됩니다. REvil은 피해자 디바이스에서 파일을 암호화(T1486)하고 파기(T1485)할 수 있습니다.

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

그림 ***19:***





8 장

2022년 6월

2022년 6월에 릴리스된, Cisco 클라우드 기반 머신 러닝 전역 위협 알림에 대한 업데이트:

• 추가 위협 탐지, 47 페이지

추가 위협 탐지

다음과 같은 새로운 위협 탐지가 포트폴리오에 추가되었습니다.

- AutoKMS HackTool
- Raspberry Robin
- UNC2447 활동

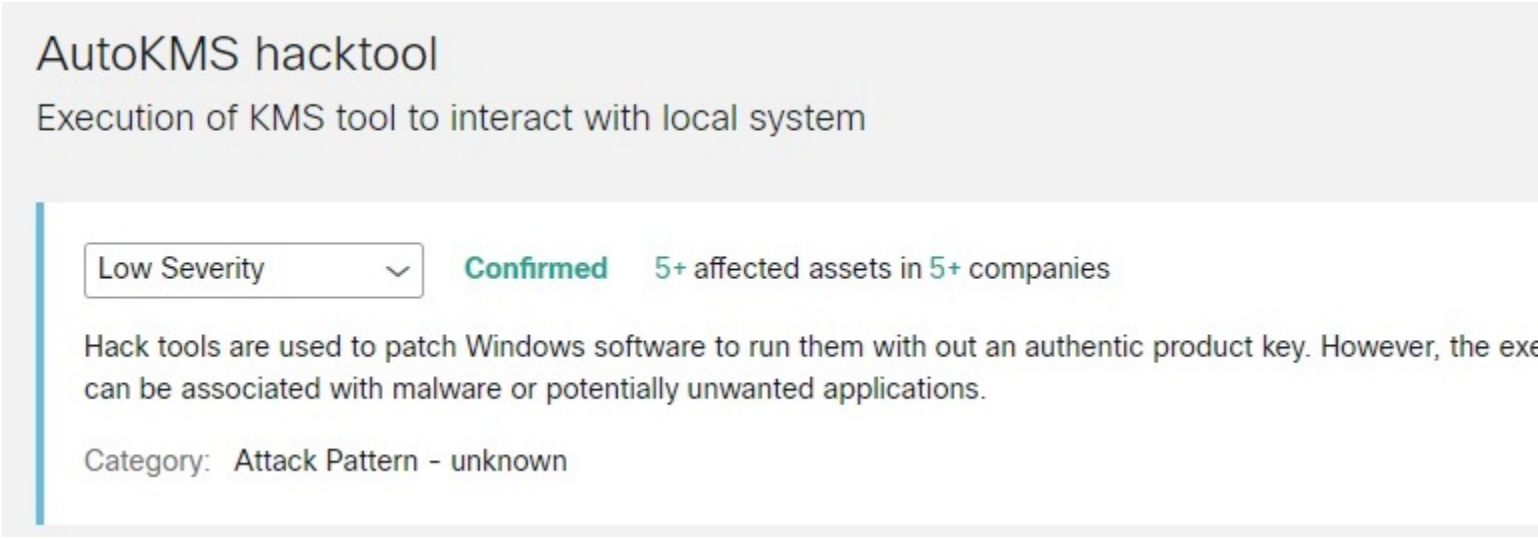
기존 위협 탐지 관련 지표도 업데이트했습니다.

AutoKMS HackTool

해킹 툴은 Windows 소프트웨어를 패치하여 정품 제품 키 없이 실행하는 용도로 사용됩니다. 그러나 이 툴의 실행은 악성코드 또는 원치 않는 애플리케이션과 관련이 있을 수 있습니다.

사용자 환경에서 AutoKMS HackTool이 탐지되었는지 확인하려면 AutoKMS HackTool Threat Detail(AutoKMS HackTool 위협 세부 정보)을 클릭하여 전역 위협 알림에서 관련 세부 정보를 확인하십시오.

그림 ***20:***

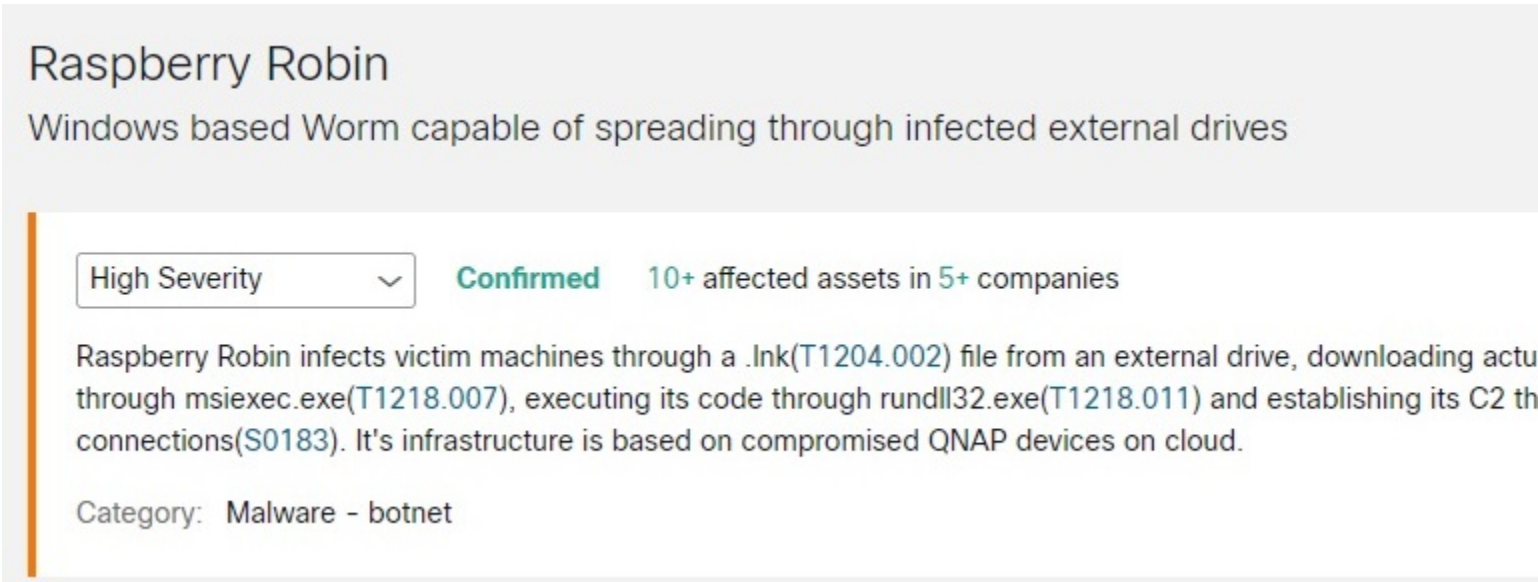


Raspberry Robin

Raspberry Robin은 외부 드라이브에서 .lnk(T1204.002) 파일을 통해 시스템을 감염시키고, msiexec.exe(T1218.007)를 통해 실제 페이로드를 다운로드하고, rundll32.exe(T1218.011)를 통해 코드를 실행하고, TOR 연결(S0183)을 통해 C2를 구성합니다. 인프라는 보안이 침해된 QNAP 디바이스를 기반으로 합니다

사용자 환경에서 Raspberry Robin이 탐지되었는지 확인하려면 Raspberry Robin Threat Detail(Raspberry Robin 위협 세부 정보)을 클릭하여 전역 위협 알림에서 관련 세부 정보를 확인하십시오.

그림 ***21:***

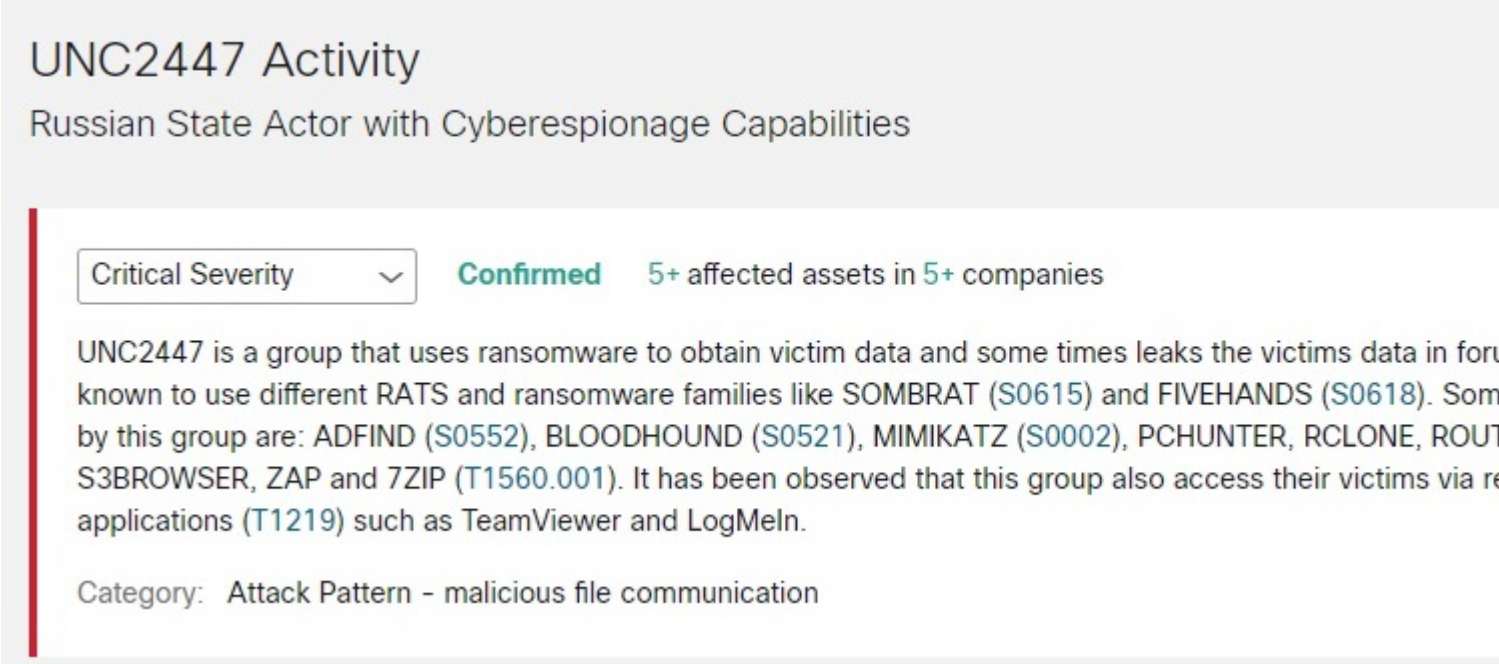


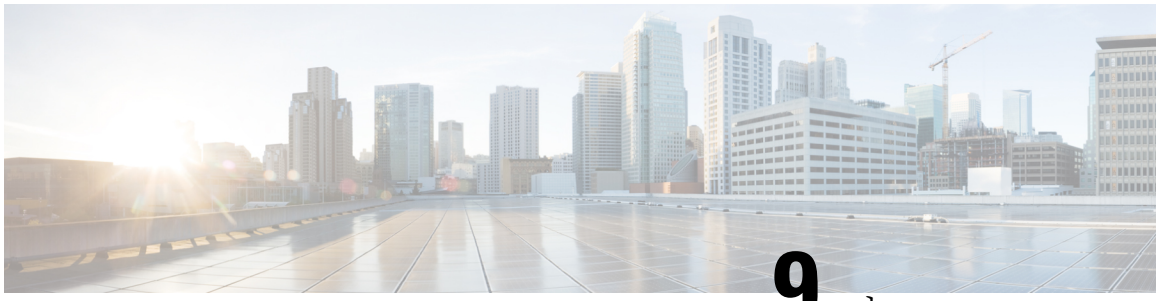
UNC2447 활동

UNC2447은 랜섬웨어를 사용하여 데이터를 가져오는 그룹으로, 피해자의 데이터를 포럼에 유출합니다. 이 그룹은 SOMBRAT(S0615)과 FIVEHANDS(S0618) 같은 다양한 RATS 및 랜섬웨어 제품군을 사용하는 것으로 알려져 있습니다. 이 그룹에서 사용하는 대표적인 툴은 ADFIND(S0552), BLOODHOUND(S0521), MIMIKATZ(S0002), PCHUNTER, RCLONE, ROUTERSCAN, S3BROWSER, ZAP, 7ZIP(T1560.001)입니다. 이 그룹은 TeamViewer나 LogMeIn 같은 원격 액세스 애플리케이션(T1219)도 사용합니다.

사용자 환경에서 UNC2447 활동이 탐지되었는지 확인하려면 UNC2447 Activity Threat Detail(UNC2447 활동 위협 세부 정보)을 클릭하여 전역 위협 알림에서 관련 세부 정보를 확인하십시오.

그림 ***22:***





9 장

2022년 5월

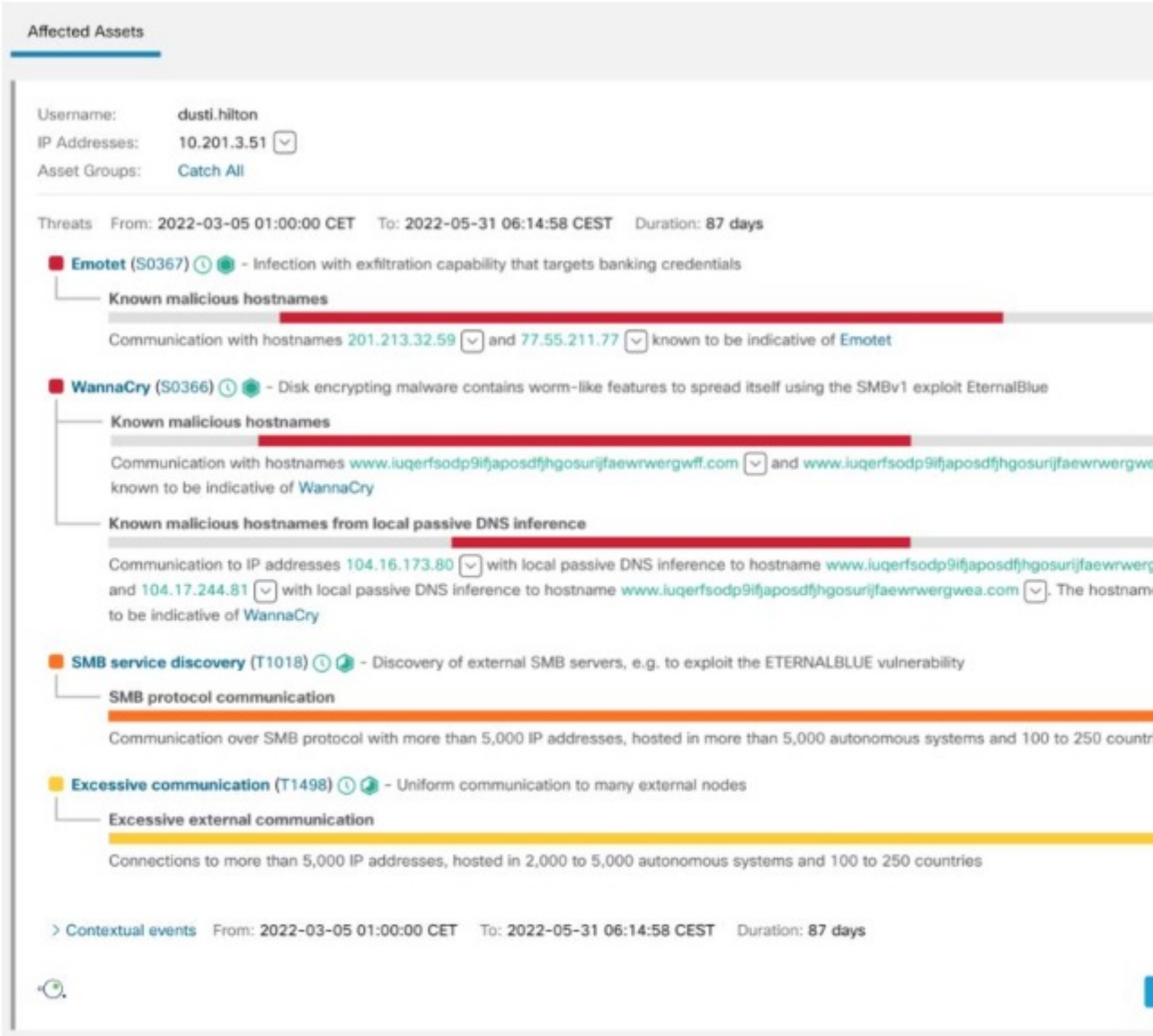
2022년 5월에 릴리스된, Cisco 클라우드 기반 머신 러닝 전역 위협 알림에 대한 업데이트:

• 향상된 알림 세부 정보 보기, 51 페이지

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 ***23:***



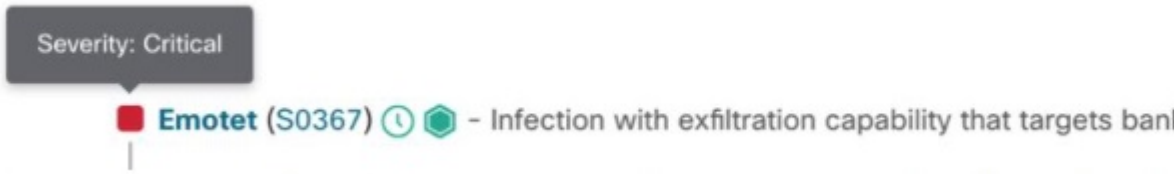
Threats(위협) 섹션의 상단에는 특정 자산에서 탐지된 모든 위협 및 해당 보안 이벤트의 총 관찰 기간이 표시됩니다.

