Cisco Threat Intelligence Director(TID)

이 장의 주제에서는 Firepower System에서 TID를 구성하고 사용하는 방법을 설명합니다.

Cisco Threat Intelligence Director(TID) 개요

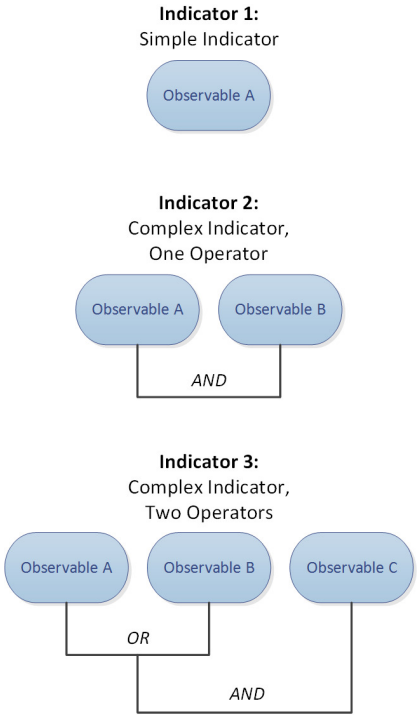
Cisco Threat Intelligence Director(TID)는 위협 인텔리전스 데이터를 운용하여 인텔리전스 데이터 집계, 방어 작업 구성, 환경 내 위협 분석에 도움이 됩니다. 이 기능은 다른 Firepower 기능을 보완하기 위한 것이며, 위협에 대한 추가 방어선을 제공합니다.

호스팅 플랫폼에 구성할 경우, TID는 위협 인텔리전스 소스에서 데이터를 수집하여 구성된 모든 매니지드 디바이스(요소)에 게시합니다. 호스팅 플랫폼과 이 릴리스에서 지원되는 요소에 대한 자세한 내용은 플랫폼, 요소 및 라이선스 요구 사항, 4 페이지를 참조하십시오.

소스에는 관찰 가능 개체를 포함하는 지표가 포함됩니다. 지표는 위협과 관련된 모든 특성을 전달하고, 개별적인 관찰 가능 개체는 위협과 관련된 개별적 특성(예: SHA-256 값)을 나타냅니다. 간단한 지표에는 하나의 관찰 가능 개체가 포함되고 복잡한 지표에는 둘 이상의 관찰 가능 개체가 포함됩니다.

관찰 가능 개체와 관찰 가능 개체 사이의 AND/OR 연산자는 다음 예에서 보듯 지표의 패턴을 형성합니다.

그림 *1:* 예*:* 지표 패턴



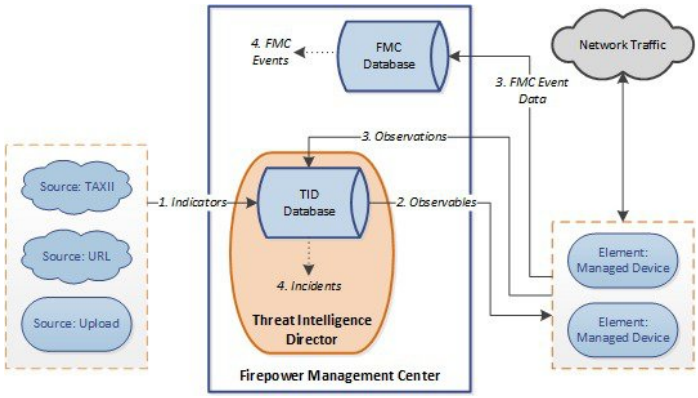
관찰 가능 개체가 요소에 게시된 후 요소는 시스템이 트래픽에서 관찰 가능 개체를 식별할 때 트래픽을 모니터링하여 관찰 가능 개체를 Firepower Management Center에 보고합니다.

Firepower Management Center는 모든 요소에서 관찰을 수집하고, TID 지표를 기준으로 관찰을 평가하며, 관찰 가능 개체의 상위 지표에 연결된 인시던트를 생성하거나 업데이트합니다.

인시던트는 지표의 패턴이 처리될 때 완전히 실현됩니다. 트래픽이 지표의 관찰 가능 개체 하나 이상과는 일치하지만 전체 패턴과는 일치하지 않는 경우, 인시던트가 부분적으로 실현됩니다. 자세한 내용은 관찰 및 사고 생성, 16 페이지를 참고하십시오.

다음 다이어그램은 샘플 Firepower System 구성에서의 데이터 흐름을 보여줍니다.

그림 *2: Firepower Management Center* 데이터 흐름



TID가 완전히 또는 부분적으로 실현되면 시스템은 구성된 작업(모니터링, 차단, 부분적으로 차단 또는 작업 없음)을 수행합니다. 자세한 내용은 수행하는 작업에 영향을 미치는 요소, 24 페이지를 참조하십시오.

TID 및 보안 인텔리전스

액세스 제어 정책의 일환으로 보안 인텔리전스는 평판 인텔리전스를 사용하여 IP 주소, URL, 도메인과의 연결을 신속하게 차단합니다. 보안 인텔리전스는 업계를 선도하는 Cisco Talos Intelligence Group(Talos)의 위협 인텔리전스에 대한 고요한 액세스를 제공합니다. Security Intelligence(보안 인텔리전스)에 대한 자세한 내용은 보안 인텔리전스 정보를 참고하십시오.

TID 다음과 같이 서드파티 소스의 보안 인텔리전스에 따라 연결을 차단하는 시스템의 기능을 강화합니다.

- **TID**는 추가 트래픽 필터링 기준을 지원합니다 - 보안 인텔리전스를 사용하여 IP 주소, URL 및 (DNS 정책이 활성화된 경우) 도메인 이름을 기반으로 트래픽을 필터링할 수 있습니다. TID는 또한 이러한 기준에 따른 필터링을 지원하며 SHA-256 해시 값에서의 필터링에 대한 지원을 추가합니다.
- **TID**는 추가 인텔리전스 수집 방법을 지원합니다 - 보안 인텔리전스와 TID를 모두 사용하면 플랫 파일을 수동으로 업로드하거나 서드파티 호스트에서 플랫 파일을 검색하도록 시스템을 구성하여 위협 인텔리전스를 시스템으로 가져올 수 있습니다. TID는 이러한 플랫 파일 관리의 유연성을 높입니다. 또한 TID는 STIX™(Structured Threat Information eXpression) 형식으로 제공되는 인텔리전스를 검색하고 수집할 수 있습니다.
- **TID**는 필터링 작업의 세분화된 제어를 제공합니다 - 보안 인텔리전스를 사용하여 네트워크, URL 또는 DNS 개체별로 필터링 기준을 지정할 수 있습니다. 보안 인텔리전스 개체(특히 목록 및 피드)는 여러 IP 주소, URL 또는 DNS 도메인 이름을 포함할 수 있지만 개체의 개별 요소가 아닌 전체 개체를 기준으로 차단 또는 차단 금지할 수 있습니다. TID를 사용하여 개별 기준(즉, 단순한 지표 또는 개별 관찰 가능 개체)의 필터링 작업을 구성할 수 있습니다.
- **TID** 구성 변경에는 재구축이 필요 없습니다 - 액세스 제어 정책에서 보안 인텔리전스 설정을 수정한 후에는 변경된 구성을 매니지드 디바이스에 다시 구축해야 합니다. TID를 사용하면 액세스 제어 정책을 매니지드 디바이스에 처음 구축한 후 재구축 없이 소스, 지표, 관찰 가능 개체를 구성할 수 있으며, 시스템은 새로운 TID 데이터를 요소에 자동으로 게시합니다.

보안 인텔리전스 또는 TID가 특정 인시던트를 처리할 수 있을 때 시스템이 수행하는 작업에 대한 자세한 내용은 TID-Firepower Management Center 작업 우선 순위, 25 페이지를 참조하십시오.

Threat Intelligence Director의 성능 영향

Firepower Management Center

경우에 따라 다음을 확인할 수 있습니다.

- 특별히 큰 STIX 소스를 수집하는 동안 시스템에 약간의 성능 문제가 발생할 수 있으며, 수집이 끝날 때까지 예상보다 시간이 더 걸릴 수 있습니다.

- 새롭거나 수정된 TID 데이터를 요소에 게시하는 데 최대 15분이 걸릴 수 있습니다.

매니지드 디바이스

특별한 성능상 영향은 없습니다. TID가 성능에 미치는 영향은 Firepower Management Center 보안 인텔리전스 기능과 동일합니다.

Cisco Threat Intelligence Director(TID) 및 고가용성 구성

고사용성 구성인 액티브 Firepower Management Center에서 TID을 호스팅하는 경우, 시스템은 TID 설정과 TID 데이터를 스탠바이 Firepower Management Center에 동기화하지 않습니다. 페일오버 후 데이터를 복구할 수 있도록 액티브 Firepower Management Center에서 정기적인 TID 데이터 백업을 수행하는 것을 권장합니다.

자세한 내용은 TID 데이터 백업 및 복구 정보, 15 페이지를 참조하십시오.

TID(Threat Intelligence Director) 요구 사항 및 사전 요건

모델 지원

Any(모든 상태)

지원되는 도메인

모든

사용자 역할

관리자

TID(Threat Intelligence Director) 사용자

추가 요구 사항

다음 주제에서는 Threat Intelligence Director를 사용하기 위한 추가 요구 사항에 대해 설명합니다.

플랫폼, 요소 및 라이선스 요구 사항

호스팅 플랫폼

물리적/가상 Firepower Management Center에서 TID를 호스팅할 수 있습니다.

- Firepower System 버전 6.2.2 이상 실행.
- 최소 15GB의 메모리로 구성.
- REST API 액세스가 활성화되도록 구성. REST API 액세스 활성화의 내용을 참조하십시오.

요소

Firepower System 버전 6.2.2 이상을 실행하는 Firepower Management Center 매니지드 디바이스는 TID 요소로 사용할 수 있습니다.

라이선싱

SHA-256 관찰 가능 개체 게시에 대한 파일 정책을 구성하려면 Firepower System에 악성코드 라이선스(기본 또는 스마트)가 필요합니다.

자세한 내용은 지원할 정책 구성 TID, 7 페이지 및 Firepower 라이선스 정보의 내용을 참조하십시오.

소스 요구 사항

소스 유형 요구 사항:

STIX

파일은 STIX 버전 1.0, 1.1, 1.1.1 또는 1.2여야 하며, STIX 설명서 (http://stixproject.github.io/documentation/suggested-practices/)의 지침을 준수해야 합니다.

STIX 파일에는 복잡한 지표가 포함될 수 있습니다.

URL 다운로드 또는 파일 업로드를 통해 설정할 경우, STIX 파일의 최대 크기는 40MB입니다. 이보다 큰 STIX 파일이 있으면 TAXII 서버를 사용하는 것이 좋습니다.

플랫 파일

파일은 행당 하나의 관찰 가능 개체가 있는 ASCII 텍스트 파일이어야 합니다.

플랫 파일에는 간단한 지표만 포함됩니다(지표당 하나의 관찰 가능 개체).

플랫 파일의 최대 크기는 500MB입니다.

TID는 다음을 지원하지 않습니다.

- 관찰 가능 개체 값을 구분하는 구분 기호 문자(예: `observable,` 은 잘못되었습니다).
- 관찰 가능 개체 값 앞뒤에 오는 문자(예: `"observable"`은 잘못되었습니다).

각 파일에는 한 가지 유형의 콘텐츠만 포함되어야 합니다.

- `SHA-256` - SHA-256 해시 값.
- `Domain` - RFC 1035에서 정의된 도메인 이름.
- `URL` - RFC 1738에서 정의된 URL.

참고 TID 포트, 프로토콜 또는 인증 정보를 포함하는 모든 URL을 표준화하고 지표를 탐지할 때 표준화된 버전을 사용합니다. 예를 들어 TID는 다음 URL 중 하나를 표준화합니다.

```
http://example.com/index.htm
http://example.com:8080/index.htm
example.com:8080/index.htm
example.com/index.htm
```

주로 다룹니다.

```
example.com/index.htm
```

또는 예를 들어 TID는 다음 URL을 표준화합니다.

```
http://abc@example.com:8080/index.htm
```

as

```
abc@example.com/index.htm/
```

- `IPv4` - RFC 791에서 정의된 IPv4 주소.

  TID CIDR 블록을 허용하지 않습니다.

- `IPv6` - RFC 4291에서 정의된 IPv6 주소.

  TID 프리픽스 길이를 허용하지 않습니다.

설정 방법 Cisco Threat Intelligence Director(TID)

참고 TID 구성 또는 작업 도중 문제가 발생하면 문제 해결 Cisco Threat Intelligence Director(TID), 44 페이지를 참조하십시오.

프로시저

단계 **1** 설치가 TID 실행을 위한 요구 사항을 충족하는지 확인합니다.

플랫폼, 요소 및 라이선스 요구 사항, 4 페이지의 내용을 참조하십시오.

단계 **2** 매니지드 디바이스마다 TID 지원에 필요한 정책을 구성하고 이러한 정책을 디바이스에 구축합니다.

지원할 정책 구성 TID, 7 페이지의 내용을 참조하십시오.

인텔리전스 데이터 소스를 수집하기 전이나 후에 요소를 구성할 수 있습니다.

단계 **3** TID가 수집할 인텔리전스 소스를 구성합니다.

소스 요구 사항, 5 페이지과 데이터 소스 수집 옵션, 8 페이지의 항목을 참조하십시오.

단계 **4** 아직 게시하지 않은 경우, 데이터를 요소에 게시합니다. 소스, 지표 또는 관찰 가능 개체 수준에서 TID 데이터 일시 중지 또는 게시, 41 페이지의 내용을 참조하십시오.

다음에 수행할 작업

- 정기적으로 예약된 백업에 TID를 포함시킵니다. TID 데이터 백업 및 복구 정보, 15 페이지의 내용을 참조하십시오.

  Firepower Management Center 구축이 고가용성(HA) 구성인 경우, Cisco Threat Intelligence Director(TID) 및 고가용성 구성도 참조하십시오.

