보안 인텔리전스 차단 목록

다음 주제는 트래픽 차단 및 허용 트래픽 목록과 기본 구성 사용을 포함한 Security Intelligence의 개요를 제공합니다.

보안 인텔리전스 정보

악성 인터넷 콘텐츠를 차단하는 초기 방어선인 보안 인텔리전스는 평판 정보를 사용하여 IP 주소, URL, 도메인 이름과의 연결을 신속하게 차단합니다. 이를 보안 인텔리전스 차단 목록이라고 합니다.

보안 인텔리전스는 시스템에서 더 많은 리소스를 사용하는 평가를 수행하기 전에 이루어지는 첫 번째 액세스 제어 단계입니다. 차단 목록은 검사가 필요하지 않은 트래픽을 신속하게 제외하여 성능을 향상합니다.

참고 차단 목록을 사용하여 빠른 경로의 트래픽을 차단할 수 없습니다. 8000 Series 단축 경로는 보안 인텔리전스 필터링 이전에 지정됩니다. 단축 경로가 지정된 트래픽은 보안 인텔리전스를 비롯한 모든 추가적인 평가를 우회합니다.

사용자가 맞춤형 차단 목록을 설정할 수도 있으나, Cisco에서는 정기적으로 업데이트된 인텔리전스 피드에 대한 액세스를 제공합니다. 악성코드, 스팸, 봇넷, 피싱과 같은 보안 위협을 나타내는 사이트는 맞춤형 컨피그레이션을 업데이트하고 구축하는 속도보다 빠르게 나타났다 사라질 수 있습니다.

차단 안 함 목록 및 모니터링 전용 차단 목록을 사용하여 보안 인텔리전스 차단 목록을 세분화할 수 있습니다. 이러한 메커니즘에서는 트래픽이 차단 목록에 의해 차단되지 않지만, 일치하는 트래픽을 자동으로 신뢰하거나 일치하는 트래픽에 단축 경로를 지정하지 않습니다. 보안 인텔리전스 단계에서 차단 안 함 목록에 추가되거나 모니터링된 트래픽은 나머지 액세스 제어를 통해 추가적으로 분석됩니다.

관련 항목

보안 인텔리전스 목록 및 피드
로깅할 수 있는 기타 연결
연결 및 보안 인텔리전스 이벤트 테이블 사용

보안 인텔리전스 모범 사례

- Cisco에서 제공하는 보안 인텔리전스 피드에서 탐지한 위협을 차단하도록 액세스 제어 정책을 구성합니다. 설정 예 : 보안 인텔리전스 차단, 10 페이지의 내용을 참조하십시오.
- 사용자 지정 위협 데이터로 Cisco 제공 보안 인텔리전스 피드를 보완하거나 새로운 위협을 수동으로 차단하려는 경우:
  - IP 주소의 경우 사용자 지정 보안 인텔리전스 목록 및 피드 또는 네트워크 개체 또는 그룹을 사용합니다. 이러한 항목을 생성하려면 보안 인텔리전스 목록 및 피드, 네트워크 개체 및 해당 하위 항목을 참조하십시오. 보안 인텔리전스에 사용하려면 보안 인텔리전스 설정, 4 페이지의 내용을 참조하십시오.
  - URL 및 도메인의 경우 개체 또는 그룹이 아닌 사용자 지정 보안 인텔리전스 목록 및 피드를 사용합니다. 자세한 내용은 수동 URL 필터링 옵션의 내용을 참조하십시오.
  - 이벤트의 차단 목록에 항목을 추가할 수도 있습니다. 글로벌 및 도메인 보안 인텔리전스 목록의 내용을 참조하십시오.
- 새 피드를 테스트하거나 수동 구축을 수행하려면 작업을 차단에서 모니터링 전용으로 설정합니다. 보안 인텔리전스 모니터링, 12 페이지의 내용을 참조하십시오.
- 보안 인텔리전스 차단에서 특정 사이트 또는 주소를 제외해야 하는 경우 보안 인텔리전스 차단 재정의, 12 페이지의 내용을 참조하십시오.
- Firepower 구축이 SecureX 또는 관련 툴 Cisco SecureX Threat Response(이전의 Cisco Threat Response 또는 CTR)과 통합되어 있고 사용자 지정 보안 인텔리전스 목록 및 피드를 사용하는 경우 이러한 목록 및 피드로 SSE(Security Services Exchange)를 업데이트해야 합니다. 자세한 내용은 SSE 온라인 도움말에서 이벤트 자동 승격 구성에 대한 지침을 참조하십시오. 이 통합에 대한 일반 정보는 Cisco SecureX와의 통합의 내용을 참조하십시오
- 시스템 제공 보안 인텔리전스 범주는 시간이 지남에 따라 알림 없이 변경될 수 있습니다. 정기적으로 변경 사항을 확인하고 그에 따라 정책을 수정해야 합니다.
- 또한 악성 사이트에 대한 추가 보호를 위해 별도의 라이선싱 요건이 있는 별도의 기능인 URL 필터링도 구성해야 합니다. URL 필터링의 내용을 참조하십시오.