그림 ***24:***

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

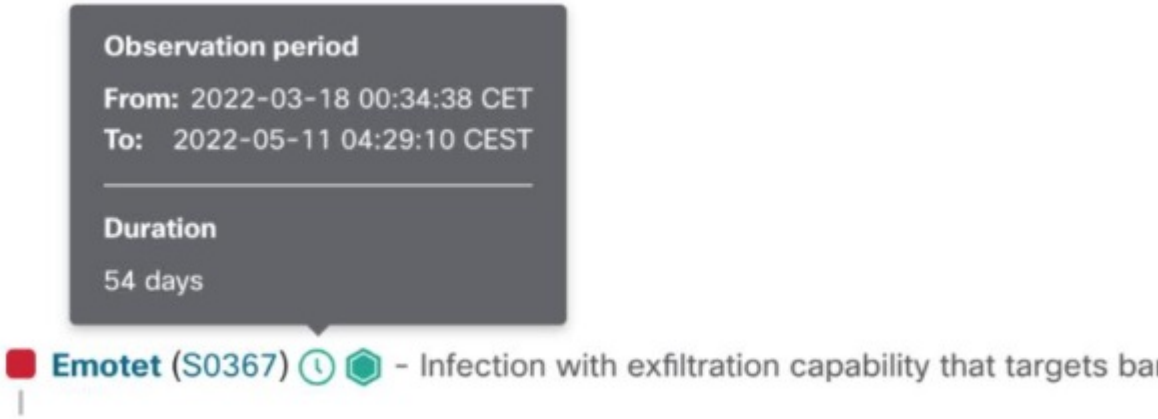
- 심각도

그림 ***25:***



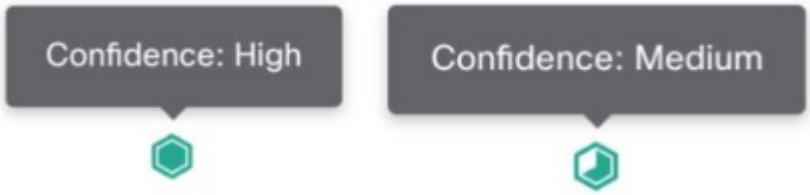
- 관찰 기간

그림 ***26:***



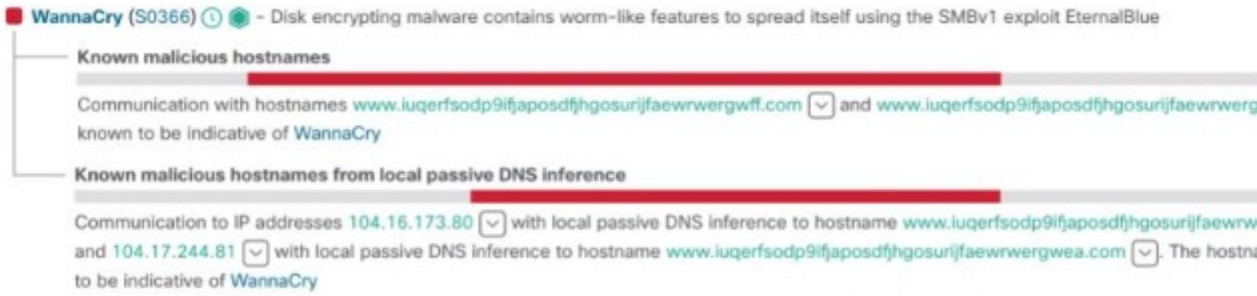
- 신뢰

그림 ***27:***



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

그림 ***28:***

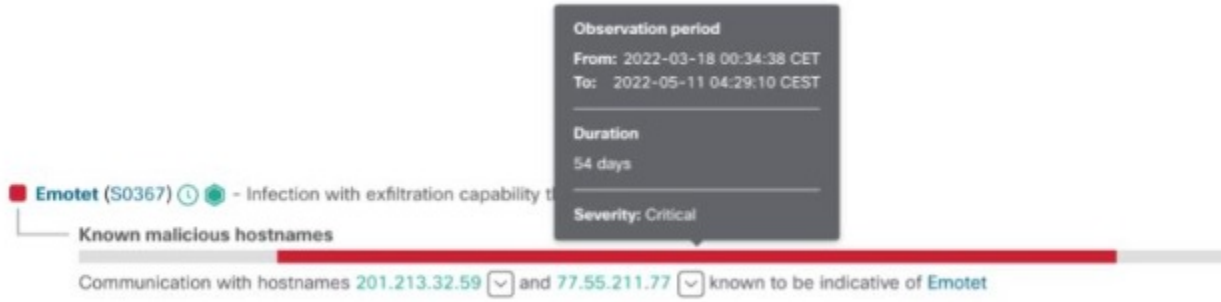


이벤트 주석에는 다른 Cisco Security 제품으로 전환하고 관찰 가능 항목에 대한 추가 정보 및 인텔리전스를 가져올 수 있는 드롭다운 메뉴가 포함되기도 합니다.

그림 ***29:***

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

그림 ***30:***



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

그림 ***31:***

10 장

2022년 4월

2022년 4월에 릴리스된, Cisco 클라우드 기반 머신 러닝 전역 위협 알림에 대한 업데이트:

• MITRE ATT&CK®와의 정렬, 57 페이지

MITRE ATT&CK®와의 정렬

전역 위협 알림의 위협 정보 레코드가 MITRE ATT&CK® 프레임워크에 맞게 조정되었습니다.

- 해당하는 경우 ATT&CK 프레임워크에서 제공하는 명명 규칙을 바로 사용합니다.
- 전역 위협 알림 위협 정보는 관련 ATT&CK Tactics(전술), Techniques(기술) 및 Software(소프트웨어) 항목에 대한 참조를 제공합니다.

그림 *32:*

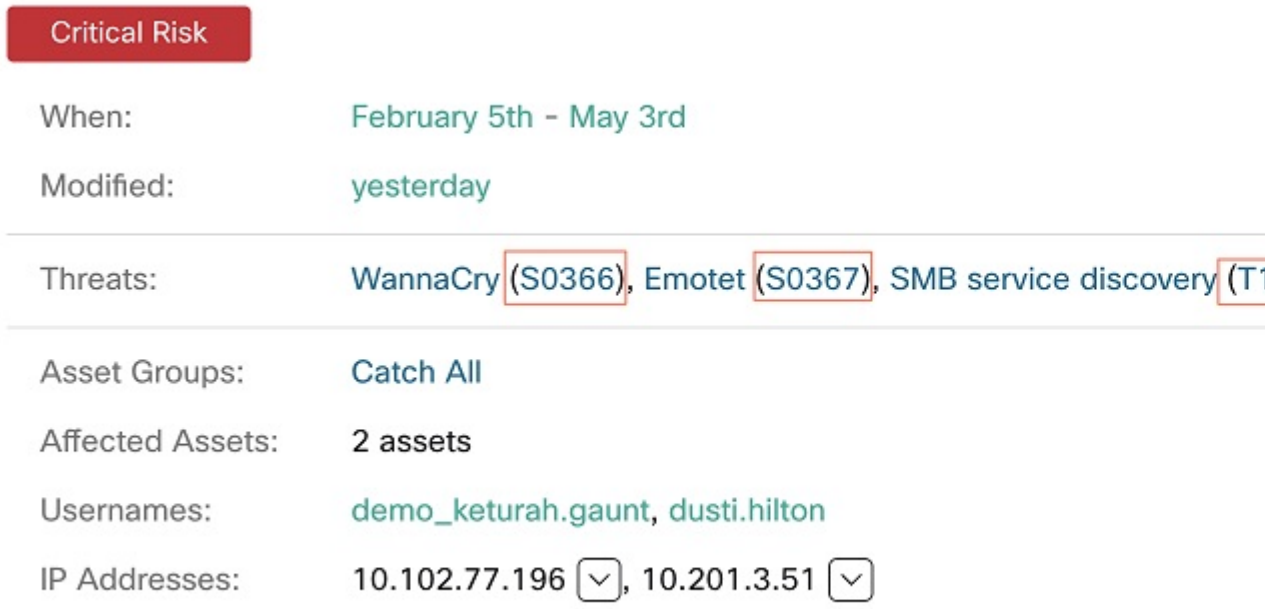
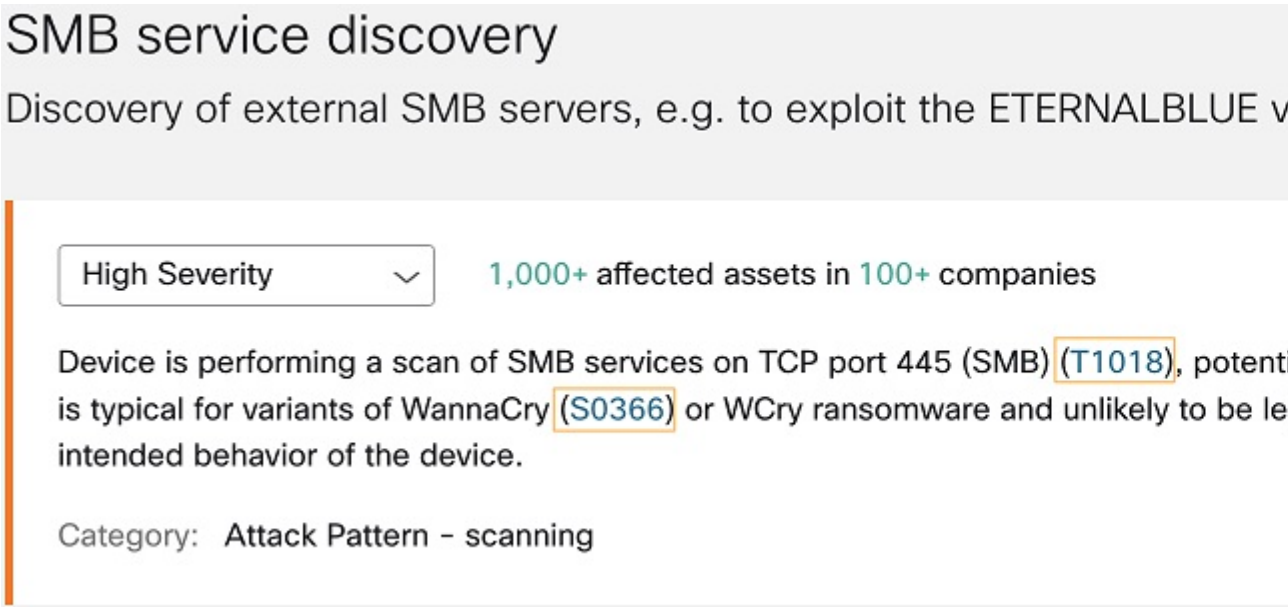


그림 *33:*



이러한 개선 사항 덕분에 인시던트 대응을 위한 기존 표준 운영 절차와의 프로세스 통합이 더 쉬워지고 새로운 분석가의 학습 곡선이 단축됩니다.

11 장

2022년 3월

2022년 3월에 릴리스된, Cisco 클라우드 기반 머신 러닝 전역 위협 알림에 대한 업데이트:

• 추가 위협 탐지, 59 페이지

추가 위협 탐지

다음과 같은 새로운 위협 탐지가 포트폴리오에 추가되었습니다.

- Cyclops Blink
- FormBook
- Gamaredon
- MuddyWater

또한 다양한 저위험 위협 탐지가 강화되었습니다.

Cyclops Blink

Cyclops Blink는 소규모 사무실/홈 오피스 네트워크 디바이스를 노리는 악성 Linux ELF 실행 파일입니다. 4가지 내장 모듈이 있어 파일을 업로드 및 다운로드하고, 시스템 정보를 검색하고(T1082), 악성 코드 버전을 업데이트할 수 있습니다. C2 명령을 사용하여 추가 모듈을 설치할 수 있습니다. 펌웨어 업데이트 프로세스(T1542.001)를 통해 지속성을 유지하고, 다운로드한 파일을 Linux API 호출(T1059.004)을 통해 실행합니다. 각 샘플에는 IP 주소 및 포트 번호 목록이 포함되어 있습니다(T1571). 실행하면 이러한 IP 주소 및 포트를 통해 C2 통신을 활성화하도록 시스템 방화벽(T1562.004)을 수정합니다.

사용자 환경에서 Cyclops Blink가 탐지되었는지 확인하려면 Cyclops Blink Threat Detail(Cyclops Blink 위협 세부 정보)을 클릭하여 전역 위협 알림에서 관련 세부 정보를 확인하십시오.

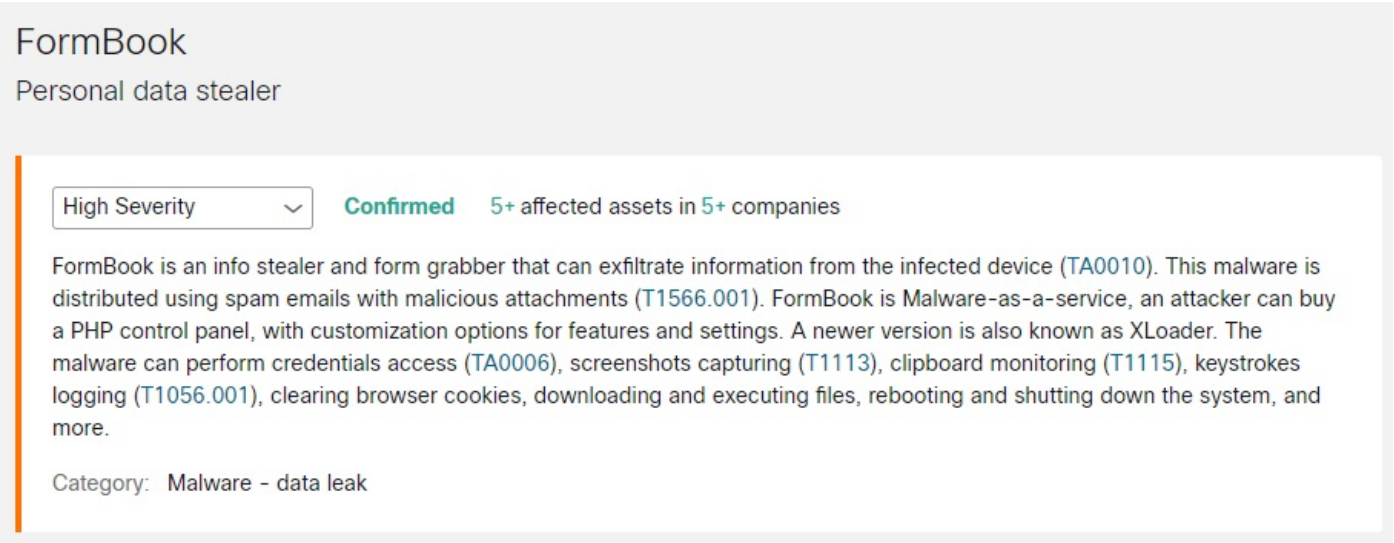
그림 ***34:***

FormBook

FormBook은 감염된 디바이스(TA0010)에서 정보를 추출할 수 있는, 정보를 훔치고 폼을 강탈하는 악성코드입니다. 이 악성코드는 악성 첨부 파일이 포함된 스팸 이메일을 사용하여 배포됩니다(T1566.001). FormBook은 MaaS(malware-as-a-service)이며, 공격자는 기능 및 설정에 대한 맞춤 설정 옵션을 제공하는 PHP 제어판을 구매할 수 있습니다. 최신 버전은 XLoader라고도 합니다. 이 악성코드는 자격 증명에 액세스하고(TA0006), 스크린샷을 캡처하고(T1113), 클립보드를 모니터링하고(T1115), 키 입력을 로깅하고(T1056.001), 브라우저 쿠키를 지우고, 파일을 다운로드 및 실행하고, 시스템을 재부팅 및 종료하는 등의 작업을 수행할 수 있습니다.