- (선택 사항) 원하는 경우, TID 기능에 대한 관리자 액세스 권한을 부여합니다. TID 액세스 권한이 있는 사용자 역할, 15 페이지 및 Firepower System 사용자 관리FMC의 사용자 계정를 참조하십시오.

- 작업 중 필요에 따라 구성을 미세 조정합니다. 예를 들어 오탐 인시던트를 생성하는 관찰 가능 개체를 차단 금지 목록에 추가합니다. Cisco Threat Intelligence Director(TID) 구성 보기 및 변경, 28 페이지의 내용을 참조하십시오.

지원할 정책 구성 **TID**

Firepower Management Center의 TID 데이터를 매니지드 디바이스(요소)에 게시하려면 액세스 제어 정책을 구성해야 합니다. 또한 관찰과 Firepower Management Center 이벤트 생성을 최대화하도록 액세스 제어 정책을 구성하는 것이 좋습니다.

TID를 지원할 매니지드 디바이스마다 아래의 단계를 수행하여 연결된 액세스 제어 정책을 구성합니다.

데이터가 게시된 후 TID를 사용하도록 구성된 요소는 현재 게시된 모든 관찰 가능 개체를 자동으로 수신합니다.

프로시저

단계 **1** 액세스 제어 정책의 **Advanced Settings(**고급 설정**)**에서 **Enable Threat Intelligence Director(Threat Intelligence Director** 활성화**)** 확인란이 선택되어 있는지 확인합니다. 이 옵션은 기본적으로 활성화되어 있습니다.

자세한 내용은 액세스 제어 정책 고급 설정를 참고하십시오.

단계 **2** 규칙이 아직 없다면 액세스 제어 정책에 규칙을 추가합니다. TID에서는 액세스 제어 정책이 적어도 하나의 규칙을 지정해야 합니다.

자세한 내용은 기본 액세스 제어 정책 만들기를 참고하십시오.

단계 **3** **Intrusion Prevention(**침입 방지**)**을 액세스 제어 정책의 기본 작업으로 선택하고 TID 탐지를 위해 트래픽을 해독하려는 경우, SSL 정책을 액세스 제어 정책에 연결합니다(액세스 제어에 다른 정책 연결 참조).

단계 **4** `SHA-256` 관찰 가능 개체가 관찰 및 Firepower Management Center 이벤트를 생성하도록 하려면,

a) 하나 이상의 **Malware Cloud Lookup(**악성코드 클라우드 조회**)** 또는 **Block Malware(**악성코드 차단**)** 파일 규칙이 포함된 파일 정책을 생성합니다.

자세한 내용은 파일 정책 구성를 참고하십시오.

b) 이 파일 정책을 액세스 제어 정책의 하나 이상의 규칙과 연결합니다.

단계 **5** `IPv4`, `IPv6`, `URL` 또는 `Domain Name`(도메인 이름) 관찰이 연결 및 보안 인텔리전스 이벤트를 생성하도록 하려면 액세스 제어 정책에서 연결 및 보안 인텔리전스 로깅을 활성화합니다.

a) 파일 정책을 호출한 액세스 제어 규칙에서 **Log at End of Connection(**연결 종료 시 로깅**)** 및 **File Events: Log Files(**파일 이벤트**:** 로그 파일**)**를 활성화합니다(아직 활성화되지 않은 경우).

자세한 내용은 액세스 제어 규칙으로 연결 로깅를 참고하십시오.

b) 보안 인텔리전스 설정에서 기본 로깅(**DNS Policy(DNS** 정책**)**, **Networks(**네트워크**)**, **URLs(URL)**)이 활성화되어 있는지 확인합니다.

자세한 내용은 보안 인텔리전스로 연결 로깅를 참고하십시오.

단계 **6** 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축의 내용을 참조하십시오.

다음에 수행할 작업

다음에서 나머지 항목 완료 설정 방법 Cisco Threat Intelligence Director(TID), 6 페이지

데이터 소스 수집 옵션

사용하려는 데이터 유형 및 전달 메커니즘에 따라 구성 옵션을 선택합니다.

이러한 데이터 유형에 대한 자세한 내용은 소스 요구 사항, 5 페이지를 참조하십시오.

표 *1:* 데이터 소스 수집 옵션

데이터 유형	수집 옵션
STIX	• TAXII 서버에서 STIX 피드 수집: 소스로 사용할 TAXII 피드 가져오기, 9 페이지의 내용을 참조하십시오. • URL에서 STIX 데이터 다운로드: URL에서 소스 가져오기, 10 페이지의 내용을 참조하십시오. • STIX 파일 업로드: 소스로 사용할 로컬 파일 업로드, 12 페이지의 내용을 참조하십시오.
플랫 파일	• URL에서 데이터 다운로드: URL에서 소스 가져오기, 10 페이지의 내용을 참조하십시오. • 플랫 파일 업로드: 소스로 사용할 로컬 파일 업로드, 12 페이지의 내용을 참조하십시오.

소스로 사용할 **TAXII** 피드 가져오기

TID 구성 또는 작업 도중 문제가 발생하면 다음을 참조하십시오. 문제 해결 Cisco Threat Intelligence Director(TID), 44 페이지

프로시저

단계 **1** 소스가 다음의 요구 사항을 충족하는지 확인합니다 소스 요구 사항, 5 페이지

단계 **2** **Intelligence(**인텔리전스**)** > **Sources(**소스**)**를 선택합니다.

단계 **3** 추가(+) 버튼을 클릭합니다.

단계 **4** 소스의 `Delivery(전달)` 방법으로 **TAXII**를 선택합니다.

단계 **5** 정보를 입력합니다.

- 호스트 서버가 암호화된 연결을 요구하는 경우, TID 소스의 TLS/SSL 설정 구성, 13 페이지에 설명된 대로 **SSL Settings(SSL** 설정**)**를 구성합니다.
- TAXII 소스의 **Action(**작업**)** 선택 항목은 변경할 수 없습니다.

  `Block(차단)`은 TAXII 소스의 **Action(**작업**)** 옵션이 아닙니다. STIX 데이터에는 시스템이 차단할 수 없는 복잡한 지표가 포함될 수 있기 때문입니다. 디바이스(요소)는 단일 관찰 가능 개체를 저장하고 이에 기반하여 작업을 수행하며, 여러 관찰 가능 개체에 기반하여 작업을 수행할 수 없습니다.

하지만 수집 후에는 소스에서 얻은 개별 관찰 가능 개체와 간단한 지표를 차단할 수 있습니다. 자세한 내용은 소스, 지표 또는 관찰 가능 개체 수준에서 TID 작업 수정, 39 페이지를 참고하십시오.

- 피드 목록이 로드되려면 시간이 약간 걸릴 수 있습니다.
- **Update Every(**다음 간격으로 업데이트**)** 간격은 TID가 TAXII 소스에서 업데이트를 가져오는 빈도를 지정합니다.

  데이터 소스가 적절히 업데이트되는 업데이트 빈도를 설정하십시오. 예를 들어 소스가 하루에 3번 업데이트되는 경우, 최신 데이터를 정기적으로 캡처하려면 1440/3 또는 480분으로 업데이트 간격을 설정합니다.
- **TTL**로 지정한 일 수가 지나면 TID는 다음을 삭제합니다.
  - 후속 소스 업데이트에 포함되지 않은 소스의 모든 지표.
  - 남아 있는 지표가 참조하지 않는 모든 관찰 가능 개체.

단계 **6** 즉시 요소에 게시하려면 **Publish(**게시**)** 슬라이더( )가 활성화되어 있는지 확인합니다.

이 옵션이 활성화되면 시스템은 초기 소스 데이터 및 모든 후속 변경 사항을 자동으로 게시합니다.

자세한 내용은 소스, 지표 또는 관찰 가능 개체 수준에서 TID 데이터 일시 중지 또는 게시, 41 페이지 섹션을 참조해 주십시오.

단계 **7** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- TAXII 피드에는 많은 양의 데이터가 포함될 수 있으므로 시스템이 모든 데이터를 수집하려면 시간이 걸릴 수 있습니다. 수집 상태를 보려면 Source(소스) 페이지를 새로 고칩니다.
- 이 소스에 대한 오류가 표시되면 마우스 포인터를 상태 아이콘 위로 가져가 세부 정보를 확인합니다.
- 초기 TID 구성을 수행하는 경우, 설정 방법 Cisco Threat Intelligence Director(TID), 6 페이지로 돌아갑니다.

URL에서 소스 가져오기

TID가 호스트에서 파일을 가져오도록 하려면 URL 소스를 구성합니다.

TID 구성 또는 작업 도중 문제가 발생하면 다음을 참조하십시오. 문제 해결 Cisco Threat Intelligence Director(TID), 44 페이지

프로시저

단계 **1** 소스가 다음의 요구 사항을 충족하는지 확인합니다 소스 요구 사항, 5 페이지

단계 **2** **Intelligence(**인텔리전스**)** > **Sources(**소스**)**를 선택합니다.

단계 **3** 추가(+) 버튼을 클릭합니다.

단계 **4** 소스의 `Delivery(전달)` 방법으로 **URL**을 선택합니다.

단계 **5** 양식을 작성합니다.

- 플랫 파일을 수집하는 경우, 소스에 포함된 데이터를 설명하는 **Type(**유형**)**을 선택합니다.
- 호스트 서버가 암호화된 연결을 요구하는 경우, TID 소스의 TLS/SSL 설정 구성, 13 페이지에 설명된 대로 **SSL Settings(SSL** 설정**)**를 구성합니다.
- Name(이름): 지표에 기반한 인시던트 정렬 및 처리를 TID 단순화하려면 소스에서 일관된 명명 체계를 사용합니다. 예를 들어 <source>-<type>.

  소스 이름을 포함하면 추가 정보 또는 피드백을 위해 소스로 돌아가기가 단순화됩니다.

  이름을 일관되게 입력해야 합니다. 예를 들어 IPv4 주소가 있는 소스에는 항상 IPV4(IPv4 또는 ipv4 또는 IP_v4 또는 IP_V4 또는 ip-v4 또는 IP-v4, IP-V4 등이 아니라)를 사용할 수 있습니다.
- STIX 파일을 수집하는 경우, `Block(차단)`은 **Action(**작업**)** 옵션이 아닙니다. STIX 데이터에는 시스템이 차단할 수 없는 복잡한 지표가 포함될 수 있기 때문입니다. 디바이스(요소)는 단일 관찰 가능 개체를 저장하고 이에 기반하여 작업을 수행하며, 여러 관찰 가능 개체에 기반하여 작업을 수행할 수 없습니다.

  하지만 수집 후에는 소스에서 얻은 개별 관찰 가능 개체와 간단한 지표를 차단할 수 있습니다. 자세한 내용은 소스, 지표 또는 관찰 가능 개체 수준에서 TID 작업 수정, 39 페이지를 참고하십시오.
- 데이터 소스가 적절히 업데이트되는 업데이트 빈도를 설정하십시오. 예를 들어 소스가 하루에 3번 업데이트되는 경우, 최신 데이터를 정기적으로 캡처하려면 1440/3 또는 480분으로 업데이트 간격을 설정합니다.
- **TTL** 간격으로 지정한 일 수가 지나면 TID는 다음을 삭제합니다.
  - 후속 소스 업데이트에 포함되지 않은 소스의 모든 지표.
  - 남아 있는 지표가 참조하지 않는 모든 관찰 가능 개체.

단계 **6** 즉시 요소에 게시하려면 **Publish(**게시**)** 슬라이더( )가 활성화되어 있는지 확인합니다.

이 옵션이 활성화되면 시스템은 초기 소스 데이터 및 모든 후속 변경 사항을 자동으로 게시합니다.

자세한 내용은 소스, 지표 또는 관찰 가능 개체 수준에서 TID 데이터 일시 중지 또는 게시, 41 페이지 섹션을 참조해 주십시오.

단계 **7** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 수집 상태를 보려면 Source(소스) 페이지를 새로 고칩니다. 오류가 표시되면 마우스 포인터를 상태 아이콘 위로 가져가 세부 정보를 확인합니다.
- 초기 TID 구성을 수행하는 경우, 설정 방법 Cisco Threat Intelligence Director(TID), 6 페이지로 돌아갑니다.

소스로 사용할 로컬 파일 업로드

이 절차는 로컬 파일의 일회성 수동 업로드에 사용하십시오.

STIX 파일을 수집할 때 TID는 STIX 파일의 콘텐츠에서 간단하거나 복잡한 지표를 생성합니다.

플랫 파일을 수집할 때 TID는 파일의 관찰 가능 개체 값마다 간단한 지표를 생성합니다.

TID 구성 또는 작업 도중 문제가 발생하면 문제 해결 Cisco Threat Intelligence Director(TID), 44 페이지를 참조하십시오.

프로시저

단계 **1** 파일이 다음의 요구 사항을 충족하는지 확인합니다. 소스 요구 사항, 5 페이지

단계 **2** **Intelligence(**인텔리전스**)** > **Sources(**소스**)**를 선택합니다.

단계 **3** 추가(➕) 버튼을 클릭합니다.

단계 **4** 소스의 `Delivery(전달)` 방법으로 **Upload(**업로드**)**를 선택합니다.

단계 **5** 양식을 작성합니다.

- 플랫 파일을 업로드하는 경우 소스에 포함된 데이터를 설명하는 **Type(**유형**)**을 선택합니다.
- Name(이름): 지표에 기반한 인시던트 정렬 및 처리를 TID 단순화하려면 소스에서 일관된 명명 체계를 사용합니다. 예를 들어 <source>-<type>.

  소스 이름을 포함하면 추가 정보 또는 피드백을 위해 소스로 돌아가기가 단순화됩니다.

  이름을 일관되게 입력해야 합니다. 예를 들어 IPv4 주소가 있는 소스에는 항상 IPV4(IPv4 또는 ipv4 또는 IP_v4 또는 IP_V4 또는 ip-v4 또는 IP-v4, IP-V4 등이 아니라)를 사용할 수 있습니다.
- STIX 파일을 업로드하는 경우, `Block(차단)`은 **Action(**작업**)** 옵션이 아닙니다. STIX 데이터에는 복잡한 지표가 포함될 수 있기 때문입니다. 디바이스(요소)는 단일 관찰 가능 개체를 저장하고 이에 기반하여 작업을 수행하며, 여러 관찰 가능 개체에 기반하여 작업을 수행할 수 없습니다.