보안 인텔리전스를 위한 라이선스 요건

FTD 라이센스

위협

기본 라이선스

보호

보안 인텔리전스 요구 사항 및 사전 요건

모델 지원

Any(모든 상태)

지원되는 도메인

모든

사용자 역할

- 관리자
- 액세스 관리자
- Network Admin(네트워크 관리자)

보안 인텔리전스 소스

- 시스템에서 제공한 피드

  Cisco에서는 도메인, URL 및 IP 주소에 대해서 정기적으로 업데이트된 인텔리전스 피드에 액세스할 수 있도록 지원합니다. 자세한 내용은 보안 인텔리전스 목록 및 피드를 참고하십시오.

  이름에 "TID"가 포함된 피드가 표시되는 경우 보안 인텔리전스에서 이 피드를 사용하지 않습니다. 대신 이 피드는 Cisco Threat Intelligence Director(TID)에 설명된 기능에 사용됩니다.

- 서드파티 피드

  서드파티 피드 - Firepower Management Center이(가) 인터넷에서 정기적으로 다운로드하는 동적 목록인 서드파티 평판 피드로 Cisco 제공 피드를 보완합니다. 맞춤형 보안 인텔리전스 피드의 내용을 참조하십시오.

- 맞춤형 차단 목록 또는 피드(또는 개체 또는 그룹)

수동으로 생성된 목록 또는 피드를 사용하여 특정 IP 주소, URL 또는 도메인 이름을 차단합니다(IP 주소의 경우 네트워크 개체 또는 그룹을 사용할 수도 있음).

예를 들어 피드에 의해 아직 차단되지 않은 악성 사이트 또는 주소를 알고 있는 경우 이러한 사이트를 맞춤형 보안 인텔리전스 목록에 추가하고 이 맞춤형 목록을 액세스 제어 정책의 보안 인텔리전스 탭에 있는 차단 목록에 추가합니다. 이 내용은 맞춤형 보안 인텔리전스 목록 및 보안 인텔리전스 설정, 4 페이지에 설명되어 있습니다.

IP 주소의 경우 목록 또는 피드 대신 네트워크 개체를 선택적으로 사용할 수 있습니다. 자세한 내용은 네트워크 개체를 참고하십시오. (URL의 경우 다른 방법보다 목록 및 피드를 사용하는 것이 좋습니다.)

- 맞춤형 차단 금지 목록 또는 피드

  특정 사이트 또는 주소에 대한 보안 인텔리전스 차단을 재정의합니다. 보안 인텔리전스 차단 재정의, 12 페이지의 내용을 참조하십시오.

- 글로벌 차단 목록(네트워크, URL 및 DNS에 하나씩)

  이벤트를 검토하는 동안 보안 인텔리전스가 해당 소스의 향후 트래픽을 처리할 수 있도록 이벤트의 IP 주소, URL 또는 도메인을 즉시 적용 가능한 전역 차단 목록에 추가할 수 있습니다. 글로벌 및 도메인 보안 인텔리전스 목록의 내용을 참조하십시오.

- 전역 차단 금지 목록(네트워크, URL 및 DNS에 하나씩)

  보안 인텔리전스가 해당 소스의 향후 트래픽을 차단하지 않도록 하려면 이벤트를 검토하는 동안 이벤트의 IP 주소, URL 또는 도메인을 해당 Global Do Not Block List(글로벌 차단 금지 목록)에 즉시 추가할 수 있습니다. 글로벌 및 도메인 보안 인텔리전스 목록의 내용을 참조하십시오.