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

그림 ***35:***



Gamaredon

Primitive Bear라고도 하는 Gamaredon은 사이버 스파이 활동을 위해 주로 정부 조직을 노리는 국가 주도형 공격자입니다. 러시아와 우크라이나 간의 긴장이 고조된 후 그룹 활동이 증가했습니다. Gamaredon은 공격의 첫 번째 단계인 스피어피싱(T1566.001)을 통해 배포되는 악의적인 Office 파일(T1204.002)을 주로 활용합니다. PowerPunch라고 하는 Powershell(T1059.001) 비컨을 사용하여 후속 단계에서 악성코드를 다운로드하고 실행합니다(T1204.002). Pterodo(S0147)와 QuietSieve는 이 악성코드가 정보 도용(TA0010) 및 기타 다양한 작업을 위해 자주 구축하는 악성코드 제품군입니다.

사용자 환경에서 Gamaredon 활동이 탐지되었는지 확인하려면 Gamaredon Activity Threat Detail(Gamaredon 활동 위협 세부 정보)을 클릭하여 전역 위협 알림에서 관련 세부 정보를 확인하십시오.

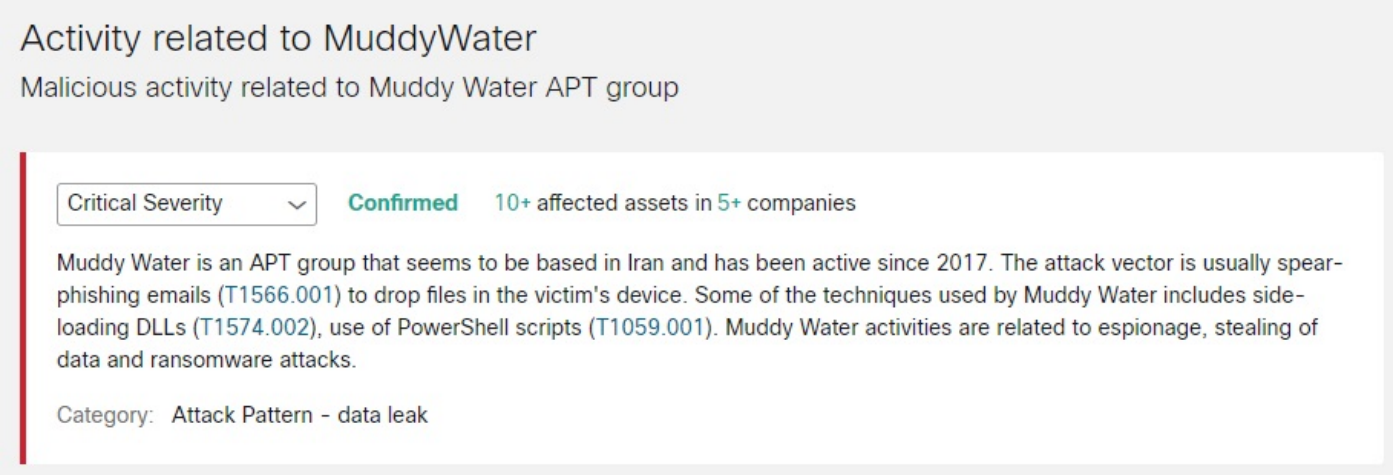
그림 ***36:***

MuddyWater

Muddywater는 이란에서 활동하는 것으로 추정되는 APT(Advanced Persistent Threat) 그룹으로, 2017년부터 활발하게 활동하고 있습니다. 일반적인 공격 벡터는 피해자의 디바이스에 파일을 드롭하는 스피어 피싱 이메일(T1566.001)입니다. Muddywater에서 사용하는 대표적인 기술은 사이드 로딩 DLL(T1574.002)과 PowerShell 스크립트 사용(T1059.001)입니다. Muddywater 활동은 스파이 활동, 데이터 도용 및 랜섬웨어 공격과 관련이 있습니다.

사용자 환경에서 Muddywater 활동이 탐지되었는지 확인하려면 Muddywater Activity Threat Detail(Muddywater 활동 위협 세부 정보)을 클릭하여 전역 위협 알림에서 관련 세부 정보를 확인하십시오.

그림 ***37:***


Activity related to MuddyWater
Malicious activity related to Muddy Water APT group
Critical Severity
Confirmed
10+ affected assets in 5+ companies
Muddy Water is an APT group that seems to be based in Iran and has been active since 2017. The attack vector is usually spear-phishing emails (T1566.001) to drop files in the victim's device. Some of the techniques used by Muddy Water includes side-loading DLLs (T1574.002), use of PowerShell scripts (T1059.001). Muddy Water activities are related to espionage, stealing of data and ransomware attacks.
Category: Attack Pattern - data leak

12 장

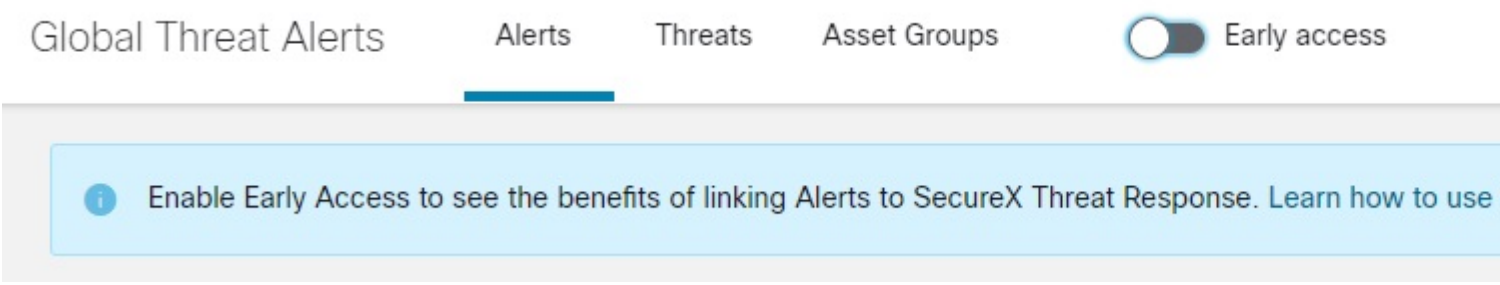
2022년 1월

2022년 1월에 릴리스된, Cisco 클라우드 기반 머신 러닝 전역 위협 알림에 대한 업데이트:

SecureX 인시던트 관리자로 알림 승격

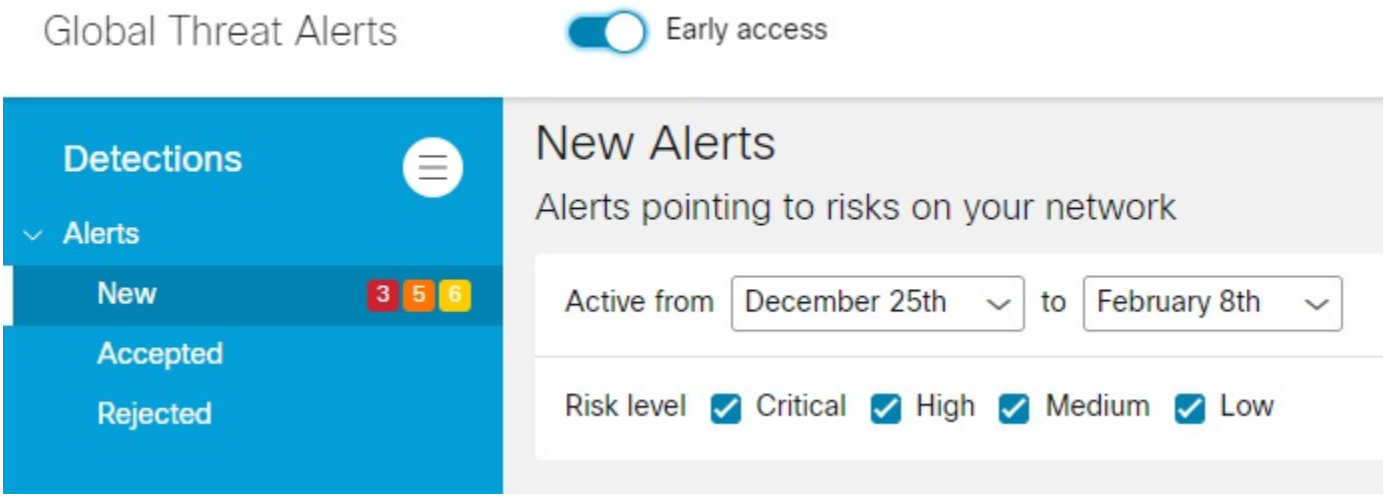
전역 위협 알림의 알림을 SecureX 인시던트 관리자로 승격하는 기능을 추가했습니다. 이 기능을 켜려면 전역 위협 알림 콘솔의 헤더에서 **Early Access(**얼리 액세스**)**를 활성화해야 합니다.

그림 ***38:*** 이 새 기능을 활성화하려면 ***Early Access(***얼리 액세스***)***를 클릭해야 합니다.



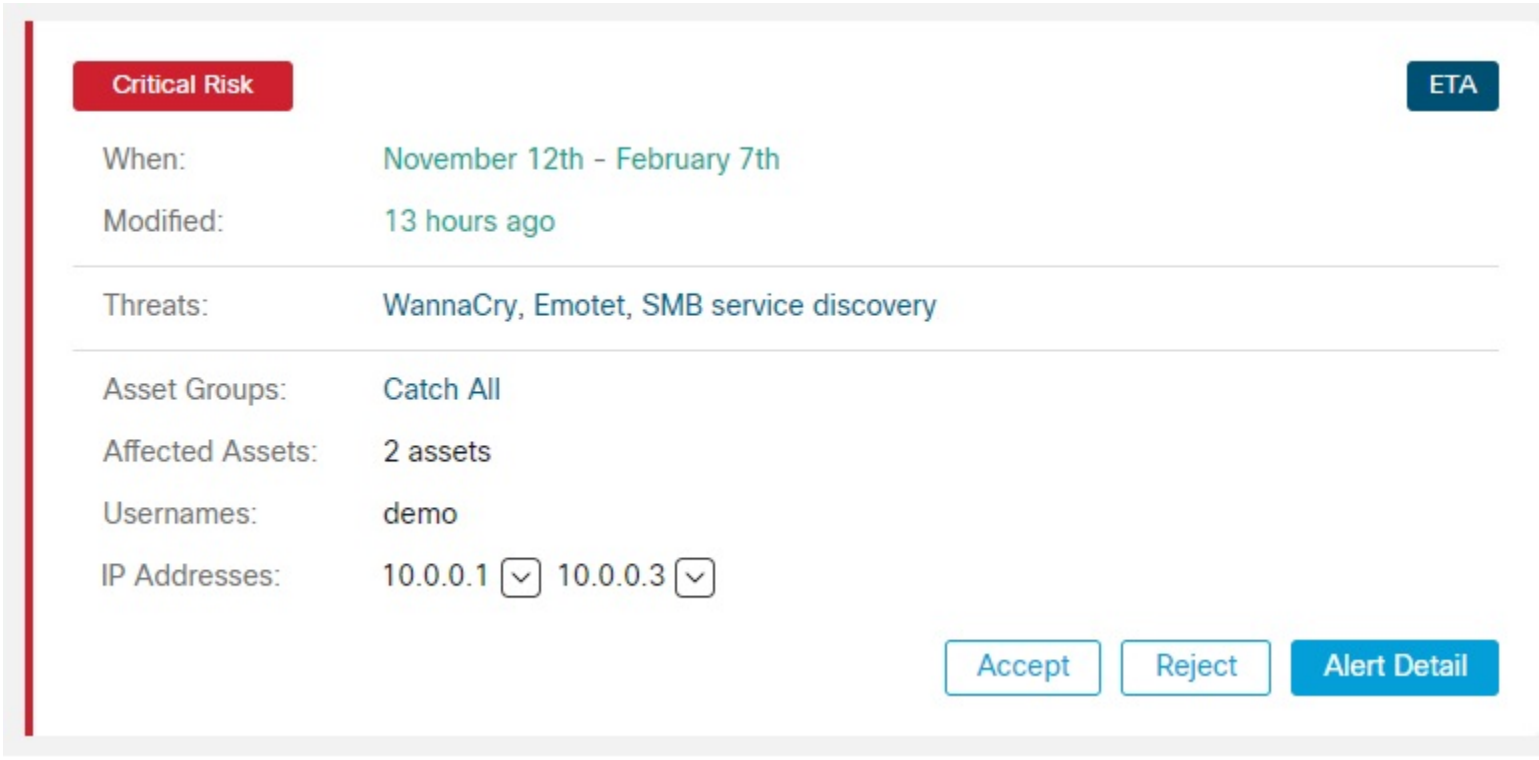
활성화되면 SecureX 인시던트 관리자가 전역 위협 알림의 기존 워크플로우를 대체합니다. 알림은 **New(**신규**)**, **Accepted(**수락됨**)** 또는 **Rejected(**거부됨**)**로 분류됩니다.

그림 *39: SecureX* 인시던트 관리자 내의 알림



Accept(수락**)** 또는 **Reject(**거부**)** 버튼을 사용하여 새 알림을 두 가지 상태 중 하나로 전환할 수 있습니다.

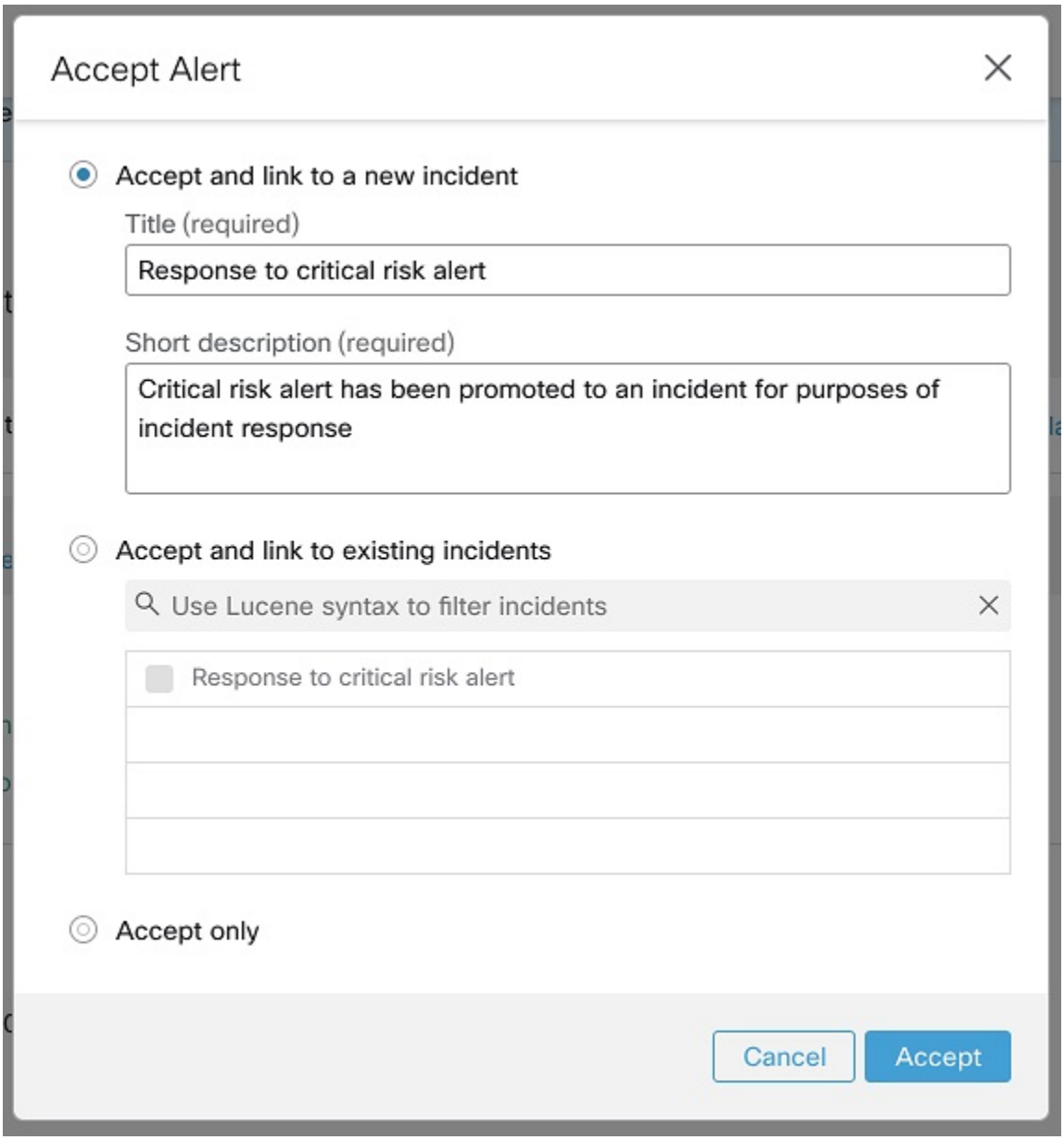
그림 *40:* 알림 수락 또는 거부



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

수락한 알림은 SecureX 인시던트 관리자에서 기존 또는 새 인시던트에 연결할 수 있습니다.