  하지만 지표 또는 관찰 가능 개체 수준에서 간단한 지표를 차단할 수 있습니다. 자세한 내용은 소스, 지표 또는 관찰 가능 개체 수준에서 TID 작업 수정, 39 페이지를 참고하십시오.
- **TTL** 간격으로 지정한 일 수가 지나면 TID는 다음을 삭제합니다.
  - 후속 업로드에 포함되지 않은 소스의 모든 지표.
  - 남아 있는 지표가 참조하지 않는 모든 관찰 가능 개체.

단계 **6** 즉시 요소에 게시하려면 **Publish(**게시**)** 슬라이더( )가 활성화되어 있는지 확인합니다.

수집 시 소스를 게시하지 않으면 나중에 모든 소스를 한 번에 게시할 수 없으며, 대신 각 관찰 가능 개체를 개별적으로 게시해야 합니다. 소스, 지표 또는 관찰 가능 개체 수준에서 TID 데이터 일시 중지 또는 게시, 41 페이지를 참조하십시오.

단계 **7** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 수집 상태를 보려면 Source(소스) 페이지를 새로 고칩니다. 오류가 표시되면 마우스 포인터를 상태 아이콘 위로 가져가 세부 정보를 확인합니다.
- 초기 TID 구성을 수행하는 경우, 설정 방법 Cisco Threat Intelligence Director(TID), 6 페이지로 돌아갑니다.

중복 표시기 처리

하나의 지표가 여러 소스에 포함된 경우, 다음과 같은 상황이 발생할 수 있습니다.

- 플랫 파일 소스의 지표 – 지표의 인스턴스마다 하나씩 인시던트를 생성하므로 특정 위협의 1회 발생으로 여러 인스턴스가 생성될 수 있습니다.
- STIX 소스의 지표 – 서로 다른 STIX 소스의 지표가 동일한 ID를 공유하는 경우, 이러한 지표를 포함하는 소스의 수에 상관없이 해당 지표에 대해 하나의 인시던트만 생성됩니다.

이후의 중복 인시던트를 방지하려면 중복된 지표 하나를 제외하고 모든 게시를 일시 중지하십시오. 소스, 지표 또는 관찰 가능 개체 수준에서 TID 데이터 일시 중지 또는 게시, 41 페이지의 내용을 참조하십시오.

TID 소스의 TLS/SSL 설정 구성

호스트 서버가 암호화된 연결을 요구하는 경우, **SSL Settings(SSL** 설정**)**를 구성합니다.

시작하기 전에

- 소스로 사용할 TAXII 피드 가져오기, 9 페이지 또는 URL에서 소스 가져오기, 10 페이지에 설명된 대로 `TAXII` 또는 `URL` 소스 구성을 시작합니다.

프로시저

단계 **1** **Edit Source(**소스 편집**)** 대화 상자에서 **SSL Settings(SSL** 설정**)** 섹션을 확장합니다.

단계 **2** 서버 인증서가 자체 서명된 경우:

a) **Self-Signed Certificate(**자체 서명 인증서**)**를 활성화합니다.

b) **SSL Hostname Verification(SSL** 호스트네임 확인**)** 방법을 선택합니다.

- `Strict(엄격)` - TID에서 소스 **URL**이 서버 인증서에서 제공된 호스트네임과 일치해야 합니다.

  호스트네임에 와일드카드가 포함된 경우, TID는 둘 이상의 서브도메인을 매칭할 수 없습니다.

- `Browser Compatible(브라우저 호환)` - TID에서 소스 **URL**이 서버 인증서에서 제공된 호스트네임과 일치해야 합니다.

  호스트네임에 와일드카드가 포함된 경우, TID는 모든 서브도메인을 매칭합니다.

- `Allow All(모두 허용)` - TID에서 소스 **URL**이 서버 인증서에서 제공된 호스트네임과 일치하지 않아도 됩니다.

예를 들어 `subdomain1.subdomain2.cisco.com`이 소스 **URL**이고 `*.cisco.com`이 서버 인증서에서 제공된 호스트네임인 경우:

- `Strict(엄격)` 호스트네임 확인이 실패합니다.
- `Browser Compatible(브라우저 호환)` 호스트네임 확인이 성공합니다.
- `Allow All(모두 허용)` 호스트네임 확인은 호스트네임 값을 완전히 무시합니다.

c) **Server Certificate(**서버 인증서**)**:

- PEM 인코딩된 자체 서명 서버 인증서에 액세스할 수 있는 경우, 텍스트 편집기에서 자체 서명 서버 인증서를 열고 `BEGIN CERTIFICATE` 및 `END CERTIFICATE` 행을 포함한 전체 텍스트 블록을 복사합니다. 이 전체 문자열을 필드에 입력합니다.
- 자체 서명 서버 인증서에 액세스할 수 없는 경우, 필드를 비워 둡니다. 소스를 저장한 후 TID는 서버에서 인증서를 검색합니다.

단계 **3** 서버가 사용자 인증서를 요구하는 경우:

a) **User Certificate(**사용자 인증서**)**를 입력합니다.

텍스트 편집기에서 PEM 인코딩된 인증서를 열고 `BEGIN CERTIFICATE` 및 `END CERTIFICATE` 행이 포함된 전체 텍스트 블록을 복사합니다. 이 전체 문자열을 필드에 입력합니다.

b) **User Private Key(**사용자 개인 키**)**를 입력합니다.

텍스트 편집기에서 개인 키 파일을 열고 `BEGIN RSA PRIVATE KEY` 및 `END RSA PRIVATE KEY` 행이 포함된 전체 텍스트 블록을 복사합니다. 이 전체 문자열을 필드에 입력합니다.

다음에 수행할 작업

- 인증서의 만료 날짜를 적어 둡니다. 현재 인증서가 만료된 후 새 서버 인증서를 입력하도록 일정 알림을 설정하는 것이 좋습니다.
- 계속 소스를 구성합니다.

• 소스로 사용할 TAXII 피드 가져오기, 9 페이지
• URL에서 소스 가져오기, 10 페이지

TID 액세스 권한이 있는 사용자 역할

Firepower Management Center 사용자 계정을 사용하여 TID 메뉴 및 페이지에 액세스할 수 있습니다.

- **Admin** 또는 **Threat Intelligence Director User** 사용자 역할이 있는 계정.
- **Intelligence** 권한을 포함하는 맞춤형 사용자 역할이 있는 계정.

또한 **Admin**, **Access Admin** 또는 **Network Admin** 사용자 역할이 있는 Firepower Management Center 사용자 계정을 사용하여 액세스 제어 정책에서 TID를 활성화하거나 비활성화할 수 있습니다.

사용자 계정에 대한 자세한 내용은 Firepower System 사용자 관리FMC의 사용자 계정를 참조하십시오.

TID 데이터 백업 및 복구 정보

Firepower Management Center를 사용하여 TID에 필요한 모든 데이터(요소 데이터, 보안 인텔리전스 이벤트, 연결 이벤트, TID 구성 및 TID 데이터)를 백업하고 복구할 수 있습니다. 자세한 내용은 백업 및 복원의 내용을 참고하십시오.

참고 고가용성 컨피그레이션인 활성 Firepower Management Center에서 TID를 호스팅하는 경우, 시스템은 TID 구성과 TID 데이터를 대기 Firepower Management Center에 동기화하지 않습니다. 페일오버 후 데이터를 복구할 수 있도록 활성 Firepower Management Center에서 정기적인 TID 데이터 백업을 수행하는 것을 권장합니다.

표 *2: TID*-관련된 파일 백업 및 복구 내용

TID-관련된 파일 내용	선택 항목 백업	선택 항목 복구
요소 데이터	구성 백업	구성 데이터 복구
Firepower Management Center 이벤트 날짜	이벤트 백업	이벤트 데이터 복원
TID 구성 및 TID 데이터	**Threat Intelligence Director** 백업	**Threat Intelligense Director** 데이터 복구

TID 인시던트 및 관찰 데이터 분석

TID 요소에 의해 생성된 인시던트 및 관찰 데이터를 분석하려면 Incident(인시던트) 테이블 및 Incident Details(인시던트 세부 사항) 페이지를 사용합니다.

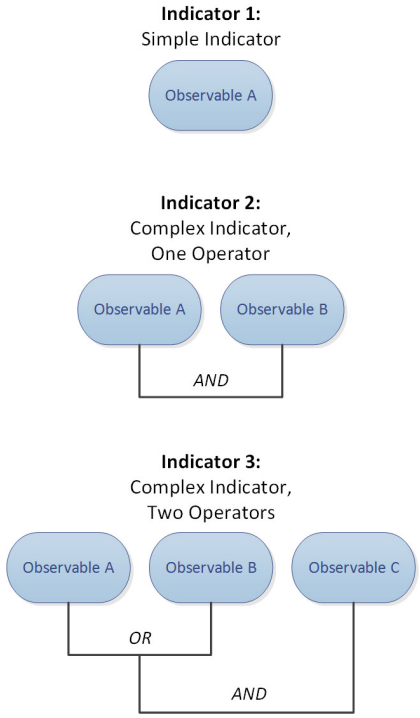
관찰 및 사고 생성

TID 지표의 첫 번째 관찰 가능 개체를 트래픽에서 볼 때 인시던트를 생성합니다. 간단한 지표는 단일 관찰 후 완전히 실현됩니다. 복잡한 지표는 하나 이상의 추가 관찰이 패턴을 충족할 때까지는 부분적으로 실현됩니다. 복잡한 지표는 단일 트랜잭션 도중에 반드시 충족될 필요는 없습니다. 각 관찰 가능 개체는 시간이 지나면서 서로 다른 트랜잭션에 의해 별도로 충족될 수 있습니다.

참고 지표의 패턴을 평가할 때 TID은 지원되지 않고 유효하지 않은 개체 그리고 Do Not Block(차단 금지) 리스트에 추가된 관찰 가능 개체는 무시합니다.

인시던트가 완전히 실현된 후 후속 관찰이 새로운 인시던트를 트리거합니다.

그림 *3:* 예*:* 지표 패턴



TID가 위의 예에서 관찰 가능 개체를 수집했고 관찰 가능 개체가 순서대로 보인 경우, 인시던트 생성은 다음과 같이 진행됩니다.

1. 시스템이 트래픽에서 관찰 가능 개체 A를 식별하는 경우, TID:

- 지표 1의 완전히 실현된 인시던트를 생성합니다.
- 지표 2 및 지표 3의 부분적으로 실현된 인시던트를 생성합니다.

2. 시스템이 트래픽에서 관찰 가능 개체 B를 식별하는 경우, TID:
   - 패턴이 충족되었기 때문에 인시던트를 지표 2의 완전 실현으로 업데이트합니다.
   - 인시던트를 지표 3의 부분적 실현으로 업데이트합니다.
3. 시스템이 트래픽에서 관찰 가능 개체 C를 식별하는 경우, TID:
   - 패턴이 충족되었기 때문에 인시던트를 지표 3의 완전 실현으로 업데이트합니다.
4. 시스템이 관찰 가능 개체 A를 두 번째 식별하는 경우, TID:
   - 지표 1의 완전히 실현된 새 인시던트를 생성합니다.
   - 지표 2 및 지표 3의 부분적으로 실현된 인시던트를 생성합니다.

특정 지표가 여러 소스에 존재하는 경우, 중복된 인시던트를 볼 수 있습니다. 자세한 내용은 문제 해결 Cisco Threat Intelligence Director(TID), 44 페이지를 참고하십시오.

인시던트는 실제 트래픽에 의해서만 생성됩니다. URL B에 대한 관찰 가능 개체가 있고 사용자가 URL B에 대한 링크를 표시하는 URL A를 방문하는 경우, 사용자가 URL B 링크를 클릭하지 않는 한 인시던트가 발생하지 않습니다.

사고 보기 및 관리

Incidents(인시던트) 페이지에는 TID에 대한 요약 정보가 표시됩니다(사고 요약 정보, 18 페이지 참조).

시작하기 전에

- 설정 방법 Cisco Threat Intelligence Director(TID), 6 페이지에 설명된 대로 기능을 구성합니다.
- 관찰 및 사고 생성, 16 페이지에 설명된 대로 관찰 및 인시던트 생성을 이해합니다.

프로시저

단계 **1** **Intelligence(**인텔리전스**)** > **Incidents(**인시던트**)**를 선택합니다.

단계 **2** 인시던트 보기:

- 하나 이상의 필터를 추가하려면 필터(🔍)을 클릭합니다. 기본 필터는 6시간입니다. 자세한 내용은 테이블 보기에서 TID 데이터 필터링, 37 페이지를 참고하십시오.
- TID에 의해 인시던트가 마지막으로 업데이트된 날짜와 시간을 보려면 **Last Updated(**마지막 업데이트**)** 열의 값 위에 마우스 커서를 올려놓습니다.

- 인시던트에 연결된 지표에 대한 자세한 정보를 보려면 **Indicator Name(**지표 이름**)** 열의 텍스트를 클릭합니다(지표 보기 및 관리, 32 페이지 참조).

단계 **3** **Incident ID(**인시던트 **ID)** 열의 값을 클릭하여 추가 세부 정보를 봅니다.

표시되는 세부 정보에 대한 설명은 사고 세부 사항, 19 페이지를 참조하십시오.

- 지표 세부 정보를 보려면 창 하단 섹션의 **Indicator(**지표**)** 제목 아래에서 지표 값(예: IP 주소 또는 SHA-256 값)을 클릭합니다.
- 관찰 세부 정보를 보려면 **Observations(**관찰**)** 제목 바로 아래 있는 관찰 왼쪽 화살표를 클릭합니다.
- Security Intelligence Events(보안 인텔리전스 이벤트) 페이지에서 이 인시던트를 보려면 관찰 세부 정보 섹션에서 **Events(**이벤트**)** 링크를 클릭합니다.