보안 인텔리전스 설정

액세스 제어 정책마다 보안 인텔리전스 옵션이 있습니다. 네트워크 개체, URL 개체 및 목록, 보안 인텔리전스 피드 및 목록을 차단 목록 또는 차단 안 함 목록에 추가할 수 있으며, 이 모두를 보안 영역으로 제한할 수 있습니다. 또한 DNS 정책을 액세스 제어 정책에 연결하고 도메인 이름을 차단 목록 또는 차단 안 함 목록에 추가할 수 있습니다.

차단 안 함 목록의 개체 수와 차단 목록의 개체 수를 합해 125개의 네트워크 개체 또는 32767개의 URL 개체 및 목록을 초과할 수 없습니다.

참고 시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축에서 리터럴 IP 주소를 사용하여 이 컨피그레이션을 제한하면 예기치 않은 결과가 발생할 수 있습니다. 하위 도메인 관리자는 재정의가 활성화된 개체를 사용하여 로컬 환경에 맞게 글로벌 컨피그레이션을 조정할 수 있습니다.

주의 액세스 제어 정책의 Security Intelligence(보안 인텔리전스)에서 차단 안 함 목록 또는 차단 목록에 여러 개체를 추가하거나 삭제하면 경우에 따라 컨피그레이션 변경 사항을 구축할 때 Snort 프로세스가 재시작되므로 트래픽 검사가 일시적으로 중단됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 아니면 추가 검사 없이 통과되는지는 대상 디바이스가 트래픽을 처리하는 방법에 따라 달라집니다. 자세한 내용은 Snort® 재시작 트래픽 동작을 참고하십시오. Snort 프로세스가 재시작되는지 여부는 검사에 사용할 수 있는 메모리에 따라 디바이스별로 달라질 수 있습니다.

시작하기 전에

- 팁 : 최소 구성 권장 사항에 대한 지침은 설정 예 : 보안 인텔리전스 차단, 10 페이지의 내용을 참조하십시오.
- 모든 옵션을 선택할 수 있게 하려면, 관리 센터에 매니지드 디바이스를 하나 이상 추가합니다.
- 수동 구축에서 또는 보안 인텔리전스 필터링을 모니터링 한정으로 설정하려면 로깅을 활성화하십시오. 보안 인텔리전스로 연결 로깅의 내용을 참조하십시오.
- 도메인에 대한 보안 인텔리전스 작업을 수행하도록 DNS 정책을 설정합니다. 자세한 내용은 DNS 정책를 참고하십시오.

프로시저

단계 **1** 액세스 제어 정책 편집기에서 **Security Intelligence(**보안 인텔리전스**)**를 클릭합니다.

컨트롤이 흐리게 표시되는 경우에는 상위 정책에서 설정이 상속되거나 컨피그레이션을 수정할 권한이 없는 것입니다. 구성이 잠금 해제되어 있으면 **Inherit from base policy(**기본 정책에서 상속**)**의 선택을 취소하여 수정을 활성화합니다.

단계 **2** 다음 옵션을 이용할 수 있습니다.

- **Networks(**네트워크**)**를 클릭하여 네트워크 개체(IP 주소)를 추가합니다.
- **URL**을 클릭하여 URL 개체를 추가합니다.

단계 **3** 차단 또는 차단 안 함 목록에 추가 할 **Available Objects(**사용 가능한 개체**)**를 찾습니다. 다음 옵션을 이용할 수 있습니다.

- **Search by name or value(**이름 또는 값으로 검색**)** 필드에 입력하여 사용할 수 있는 개체를 검색합니다. 다시 로드( ) 또는 지우기( )를 클릭하여 검색 문자열을 지웁니다.
- 요구를 충족하는 기존 목록이나 피드가 없는 경우, 추가( )을 클릭하고 **New Network List(**새 네트워크 목록**)** 또는 **New URL List(**새 **URL** 목록**)**를 선택하고 보안 인텔리전스 피드 생성 또는 새 보안 인텔리전스 목록을 다음에 업로드 Firepower Management Center의 설명에 따라 계속합니다.

- 요구를 충족하는 기존 개체가 없는 경우, 추가( )을 클릭하고 **New Network Object(**새 네트워크 개체**)** 또는 **New URL Object(**새 **URL** 개체**)**를 선택하고 네트워크 개체 생성의 설명에 따라 계속합니다.

보안 인텔리전스는 `/0` 넷마스크를 사용하는 IP 주소 차단을 무시합니다.

단계 **4** 추가할 하나 이상의 사용 가능한 개체를 선택합니다.

단계 **5** (선택 사항) **Available Zone(**가용 영역**)**을 선택하여 선택된 개체를 영역별로 제한합니다.