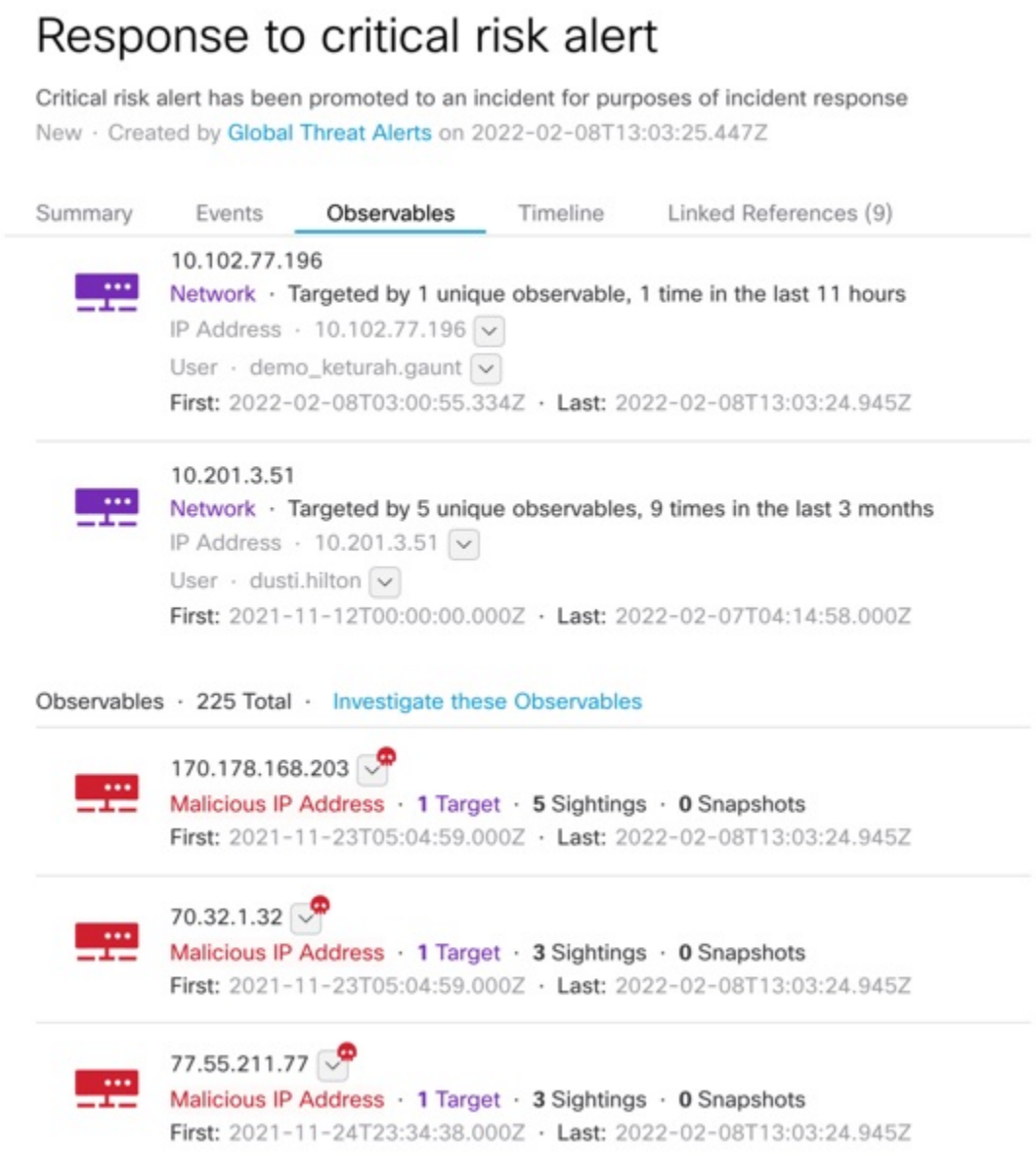
그림 *41:* 인시던트에 연결 옵션을 이용해 알림 수락



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.

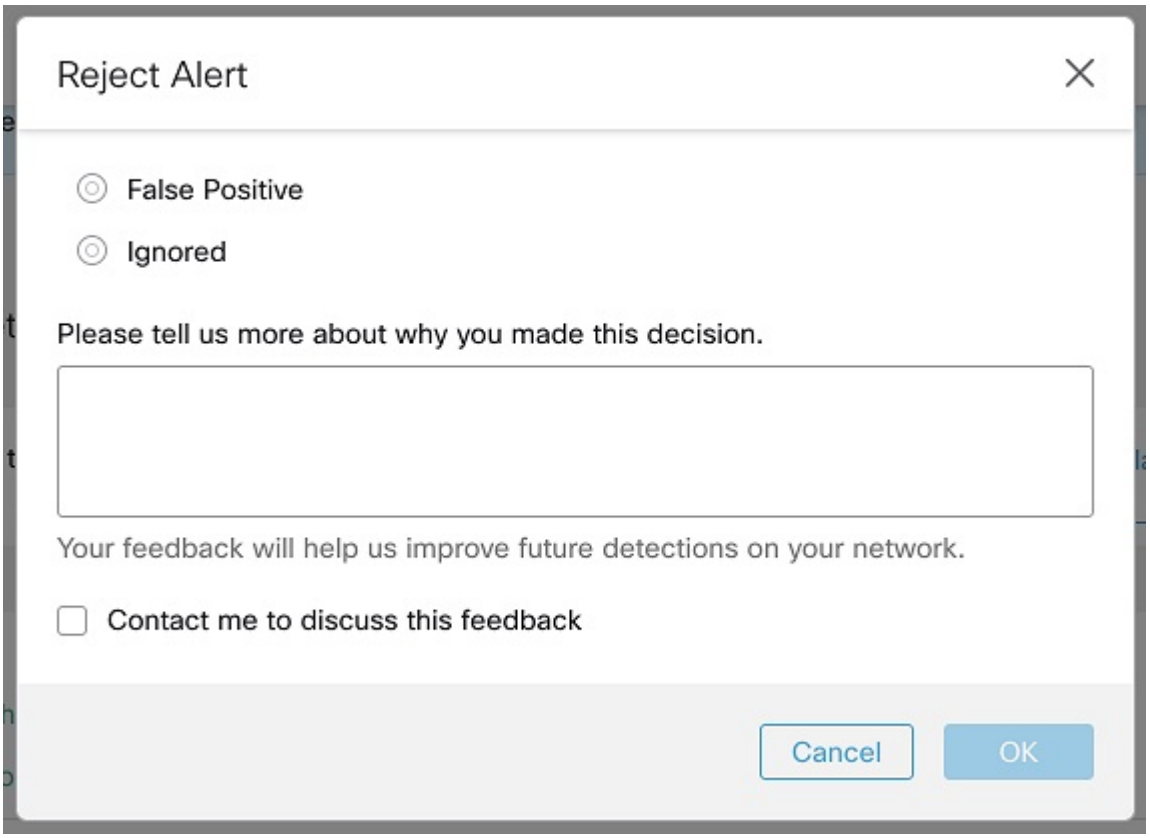
그림 42: 인시던트 요약의 예

그림 *43:* 인시던트 관찰 가능 항목의 예



알림을 인시던트로 승격하는 것이 바람직하지 않다면 거부하면 됩니다. 이 경우 Cisco 팀에 피드백을 보내 알림을 거부한 이유를 통보할 수 있습니다. 감사합니다. 귀하의 소중한 피드백은 네트워크에서의 향후 탐지를 개선하는 데 도움이 됩니다.

그림 *44:* 알림 거부 및 피드백 제공



추가 위협 탐지

다음과 같은 새로운 위협 탐지가 포트폴리오에 추가되었습니다.

- IceID
- Lemon Duck

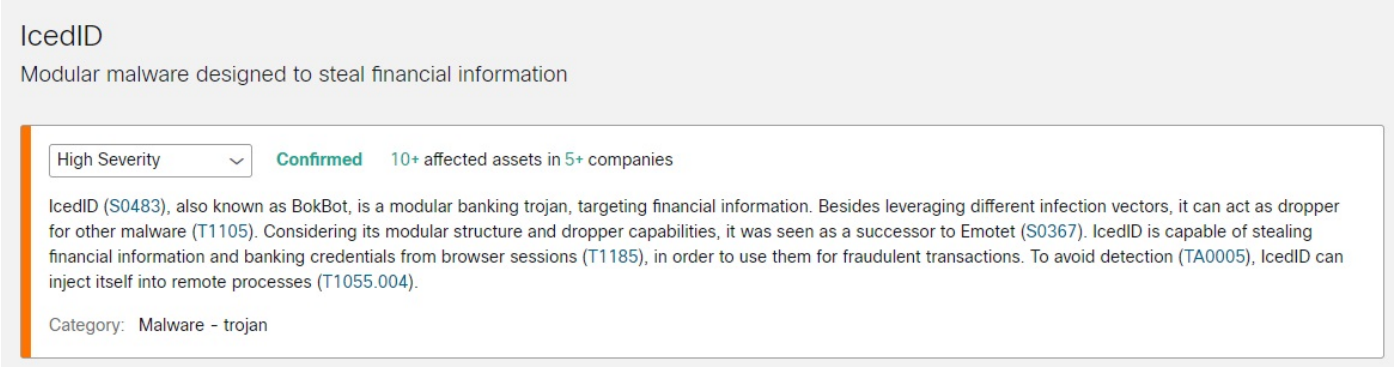
또한 다양한 저위험 위협 탐지가 강화되었습니다.

IceID

BokBot이라고도 하는 IcedID(S0483)는 금융 정보를 노리는 모듈형 뱅킹 트로이 목마입니다. 다양한 감염 벡터를 활용하며, 다른 악성코드에 대한 드로퍼 역할을 하기도 합니다(T1105). 모듈형 구조와 드로퍼 기능 때문에 Emotet(S0367)의 후속으로 간주됩니다. IceID는 브라우저 세션(T1185)에서 금융 정보 및 뱅킹 자격 증명을 훔쳐 사기 거래에 사용합니다. IcedID는 탐지(TA0005)를 방지하기 위해 자신을 원격 프로세스(T1055.004)에 삽입하기도 합니다.

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

그림 ***45:***

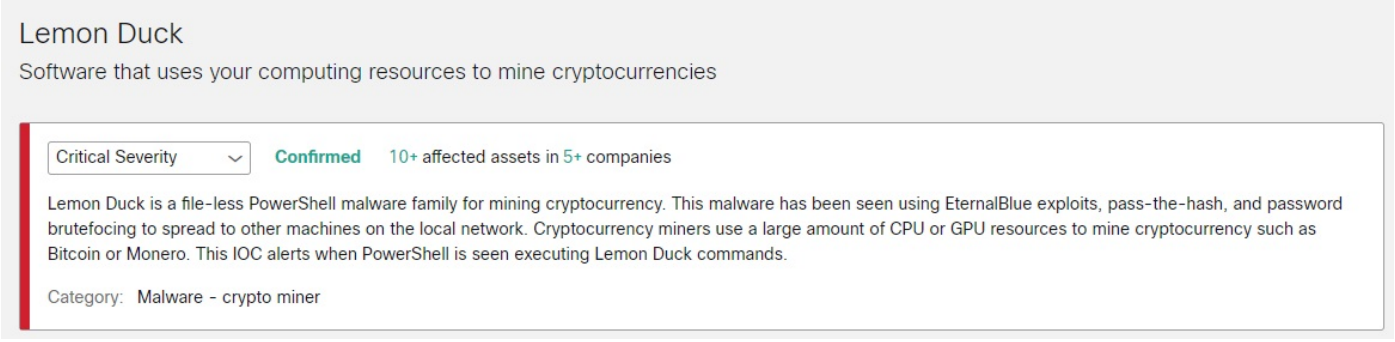


Lemon Duck

Lemon Duck은 암호화폐 채굴을 위한 파일 없는 PowerShell 악성코드에 속합니다. 이 악성코드는 EternalBlue 익스플로잇, 해시 통과 및 비밀번호 무차별 대입을 사용하여 로컬 네트워크의 다른 시스템으로 확산됩니다. 암호화폐 채굴기는 대량의 CPU 또는 GPU 리소스를 사용하여 비트코인이나 모네로 같은 암호화폐를 채굴합니다.

사용자 환경에서 Lemon Duck이 탐지되었는지 확인하려면 Lemon Duck Threat Detail(Lemon Duck 위협 세부 정보)을 클릭하여 전역 위협 알림에서 관련 세부 정보를 확인하십시오.

그림 ***46:***



13 장

2021년 12월

2021년 12월에 릴리스된, Cisco 클라우드 기반 머신 러닝 전역 위협 알림에 대한 업데이트:

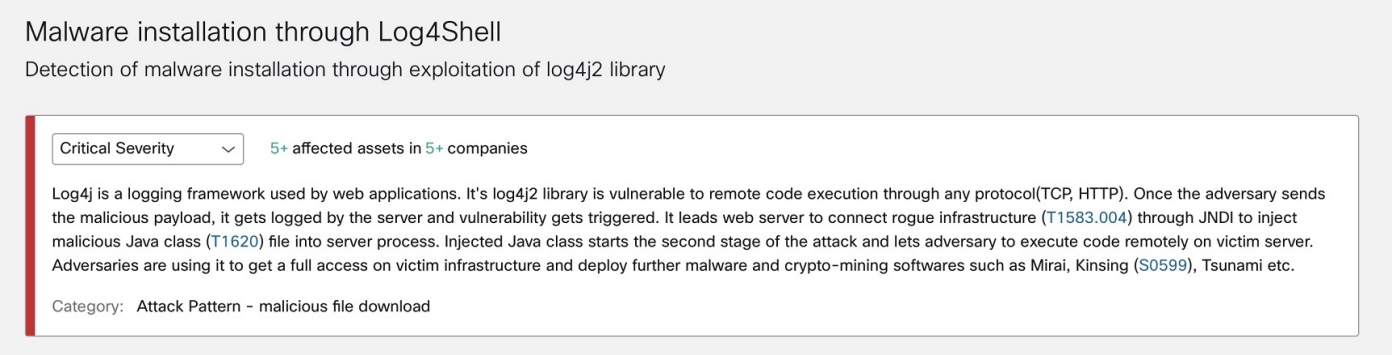
새 Log4Shell 탐지

최근에 발견된 Log4j 취약성과 관련된 두 가지 유형의 탐지를 포함한 새로운 위협 탐지가 포트폴리오에 추가되었습니다.

Log4Shell을 통한 악성코드 설치

이미 성공을 거둔 Log4j 익스플로잇을 탐지했습니다. Log4j는 웹 애플리케이션에서 사용하는 로깅 프레임워크입니다. Log4j의 log4j2 라이브러리는 아무 프로토콜(TCP, HTTP)을 통한 RCE(Remote Code Execution)에 취약합니다. 공격자가 악성 페이로드를 전송하면 서버에 로깅되고 취약성이 트리거됩니다. 웹 서버가 JNDI를 통해 비인가 인프라(T1583.004)에 연결하고 악성 Java 클래스(T1620) 파일을 서버 프로세스에 삽입하게 합니다. 삽입된 Java 클래스는 공격의 두 번째 단계를 시작하여, 공격자가 피해자의 서버에서 원격으로 코드를 실행할 수 있게 합니다. 공격자는 이를 이용하여 피해자의 인프라에 대한 전체 액세스 권한을 얻고 추가 악성코드 및 암호화폐 채굴 소프트웨어(예: Mirai, Kinsing(S0599), Tsunami)를 구축합니다.