단계 **4** (선택 사항) 인시던트 세부 정보 페이지에서 설명 정보를 입력합니다.

팁: 아래 옵션의 일관성과 효용성을 최대화하려면 명명 규칙, 카테고리 선택, 신뢰도 기준을 미리 계획하고 문서화하십시오.

- **Name(**이름**)**, **Description(**설명**)**, **Category(**카테고리**)** 필드에 원하는 값을 입력합니다.
- **Confidence(**신뢰도**)**의 등급 레벨을 클릭합니다.
- **Status(**상태**)** 필드의 드롭다운 목록에서 값을 선택하여 인시던트에 대한 조사 상태를 표시합니다.

사고 요약 정보

Incident(인시던트) 페이지에는 모든 TID 인시던트의 요약 정보가 표시됩니다.

표 ***3:*** 사고 요약 정보

필드	설명
Last Updated(마지막 업데이트 날짜**)**	시스템 또는 사용자가 인시던트를 마지막으로 업데이트한 후 경과한 일 수입니다. 업데이트 날짜와 시간을 보려면 이 열의 값 위에 마우스 커서를 올려놓습니다.

필드	설명
인시던트 **ID**	인시던트의 고유 식별자입니다. 이 ID는 다음 형식을 갖습니다. `<type>-<date>-<number>` • `<type>` - 인시던트에 관련된 지표 또는 관찰 가능 개체의 유형. 간단한 지표의 경우, 이 값은 관찰 가능 개체 유형(`IP`(IPv4 또는 IPv6), `URL`(URL), `DOM`(도메인) 또는 `SHA`(SHA-256))을 나타냅니다. 복잡한 지표의 경우, 이 값은 `COM`입니다. • `<date>` - 인시던트가 생성된 날짜(*yyyymmdd*). • `<number>` - 일일 인시던트 번호, 즉 인시던트의 일일 발생 시퀀스 중 어디에서 인시던트가 발생하는지 지정하는 번호입니다. 이 시퀀스는 0부터 시작됩니다. 예를 들어 `DOM-20170828-10`은 해당 날짜에 생성된 11번째 인시던트입니다. 시스템은 식별자 옆에 인시던트가 부분적으로 실현되는지 완전히 실현되는지 보여주는 아이콘을 표시합니다. 자세한 내용은 관찰 및 사고 생성, 16 페이지를 참고하십시오.
지표 이름	인시던트에 관련된 지표의 이름입니다. 지표에 대한 추가 정보를 보려면 이 열의 값을 클릭합니다(지표 보기 및 관리, 32 페이지 참조).
유형	인시던트에 관련된 지표의 유형입니다. • 단일 관찰 가능 개체를 포함하는 지표는 데이터 유형(`URL`, `SHA-256` 등)을 표시합니다. • 둘 이상의 관찰 가능 개체를 포함하는 지표는 `Complex`로 표시됩니다.
수행한 작업	인시던트와 관련하여 시스템에서 수행한 작업입니다. 자세한 내용은 사고 세부 사항, 19 페이지를 참고하십시오.
상태	인시던트에 대한 조사의 상태입니다. 자세한 내용은 사고 세부 사항, 19 페이지를 참고하십시오.
삭제()	인시던트를 영구적으로 삭제하려면 이 아이콘을 클릭합니다.

사고 세부 사항

Indicdent Details(인시던트 세부 사항) 창에는 단일 TID 인시던트에 대한 정보가 표시됩니다. 이 창은 2개의 섹션으로 나뉩니다.

- 인시던트 세부 사항: 기본 정보, 19 페이지
- 사고 세부 사항: 지표 및 관찰, 21 페이지

인시던트 세부 사항: 기본 정보

Incident Details(인시던트 세부 사항) 창의 상단 섹션은 아래에 설명된 정보를 제공합니다.

표 *4: Basic Incident Information(*기본 인시던트 정보*)* 필드

필드	설명
Partially-Realized *IncidentID* 또는 **Fully-Realized** *IncidentID*	인시던트의 고유 식별자 외에 인시던트의 상태(부분적으로 실현 또는 완전히 실현)를 나타내는 아이콘입니다. 참고 인시던트의 상태를 확인할 때 TID는 지원되지 않으며 유효하지 않은 관찰 가능 개체와 차단 안 함 목록의 관찰 가능 개체를 무시합니다.
열림	인시던트를 마지막으로 업데이트한 날짜와 시간입니다.
이름	사용자가 직접 입력하는 선택적인 맞춤형 인시던트 이름입니다. 팁: Description(설명) 필드(창의 하단)에 소스의 정보가 있는 경우, 해당 필드의 정보를 사용하여 인시던트의 이름을 지정합니다.
설명	사용자가 직접 입력하는 선택적인 맞춤형 인시던트 설명입니다. 팁: Description(설명) 필드(창의 하단)에 소스의 정보가 있는 경우, 해당 필드의 정보를 사용하여 인시던트를 설명합니다.
감시	인시던트 내의 관찰 횟수입니다.
확신	인시던트의 상대적 중요성을 표시하기 위해 직접 선택할 수 있는 선택적 등급입니다.
수행한 작업	`Monitored(모니터링됨)`, `Blocked(차단됨)` 또는 `Partially Blocked(부분적으로 차단됨)`와 같이 시스템이 수행한 작업입니다. `Partially Blocked(부분적으로 차단됨)`는 인시던트에 `Monitored(모니터링됨)` 관찰과 `Blocked(차단됨)` 관찰이 모두 포함됨을 나타냅니다. 참고 **Action Taken(**수행한 작업**)**은 반드시 TID에서 선택한 작업이 아니라 시스템이 수행한 작업을 나타냅니다. 자세한 내용은 TID-Firepower Management Center 작업 우선 순위, 25 페이지를 참고하십시오.
카테고리	사용자가 인시던트에 직접 추가하는 선택적 맞춤형 태그 또는 키워드입니다.
상태	인시던트 분석의 현재 상태를 나타내는 값입니다. **Status(**상태**)**를 처음 변경하기 전까지 모든 인시던트는 `New(신규)`입니다. 이 필드는 선택 항목입니다. 조직의 요구 사항에 따라 다음과 같은 상태 값을 사용하는 것이 좋습니다. • `New(신규)` - 인시던트에 조사가 필요하지만 조사를 아직 시작하지 않았습니다. • `Open(열림)` - 현재 인시던트를 조사하고 있습니다. • `Closed(닫힘)` - 인시던트를 조사했고 조치를 취했습니다. • `Rejected(거부됨)` - 인시던트를 조사했고 취할 조치가 없다고 결정했습니다.

필드	설명
삭제( )	이 아이콘을 클릭하면 이 인시던트가 영구적으로 삭제됩니다.

사고 세부 사항: 지표 및 관찰

Incident Details(인시던트 세부 사항) 창의 하단 섹션은 지표 및 관찰 정보의 자세한 보기를 제공합니다. 이 정보는 **Indicator(**지표**)** 필드, 지표 패턴, **Observations(**관찰**)** 필드로 구성됩니다.

지표 섹션

처음으로 지표 세부 정보를 볼 때 이 섹션에는 지표 이름만 표시됩니다.

Indicator(지표) 페이지에서 지표를 보려면 지표 이름을 클릭합니다.

지표에서 나가지 않고 더 많은 지표 세부 정보를 보려면 지표 이름 옆의 아래쪽 화살표를 클릭합니다. 세부 사항 필드에는 다음이 포함됩니다.

표 ***5:*** 지표 필드

필드	설명
설명	소스에서 제공하는 지표 설명입니다.
소스	지표가 포함된 소스입니다. 전체 소스 세부 사항에 액세스하려면 이 링크를 클릭합니다.
만료	소스의 **TTL** 값에 따라 인시던트가 만료되는 날짜와 시간입니다.
조치	지표와 관련된 조치입니다. 자세한 내용은 소스, 지표 또는 관찰 가능 개체 수준에서 TID 작업 수정, 39 페이지를 참고하십시오.
게시	지표의 게시 설정입니다. 자세한 내용은 소스, 지표 또는 관찰 가능 개체 수준에서 TID 데이터 일시 중지 또는 게시, 41 페이지를 참고하십시오.
STIX 다운로드	소스 유형이 `STIX`인 경우, 이 버튼을 클릭하여 STIX 파일을 다운로드합니다.

지표 패턴

지표 패턴은 지표를 구성하는 관찰 가능 개체와 연산자를 그림으로 나타낸 것입니다. 연산자는 지표 내에서 관찰 가능 개체를 연결합니다. AND 관계는 **AND** 연산자로 표시됩니다. OR 관계는 **OR** 연산자로 또는 여러 관찰 가능 개체를 밀접히 그룹화하여 표시됩니다.

패턴의 관찰 가능 개체가 이미 보인 경우, 관찰 가능 개체 상자는 흰색입니다. 관찰 가능 개체가 아직 보이지 않은 경우, 관찰 가능 개체 상자는 회색입니다.

지표 패턴에서,

- **Whitelist(**화이트리스트**)** 버튼을 클릭하여 차단 안 함 목록에 관찰 가능 개체를 추가합니다. 이 아이콘은 흰색 및 회색 관찰 가능 개체 상자에 있습니다. 자세한 내용은 차단 금지 목록에 TID 관찰 가능 항목 추가 , 43 페이지를 참고하십시오.
- 흰색 관찰 가능 개체 상자 위에 커서를 올려놓으면 **Observations(**관찰**)** 섹션에서 관련 관찰이 강조 표시됩니다.
- 흰색 관찰 가능 개체 상자를 클릭하면 시스템은 **Observations(**관찰**)** 섹션에서 관련 관찰을 강조 표시하고, 해당 관찰을 보기로 스크롤하며(여러 관찰이 있는 경우), 해당 관찰의 상세한 표시를 확장합니다.
- 지표 패턴에서 회색 관찰 가능 개체 상자 위에 커서를 올려놓거나 클릭하면 **Observations(**관찰**)** 섹션에 아무 변화도 없습니다. 관찰 가능 개체가 보이지 않으므로 아직 표시할 관찰 세부 정보가 없습니다.

관찰 섹션

기본적으로 **Observations(**관찰**)** 섹션에는 다음을 포함한 요약 정보가 표시됩니다.

- 관찰을 트리거한 관찰 가능 개체의 유형(예를 들어 도메인)
- 관찰 가능 개체를 구성하는 데이터
- 관찰이 첫 번째 관찰인지 후속 관찰인지 여부(예를 들어 첫 번째 또는 세 번째)

참고 단일 관찰 가능 개체가 세 번 이상 보인 경우, TID는 첫 번째 및 마지막 관찰 세부 사항을 표시합니다. 중간 관찰에 대한 세부 사항은 사용할 수 없습니다.

- 관찰 날짜 및 시간
- 관찰 가능 개체에 대해 구성된 작업

Observations(관찰**)** 섹션에서 관찰 위에 커서를 올려놓으면 지표 패턴에서 관련된 관찰 가능 개체가 강조 표시됩니다.

Observations(관찰**)** 섹션에서 관찰을 클릭하면 시스템은 지표 패턴에서 관련된 관찰 가능 개체를 강조 표시하고 첫 번째 관련 가능 개체를 보기로 스크롤합니다(여러 관찰 가능 개체가 있는 경우). 관찰을 클릭하면 **Observations(**관찰**)** 섹션에서 관찰의 세부 사항이 확장됩니다.

관찰 세부 사항에는 다음 필드가 포함됩니다.

표 ***6:*** 관찰 세부 정보 필드

필드	설명
소스	관찰을 트리거한 트래픽의 소스 IP 주소와 포트입니다.

필드	설명
대상	관찰을 트리거한 트래픽의 대상 IP 주소와 포트입니다.
추가 정보	관찰을 트리거한 트래픽과 관련된 DNS 및 인증 정보입니다.
Events(이벤트**)**	클릭 가능한 이 링크에는 관찰이 연결, 보안 인텔리전스, 파일 또는 악성코드 이벤트를 생성했는지 표시됩니다. Firepower Management Center 이벤트 테이블의 이벤트를 보려면 링크를 클릭합니다(연결 이벤트 정보 참조).

TID 관찰에 대한 이벤트 보기

TID 관찰이 생성하는 Firepower Management Center 이벤트에 대한 자세한 내용은 Firepower Management Center 이벤트의 TID 관찰, 23 페이지를 참조하십시오.

TID 관련 이벤트에 대해 로깅되는 시스템 작업은 TID와 다른 Firepower Management Center 기능의 상호 작용에 따라 달라질 수 있습니다. 작업 우선 순위에 대한 자세한 내용은 TID-Firepower Management Center 작업 우선 순위, 25 페이지를 참조하십시오.

시작하기 전에

- 설정 방법 Cisco Threat Intelligence Director(TID), 6 페이지에 설명된 대로 기능을 구성합니다.
- 지원할 정책 구성 TID, 7 페이지에 설명된 대로 TID에 필요한 이벤트 로깅을 활성화했는지 확인합니다.

프로시저

단계 **1** **Intelligence(**인텔리전스**)** > **Incidents(**인시던트**)**를 선택합니다.

단계 **2** 인시던트의 **Incident ID(**인시던트 **ID)** 값을 클릭합니다.

단계 **3** 관찰 상자를 표시하려면 **Indicator(**지표**)** 섹션에서 관찰을 클릭합니다.

단계 **4** 관찰 상자 왼쪽 상단 모서리에 있는 화살표를 클릭하여 관찰 상자를 확장합니다.

단계 **5** 관찰 정보에서 **Events(**이벤트**)** 링크를 클릭합니다. 보안 인텔리전스 표시에 대한 자세한 내용은 연결 이벤트 정보를 참조하십시오.

Firepower Management Center 이벤트의 TID 관찰

액세스 제어 정책을 완전히 구성하면 TID 관찰은 다음 Firepower Management Center 이벤트를 생성합니다.