시스템에서 제공한 보안 인텔리전스 목록은 영역별로 제한할 수 없습니다.

단계 **6** **Add to Do Not Block list(**차단 안 함 목록에 추가**)** 또는 **Add to Block list(**차단 목록에 추가**)**를 클릭하거나 선택한 항목을 클릭하고 차단 안 함 또는 차단 목록으로 끕니다.

차단 안 함 또는 차단 목록에서 개체를 제거하려면 삭제( )을 클릭합니다. 여러 개체를 제거하려면 여러 개체를 선택하고 **Delete Selected(**선택한 항목 삭제**)**를 마우스 오른쪽 버튼으로 클릭합니다.

단계 **7** (선택 사항) **Block List(**차단 목록**)**에서 마우스 오른쪽 버튼으로 개체를 클릭한 다음 **Monitor-only (do not block)(**모니터링 한정**(**차단 안 함**))**을 선택하여 차단 목록에 추가된 개체를 모니터링 한정으로 설정합니다.

시스템에서 제공한 전역 보안 인텔리전스 목록을 모니터링용으로만 설정할 수 없습니다.

단계 **8** **DNS Policy(DNS** 정책**)** 드롭다운 목록에서 DNS 정책을 선택합니다.

단계 **9** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축의 내용을 참조하십시오.

관련 항목

보안 인텔리전스 목록 및 피드
Snort® 재시작 시나리오

보안 인텔리전스 옵션

액세스 제어 정책 편집기의 Security Intelligence(보안 인텔리전스) 탭을 사용하여 네트워크(IP 주소) 및 URL 보안 인텔리전스를 설정하고 도메인에 대해 보안 인텔리전스를 설정한 DNS 정책과 액세스 제어 정책을 연결합니다.

사용 가능한 개체

사용 가능한 개체는 다음과 같습니다.

- 시스템에서 제공하는 피드로 채워진 보안 인텔리전스 범주입니다.

  자세한 내용은 보안 인텔리전스 카테고리, 8 페이지 섹션을 참조해 주십시오.

- 시스템에서 제공하는 전역 차단 및 차단 안 함 목록입니다.

  자세한 내용은 보안 인텔리전스 소스, 3 페이지를 참조하십시오.

- Security Intelligence(보안 인텔리전스)에는 Object(개체) > Object Management(개체 관리) > Security Intelligence(보안 인텔리전스) 아래에서 생성되는 피드와 목록이 나열됩니다.

  자세한 내용은 보안 인텔리전스 소스, 3 페이지를 참조하십시오.

- Object(개체) > Object Management(개체 관리) 아래의 해당 페이지에 설정된 네트워크 및 URL 개체와 그룹입니다. 이는 이전 글머리 기호의 보안 인텔리전스 개체와 다릅니다.

  네트워크 개체에 대한 자세한 내용은 네트워크 개체의 내용을 참조하십시오. (URL의 경우, 개체 또는 그룹 대신 보안 인텔리전스 목록 또는 피드를 사용합니다.)

사용 가능한 영역

시스템에서 제공하는 전역 목록을 제외하고 보안 인텔리전스 필터링을 영역별로 제한할 수 있습니다.

예를 들면, 성능을 개선하기 위해 대상 엔타이틀먼트를 지정할 수 있습니다. 보다 구체적으로는, 이메일 트래픽을 처리하는 보안 영역에 대해서만 스팸을 차단할 수 있습니다.

여러 영역에서 하나의 개체를 대상으로 보안 인텔리전스 필터링을 수행하려면 개체를 각 영역에 대해 별개로 차단 목록 또는 차단 안 함 목록에 추가해야 합니다.

DNS 정책

보안 인텔리전스를 사용하여 DNS 트래픽을 일치시키려면 보안 인텔리전스 설정에 대한 DNS 정책을 선택해야 합니다.

DNS 목록 또는 피드를 기준으로 차단 목록 또는 차단 안 함 목록에 추가하거나 트래픽을 모니터링하려면 다음을 수행해야 합니다.

- DNS 보안 인텔리전스 목록 및 피드를 구성합니다. 보안 인텔리전스 목록 및 피드의 내용을 참조하십시오.
- DNS 정책을 생성합니다. 자세한 내용은 기본 DNS 정책 생성를 참조하십시오.
- DNS 목록 또는 피드를 참조하는 DNS 규칙을 설정합니다. 자세한 내용은 DNS 규칙 생성 및 편집를 참조하십시오.
- 액세스 제어 정책의 일부로 DNS 정책을 구축하기 때문에 두 정책을 모두 연결해야 합니다. 자세한 내용은 DNS 정책 구축를 참조하십시오.