그림 *47:*

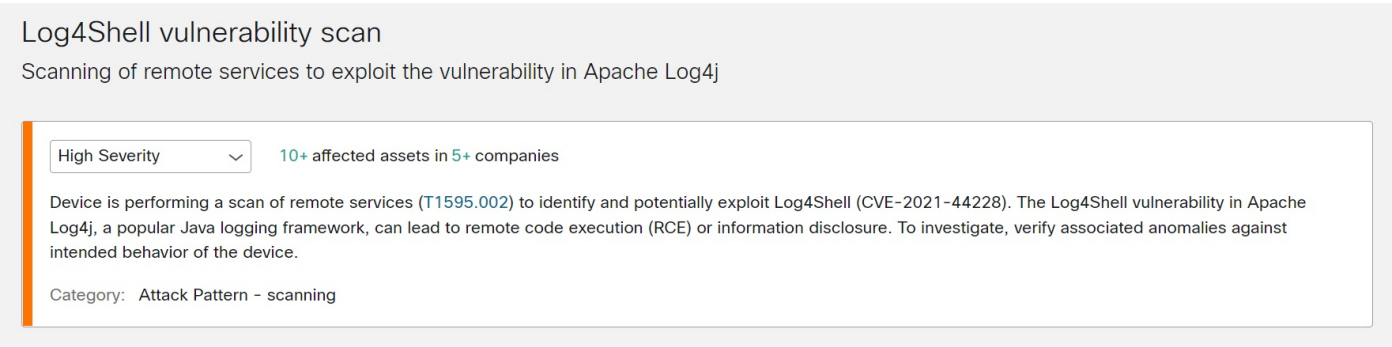


자신의 환경에서 **Log4Shell**을 통한 악성코드 설치가 탐지되었는지 확인하려면 **Malware installation through Log4Shell(Log4Shell**을 통한 악성코드 설치)를 클릭하여 전역 위협 알림에서 세부 정보를 확인하십시오.

Log4Shell 취약성 스캔

Log4Shell(CVE-2021-44228)을 식별하고 잠재적으로 익스플로잇하기 위해 원격 서비스(T1595.002) 스캔을 수행하는 디바이스가 탐지되었습니다. 인기 있는 Java 로깅 프레임워크인 Apache Log4j의 Log4Shell 취약성 때문에 RCE(Remote Code Execution) 또는 정보 노출이 발생할 수 있습니다. 트리거된 알림은 스캔을 수행 중인 원치 않는 애플리케이션 또는 악성코드가 있으며, 침투에 대한 테스트 활동이 진행 중임을 의미할 수 있습니다. 조사하려면 디바이스의 의도된 동작을 상대로 관련 변칙을 확인해야 합니다.

그림 *48:*



사용자 환경에서 **Log4Shell** 취약성 스캔이 탐지되었는지 확인하려면 **Log4Shell vulnerability scan(Log4Shell** 취약성 스캔**)**을 클릭하여 전역 위협 알림에서 관련 세부 정보를 확인하십시오.

새 **SNI** 스푸핑 탐지기

공격자는 다양한 기법을 사용하여 네트워크 보호 메커니즘을 방지합니다. SNI(Server Name Identification) 스푸핑은 도메인 기반 네트워크 보호 메커니즘을 방지하는 데 자주 사용하는 기술입니다. 이 기법은 SNI 필드에 잘 알려진 도메인 이름을 사용하고, 잘 알려진 도메인이 호스팅되는 IP 주

소가 아닌 서버 IP 주소를 사용합니다. 잘 알려진 SNI와 다른 서버 IP 주소를 조합하여 도메인 기반 보안 검사를 통과하고 허용되지 않는 서버에 도달합니다.

그림 ***49:***

새로운 SNI 스푸핑 탐지기는 SNI와 IP 주소가 일치하지 않는 불일치를 식별합니다. 탐지기는 ETA(encrypted traffic analysis)를 사용하여 SNI 필드에서 도메인을 추출하고, 관찰된 서버 IP 주소를 도메인이 일반적으로 호스팅되는 IP 주소의 전역 통계 모델과 비교합니다. 관찰된 서버 IP 주소가 모델과 일치하지 않으면 SNI 필드의 도메인이 스푸핑 중일 수 있으며, 네트워크 트래픽이 원치 않는 서버로 라우팅되고 있다는 뜻입니다. 불일치는 SNI 확장의 인기 있는 호스트 이름이 실제로 연결되는 IP 주소에서 호스팅될 가능성이 낮음을 의미합니다.

Alert(알림**) > Alert detail(**알림 세부 정보**) > Security events(**보안 이벤트**)**에서 확인할 수 있습니다.

추가 위협 탐지

다음과 같은 새로운 위협 탐지가 포트폴리오에 추가되었습니다.

- FluBot
- LokiBot
- Phorpiex
- Raccoon
- TrickBot

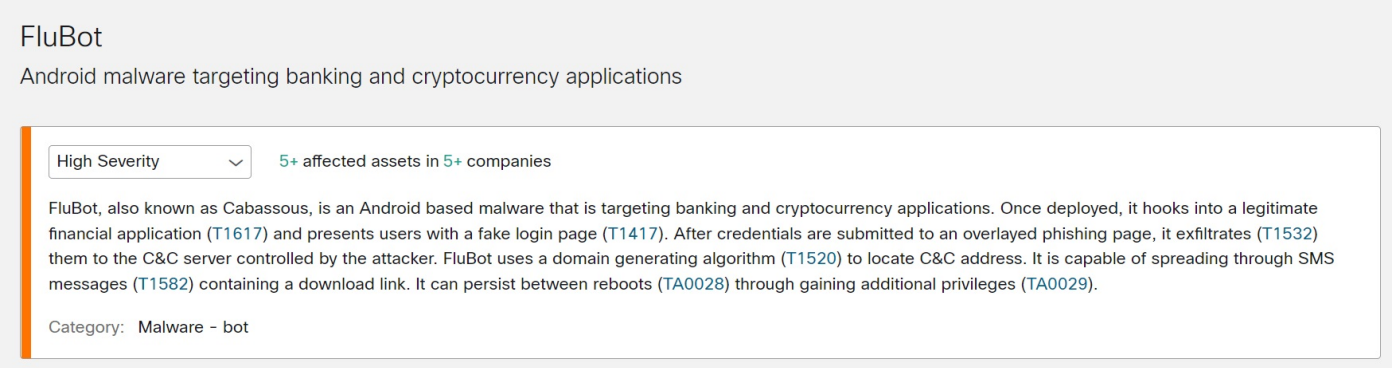
또한 애드 인젝터, 암호화폐 채굴기, 악성 광고, 악성코드 배포, 스팸 추적 같은 다양한 저위험 위협 탐지 기능이 강화되었습니다.

FluBot

FluBot(Cabassous라고도 함)은 스페인 시장 내 뱅킹 및 암호화폐 애플리케이션을 노리는 안드로이드 기반 악성코드입니다. 이 악성코드는 합법적인 금융 애플리케이션(T1617)을 가로채고 사용자에게 가짜 로그인 페이지를 제공합니다(T1417). 오버레이된 피싱 페이지에 자격 증명이 제출되면 이 악성코드는 자격 증명을(T1532) 공격자가 제어하는 명령 및 제어 서버로 추출합니다. FluBot은 도메인 생성 알고리즘(T1520)을 사용하여 명령 및 제어 주소를 찾습니다. 다운로드 링크가 포함된 SMS 메시지(T1582)를 통해 확산될 수 있으며, 추가 권한(TA0029)을 얻은 후 리부팅(TA0028)을 통해 영구적으로 유지됩니다.

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

그림 ***50:***

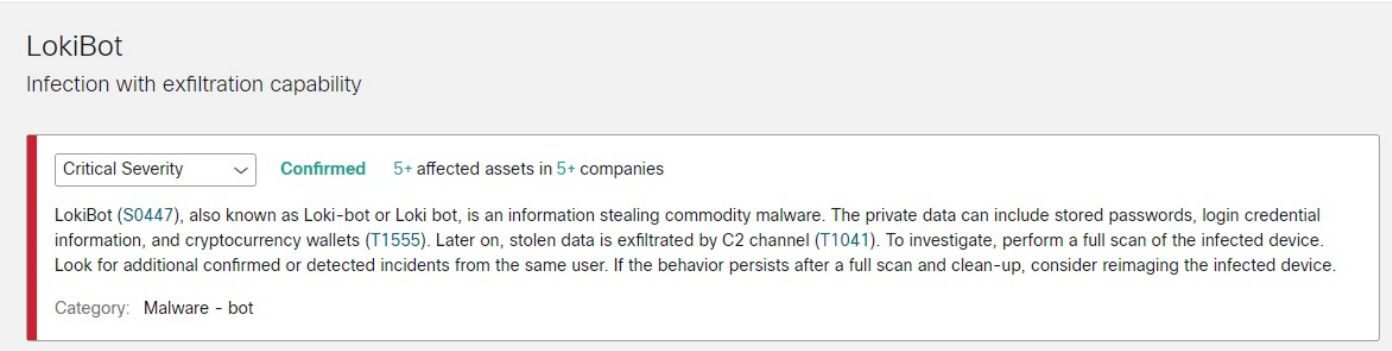


LokiBot

Loki-봇 또는 Loki 봇이라고도 하는 LokiBot(S0447)은 정보를 훔치는 상용 악성코드입니다. 이 악성코드는 저장된 비밀번호, 로그인 자격 증명 및 암호화폐 지갑(T1555) 등의 비공개 데이터도 훔칠 수 있습니다. 도난당한 데이터는 나중에 C2 채널(T1041)을 통해 추출됩니다. 조사하려면 감염된 디바이스의 전체 스캔을 수행해야 합니다. 동일한 사용자의 추가로 확인되거나 탐지된 인시던트를 찾아 보십시오. 전체 스캔 및 정리 후에도 문제가 해결되지 않는다면 감염된 디바이스 이미지 재설치를 고려해야 합니다.

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

그림 ***51:***

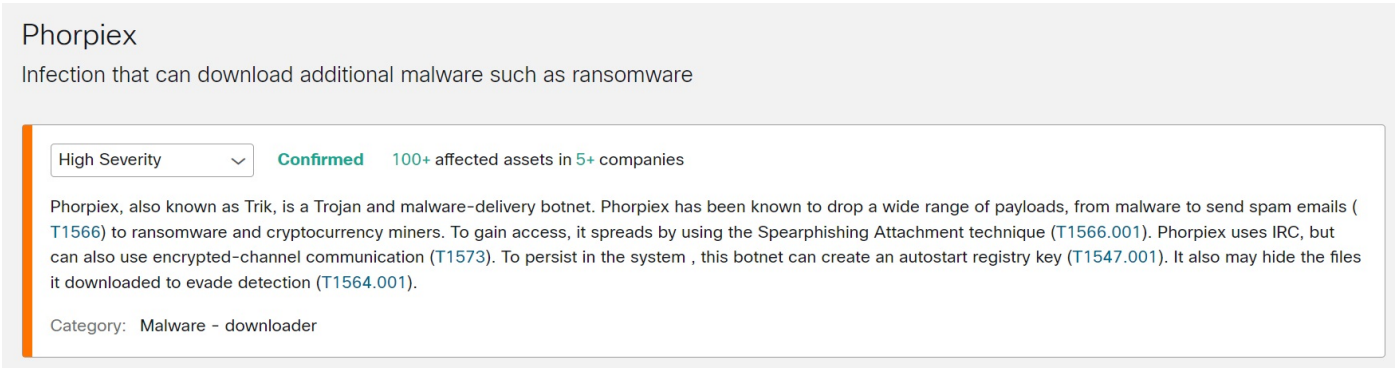


Phorpiex

Phorpiex는 운영 체제를 감염시켜 추가 악성코드를 전달하는 트로이 목마 및 웜입니다. Phorpiex는 랜섬웨어, 암호화폐 채굴기, 스팸 이메일을 전송하는 악성코드 같은 다양한 페이로드를 드롭한다고 합니다(T1566). 액세스 권한을 얻기 위해 스피어피싱 첨부 기술(T1566.001)을 사용하여 확산됩니다. Phorpiex는 IRC를 사용하지만 암호화된 채널 통신(T1573)을 사용할 수도 있습니다. 시스템에서 유지되기 위해 이 봇넷은 자동 시작 레지스트리 키(T1547.001)를 생성합니다. 탐지를 회피하기 위해 다운로드한 파일을 숨기기도 합니다(T1564.001).

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

그림 ***52:***



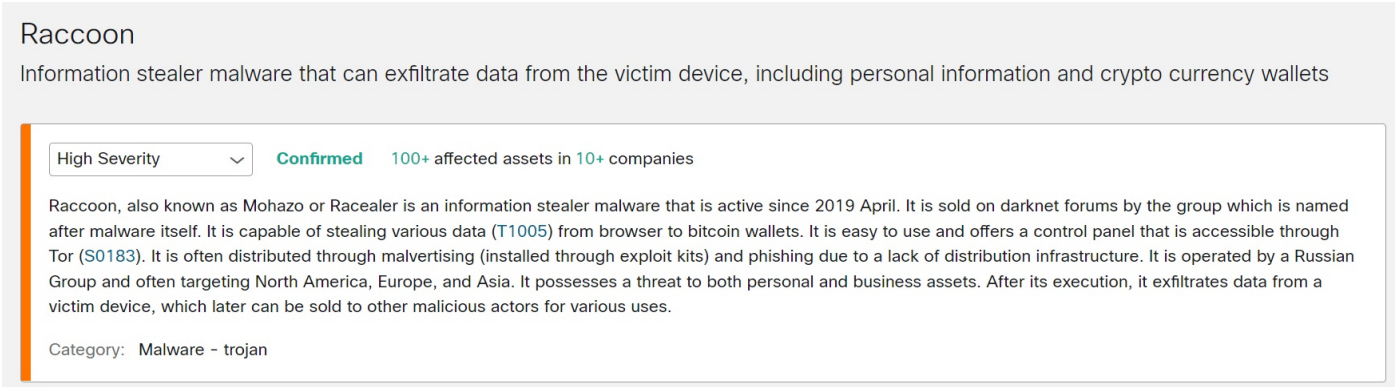
Raccoon

Raccoon(Mohazo 또는 Racealer라고도 함)은 2019년 4월 이후 활성화된, 정보를 훔치는 악성코드입니다. 브라우저의 데이터를 훔쳐(T1005) 비트코인 지갑으로 보낼 수 있으며, 개인 및 비즈니스 자산 모두에 위협이 됩니다. Raccoon은 피해자의 디바이스에서 데이터를 추출하여, 이러한 데이터는 나중에 다양한 용도로 다른 악의적인 공격자에게 판매됩니다.

Raccoon은 악성코드 자체의 이름을 딴 그룹에 의해 다크넷 포럼에서 판매되며, 북미와 유럽 및 아시아를 주로 노리는 러시아 그룹에서 운영합니다. Tor를 통해 액세스할 수 있는 제어 패널로 쉽게 사용할 수 있습니다(S0183). Raccoon은 배포 인프라 부족 때문에 주로 (익스플로잇 킷을 통해 설치되는) 멀버타이징과 피싱을 통해 배포됩니다.

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

그림 ***53:***

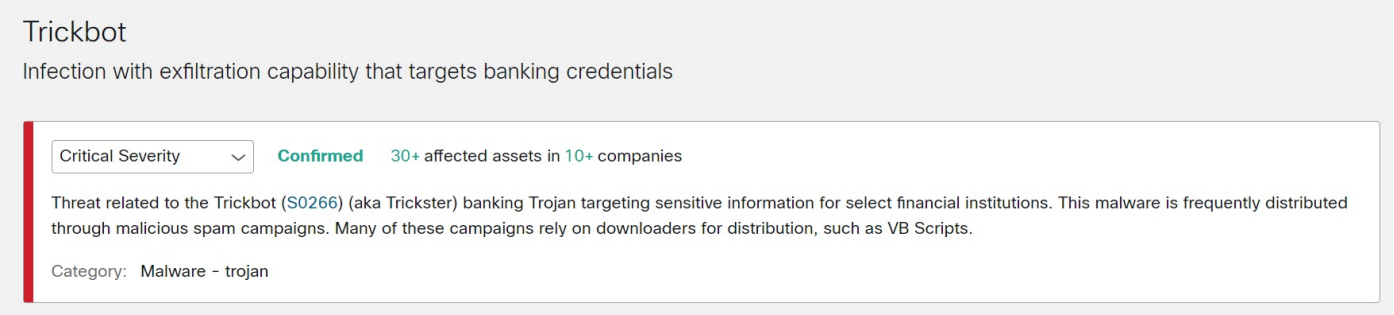


TrickBot

Trickster라고도 하는 TrickBot(S0266)은 일부 금융 기관의 민감한 정보를 노리는 뱅킹 트로이 목마입니다. 이 악성코드는 주로 악성 스팸 캠페인을 통해 배포됩니다. 이러한 캠페인 대부분은 VB 스크립트 같은 다운로더를 사용하여 배포됩니다.