표 *7: Firepower Management Center* 관찰이 생성하는 이벤트

관찰 콘텐츠	연결 이벤트 테이블	보안 인텔리전스 이벤트 테이블	파일 이벤트 테이블	악성코드 이벤트 테이블
SHA-256	예	아니요	예	예, 속성이 악성코드 또는 맞춤형 탐지인 경우.
도메인 이름, **URL** 또는 **IPv4/IPv6**	Yes(예) TID 관련 연결 이벤트는 TID 관련 보안 인텔리전스 카테고리 값으로 식별됩니다.	Yes(예) TID 관련 보안 인텔리전스 이벤트는 TID 관련 보안 인텔리전스 카테고리 값으로 식별됩니다.	아니요	아니요

수행하는 작업에 영향을 미치는 요소

TID 관찰 가능 개체와 일치하는 트래픽이 탐지될 때 시스템이 수행하는 작업과 작업을 수행하는 시기는 여러 요인이 결정합니다.

- 보안 인텔리전스와 같은 기능은 TID 전에 작업을 수행합니다. 자세한 내용은 TID-Firepower Management Center 작업 우선 순위, 25 페이지 섹션을 참조해 주십시오.
- 일반적으로는 관찰 가능 개체에 대해 구성된 작업(상위 지표 또는 소스에 대해 구성된 작업과 다를 수 있음)이 수행됩니다.
- STIX 소스에는 복잡한 지표가 포함될 수 있으므로 소스에 대한 작업 설정은 Monitor(모니터링)으로만 설정할 수 있습니다. 하지만 STIX 피드 또는 파일에 포함된 개별적인 간단한 지표 또는 관찰 가능 개체는 Block(차단)으로 설정할 수 있습니다.
- 지표 및 관찰 가능 개체에 대한 작업 설정은 상속되거나 상속을 재정의하도록 개별적으로 구성될 수 있습니다. TID 구성의 상속, 37 페이지 및 소스, 지표 또는 관찰 가능 개체 수준에서 TID 작업 수정, 39 페이지를 참조하십시오.
- 아니면 실행 가능한 트래픽이 차단 안 함 목록에 있을 수 있습니다. 자세한 내용은 차단 금지 목록에 TID 관찰 가능 항목 추가, 43 페이지 섹션을 참조해 주십시오.
- 부분적으로 실현된 인시던트 및 완전히 실현된 인시던트에 대해 구성된 작업이 수행됩니다.
- 복잡한 지표에 기반하는 인시던트는 부분적으로 차단될 수 있습니다. 이는 지표에 모니터링되는 관찰과 차단된 관찰이 모두 포함된 경우에 발생할 수 있습니다.
- 게시를 일시 중지하면 시스템이 수행하는 작업에 영향을 미칩니다. 게시 일시 중지 정보, 40 페이지 및 소스, 지표 또는 관찰 가능 개체 수준에서 TID 데이터 일시 중지 또는 게시, 41 페이지를 참조하십시오.
- TID 기능을 일시 중지하면 모든 작업이 수행되지 않습니다. 기능을 다시 시작한 후 실행 가능한 데이터가 전과 다를 수 있습니다. 자세한 내용은 TID 일시 중지 및 요소에서 TID 데이터 제거, 41 페이지를 참조하십시오.

TID-Firepower Management Center 작업 우선 순위

TID 관찰 가능 개체 작업이 Firepower Management Center 정책 작업과 충돌하는 경우, 시스템은 다음과 같이 작업 우선 순위를 지정합니다.

- 보안 인텔리전스 차단 금지
- TID 차단
- 보안 인텔리전스 차단
- TID 모니터링
- 보안 인텔리전스 모니터링

구체적으로,

표 ***8: TID URL*** 관찰 가능 개체 작업 대 보안 인텔리전스 작업

설정: 보안 인텔리전스 작업	설정: **TID** 관찰 가능 개체 작업	**TID** 인시던트 필드: 수행한 작업	보안 인텔리전스 이벤트 필드:		
			조치	보안 인텔리전스 카테고리	이유
화이트리스트	Monitor(모니터링) 또는 Block(차단)	TID 인시던트 없음	보안 인텔리전스 이벤트 없음		
차단	모니터링	차단됨	차단	시스템 분석에서 결정. 다음 참조. 보안 인텔리전스 카테고리	URL 차단
	차단	차단됨	차단	TID URL 차단	URL 차단
모니터링	모니터링	모니터링됨	보안 인텔리전스 및 TID 후에 처리되는 액세스 제어 규칙에 의해 결정됩니다.	TID URL 모니터링	URL 모니터링
	차단	차단됨	차단	TID URL 차단	URL 차단

표 *9: TID IPv4/IPv6* 관찰 가능 개체 작업 대 보안 인텔리전스 작업

설정: 보안 인텔리전스 작업	설정: **TID** 관찰 가능 개체 작업	**TID** 인시던트 필드: 수행한 작업	보안 인텔리전스 이벤트 필드:		
			조치	보안 인텔리전스 카테고리	이유
화이트리스트	Monitor(모니터링) 또는 Block(차단)	TID 인시던트 없음	보안 인텔리전스 이벤트 없음		
차단	모니터링	TID 인시던트 없음	차단	시스템 분석에서 결정. 다음 참조. 보안 인텔리전스 카테고리	IP 차단
	차단	차단됨	차단	TID IPv4 차단 TID IPv6 차단	IP 차단
모니터링	모니터링	모니터링됨	보안 인텔리전스 및 TID 후에 처리되는 액세스 제어 규칙에 의해 결정됩니다.	TID IPv4 모니터링 TID IPv6 모니터링	IP Monitor
	차단	차단됨	차단	TID IPv4 차단 TID IPv6 차단	IP 차단

표 *10: TID* 도메인 이름 관찰 가능 개체 작업 대 *DNS* 정책 작업

설정: **DNS** 정책 작업	설정: **TID** 도메인 이름 관찰 가능 개체 작업	**TID**인시던트필드:수행한 작업	보안 인텔리전스 이벤트 필드:		
			조치	보안 인텔리전스 카테고리	이유
화이트리스트	Monitor(모니터링) 또는 Block(차단)	TID 인시던트 없음	보안 인텔리전스 이벤트 없음		
삭제, 도메인을 찾을 수 없음 싱크 홀 - 로그 싱크 홀 - 차단 및 로그	모니터링	차단됨	차단	시스템 분석에서 결정. 다음 참조. 보안 인텔리전스 카테고리	DNS 차단
	차단	차단됨	차단	TID 도메인 이름 차단	DNS 차단

설정: **DNS** 정책 작업	설정: **TID** 도메인 이름 관찰 가능 개체 작업	**TID**인시던트필드:수행한작업	보안 인텔리전스 이벤트 필드:		
			조치	보안 인텔리전스 카테고리	이유
모니터링	모니터링	모니터링됨	보안 인텔리전스 및 TID 후에 처리되는 액세스 제어 규칙에 의해 결정됩니다.	TID 도메인 이름 모니터링	DNS 모니터링
	차단	차단됨	차단	TID 도메인 이름 차단	DNS 차단

표 ***11: TID SHA-256*** 관찰 가능 개체 작업 대 악성코드 클라우드 조회 파일 정책

파일 속성	**TID SHA-256** 관찰 가능 개체 작업	**TID** 인시던트의 수행한 작업	파일 이벤트의 작업	악성코드 이벤트의 작업
정상	Monitor(모니터링) 또는 Block(차단)	모니터링됨	악성코드 클라우드 조회	해당 없음
악성코드	Monitor(모니터링) 또는 Block(차단)	모니터링됨	악성코드 클라우드 조회	해당 없음
Custom	Monitor(모니터링) 또는 Block(차단)	모니터링됨	• 악성코드 클라우드 조회, SHA-256이 맞춤형 탐지 목록에 없는 경우. • 맞춤형 탐지, SHA-256이 맞춤형 탐지 목록에 있는 경우.	• 악성코드 클라우드 조회, SHA-256이 맞춤형 탐지 목록에 없는 경우. • 맞춤형 탐지, SHA-256이 맞춤형 탐지 목록에 있는 경우.
알 수 없음	Monitor(모니터링) 또는 Block(차단)	모니터링됨	악성코드 클라우드 조회	해당 없음

참고 TID 매칭은 시스템이 동적 분석을 위해 파일을 전송하기 전에 이루어집니다.

표 ***12: TID SHA-256*** 관찰 가능 개체 작업 대 악성코드 파일 차단 정책

파일 속성	**TID SHA-256** 관찰 가능 개체 작업	**TID** 인시던트의 수행한 작업	파일 이벤트의 작업	악성코드 이벤트의 작업
Clean(안전) 또는 Unknown(알 수 없음)	모니터링	모니터링됨	악성코드 클라우드 조회	해당 없음
	차단	차단됨	• TID 차단, SHA-256이 맞춤형 탐지 목록에 없는 경우. 수정된 파일 속성은 Custom(맞춤형) 입니다. • 맞춤형 탐지 차단, SHA-256이 맞춤형 탐지 목록에 있는 경우.	TID 차단 수정된 파일 속성은 Custom(맞춤형) 입니다.
Malware(악성코드) 또는 Custom(맞춤형)	모니터링	차단됨	악성코드 차단	악성코드 차단
	차단	차단됨	• TID 차단, SHA-256이 맞춤형 탐지 목록에 없는 경우. 수정된 파일 속성은 Custom(맞춤형) 입니다. • 맞춤형 탐지 차단, SHA-256이 맞춤형 탐지 목록에 있는 경우.	TID 차단 수정된 파일 속성은 Custom(맞춤형) 입니다.

Cisco Threat Intelligence Director(TID) 구성 보기 및 변경

다음 정보를 사용하여 구성을 검토하고 필요에 따라 미세 조정합니다.

요소(매니지드 디바이스)의 TID 상태 보기

Firepower Management Center에 매니지드 디바이스로 등록된 모든 디바이스는 Elements(요소) 페이지에 자동으로 표시됩니다. 올바로 구성된 모든 요소(지원할 정책 구성 TID, 7 페이지에 지정된 대로)는 요소가 추가되기 전에 수집된 관찰 가능 개체를 포함하여 현재 게시된 모든 관찰 가능 개체를 수신합니다.

프로시저

단계 **1** **Intelligence(**인텔리전스**)** > **Elements(**요소**)**를 선택합니다.

단계 **2** 요소가 연결되어 있고 TID이(가) 활성화되어 있는지 확인하려면 요소 이름 옆에 있는 아이콘 위에 마우스를 올려 놓습니다.

참고 구축 후 적용된 액세스 제어 정책 및 TID 활성화 여부를 포함하여 이 페이지의 정보가 업데이트되는 데 최대 5분이 걸릴 수 있습니다.

소스 보기 및 관리

Source(소스) 페이지에는 구성된 모든 소스에 대한 요약 정보가 표시됩니다(소스 요약 정보, 30 페이지 참조).

프로시저

단계 **1** **Intelligence(**인텔리전스**)** > **Sources(**소스**)**를 선택합니다.

단계 **2** 소스 보기:

- 페이지에 표시된 소스를 필터링하려면 필터( )을 클릭합니다. 자세한 내용은 테이블 보기에서 TID 데이터 필터링, 37 페이지를 참고하십시오.
- 자세한 수집 상태를 보려면 **Status(**상태**)** 열에 있는 텍스트 위에 커서를 올려놓습니다. 자세한 내용은 소스 상태 세부 사항, 31 페이지를 참고하십시오.

단계 **3** 소스 관리:

- **Action(**작업**)** 설정을 수정하려면 소스, 지표 또는 관찰 가능 개체 수준에서 TID 작업 수정, 39 페이지를 참조하십시오. 작업이 고정되어 있다면 그것이 소스 **Type(**유형**)**에 대해 지원되는 유일한 작업입니다.
- **Publish(**게시**)** 설정을 수정하려면 슬라이더( )를 클릭합니다. 자세한 내용은 소스, 지표 또는 관찰 가능 개체 수준에서 TID 데이터 일시 중지 또는 게시, 41 페이지를 참고하십시오.

- 소스 TID 업데이트를 일시 중지하거나 재개하려면 **Pause Updates(**업데이트 일시 중지**)** 또는 **Resume Updates(**업데이트가 재개**)**를 클릭합니다. 업데이트를 일시 중지하면 업데이트는 일시 중지되지만 기존 지표와 관찰 가능 개체는 TID에 남아 있습니다.
- 소스를 삭제하려면 삭제( )을 클릭합니다. 소스가 여전히 처리 중이면 아이콘이 회색으로 표시됩니다. 소스를 삭제하면 해당 소스에 연결된 모든 지표가 삭제됩니다. 연결된 관찰 가능 개체도 삭제될 수 있지만 시스템에 남아 있는 지표와 연결된 경우에는 보존됩니다.

소스 요약 정보

Source(소스) 페이지에는 구성된 모든 소스의 요약 정보가 표시됩니다. 아래 표에는 요약 표시의 필드에 대한 간략한 설명이 나와 있습니다. 이러한 필드에 대한 자세한 내용은 소스와 관련된 구성 항목의 설명을 참조하십시오(데이터 소스 수집 옵션, 8 페이지 참조).

표 ***13:*** 소스 요약 정보

필드	설명
이름	소스 이름입니다.
유형	소스의 데이터 형식입니다(STIX 또는 플랫 파일).
전달	TID가 소스 검색에 사용하는 방법입니다.
조치	이 소스 내에 포함된 데이터와 일치하는 트래픽에 대해 시스템이 수행하도록 구성된 작업(Block(차단) 또는 Monitor(모니터링))입니다. 가용성, 상속, 상속 재정의 등 TID 작업에 대한 자세한 내용은 수행하는 작업에 영향을 미치는 요소, 24 페이지를 참조하십시오.
게시	TID가 소스의 데이터를 등록된 요소(TID를 지원하도록 구성된 매니지드 디바이스)에 게시하는지 여부를 지정하는 켜기 또는 끄기 토글입니다. 지표는 상위 소스로부터 **Publish(**게시**)** 설정을 상속할 수 있고, 관찰 가능 개체는 상위 지표로부터 **Publish(**게시**)** 설정을 상속할 수 있습니다. 자세한 내용은 TID 구성의 상속, 37 페이지를 참고하십시오.
Last Updated(마지막 업데이트 날짜**)**	TID가 소스를 마지막으로 업데이트한 날짜와 시간입니다.