차단 안 함 목록

보안 인텔리전스 차단 재정의, 12 페이지의 내용을 참조하십시오.

목록의 모든 개체를 선택하려면 개체를 마우스 오른쪽 버튼으로 클릭합니다.

차단 목록

이 장의 설정 예 : 보안 인텔리전스 차단, 10 페이지 및 기타 주제를 참조하십시오.

차단 목록의 시각적 표시기에 대한 설명은 차단 목록 아이콘, 10 페이지의 내용을 참조하십시오.

목록의 모든 개체를 선택하려면 개체를 마우스 오른쪽 버튼으로 클릭합니다.

로깅

기본적으로 활성화되어 있는 보안 인텔리전스 로깅은 액세스 제어 정책의 대상 디바이스에 의해 처리되는 차단된 연결 및 모니터링되는 연결을 모두 로깅합니다. 그러나 시스템은 차단 안 함 목록에 일치하는 연결은 로깅하지 않습니다. 차단 안 함 목록으로 분류된 연결의 로깅은 최종 처리에 따라 다릅니다. 차단 목록의 연결에 대해 로깅을 활성화해야 해당 목록의 개체를 모니터링 전용으로 설정할 수 있습니다.

로깅 설정을 활성화, 비활성화 또는 확인하려면 차단 목록에서 개체를 마우스 오른쪽 버튼으로 클릭합니다.

관련 항목

글로벌 및 도메인 보안 인텔리전스 목록
보안 인텔리전스 목록 및 멀티테넌시

보안 인텔리전스 카테고리

보안 인텔리전스 범주는 보안 인텔리전스 목록 및 피드에 설명된 시스템 제공 피드에 의해 결정됩니다.

이러한 범주는 다음 위치에서 사용됩니다.

- 액세스 제어 정책의 Security Intelligence(보안 인텔리전스) 탭에 있는 Networks(네트워크) 하위 탭
- 액세스 제어 정책의 Security Intelligence(보안 인텔리전스) 탭에서 Networks(네트워크) 탭 옆에 있는 URL 하위 탭
- DNS 규칙 구성 페이지의 DNS 탭에 있는 DNS 정책에서
- 트래픽이 위 위치의 차단 또는 모니터링 구성과 일치할 때 생성되는 이벤트에서

참고 조직에서 Cisco Threat Intelligence Director(TID)을(를) 사용하는 경우: 이벤트를 확인할 때, `TID URL Block(TID URL 차단)` 같은 작업을 TID가 수행했음을 알리는 범주가 표시될 수도 있습니다.

Talos가 클라우드에서 범주를 업데이트하며, 이 목록은 Firepower 릴리스와 관계 없이 변경될 수 있습니다.

표 ***1: Cisco Talos Intelligence Group(Talos)*** 피드 카테고리

보안인텔리전스카테고리	설명
Attackers	아웃바운드의 악의적 활동으로 알려진 액티브 스캐너 및 호스트
Banking_fraud	전자 뱅킹과 관련된 사기성 활동을 수행하는 사이트
Bogon	bogon 네트워크 및 할당되지 않은 IP 주소
Bots	바이너리 악성코드 드로퍼를 호스팅하는 사이트
CnC	봇넷용 CnC(Command-and-Control) 서버를 호스팅하는 사이트
Cryptomining	크립토마이닝 마이닝을 위해 풀 및 월렛에 대한 원격 액세스를 제공하는 호스트
Dga	CnC 서버에서 RP(Rendezvous Point) 역할을 하는 많은 수의 도메인 이름을 생성하는 데 사용되는 악성코드 알고리즘
Exploitkit	클라이언트에서 소프트웨어 취약성을 식별하도록 설계된 소프트웨어 킷
High_risk	보안 그래프의 OpenDNS 예측 보안 알고리즘과 일치하는 도메인 및 호스트 이름
Ioc	IOC(Indicator of Compromise)에 관련된 것으로 관찰된 호스트
Link_sharing	저작권이 있는 파일을 허가 없이 공유하는 웹사이트
Malicious	반드시 더 세부적인 또 다른 위협 범주에 해당하지는 않지만 악의적인 행동을 보이는 사이트
Malware	악성코드 바이너리 또는 익스플로잇 킷을 호스팅하는 사이트
Newly_seen	최근에 등록되었거나 텔레메트리를 통해 아직 확인되지 않은 도메인
Open_proxy	익명의 웹 브라우징을 허용하는 오픈 프록시
Open_relay	스팸에 사용되는 것으로 알려진 오픈 메일 릴레이
Phishing	피싱 페이지를 호스팅하는 사이트
Response	악성 활동 또는 의심스러운 활동에 적극적으로 참여하고 있는 IP 주소 및 URL
Spam	스팸을 전송하는 것으로 알려진 메일 호스트
Spyware	스파이웨어 및 애드웨어 활동을 포함, 제공 또는 지원하는 것으로 알려진 사이트
Suspicious	알려진 악성코드와 유사한 특성을 지니고 있으며 의심스러워 보이는 파일