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

그림 ***54:***



14 장

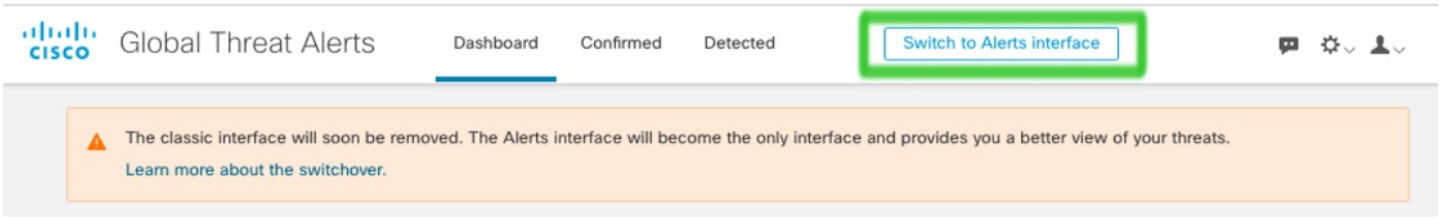
2021년 8월

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

클래식 인터페이스 해제됨

6월에는 클래식 인터페이스에서 알림 인터페이스로의 전환을 권장했습니다.

그림 ***55:***



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

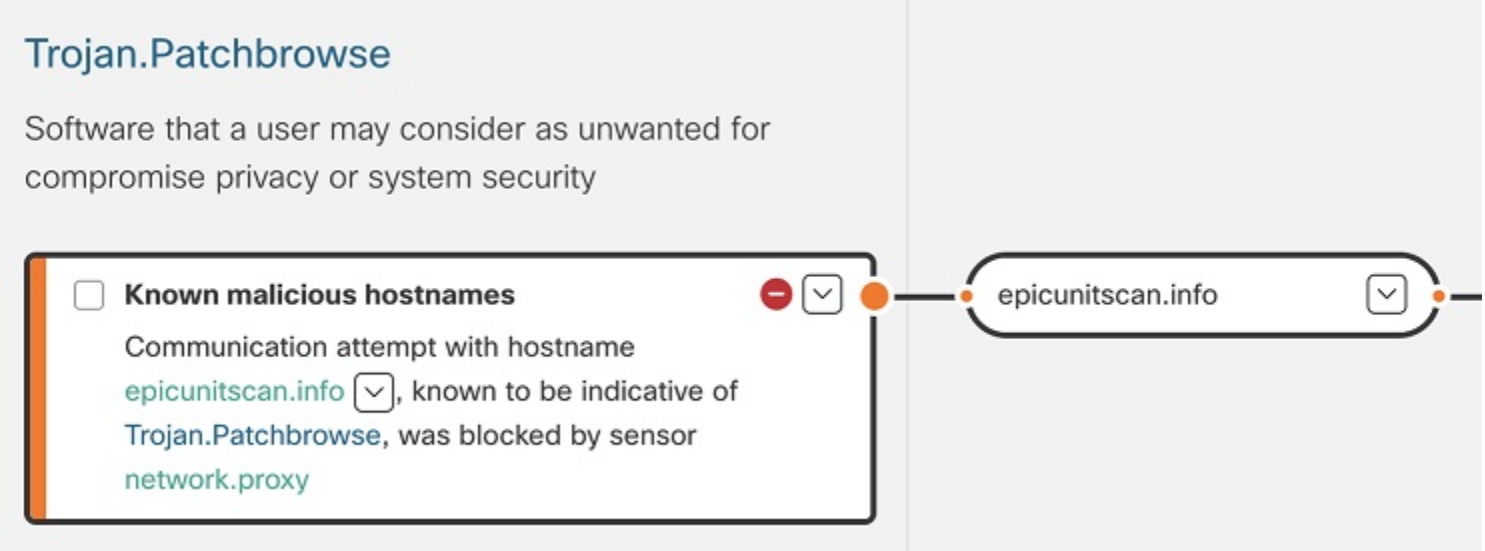
스캔 및 차단된 통신 처리 개선

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 ***56:*** 예*:* 프록시에 의해 통신 시도가 차단되었음을 알려주는 보안 이벤트



15 장

2021년 6월

2021년 6월에 릴리스된, Cisco 클라우드 기반 머신 러닝 전역 위협 알림에 대한 업데이트:

자동화 지원을 위한 새 REST API

이제 새로운 REST API를 통해 전역 위협 알림 대시보드에 표시되는 모든 데이터를 확인할 수 있습니다. 이 대시보드를 사용하여 단일 알림의 콘텐츠를 다운로드하고, 나아가 모든 알림을 네트워크의 서드파티 SIEM으로 스트리밍하여 전체 데이터 수집 프로세스를 자동화할 수도 있습니다.

API는 읽기 전용이 아닙니다. 사용자는 전역 위협 알림 환경의 컨피그레이션을 변경할 수 있습니다 예를 들어 중요 자산 그룹의 특정 비즈니스 가치를 높이거나 위협에 할당된 심각도를 변경할 수 있습니다.

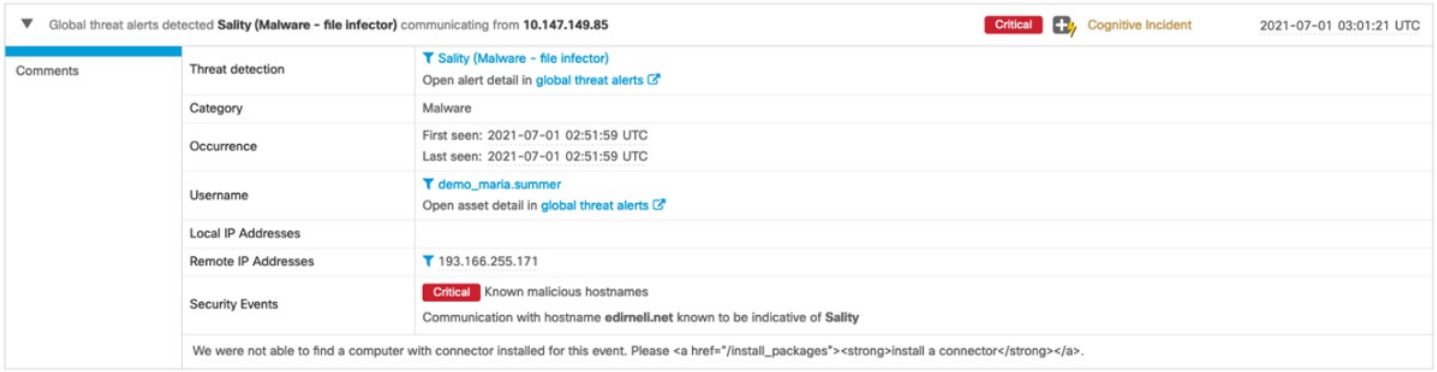
API 가능성을 확인하려면 https://api.cta.eu.amp.cisco.com을 참조하십시오. API 가능성을 자세히 설명하는 사양 및 사용 사례와 추가 통합을 위한 예제 스크립트를 확인할 수 있습니다.

새 REST API에 관한 자세한 내용은 전역 위협 알림 REST API가 릴리스되었습니다!를 참조하십시오.

Secure Endpoint 통합 업데이트

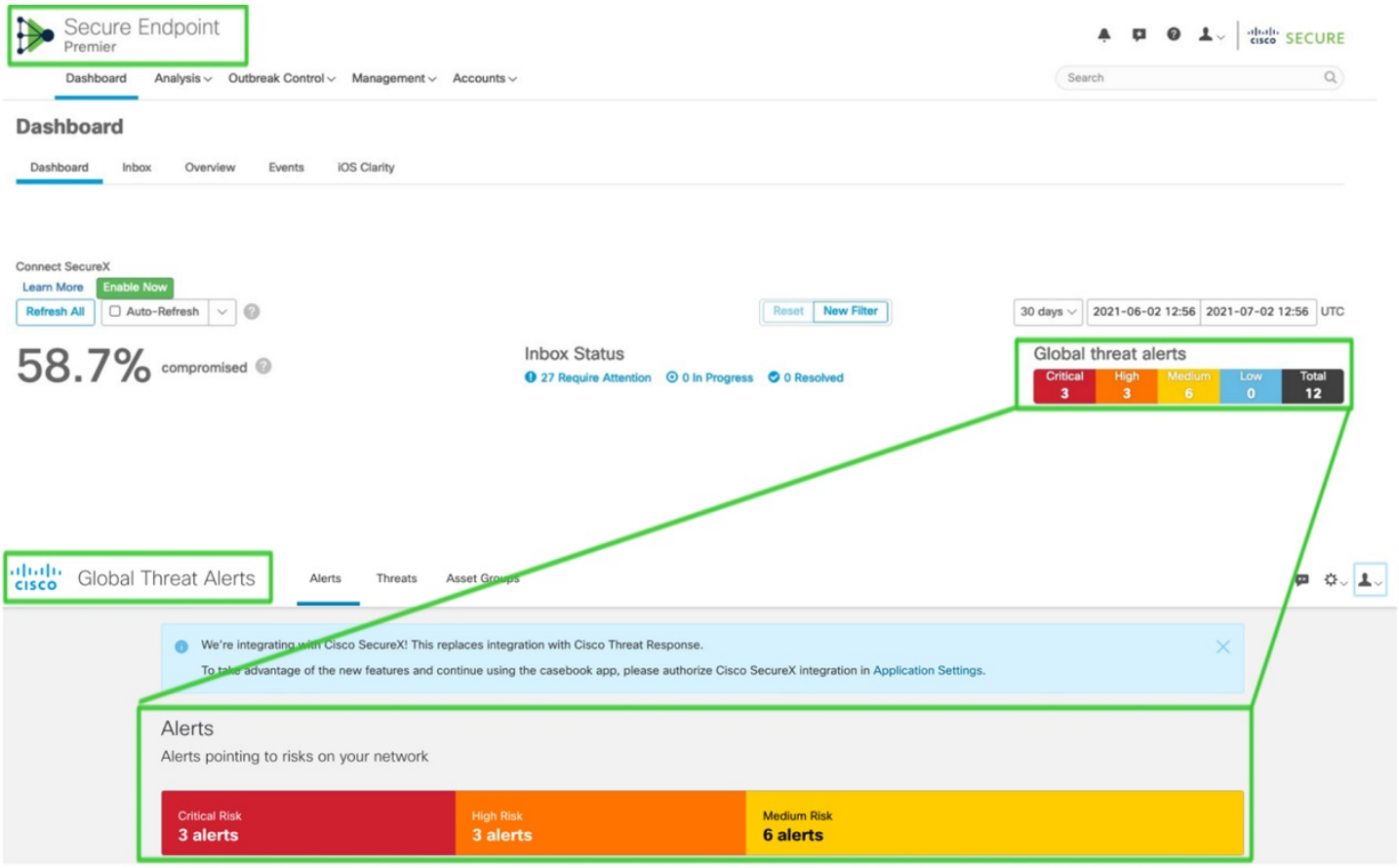
전역 위협 알림의 탐지 항목이 Secure Endpoint에 표시되는 방식을 업데이트했습니다. 이제 탐지 항목은 콘솔에서 이벤트로 표시되며, 알림 인터페이스에 바로 연결됩니다. 따라서 알림 인터페이스의 위협 심각도 변경 사항은 이러한 이벤트에 반영됩니다.

그림 ***57:*** 이제 전역 위협 알림 탐지가 ***Secure Endpoint*** 콘솔에서 이벤트로 표시됩니다.



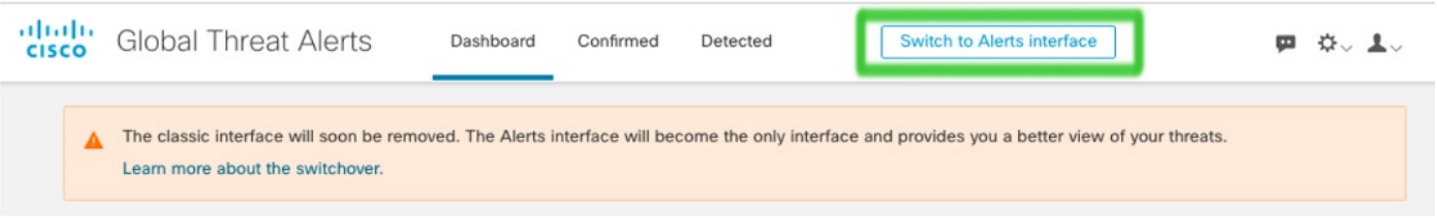
전역 위협 알림 인터페이스에서 알림의 상태 또는 위험이 변경되면, Secure Endpoint 콘솔의 알림 개요에 반영됩니다.

그림 ***58:***



호환성 문제를 방지하기 위해 클래식 인터페이스는 곧 사용이 중단되므로, 클래식 인터페이스에서 알림 인터페이스로 전환하는 것이 좋습니다. 전역 위협 알림 대시보드에서 **Switch to Alerts interface(**알림 인터페이스로 전환**)** 버튼을 클릭합니다.

그림 *59:*



STIX/TAXII API 업데이트

이제 STIX/TAXII API 피드에서 제공하는 탐지 링크 및 위협 용어가 전역 위협 알림 대시보드의 알림 인터페이스와 호환됩니다.

그림 *60:*

```
<s:Incident xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
            xsi:type="inc:IncidentType"
            URL="https://cta.eu.amp.cisco.com/ui/assets/demo_3399f455c51cf4879ce08796f0dee9613832f2bd165127f4f7e5fabcc825979c"
            id="cta:incident-demo_a304ea5e63d526a9077406ada15697554bbb1d3ea7d2b49f1773c0ee104ede1d">
   <inc:Title>njRAT</inc:Title>
   <inc:Victim>
      <sc:Name>demo_sook.putnam</sc:Name>
   </inc:Victim>
   <inc:Impact_Assessment>
      <inc:Impact_Qualification>Catastrophic</inc:Impact_Qualification>
   </inc:Impact_Assessment>
   <inc:Related_Indicators>
      <inc:Related_Indicator>
         <sc:Indicator xsi:type="ind:IndicatorType"
                       id="cta:indicator-demo_6a0d469ac3f4383b00f6b221fe4c7d88fa70161089a75fa8b6c8058985dc981e">
            <ind:Observable>
               <c:Observable_Composition operator="AND">
                  <c:Observable>
                     <c:Object>
```

위협 문구 및 분류가 변경되었으므로 STIX/TAXII API에서 제공하는 툴 및 SIEM에서 비호환성 문제와 손상된 종속성을 확인하는 것이 좋습니다.