필드	설명
상태	소스의 현재 상태: • **New(**신규**)** - 소스가 새로 생성되었습니다. • **Scheduled(**예약됨**)** - 초기 다운로드 또는 후속 업데이트가 예약되었지만 아직 진행 중이 아닙니다. • **Downloading(**다운로드 중**)** - TID가 초기 다운로드 또는 업데이트 새로 고침을 수행 중입니다. • **Parsing(**구문 분석 중**)** 또는 **Processing(**처리 중**)** - TID가 소스를 수집하고 있습니다. • **Completed(**완료**)** - TID가 소스 수집을 완료했습니다. • **Completed with Errors(**오류와 함께 완료**)** - TID가 소스 수집을 완료했지만, 일부 관측 가능 개체가 지원되지 않거나 잘못되었습니다. • **Error(**오류**)** - TID에 문제가 발생했습니다. 소스가 **Update Frequency(**업데이트 빈도**)**가 지정된 TAXII 또는 URL 소스이고 업데이트가 일시 중지되지 않은 경우, TID는 예약된 다음 업데이트에서 다시 시도합니다. 상태를 업데이트하려면 페이지를 새로 고칩니다.
수정( )	이 아이콘을 클릭하면 소스에 대한 설정을 수정할 수 있습니다.
삭제( )	이 아이콘을 클릭하면 소스가 영구적으로 삭제됩니다.

소스 상태 세부 사항

Sources(소스) 요약 페이지에서 소스의 **Status(**상태**)** 값에 커서를 올려놓으면 TID에서 아래 설명된 추가 세부 정보를 제공합니다.

데이터	설명
상태 메시지	소스의 현재 상태를 간략하게 설명합니다.
마지막 업데이트 날짜	TID가 소스를 마지막으로 업데이트한 날짜와 시간을 지정합니다.
다음 업데이트	TAXII 및 URL 소스의 경우, 이 값은 TID가 다음에 소스를 업데이트할 시기를 지정합니다.

데이터	설명
지표	지표 개수를 지정합니다. • **Consumed(**사용됨**)** - 가장 최근 소스 업데이트 중에 TID가 처리한 지표 수입니다. 이 숫자는 수집 또는 삭제 여부에 상관없이 업데이트에 포함된 모든 지표를 나타냅니다. • **Discarded(**삭제됨**)** - 가장 최근 업데이트 중에 시스템이 TID에 추가하지 않은 잘못된 형식의 지표 수입니다. 참고 TAXII 소스의 경우, TAXII 업데이트는 기존 데이터를 교체하지 않고 증분 데이터를 추가하기 때문에 TID에서는 별도의 **Last Update(**마지막 업데이트**)** 및 **Total(**총**)** 지표 개수를 제공합니다. 다른 소스 유형의 지표는 소스가 기존 데이터 세트를 완전히 대체하므로 TID는 **Last Update(**마지막 업데이트**)** 개수만 제공합니다. 지표의 모든 관찰 가능 개체가 **Invalid(**잘못됨**)**인 경우, TID는 지표를 삭제합니다.
관찰 가능 항목	관찰 가능 개체 개수를 지정합니다. • **Consumed(**사용됨**)** - 가장 최근 소스 업데이트 중에 TID가 처리한 관찰 가능 개체 수입니다. 이 숫자는 수집 또는 삭제 여부에 상관없이 업데이트에 포함된 모든 관찰 가능 개체를 나타냅니다. • **Unsupported(**지원되지 않음**)** - 가장 최근 업데이트 중에 시스템이 TID에 추가하지 않은 지원되지 않는 관찰 가능 개체 수입니다. 지원되는 관찰 가능 개체 유형에 대한 자세한 내용은 소스 요구 사항, 5 페이지의 콘텐츠 유형에 대한 정보를 참조하십시오. • **Invalid(**유효하지 않음**)** - 가장 최근 업데이트 중에 시스템이 TID에 추가하지 않은 유효하지 않은 관찰 가능 개체 수입니다. 유효하지 않은 관찰 가능 개체는 잘못 구성된 관찰 가능 개체입니다. 예를 들어 `10.10.10.10.123`는 유효한 IPv4 주소가 아닙니다. 참고 TAXII 소스의 경우, TAXII 업데이트는 기존 데이터를 교체하지 않고 증분 데이터를 추가하기 때문에 TID에서는 별도의 **Last Update(**마지막 업데이트**)** 및 **Total(**총**)** 관찰 가능 개체 개수를 제공합니다. 다른 소스 유형의 관찰 가능 개체는 소스가 기존 데이터 세트를 완전히 대체하므로 TID는 **Last Update(**마지막 업데이트**)** 개수만 제공합니다.

지표 보기 및 관리

지표는 수집된 소스에서 자동으로 생성됩니다. 이 페이지의 정보에 대한 자세한 내용은 지표 요약 정보, 33 페이지를 참조하십시오.

프로시저

단계 **1** **Intelligence(**인텔리전스**)** > **Sources(**소스**)**를 선택합니다.

단계 **2** **Indicators(**지표**)**를 클릭합니다.

단계 **3** 현재 지표 보기:

- 페이지에 표시된 지표를 필터링하려면 필터( )을 클릭합니다. 자세한 내용은 테이블 보기에서 TID 데이터 필터링, 37 페이지를 참고하십시오.
- 지표(연결된 관찰 가능 개체 포함)에 대한 추가 세부 정보를 보려면 지표 이름을 클릭합니다. 자세한 내용은 지표 세부사항, 34 페이지를 참고하십시오.
- **Incidents(**인시던트**)** 열에서 번호를 클릭하여 지표에 연결된 인시던트에 대한 정보를 보거나 인시던트 위에 커서를 올려놓아 인시던트가 완전히 실현되었는지 부분적으로 실현되었는지 확인합니다.
- TID가 소스로부터 지표 수집을 완료했는지 확인하려면 **Status(**상태**)** 열을 보십시오.

단계 **4** 현재 지표 관리:

- **Action(**작업**)**을 수정하려면 소스, 지표 또는 관찰 가능 개체 수준에서 TID 작업 수정, 39 페이지를 참조하십시오. 작업이 고정되어 있다면 그것이 소스 **Type(**유형**)**에 대해 지원되는 유일한 작업입니다.
- **Publish(**게시**)** 설정을 수정하려면 소스, 지표 또는 관찰 가능 개체 수준에서 TID 데이터 일시 중지 또는 게시, 41 페이지를 참조하십시오.
- 지표의 관찰 가능 개체 하나 이상을 차단 안 함 목록에 추가하려면 지표 이름을 클릭하여 Indicator Details(지표 세부 사항) 페이지에 액세스합니다. 자세한 내용은 차단 금지 목록에 TID 관찰 가능 항목 추가 , 43 페이지를 참고하십시오.

지표 요약 정보

Indicators(지표) 페이지에는 구성된 소스에 연결된 모든 지표에 대한 요약 정보가 표시 됩니다.

표 ***14:*** 지표 요약 정보

필드	설명
유형	• 단일 관찰 가능 개체를 갖는 지표는 해당 관찰 가능 개체의 데이터 유형(URL, SHA-256 등)을 나열합니다. • 둘 이상의 관찰 가능 개체를 포함하는 지표는 `Complex`로 나열됩니다. 특정 관찰 가능 개체를 보려면 유형 위에 커서를 올려놓습니다.
이름	지표 이름입니다.

필드	설명
소스	지표가 포함된 소스입니다(상위 소스).
인시던트	지표와 연결된 인시던트에 대한 정보: • 인시던트가 부분적으로 실현되는지 완전히 실현되는지 지정하는 아이콘 • 지표에 연결된 인시던트 수
조치	지표와 관련된 조치입니다. 자세한 내용은 소스, 지표 또는 관찰 가능 개체 수준에서 TID 작업 수정, 39 페이지를 참고하십시오. 지표는 상위 소스로부터 **Action(**작업**)** 설정을 상속할 수 있고, 관찰 가능 개체는 상위 지표로부터 **Action(**작업**)** 설정을 상속할 수 있습니다. 자세한 내용은 TID 구성의 상속, 37 페이지를 참고하십시오.
게시	지표의 게시 설정입니다. 자세한 내용은 소스, 지표 또는 관찰 가능 개체 수준에서 TID 데이터 일시 중지 또는 게시, 41 페이지를 참고하십시오. 지표는 상위 소스로부터 **Publish(**게시**)** 설정을 상속할 수 있고, 관찰 가능 개체는 상위 지표로부터 **Publish(**게시**)** 설정을 상속할 수 있습니다. 자세한 내용은 TID 구성의 상속, 37 페이지를 참고하십시오.
Last Updated(마지막 업데이트 날짜**)**	TID가 지표를 마지막으로 업데이트한 날짜와 시간입니다.
상태	지표의 현재 상태: • **Pending(**보류 중**)** - TID가 지표의 관찰 가능 개체를 수집하는 중입니다. • **Completed(**완료**)** - TID가 지표의 모든 관찰 가능 개체를 성공적으로 수집했습니다. • **Completed With Errors(**오류와 함께 완료**)** - TID가 지표 수집을 완료했지만 일부 관측 가능 개체가 지원되지 않거나 유효하지 않습니다.

지표 세부사항

Indicator Details(지표 세부 사항) 페이지에는 인시던트의 지표 및 관찰 가능 개체가 표시됩니다.

표 ***15:*** 지표 세부 사항 정보

필드	설명
이름	지표 이름입니다.
설명	소스에서 제공하는 지표 설명입니다.

필드	설명
소스	지표가 포함된 소스입니다.
만료	소스의 **TTL** 값에 따라 지표가 만료되는 날짜와 시간입니다.
조치	지표와 관련된 조치입니다. 자세한 내용은 소스, 지표 또는 관찰 가능 개체 수준에서 TID 작업 수정, 39 페이지를 참고하십시오. 지표는 상위 소스로부터 **Action(**작업**)** 설정을 상속할 수 있고, 관찰 가능 개체는 상위 지표로부터 **Action(**작업**)** 설정을 상속할 수 있습니다. 자세한 내용은 TID 구성의 상속, 37 페이지를 참고하십시오.
게시	지표의 게시 설정입니다. 자세한 내용은 소스, 지표 또는 관찰 가능 개체 수준에서 TID 데이터 일시 중지 또는 게시, 41 페이지를 참고하십시오. 지표는 상위 소스로부터 **Publish(**게시**)** 설정을 상속할 수 있고, 관찰 가능 개체는 상위 지표로부터 **Publish(**게시**)** 설정을 상속할 수 있습니다. 자세한 내용은 TID 구성의 상속, 37 페이지를 참고하십시오.
지표 패턴	지표의 패턴을 구성하는 관찰 가능 개체와 연산자입니다. 연산자는 지표 내에서 관찰 가능 개체를 연결합니다. AND 관계는 **AND** 연산자로 표시됩니다. OR 관계는 **OR** 연산자로 또는 여러 관찰 가능 개체를 밀접히 그룹화하여 표시됩니다. 필요에 따라 **Whitelist(**화이트리스트**)** 버튼을 클릭하여 차단 안 함 목록에 관찰 가능 개체를 추가합니다. 자세한 내용은 차단 금지 목록에 TID 관찰 가능 항목 추가 , 43 페이지를 참고하십시오.

관찰 가능 개체 보기 및 관리

Observables(관찰 가능 개체) 페이지에는 성공적으로 수집된 모든 관찰 가능 개체가 표시됩니다(관찰 가능 개체 요약 정보, 36 페이지 참조).

시작하기 전에

- 소스로 사용할 TAXII 피드 가져오기, 9 페이지, URL에서 소스 가져오기, 10 페이지, 또는 소스로 사용할 로컬 파일 업로드, 12 페이지에 설명된 대로 하나 이상의 소스를 구성합니다.

프로시저

단계 **1** **Intelligence(**인텔리전스**)** > **Sources(**소스**)**를 선택합니다.

단계 **2** 관찰 가능 개체를 클릭 합니다.

단계 **3** 현재 관찰 가능 개체 보기:

- 페이지에 표시된 관찰 가능 개체를 필터링하려면 필터( )을 클릭합니다. 자세한 내용은 테이블 보기에서 TID 데이터 필터링, 37 페이지를 참고하십시오.

- **Value(**값**)** 열의 정보가 잘린 경우, 값 위에 커서를 올려놓습니다.
- 관찰 가능 개체를 포함하는 지표를 보려면 **Indicators(**지표**)** 열에서 숫자를 클릭합니다. 관찰 가능 개체 값을 필터로 하여 Incident(인시던트) 페이지가 열립니다. 자세한 내용은 지표 보기 및 관리, 32 페이지를 참고하십시오.

단계 **4** 현재 관찰 가능 개체 관리:

- **Action(**작업**)**을 수정하려면 소스, 지표 또는 관찰 가능 개체 수준에서 TID 작업 수정, 39 페이지를 참조하십시오.
- 관찰 가능 개체의 **Publish(**게시**)** 설정을 수정하려면 소스, 지표 또는 관찰 가능 개체 수준에서 TID 데이터 일시 중지 또는 게시, 41 페이지를 참조하십시오.
- 관찰 가능 개체의 만료 날짜를 변경하려면 상위 소스의 **TTL**을 수정합니다. 자세한 내용은 소스 보기 및 관리, 29 페이지를 참고하십시오.
- **Whitelist(**화이트리스트**)** 버튼을 클릭하여 차단 금지 목록에 관찰 가능 개체를 추가합니다. 자세한 내용은 차단 금지 목록에 TID 관찰 가능 항목 추가 , 43 페이지를 참고하십시오.

관찰 가능 개체 요약 정보

관찰 가능 개체 페이지에는 모든 수집 된 관찰 가능 개체에 대 한 요약 정보가 표시 됩니다.