보안인텔리전스카테고리	설명
tor_exit_node	Tor Anonymizer 네트워크에 대한 종료 노드 서비스를 제공하는 것으로 알려진 호스트

차단 목록 아이콘

액세스 제어 정책에서 Security Intelligence(보안 인텔리전스) 탭의 Block(차단) 목록에 다음과 같은 시각적 표시가 나타날 수 있습니다.

아이콘 또는 시각적 표시	설명
차단( )	개체가 차단으로 설정되어 있습니다.
모니터( )	개체가 모니터링 전용으로 설정되어 있습니다. 보안 인텔리전스 모니터링, 12 페이지의 내용을 참조하십시오.
개체는 취소선 텍스트로 표시됩니다.	동일한 개체가 차단 금지 목록에 있으면 차단이 무시됩니다.

설정 예: 보안 인텔리전스 차단

시스템의 정기적으로 업데이트되는 보안 인텔리전스 피드에서 탐지할 수 있는 모든 위협을 차단하도록 액세스 제어 정책을 설정합니다.

차단 목록의 개체 수와 차단 안 함 목록의 개체 수를 합해 125개의 네트워크 개체 또는 32767개의 URL 개체 및 목록을 초과할 수 없습니다.

참고 시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축에서 리터럴 IP 주소를 사용하여 이 컨피그레이션을 제한하면 예기치 않은 결과가 발생할 수 있습니다. 하위 도메인 관리자는 재정의가 활성화된 개체를 사용하여 로컬 환경에 맞게 글로벌 컨피그레이션을 조정할 수 있습니다.

주의 액세스 제어 정책의 Security Intelligence(보안 인텔리전스)에서 차단 목록 또는 차단 안 함 목록에 여러 개체를 추가하거나 삭제하면 경우에 따라 컨피그레이션 변경 사항을 구축할 때 Snort 프로세스가 재시작되므로 트래픽 검사가 일시적으로 중단됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 아니면 추가 검사 없이 통과되는지는 대상 디바이스가 트래픽을 처리하는 방법에 따라 달라집니다. 자세한 내용은 Snort® 재시작 트래픽 동작을 참고하십시오. Snort 프로세스가 재시작되는지 여부는 검사에 사용할 수 있는 메모리에 따라 디바이스별로 달라질 수 있습니다.

시작하기 전에

- 모든 옵션을 선택할 수 있게 하려면, 관리 센터에 매니지드 디바이스를 하나 이상 추가합니다.
- 도메인에 대한 모든 보안 인텔리전스 위협 범주를 차단하도록 DNS 정책을 설정합니다. 자세한 내용은 DNS 정책를 참고하십시오.
- 차단할 사용자 지정 엔터티 목록이 있거나 있을 예정인 경우 각 유형(URL, DNS, 네트워크)의 보안 인텔리전스 개체를 생성합니다. 보안 인텔리전스 목록 및 피드의 내용을 참조하십시오.

프로시저

단계 **1** **Policies(**정책**) > Access Control(**액세스 제어**)**을 클릭합니다.

단계 **2** 새로운 액세스 제어 정책을 만들거나 기존 정책을 편집합니다.

단계 **3** 액세스 제어 정책 편집기에서 **Security Intelligence(**보안 인텔리전스**)**를 클릭합니다.

컨트롤이 흐리게 표시되는 경우에는 상위 정책에서 설정이 상속되거나 컨피그레이션을 수정할 권한이 없는 것입니다. 구성이 잠금 해제되어 있으면 **Inherit from base policy(**기본 정책에서 상속**)**의 선택을 취소하여 수정을 활성화합니다.