16 장

2021년 5월

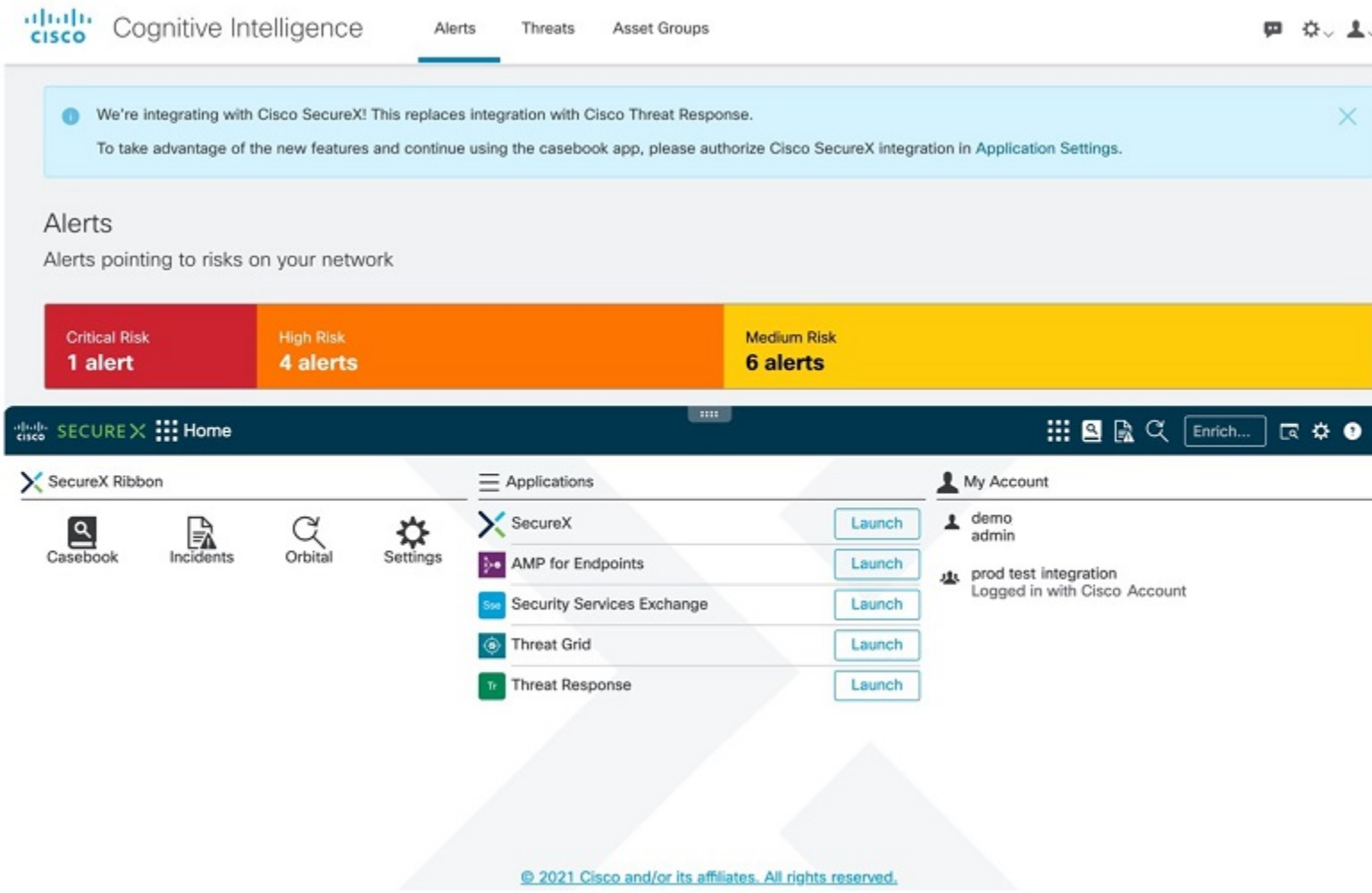
2021년 5월에 릴리스된, Cisco 클라우드 기반 머신 러닝 전역 위협 알림에 대한 업데이트:

SecureX 리본 지원

SecureX는 가시성을 통합하고, 자동화를 활성화하고, 사고 대응 워크플로우를 가속화하고, 위협 추적을 개선하는 중앙 집중식 콘솔이자 분산형 기능 집합입니다. 이러한 분산형 기능은 SecureX 리본에서 앱 및 툴의 형태로 표시됩니다.

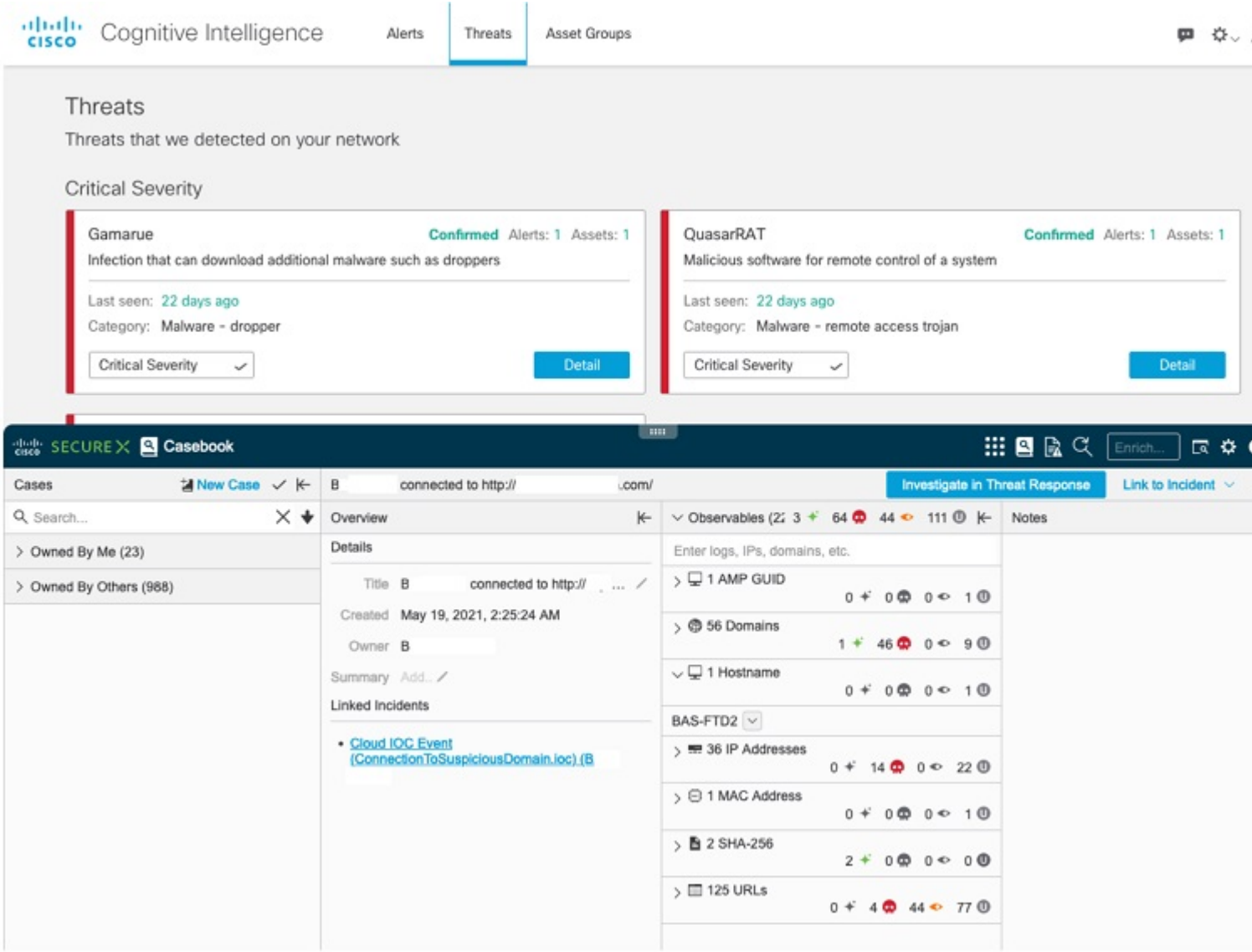
이제 SecureX 리본을 페이지 하단에 있는 전역 위협 알림에서도 사용할 수 있으며, 대시보드와 사용자 환경 내 다른 보안 제품 사이를 이동할 때도 계속 표시됩니다. 따라서 발견한 내용을 케이스북 및 인시던트와 쉽게 연결할 수 있습니다.

그림 *61:* 페이지 하단에 있는 ***SecureX*** 리본



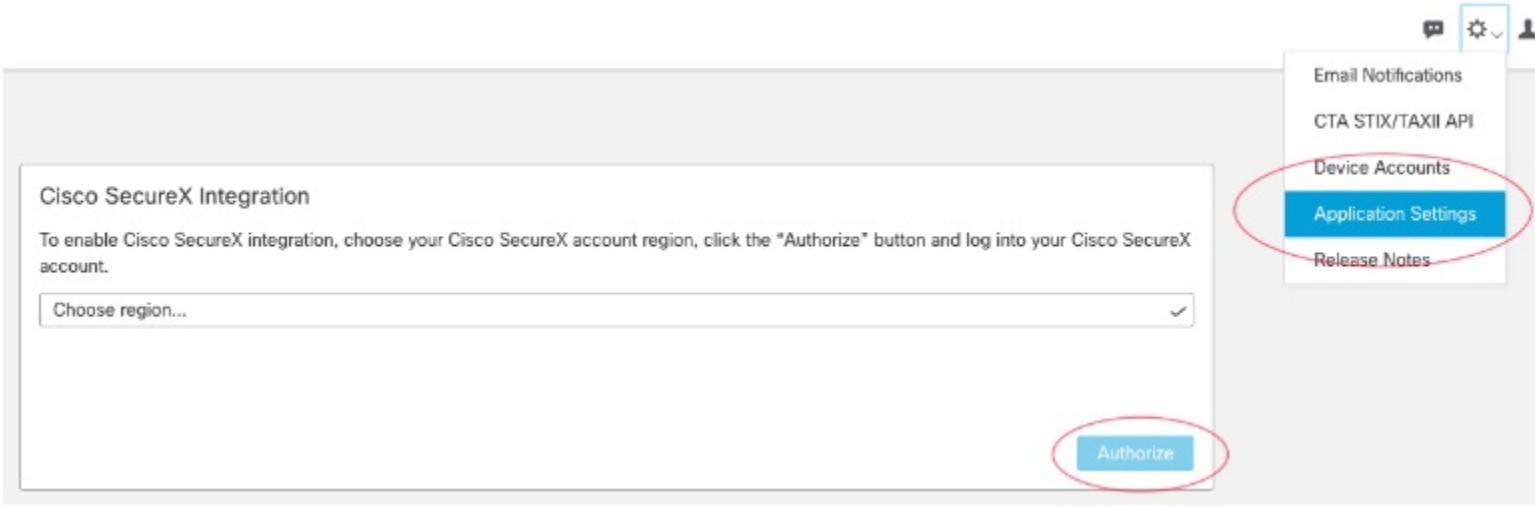
리본을 사용하여 케이스북, 설정 및 기타 앱에 액세스할 수 있습니다. 또한 강화를 위해 인시던트를 보고 관찰 가능 항목을 검색할 수도 있습니다.

그림 62: 예: SecureX 리본을 사용하여 케이스북에 액세스



이 기능을 활성화하려면 사용자는 SecureX 계정을 확보하고 Application Settings(애플리케이션 설정)에서 통합에 권한을 부여해야 합니다.

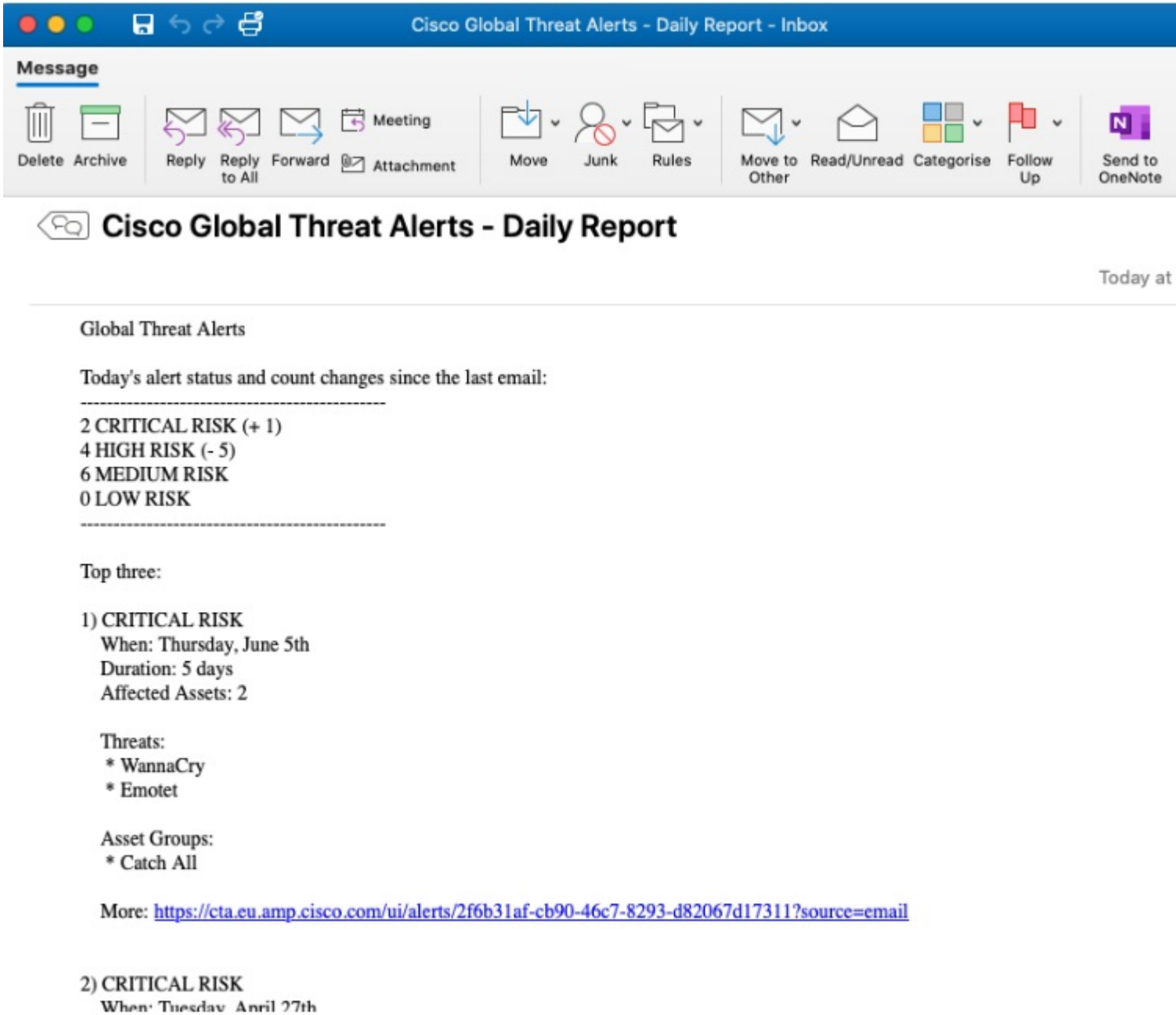
그림 ***63: Application Settings(***애플리케이션 설정***)***로 이동하여 ***SecureX***와의 통합 권한 부여



업데이트된 일일 보고서 이메일

이메일 알림 서비스가 업데이트되어 알림 대시보드와 호환되는 콘텐츠를 이메일로 전송합니다. 일일 보고서 이메일은 알림의 현재 상태 및 보고된 알림 수의 최근 변경 사항을 알려줍니다.

그림 **64:** 예: 업데이트된 일일 보고서 이메일



이 서비스를 활성화하려면 전역 설정 메뉴에서 Email Notifications(이메일 알림)를 선택하고 일일 보고서를 수신할 이메일 주소를 입력해야 합니다.

17 장

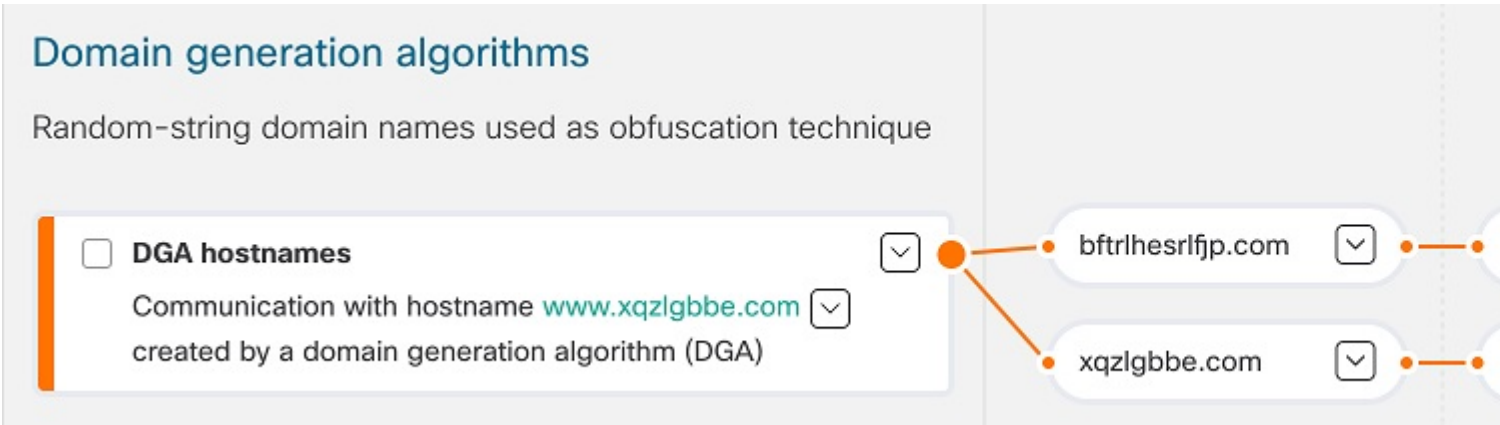
2021년 4월

2021년 4월에 릴리스된, Cisco 클라우드 기반 머신 러닝 전역 위협 알림에 대한 업데이트:

새 DGA 2.0 분류자

DGA(Domain Generation Algorithm)는 임의로 호스트 이름을 생성하여 차단 기능이 있는 보안 제품을 우회하는 용도로 공격자가 사용합니다. 이러한 알고리즘은 주로 봇넷 및 애드웨어에서의 통신에 사용합니다. 동적으로 생성되기 때문에 원래는 차단되어야 하는, 정적인 서명 기반 감시 목록에 의존하는 보안 제품을 우회할 수 있습니다.