표 ***16:*** 관찰 가능 개체 요약 정보

필드	설명
유형	관찰 가능 개체 데이터 유형: `SHA-256`, 도메인, `URL`, `IPv4`또는 `IPv6`.
값	관찰 가능 개체를 구성하는 데이터입니다.
지표	관찰 가능 개체를 포함하는 상위 지표의 수입니다.
조치	관찰 가능 개체에 대해 구성된 작업입니다. 자세한 내용은 소스, 지표 또는 관찰 가능 개체 수준에서 TID 작업 수정, 39 페이지를 참고하십시오. 지표는 상위 소스로부터 **Action(**작업**)** 설정을 상속할 수 있고, 관찰 가능 개체는 상위 지표로부터 **Action(**작업**)** 설정을 상속할 수 있습니다. 자세한 내용은 TID 구성의 상속, 37 페이지를 참고하십시오.
게시	관찰 가능 개체의 게시 설정입니다(소스, 지표 또는 관찰 가능 개체 수준에서 TID 데이터 일시 중지 또는 게시, 41 페이지 참조). 지표는 상위 소스로부터 **Publish(**게시**)** 설정을 상속할 수 있고, 관찰 가능 개체는 상위 지표로부터 **Publish(**게시**)** 설정을 상속할 수 있습니다. 자세한 내용은 TID 구성의 상속, 37 페이지를 참고하십시오.

필드	설명
업데이트 위치:	TID가 관찰 가능 개체를 마지막으로 업데이트한 날짜와 시간입니다.
만료	관찰 가능 개체가 상위 지표의 **TTL**에 따라 TID에서 자동으로 제거될 날짜입니다.
화이트리스트 버튼	이 버튼을 클릭하면 차단 안 함 목록에 관찰 가능 항목이 추가됩니다. 차단 금지 목록에 TID 관찰 가능 항목 추가 , 43 페이지의 내용을 참조하십시오.

테이블 보기에서 TID 데이터 필터링

프로시저

단계 **1** 다음 TID 테이블 보기 중 하나를 선택합니다.

- **Intelligence(**인텔리전스**)** > **Incidents(**인시던트**)**
- **Intelligence(**인텔리전스**)** > **Sources(**소스**)**
- **Intelligence(**인텔리전스**)** > **Sources(**소스**)** > **Indicators(**지표**)**
- **Intelligence(**인텔리전스**)** > **Sources(**소스**)** > **Observables(**관찰 가능 개체**)**

단계 **2** 필터(🔍)을 클릭하고 필터 속성을 선택합니다.

단계 **3** 해당 필터 속성의 값을 선택하거나 입력합니다.

필터는 대/소문자를 구분합니다.

단계 **4** (선택 사항) 여러 속성을 필터링하려면 필터(🔍)을 클릭하고 2단계와 3단계를 반복합니다.

단계 **5** 필터를 마지막으로 적용한 이후의 변경 사항을 취소하려면 **Cancel(**취소**)**을 클릭합니다.

단계 **6** 필터를 적용하여 테이블을 새로 고치려면 **Apply(**적용**)**를 클릭합니다.

단계 **7** 필터 속성을 개별적으로 제거하려면 필터 속성 옆에 있는 제거(×)을 클릭하고 **Apply(**적용**)**를 클릭하여 테이블을 새로 고칩니다.

TID 구성의 상속

TID는 소스로부터 인텔리전스 데이터를 수집할 때 해당 소스의 하위 개체로 지표와 관찰 가능 개체를 생성합니다. 이러한 하위 개체는 생성될 때 상위 구성에서 **Action(**작업**)** 및 **Publish(**게시**)** 설정을 상속합니다

지표는 상위 소스에서 이러한 설정을 상속합니다. 지표는 하나의 상위 소스만 가질 수 있습니다.

관찰 가능 개체는 상위 지표에서 이러한 설정을 상속합니다. 관찰 가능 개체는 여러 상위 지표를 가질 수 있습니다.

자세한 내용은 다음 링크를 참조하십시오.

- 여러 상위에서 TID 설정 상속, 38 페이지
- 상속된 TID 설정 재정의 정보, 38 페이지

여러 상위에서 TID 설정 상속

관찰 가능 개체에 여러 상위 지표가 있는 경우, 시스템은 모든 상위 항목에서 상속한 설정을 비교하여 가장 안전한 옵션을 관찰 가능 개체에 할당합니다. 그 결과는 다음과 같습니다.

- **Action(작업)**: `Block(차단)`이 `Monitor(모니터링)`보다 안전합니다
- **Publish(게시)**: `On`가 `Off`보다 안전합니다

예를 들어 SourceA는 IndicatorA 및 관련 ObservableA에 기여할 수 있습니다.

설정	SourceA	IndicatorA	ObservableA
조치	차단	차단	차단
게시	`Off`	`Off`	`Off`

SourceB가 ObservableA도 포함하는 IndicatorB에 나중에 기여하는 경우, 시스템은 ObservableA를 다음과 같이 수정합니다.

설정	SourceB	IndicatorB	ObservableA
조치	모니터링	모니터링	`Block(차단)` (IndicatorA에서 상속)
게시	켜기	켜기	`On` (IndicatorB에서 상속)

이 예에서 ObservableA에는 두 가지 상위 항목이 있습니다. **Action(작업)** 설정의 상위 항목 하나와 **Publish(게시)** 설정의 상위 항목 하나입니다. 관찰 가능 개체의 설정을 수동으로 편집한 다음 설정을 되돌리면 시스템은 **Action(작업)** 설정을 IndicatorA 값으로, **Publish(게시)** 설정을 IndicatorB 값으로 설정합니다.

상속된 TID 설정 재정의 정보

상속된 설정을 재정의하려면 하위 수준에서 설정을 변경합니다(소스, 지표 또는 관찰 가능 개체 수준에서 TID 작업 수정, 39 페이지 및 소스, 지표 또는 관찰 가능 개체 수준에서 TID 데이터 일시 중지 또는 게시, 41 페이지 참조). 상속된 설정을 재정의하면 하위 개체는 상위 개체의 변경에도 불구하고 해당 설정을 유지합니다.

예를 들어 재정의 없이 다음과 같은 원래 설정으로 시작할 수 있습니다.

설정	SourceA	IndicatorA	ObservableA1	ObservableA2
게시	끄기	끄기	끄기	끄기

IndicatorA에 대한 설정을 재정의하는 경우, 설정은 다음과 같습니다.

설정	SourceA	IndicatorA	ObservableA1	ObservableA2
게시	끄기	켜기	켜기	켜기

이 경우, SourceA의 **Publish(**게시**)** 설정 변경은 더 이상 자동으로 IndicatorA로 캐스케이딩되지 않습니다. 하지만 IndicatorA에서 ObservableA1 및 ObservableA2로의 상속은 계속되는데, 현재 관찰 가능 개체 설정이 값을 재정의하도록 설정되어 있지 않기 때문입니다.

나중에 ObservableA1에 대한 설정을 재정의하는 경우:

설정	SourceA	IndicatorA	ObservableA1	ObservableA2
게시	끄기	켜기	끄기	켜기

IndicatorA의 **Publish(**게시**)** 설정 변경은 더 이상 자동으로 ObservableA1으로 캐스케이딩되지 않습니다. 하지만 이러한 변경 사항은 계속해서 ObservableA2로 캐스케이딩됩니다. 값을 재정의하도록 설정되어 있지 않기 때문입니다.

관찰 가능 개체 수준에서는 재정의 설정에서 상속된 설정으로 되돌릴 수 있으며, 시스템은 설정 변경을 상위 지표에서 해당 관찰 가능 개체로 자동으로 캐스케이딩하는 작업을 재개합니다.

소스, 지표 또는 관찰 가능 개체 수준에서 TID 작업 수정

참고:

- 상위 항목의 작업을 수정하면 모든 하위 항목의 작업이 설정됩니다. 소스 수준에서 작업을 수정하면 소스의 모든 지표의 작업이 설정됩니다. 지표 수준에서 작업을 수정하면 지표의 모든 관찰 가능 개체의 작업이 설정됩니다.
- 하위 항목의 작업을 수정하면 상속이 중단됩니다. 지표 수준에서 작업을 수정하고 이후에 소스 수준에서 수정하면 개별 지표의 작업을 수정할 때까지 지표의 작업은 보존됩니다. 관찰 가능 개체 수준에서 작업을 수정하고 이후에 지표 수준에서 수정하면 개별 관찰 가능 개체의 작업을 수정할 때까지 관찰 가능 개체의 작업은 보존됩니다. 관찰 가능 개체 수준에서는 상위 지표의 작업으로 자동으로 되돌릴 수 있습니다. 상속에 대한 자세한 내용은 TID 구성의 상속, 37 페이지를 참조하십시오.

다른 수행하는 작업에 영향을 미치는 요소, 24 페이지도 검토하는 것이 좋습니다.

프로시저

단계 **1** 다음 중 하나를 선택합니다.

- **Intelligence(**인텔리전스**)** > **Sources(**소스**)**

참고 TID 소스 수준에서 TAXII 소스 차단을 지원하지 않습니다. TAXII 소스에 간단한 지표가 포함된 경우, 지표 또는 관찰 가능 개체 수준에서 차단할 수 있습니다.

- **Intelligence(**인텔리전스**)** > **Sources(**소스**)** > **Indicators(**지표**)**

  참고 TID 복잡한 지표의 차단를 지원하지 않습니다. 대신 복잡한 지표 내의 개별적 관찰 가능 개체를 차단합니다.

- **Intelligence(**인텔리전스**)** > **Sources(**소스**)** > **Observables(**관찰 가능 개체**)**

단계 **2** **Action(**작업**)** 드롭다운을 사용하여 `Monitor(모니터링)`(모니터( ))) 또는 `Block(차단)`(차단( ))을 선택합니다.

단계 **3** (관찰 가능 개체만 해당) 상위 지표로부터의 작업 설정 상속을 재개하려면 관찰 가능 개체의 **Action(**작업**)** 설정 옆에 있는 되돌리기를 클릭합니다.

게시 일시 중지 정보

- 기능 수준에서 게시를 일시 중지하면 시스템은 요소에 저장된 모든 TID 관찰 가능 개체를 제거합니다. 즉, TID는 위협을 탐지하거나 모니터링하거나 차단할 수 없습니다. 시스템의 다른 보안 기능은 영향을 받지 않습니다.
- 소스, 지표 또는 관찰 가능 개체 수준에서 게시를 일시 중지하는 경우, 시스템은 일시 중지된 TID 관찰 가능 개체를 요소에서 제거하므로 트래픽과의 매칭이 방지됩니다.
- 상위 항목의 게시를 일시 중지하면 모든 하위 항목이 일시 중지됩니다. 소스 수준에서 게시를 일시 중지하면 모든 해당 지표의 게시가 일시 중지됩니다. 지표 수준에서 게시를 일시 중지하면 모든 해당 관찰 가능 개체의 게시가 일시 중지됩니다.
- 하위 항목의 게시를 일시 중지하면 상속이 중단됩니다. 지표 수준에서 게시를 일시 중지하고 이후에 소스 수준에서 게시하면 지표의 개별 설정을 변경할 때까지 지표의 게시가 계속 일시 중지됩니다. 관찰 가능 개체 수준에서 게시를 일시 중지하고 이후에 지표 수준에서 게시하면 관찰 가능 개체의 개별 설정을 변경할 때까지 관찰 가능 개체의 게시가 계속 일시 중지됩니다. 관찰 가능 개체 수준에서는 상위 지표의 게시 상태로 자동으로 되돌릴 수 있습니다. 상속에 대한 자세한 내용은 TID 구성의 상속, 37 페이지를 참조하십시오.
- 업로드된 소스의 게시는 지표 수준에서만 일시 중지할 수 있습니다.
- 관찰 가능 대상에 대한 게시 일시 중지와 관찰 가능 항목을 차단 안 함 목록에 추가하는 것에 대한 비교는 차단 금지 목록에 TID 관찰 가능 항목 추가 , 43 페이지의 내용을 참조하십시오.
- 개별 관찰 가능 개체 또는 지표의 게시/일시 중지 설정을 지정했다면 소스 업데이트에 동일한 관찰 가능 개체 또는 지표가 포함된 경우, 소스 업데이트는 해당 설정을 변경하지 않습니다.
- 게시는 개체 관리 페이지에서 비활성화할 수 있습니다. 관찰 가능 개체 게시 빈도 수정, 42 페이지의 내용을 참조하십시오.

- Source(소프) 페이지의 업데이트 일시 중지 옵션은 데이터를 요소에 게시하는 것과 관련이 없고, 피드의 Firepower Management Center에서의 소스 업데이트에 적용됩니다.

TID 일시 중지 및 요소에서 TID 데이터 제거

주의 이 설정은 모든 요소에 대한 게시를 일시 중지하고, 요소에 저장된 모든 TID 관찰 가능 개체를 제거하며, TID 기능을 사용하여 트래픽 검사를 중지합니다.

더 세부적인 수준에서 관찰 가능 개체를 비활성화하려면 소스, 지표 또는 관찰 가능 개체 수준에서 TID 데이터 일시 중지 또는 게시, 41 페이지를 참조하십시오.

관리 센터의 데이터(기존 인시던트 및 구성된 소스, 지표, 관찰 가능 개체 및 소스 수집)는 이 설정의 영향을 받지 않습니다.

프로시저

단계 1 **Intelligence(**인텔리전스**)** > **Settings(**설정**)**를 선택합니다.

단계 2 **Pause(**일시 중지**)**를 클릭합니다.

다음에 수행할 작업

요소에서의 TID 데이터 동기화와 관찰 생성을 재개할 준비가 되면 이 페이지에서 수동으로 게시를 재개합니다. 관리 센터의 기존 관찰 가능 개체가 모든 요소에 게시됩니다.

소스, 지표 또는 관찰 가능 개체 수준에서 TID 데이터 일시 중지 또는 게시

소스 수준에서 게시가 활성화되면 시스템은 초기 소스 데이터 및 다음을 포함한 모든 후속 변경 사항을 자동으로 게시합니다.