단계 **4** IP 주소에 대한 차단 기준을 추가하려면 **Networks(**네트워크**)**를 클릭합니다.

a) Networks(네트워크) 목록에서 아래로 스크롤하여 Global(전역) 목록 아래에 나열된 모든 위협 범주를 선택합니다.
b) 해당하는 경우 이러한 위협을 차단할 보안 영역을 선택합니다.
c) **Add to Block List(**차단 목록에 추가**)**를 클릭합니다.
d) 차단할 주소가 있는 맞춤형 목록 또는 피드를 생성한 경우 위와 동일한 단계를 사용하여 차단 목록에 추가합니다.

단계 **5** URL에 대한 차단 기준을 추가하려면 **URL**을 클릭하고 네트워크에 대해 수행한 단계를 반복합니다.

단계 **6** **DNS Policy(DNS** 정책**)** 드롭다운 목록에서 DNS 정책을 선택합니다. DNS 정책 개요의 내용을 참조하십시오.

단계 **7** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 이러한 연결에 대한 로깅을 활성화합니다. 보안 인텔리전스로 연결 로깅의 내용을 참조하십시오.
- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축의 내용을 참조하십시오.

보안 인텔리전스 모니터링

모니터링은 보안 인텔리전스에 의해 차단되었지만 트래픽을 차단하지는 않는 트래픽에 대한 연결 이벤트를 로깅합니다. 모니터링은 특히 다음에 유용합니다.

- 피드를 구현하기 전에 테스트합니다.

  서드파티 피드 사용에 대한 차단을 실행하기 전에 해당 피드 테스트를 원하는 시나리오를 고려해 보십시오. 피드를 모니터링 한정으로 설정하면, 시스템은 시스템이 추가 분석을 위해 차단할 수도 있었던 연결을 허용하며, 사용자 평가를 위해 각 연결의 레코드를 로깅합니다.

- 패시브 구축-성능 최적화

  수동으로 구축된 매니지드 디바이스는 트래픽 흐름에 영향을 줄 수 없으며, 트래픽을 차단하도록 시스템을 구성해도 이점이 없습니다. 또한, 차단된 연결이 수동 배포에서 실제로 차단되는 것은 아니기 때문에 시스템은 각 차단된 연결에 대한 여러 초기 연결 이벤트를 보고할 수 있습니다.

보안 인텔리전스 피드를 구성하려면 다음을 수행합니다.

의 지침에 따라 보안 인텔리전스 차단을 구성한 후 Block (차단) 목록에서 해당하는 각 개체를 마우스 오른쪽 버튼으로 클릭하고 Monitor-only (모니터링 전용)를 선택합니다.설정 예 : 보안 인텔리전스 차단, 10 페이지 시스템에서 제공한 보안 인텔리전스 목록을 모니터링용으로만 설정할 수 없습니다.

보안 인텔리전스 차단 재정의

아니면 Do Not Block(차단 안 함) 목록을 사용하여 특정 도메인, URL 또는 IP 주소가 보안 인텔리전스 목록 또는 피드에 의해 차단되지 않도록 제외할 수 있습니다.

예를 들어, 다음이 가능합니다.

- 평판이 좋은 보안 인텔리전스 피드에서 가끔 오탐 블록을 재정의합니다.
- 평판을 기준으로 특정 트래픽을 조기에 차단하는 대신 심층적으로 검사
- 보안 인텔리전스 차단에서 영역을 기준으로 달리 제한되는 트랜잭션 제외

  잘못 분류된 URL을 Do Not Block(차단 안 함) 목록에 추가한 다음 이러한 URL에 액세스해야 하는 조직 내 사용자들이 사용하는 보안 영역을 사용하여 Do Not Block(차단 안 함) 개체를 제한할 수 있습니다. 이렇게 하면 업무상 필요가 있는 사용자만 Do Not Block(차단 안 함) 목록에 추가된 URL에 액세스할 수 있습니다.

참고 Do Not Block(차단 안 함) 목록의 항목은 자동으로 신뢰되거나 빠른 경로가 아닙니다. 이 트래픽은 나머지 액세스 제어를 통해 의도적으로 추가 분석될 수 있습니다.

프로시저

단계 **1** 옵션 1: 이벤트의 IP 주소, URL 또는 도메인을 Global Do Not Block(전역 차단 금지) 목록에 추가합니다. 글로벌 및 도메인 보안 인텔리전스 목록의 내용을 참조하십시오.