그림 ***65:*** 예***: DGA***에 의해 난독화 차단기에 생성된 임의 문자열 도메인



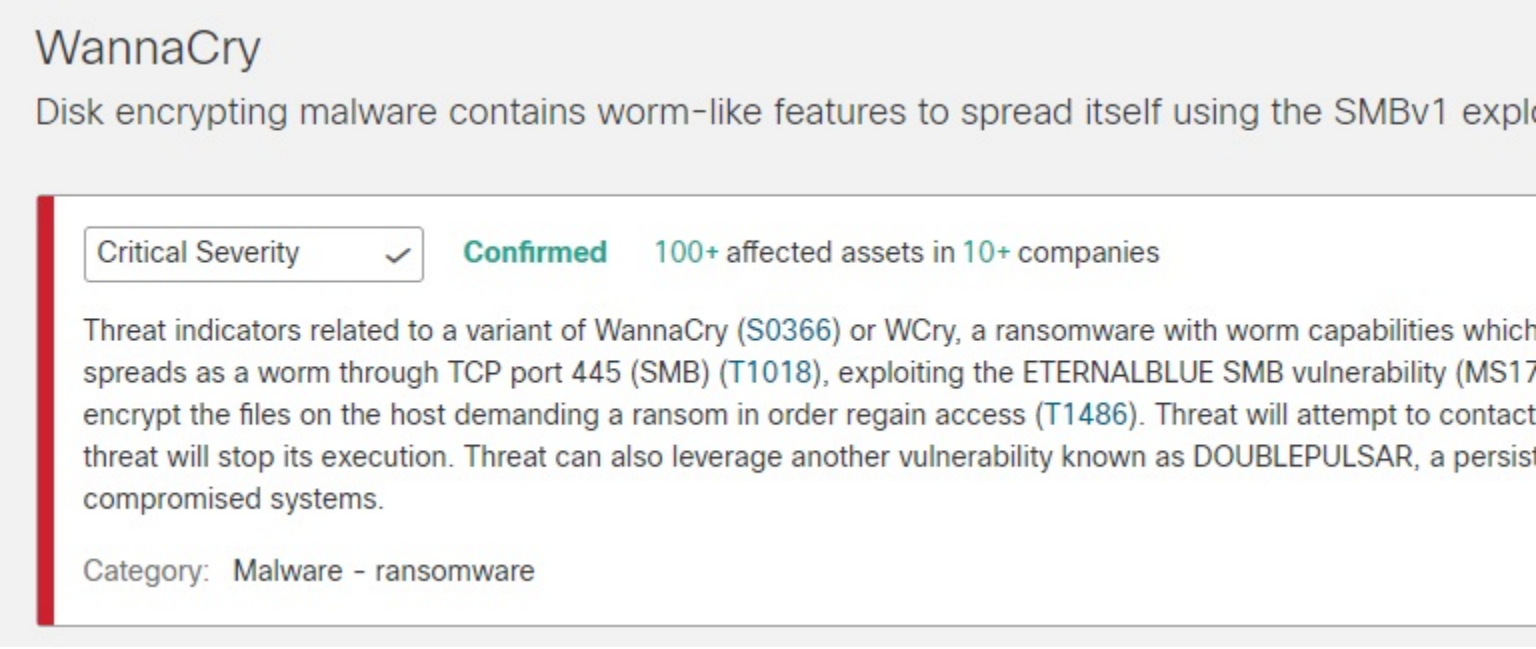
2015년부터 전역 위협 경고는 DGA 도메인 탐지를 지원했지만, DGA 2.0 분류자는 기존의 무작위 포리스트가 아닌 신경망(텍스트 처리를 위한 최첨단 솔루션)을 기반으로 구축된 새로운 모델입니다. 이러한 아키텍처 갱신과 새로 제작된 교육 집합은 오탐을 생성 하는 동안 재현율(정탐 수)을 두 배로 높이고 오탐을 줄입니다.

Alert(알림**)** > **Alert detail(**알림 세부 정보**)** > **Security events(**보안 이벤트**)**에서 확인할 수 있습니다.

알림 설명의 새 **MITRE** 참조

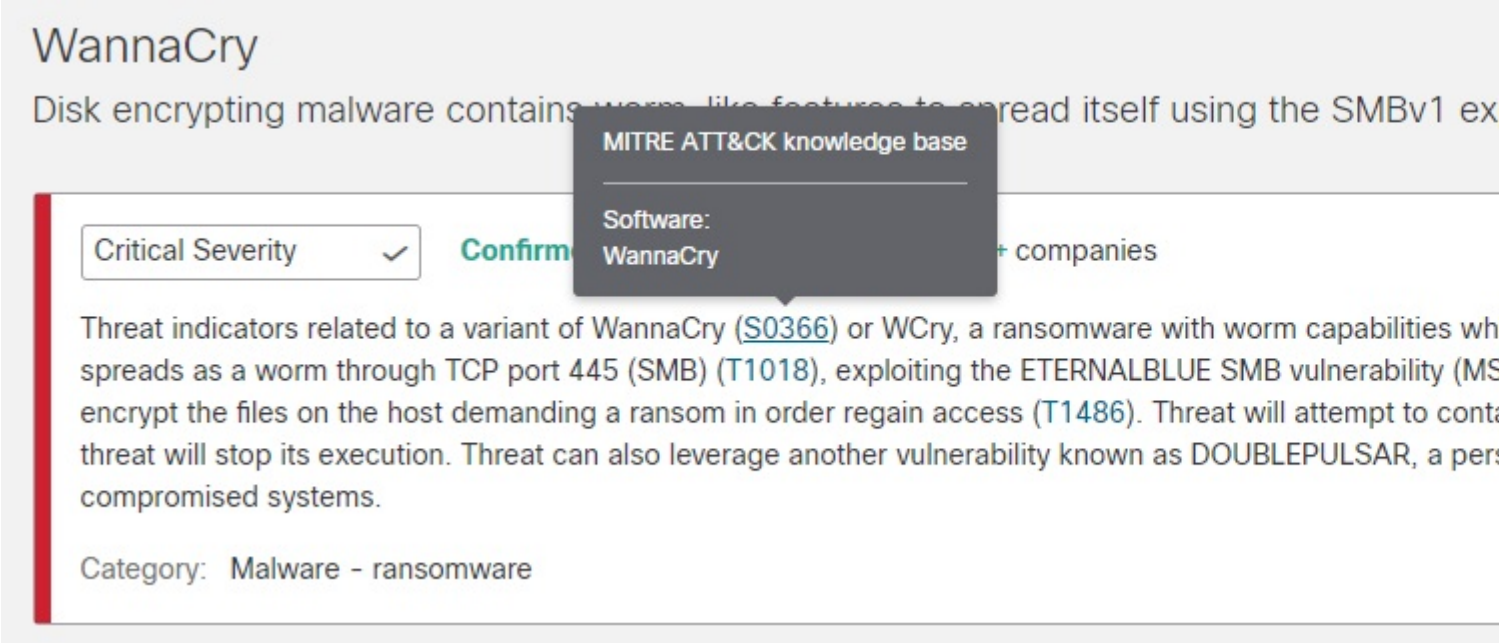
(사용 가능한 경우) 알림 설명에 MITRE 참조가 바로 추가되기 때문에 추가 정보에 편리하게 액세스할 수 있습니다.

그림 ***66:*** 예***: WannaCry*** 설명에 있는 ***4***가지 ***MITER*** 참조***(S0366, T1018, T1210, T1486)***



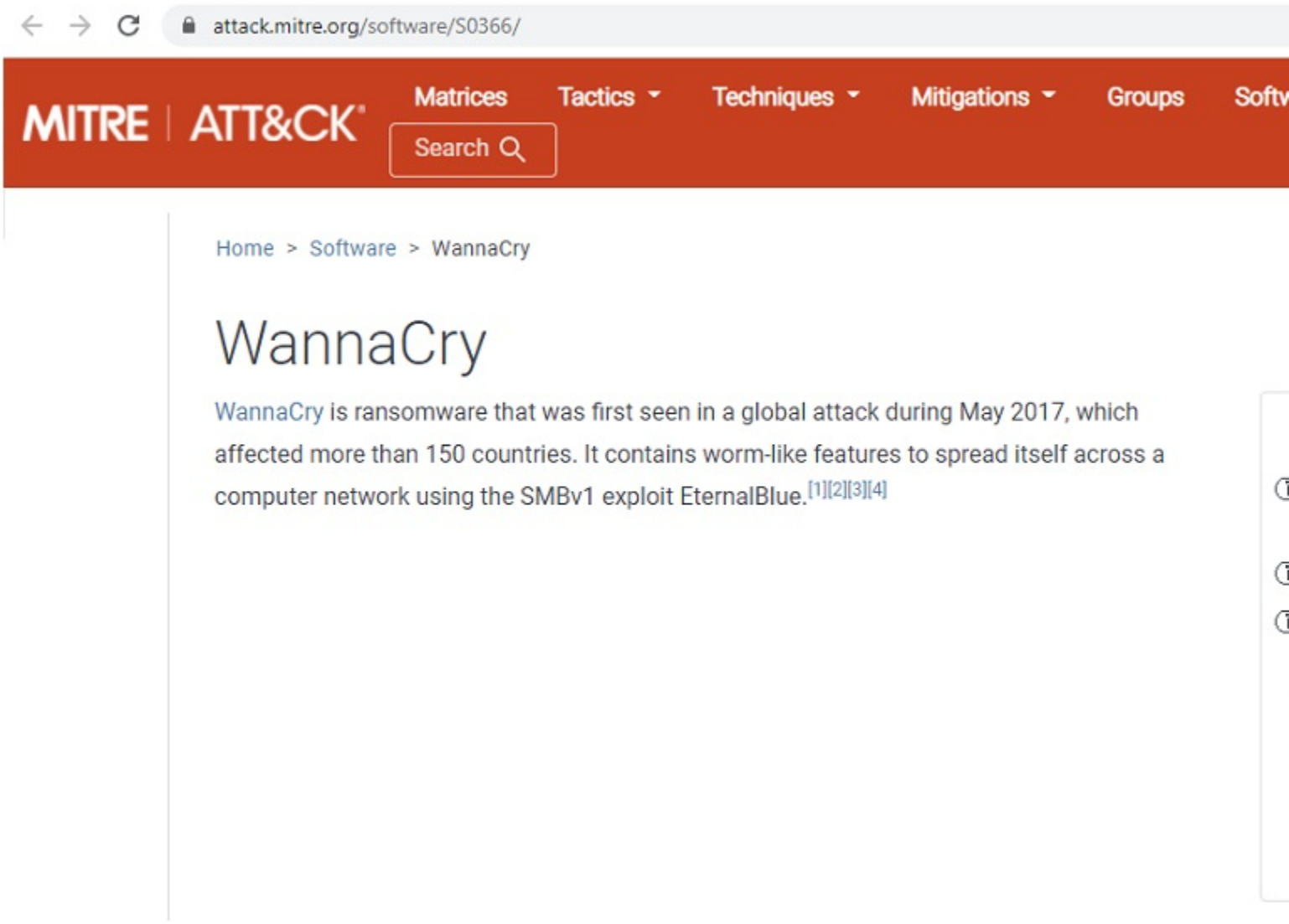
알림 및 알림 설명에 대한 추가 세부 정보를 찾으십니까? ID 번호를 클릭하여...

그림 ***67:*** 예***: S0366***에 대한 ***MITRE ATT&CK*** 기술 자료에 포함된 링크



...MITRE ATT&CK 기술 자료와 특정 위협에 대한 추가 정보 및 상세정보를 제공하는 새 브라우저 페이지를 여십시오.

그림 ***68: S0366***에 대한 추가 정보 및 세부 정보를 제공하는 ***MITRE ATT&CK*** 페이지



18 장

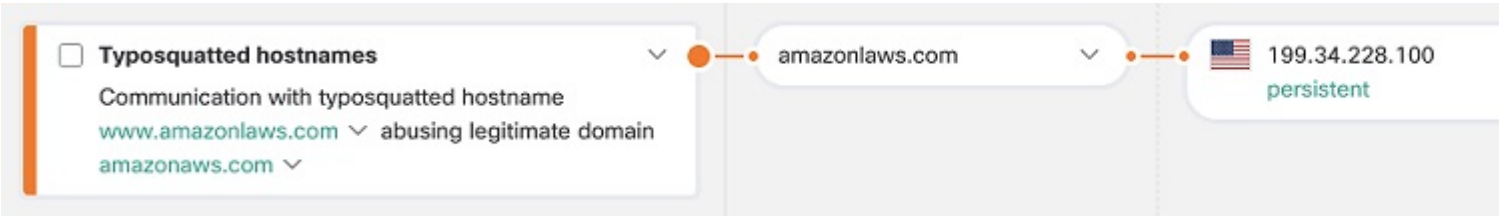
2021년 3월

Cisco 클라우드 기반 머신 러닝 전역 위협 알림에 대해 2021년 3월에 릴리스된 업데이트:

새 타이포스쿼팅 분류자

타이포스쿼팅은 URL 하이재킹의 한 형태로, 사용자가 웹 브라우저에 URL을 입력할 때 발생하는 오타(타이포)를 이용합니다. 그 결과 사용자는 공격자 소유의 대체 웹사이트에 연결됩니다. 타이포스쿼팅 URL은 다음과 같이 합법적인 URL과 유사하게 보입니다.

그림 ***69:*** 예*:* 다른 문자가 추가된 타이포스쿼팅한 호스트 이름



타이포스쿼팅 URL은 대부분 온라인 스캠으로 연결됩니다. 대표적인 예는 광고를 통해 수익을 창출하는 광고 페이지나 사용자의 정보를 훔치는 데 사용하는 피싱 페이지입니다.

그림 *70:* 예*: Amazon AWS*로 이동하려는 사용자를 노리는 광고 페이지

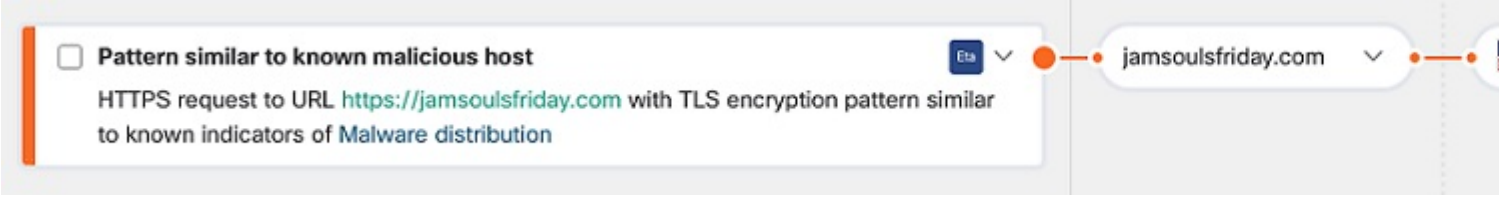
새로운 분류자의 목적은 가장 많이 사용하는 도메인을 대상으로 하는 타이포스쿼팅 도메인으로부터 사용자를 보호하는 것입니다. 분류자는 도메인의 유사성을 계산하여 가장 인기 있는 도메인과 유사한 도메인을 효과적으로 식별합니다. 그런 다음 분류자는 타이포스쿼팅 도메인 나이와 같은 추가 매개변수를 기반으로 위협의 심각도를 결정합니다.

Alert(알림**)** > **Alert detail(**알림 세부 정보**)** > **Security events(**보안 이벤트**)**에서 확인할 수 있습니다.

새 **TLS** 패턴 분류자

새 분류자는 TLS(Transport Layer Security) 핑거프린팅 기술을 이용해 구축됩니다. 분류자는 ETA(Encrypted Traffic Analytics)의 TLS 헤더와 추가 전역 및 로컬 상황별 기능을 고려하여, TLS 공간을 기반으로 의심스러운 애플리케이션과 악성 애플리케이션을 탐지합니다. 분류자는 암호화된 통신을 분석하여, HTTP를 이용해 통신하는 위협을 대상으로 하는 모델의 기능을 확장합니다.

그림 ***71:*** 예*:* 악성으로 알려진 호스트와 유사한 ***TLS*** 패턴



Alert(알림**)** > **Alert detail(**알림 세부 정보**)** > **Security events(**보안 이벤트**)**에서 확인할 수 있습니다.

19 장

2021년 3월 이전

2021년 3월 이전

2021년 3월 이전에 릴리스된 업데이트는 Cisco 커뮤니티 보안 블로그에 보관되며 **Cognitive Intelligence** 레이블과 **cognitive-release-notes** 태그가 표시됩니다.