- 주기적 소스 새로 고침에 따른 변경 사항
- 시스템 작업(예를 들어 **TTL** 만료)에서 발생하는 변경 사항
- 사용자가 시작한 변경(예: 지표 또는 관찰 가능 개체의 **Action(**작업**)** 설정 변경)

참고 디바이스(요소)에서 한 번에 모든 TID 관찰 가능 개체를 제거하려면 TID 일시 중지 및 요소에서 TID 데이터 제거, 41 페이지를 참조하십시오.

시작하기 전에

게시를 일시 중지하기 전에 게시 일시 중지 정보, 40 페이지에 설명된 영향을 이해하십시오.

프로시저

단계 **1** 다음 중 하나를 선택합니다.

- **Intelligence(**인텔리전스**)** > **Sources(**소스**)**
- **Intelligence(**인텔리전스**)** > **Sources(**소스**)** > **Indicators(**지표**)**
- **Intelligence(**인텔리전스**)** > **Sources(**소스**)** > **Observables(**관찰 가능 개체**)**

단계 **2** **Publish(**게시**)** 슬라이더( )를 찾고 이를 사용해서 게시를 요소로 전환합니다.

단계 **3** (관찰 가능 개체만 해당) 상위 지표로부터의 게시 설정 상속을 재개하려면 관찰 가능 개체의 **Publish(**게시**)** 설정 옆에 있는 **Revert(**되돌리기**)**를 클릭합니다.

다음에 수행할 작업

- 요소가 변경 사항을 수신하도록 10분 이상 기다립니다. 큰 소스와 관련된 변경 사항은 이보다 시간이 더 걸립니다.
- (선택 사항) 관찰 가능 개체 수준에서 TID 데이터의 게시 빈도를 변경합니다(관찰 가능 개체 게시 빈도 수정, 42 페이지 참조).

관찰 가능 개체 게시 빈도 수정

기본적으로 시스템은 5분마다 관찰 가능 개체를 TID 요소에 게시합니다. 이 절차를 사용하여 이 간격을 다른 값으로 설정하십시오.

시작하기 전에

- 관찰 가능 개체 수준에서 TID 데이터 게시를 활성화합니다(소스, 지표 또는 관찰 가능 개체 수준에서 TID 데이터 일시 중지 또는 게시, 41 페이지 참조).

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.

단계 **2** **Security Intelligence(**보안 인텔리전스**)** > **Network Feeds and Lists(**네트워크 목록 및 피드**)**를 선택합니다.

단계 **3** **Cisco-TID-Feed**옆에 있는 수정 아이콘을 클릭합니다.

단계 **4** **Update Frequency(**업데이트 빈도**)** 드롭다운 목록에서 값을 선택합니다.

- 요소에 대한 관찰 가능 개체 데이터 게시를 중지하려면 **Disable(**비활성화**)**을 선택합니다.
- 관찰 가능 개체 게시 간격을 설정하려면 다른 값을 선택합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

차단 금지 목록에 TID 관찰 가능 항목 추가

간단한 지표의 관찰 가능 개체를 지정된 **Action(**작업**)**에서 제외하려면(모니터링 또는 차단 없이 트래픽이 통과하도록 하려면) 해당 관찰 가능 개체를 차단 금지 목록에 추가할 수 있습니다.

복잡한 지표에서 TID는 트래픽을 평가할 때 차단 금지 목록에 추가된 관찰 가능 개체를 무시하지만 해당 지표의 다른 관찰 가능 개체는 여전히 평가됩니다. 예를 들어 지표에 AND 연산자로 연결된 Observable 1과 Observable 2가 포함되어 있고 Observable 1을 차단 금지 목록에 추가하려는 경우, TID는 Observable 2가 보일 때 완전히 실현된 인시던트를 생성합니다.

이에 비해 동일한 복잡한 지표에서 Observable 1을 차단 금지 목록에 추가하는 대신 Observable 1의 게시를 비활성화하면 TID는 Observable 2가 보일 때 부분적으로 실현된 인시던트를 생성합니다.

화이트리스트 버튼(☑)은 지표 세부 사항 페이지 및 관찰 가능 개체 페이지에 표시됩니다. 차단 금지 목록에 관찰 가능 항목을 추가하려면 해당 아이콘을 클릭합니다.

참고 관찰 가능 개체를 차단 금지 목록에 추가하는 경우, 관찰 가능 개체의 **Action(**작업**)** 설정이 상속된 값이건 재정의 값이건 상관없이 차단 금지 목록이 해당 설정에 우선합니다.

소스 업데이트에 동일한 관찰 가능 개체가 포함된 경우 해당 업데이트는 개별 관찰 가능 개체의 차단 금지 목록 설정에 영향을 주지 않습니다.

차단 금지 목록에 TID 관찰 가능 항목 추가

차단 안 함 목록 사용에 대한 자세한 내용은 차단 금지 목록에 TID 관찰 가능 항목 추가 , 43 페이지의 내용을 참조하십시오.

팁 "차단 안 함 목록에 추가" 버튼(☑)은 웹 인터페이스 여러 위치에 표시될 수 있습니다. 이러한 위치 어디서나 이 버튼을 클릭하여 관찰 가능 개체를 차단 안 함 목록에 추가할 수 있습니다.

프로시저

단계 **1** **Intelligence(**인텔리전스**) > Sources(**소스**) > Observables(**관찰 가능 개체**)**를 클릭합니다.

단계 **2** 허용하려는 관찰 가능 개체로 이동합니다.

단계 **3** 해당 관찰 가능 개체에 대해 (**Whitelist(**화이트리스트**)**)를 클릭합니다.

다음에 수행할 작업

(선택 사항) 차단 안 함 목록에서 관찰 가능 개체를 제거해야 하는 경우, 버튼을 다시 클릭합니다.

STIX 소스 파일 보기

프로시저

단계 **1** **Intelligence(**인텔리전스**) > Sources(**소스**) > Indicators(**지표**)**를 선택합니다.
단계 **2** 지표 이름을 클릭합니다.
단계 **3** **Download STIX(STIX** 다운로드**)**를 클릭합니다.
단계 **4** 텍스트 편집기에서 파일을 엽니다.

문제 해결 Cisco Threat Intelligence Director(TID)

다음 섹션에서는 일반적인 TID 문제의 가능한 해결책과 완화 방법을 설명합니다.

플랫 파일 소스 가져오기 또는 업로드에서 오류 발생

시스템이 플랫 파일 소스를 가져오지 못하거나 업로드하지 못하는 경우, 플랫 파일의 데이터가 **Intelligence(**인텔리전스**) > Sources(**소스**)** 페이지의 **Type(**유형**)** 열과 일치하는지 확인합니다.

TAXII 또는 **URL** 소스 업데이트에서 오류 발생

TAXII 또는 URL 소스 업데이트에서 소스 상태 오류가 발생하는 경우, 서버 인증서가 만료되지 않았는지 확인합니다. 인증서가 만료된 경우, TID가 새 인증서를 검색할 수 있도록 새 서버 인증서를 입력하거나 기존 서버 인증서를 삭제합니다. 자세한 내용은 TID 소스의 TLS/SSL 설정 구성, 13 페이지를 참고하십시오.

지표 또는 소스에 **"**차단**"** 작업을 사용할 수 없고 **"**모니터링**"**만 사용 가능

지표 또는 소스에서 개별 관찰 가능 개체의 작업을 변경할 수 있습니다.

TID 테이블 보기가 **"**결과 없음**"**을 반환

테이블 보기에는 **Sources(**소스**)**, **Indicators(**지표**)**, **Observables(**관찰 가능 개체**)**, **Incidents(**인시던트**)** 페이지가 포함됩니다.

TID 테이블 보기 중 하나에서 데이터가 보이지 않는 경우:

- 테이블 필터를 확인하고 **Last Updated(**마지막 업데이트**)** 필터 속성의 기간을 확장하는 것이 좋습니다(테이블 보기에서 TID 데이터 필터링, 37 페이지 참조).
- 소스를 올바르게 구성했는지 확인합니다(데이터 소스 수집 옵션, 8 페이지 참조).
- 액세스 제어 정책 및 관련 정책이 TID를 지원하도록 구성되었는지 확인합니다(지원할 정책 구성 TID, 7 페이지 참조). 예를 들어 SHA-256 관찰 가능 개체가 관찰을 생성하지 않는 경우, 구축된 액세스 제어 정책에 **Malware Cloud Lookup(**악성코드 클라우드 조회**)** 또는 **Block Malware(**악성코드 차단**)** 파일 정책을 호출하는 하나 이상의 액세스 제어 규칙이 포함되어 있는지 확인합니다.
- TID 지원 액세스 제어 정책과 관련 정책을 요소에 구축했는지 확인합니다(컨피그레이션 변경 사항 구축 참조).
- 기능 수준에서 TID 데이터 게시를 일시 중지하지 않았는지 확인합니다(TID 일시 중지 및 요소에서 TID 데이터 제거, 41 페이지 참조).

시스템이 느려지거나 성능 저하

성능에 미치는 영향에 대한 자세한 내용은 Threat Intelligence Director의 성능 영향, 3 페이지를 참조하십시오.

Firepower Management Center 테이블 보기에 **TID** 데이터가 표시되지 않음

관찰 가능 개체를 요소에 게시하지만 연결, 보안 인텔리전스, 파일 또는 악성코드 이벤트 테이블에 TID 데이터가 표시되지 않는 경우, 요소에 구축된 액세스 제어 및 파일 정책을 확인합니다. 자세한 내용은 지원할 정책 구성 TID, 7 페이지를 참고하십시오.

하나 이상의 요소가 **TID** 데이터에 압도됨

TID 데이터가 하나 이상의 디바이스를 압도하는 경우, TID 게시를 일시 중지하고 요소에 저장된 데이터를 제거하는 것이 좋습니다. 자세한 내용은 TID 일시 중지 및 요소에서 TID 데이터 제거, 41 페이지를 참고하십시오.

시스템은 **TID** 차단 대신 악성코드 클라우드 조회를 수행

이것은 의도적인 것입니다. 자세한 내용은 TID-Firepower Management Center 작업 우선 순위, 25 페이지를 참고하십시오.

시스템은 **TID** 작업 대신 보안 인텔리전스 또는 **DNS** 정책 작업을 수행

이것은 의도적인 것입니다. 자세한 내용은 TID-Firepower Management Center 작업 우선 순위, 25 페이지를 참고하십시오.

TID가 비활성화됨

- 어플라이언스에 메모리를 추가합니다. Threat Intelligence Director는 메모리가 15GB 이상인 어플라이언스에서만 사용할 수 있습니다.

- Firepower Management Center에 대한 REST API 액세스를 활성화합니다. 자세한 내용은 REST API 액세스 활성화를 참고하십시오.

시스템이 예상대로 **TID** 인시던트를 생성하지 않거나 **TID** 작업을 수행하지 않음

- 모든 매니지드 디바이스가 TID에 대해 적절히 활성화 및 구성되었는지 확인합니다. 요소(매니지드 디바이스)의 TID 상태 보기, 29 페이지 및 지원할 정책 구성 TID, 7 페이지를 참조하십시오.
- 변경 사항이 요소에 게시되려면 적어도 5~10분이 걸리며, 많은 데이터 피드를 게시하는 경우에는 더 오래 걸릴 수 있습니다.
- 관찰 가능 개체에 대한 작업 설정을 확인합니다. 관찰 가능 개체 보기 및 관리, 35 페이지의 내용을 참조하십시오.
- 시스템이 수행하는 TID 작업에 영향을 미치는 다른 요인의 목록은 수행하는 작업에 영향을 미치는 요소, 24 페이지를 참조하십시오.
- 요소(매니지드 디바이스)에 있어야 할 위협 데이터가 없을 수 있습니다. 게시 일시 중지 정보, 40 페이지의 내용을 참조하십시오.

특정 위협 **1**회 발생에서 여러 인시던트가 생성

이것은 하나의 지표가 여러 소스에 포함된 경우에 발생할 수 있습니다.

자세한 내용은 중복 표시기 처리, 13 페이지를 참조하십시오.

기록Cisco Threat Intelligence Director(TID)

기능	버전	세부 사항
작업 우선순위 변경	6.5	

기능	버전	세부 사항
		이 변경 사항은 둘 이상의 Firepower 기능이 특정 관찰 가능 개체에 적용할 수 있을 때 적용됩니다. TID 차단/모니터링 관찰 가능 작업이 보안 인텔리전스로 인한 차단/모니터링에 우선하도록 변경되었습니다. 중요 시스템은 예전과 같은 방식으로 트래픽을 효율적으로 처리합니다. 이전에 차단된 트래픽은 계속 차단되고, 모니터링되는 트래픽은 계속 모니터링됩니다. 이렇게 하면 이벤트에 보고된 구성 요소가 작업을 담당하는 것으로 변경됩니다. 더 많은 TID 인시던트가 생성될 수도 있습니다. • 트래픽이 보안 인텔리전스 차단 작업과 일치하더라도 TID 관찰 가능 개체 차단 작업을 설정하는 경우: • 연결 이벤트의 보안 인텔리전스 범주는 TID 블록의 변형입니다. • 시스템은 차단된 작업으로 TID 인시던트를 생성합니다. • 트래픽이 보안 인텔리전스 모니터 규칙과도 일치하더라도 TID 관찰 가능 개체 모니터 작업을 설정하는 경우: • 연결 이벤트의 보안 인텔리전스 범주는 TID 모니터링의 변형입니다. • 시스템은 모니터링된 작업으로 TID 인시던트를 생성합니다. 이전에는 이러한 경우 시스템에서 분석별로 범주를 보고하지만, TID 인시던트를 생성하지는 않았습니다.

기능	버전	세부 사항
Cisco Threat Intelligence Director(TID)	6.2.2	도입된 기능: 외부 소스의 위협 인텔리전스를 사용하여 위협을 식별하고 처리할 수 있습니다. 새로운 화면: 여러 탭이 포함된 새로운 최상위 **Intelligence(**인텔리전스**)** 메뉴. 지원되는 플랫폼: Firepower Management Center