단계 **2** 옵션 2: 맞춤형 보안 인텔리전스 목록 또는 피드를 사용합니다.

a) 맞춤형 보안 인텔리전스 목록 또는 피드를 생성합니다. 맞춤형 보안 인텔리전스 목록 또는 보안 인텔리전스 피드 생성를 참조하십시오.

b) IP 주소(네트워크) 및 URL의 경우: 액세스 제어 정책을 수정하려면 Security Intelligence(보안 인텔리전스) 탭을 클릭한 다음 Networks or URLs(네트워크 또는 URL) 하위 탭에서 맞춤형 목록 또는 피드를 클릭하고 **Add to Do Not Block List(**차단 안 함 목록에 추가**)**를 클릭합니다.

c) 변경 내용을 저장합니다.

d) 도메인(DNS)의 경우: 보안 인텔리전스 옵션, 6 페이지 항목의 "DNS 정책"섹션을 참조하십시오.

e) 변경 사항을 배포합니다.

보안 인텔리전스 문제 해결

사용 가능한 옵션 목록에 보안 인텔리전스 범주가 없음

증상**:** 액세스 제어 정책의 Security Intelligence(보안 인텔리전스) 탭에서, 보안 인텔리전스 범주(CnC, Exploitkit 등)는 Available Options(사용 가능한 옵션)의 Networks(네트워크) 탭에 표시되지 않습니다.

원인**:**

- 이러한 범주는 관리 센터에 하나 이상의 매니지드 디바이스를 추가할 때까지 표시되지 않습니다. 모든 TALOS 피드를 가져오려면 디바이스를 추가해야 합니다.
- URL 필터링 기능은 보안 인텔리전스 기능과 다른 범주 집합을 사용합니다. 표시되는 범주는 URL 필터링 범주일 수 있습니다. URL 필터링 범주를 보려면 액세스 제어 규칙의 **URL** 탭을 확인하십시오.

메모리 사용 문제 해결

증상**:** 보안 인텔리전스 차단 목록에 의해 차단되어야 하는 연결이 대신 액세스 제어 규칙에 의해 평가됩니다. 보안 인텔리전스 상태 모듈이 메모리가 부족하다고 알립합니다.

원인**:** 메모리 제한. Cisco Intelligence Feeds는 Cisco Talos Intelligence Group(Talos)의 최신 위협 인텔리전스에 기반합니다. 이러한 피드는 시간이 지남에 따라 커지는 경향이 있습니다. Firepower 디바이스는 피드 업데이트를 수신할 때 보안 인텔리전스에 할당한 메모리에 최대한 많은 항목을 로드합니다. 디바이스가 모든 항목을 로드할 수 없는 경우, 정상적으로 트래픽을 차단하지 못할 수 있습니다. 차단 목록에 의해 차단되어야 하는 일부 연결이 차단되는 대신 액세스 제어 규칙에 의해 계속 평가됩니다.

영향을 받는 플랫폼**:** 메모리가 적은 디바이스는 많은 보안 인텔리전스 범주를 차단 목록에 포함하거나 범주와 평판을 기준으로 URL도 필터링하는 경우, 이 문제가 발생할 가능성이 특히 높습니다. 이러한 디바이스에는 Firepower 7010, 7020, 7030; 5508-X, 5516-X NGIPSv가 포함됩니다.

해결 방법**:** 이 문제가 발생하고 있다고 생각하는 경우, 영향을 받는 디바이스에 설정을 다시 구축하십시오. 이렇게 하면 보안 인텔리전스에 더 많은 메모리를 할당할 수 있습니다. 문제가 계속되면 Cisco TAC(Technical Assistance Center)에 문의하십시오. 문제 확인을 돕고 구축에 적합한 솔루션을 제안할 수 있습니다.

보안 인텔리전스 차단 목록 히스토리

기능	버전	세부 사항
새로운 보안 인텔리전스 범주	모두	Talos는 다음과 같은 새로운 보안 인텔리전스 범주를 추가했습니다. • banking_fraud • ioc • high_risk • link_sharing • 발생하는 것만은 아님 • newly_seen • 스파이웨어 액세스 제어 및 DNS 정책을 업데이트하여 새 범주를 처리하고 향후 변경 사항을 주기적으로 확인해야 합니다. 신규/수정 페이지: Security Intelligence(보안 인텔리전스) 탭, Networks and URLs(네트워크 및 URL) 하위 탭; DNS 정책의 DNS 규칙 지원되는 플랫폼: FMC