보안 인텔리전스

보안 인텔리전스 정책을 사용하면 소스/대상 IP 주소 또는 대상 URL을 기준으로 원치 않는 트래픽을 미리 삭제할 수 있습니다. 다음 주제에서는 보안 인텔리전스를 구현하는 방법에 대해 설명합니다.

보안 인텔리전스 정보

보안 인텔리전스 정책을 사용하면 소스/대상 IP 주소 또는 대상 URL을 기준으로 원치 않는 트래픽을 미리 삭제할 수 있습니다. 시스템은 액세스 제어 정책을 사용하여 이 원치 않는 트래픽을 평가 전에 삭제하며, 이에 따라 사용된 시스템 리소스의 양이 줄어듭니다.

다음을 기반으로 트래픽을 차단할 수 있습니다.

- Cisco Talos Intelligence Group(Talos) 피드 - Talos에서는 정기적으로 업데이트되는 보안 인텔리전스 피드에 액세스할 수 있도록 지원합니다. 악성코드, 스팸, 봇넷, 피싱과 같은 보안 위협을 나타내는 사이트는 맞춤형 컨피그레이션을 업데이트하고 구축하는 속도보다 빠르게 나타났다 사라질 수 있습니다. 시스템에서는 피드 업데이트를 정기적으로 다운로드하므로 컨피그레이션을 재구축하지 않아도 새로운 위협 인텔리전스를 사용할 수 있습니다.

참고 Talos 피드는 기본적으로 1시간마다 업데이트됩니다. **Device(**디바이스**)** > **Updates(**업데이트**)** 페이지에서 업데이트 빈도를 변경할 수 있으며, 요구에 따라 피드를 업데이트할 수도 있습니다.

- 네트워크 및 URL 개체 — 차단하고 싶은 특정 IP 주소 또는 URL을 알고 있는 경우, 이에 대한 개체를 생성하여 차단 목록 또는 예외 목록에 추가할 수 있습니다. FQDN 또는 범위 사양을 갖춘 네트워크 개체는 사용할 수 없다는 점에 유의하십시오.

IP 주소(네트워크) 및 URL에 대한 별도의 목록을 생성합니다.

참고 HTTP/HTTPS 요청이 호스트 이름 대신 IP 주소를 사용하는 URL에 대한 요청인 경우, 시스템에서는 네트워크 주소 목록에서 IP 주소 평판을 조회합니다. 네트워크 및 URL 목록에서 IP 주소를 복제할 필요가 없습니다.

차단 목록에 대한 예외 설정

각 차단 목록에 대해 do not block list(차단 안 함 목록)이라고도 하는 관련 예외 목록을 생성할 수 있습니다. 예외 목록을 사용하는 유일한 목적은 차단 목록에 표시되는 IP 주소 또는 URL을 제외하는 것입니다. 즉, 사용해야 하고 안전하다고 알고 있는데 차단 목록에 구성된 피드에 있는 주소 또는 URL을 찾은 경우, 차단 목록에서 범주를 완전히 제거하지 않고도 네트워크/URL을 제외할 수 있습니다.

제외된 트래픽은 나중에 액세스 제어 정책을 기준으로 평가됩니다. 연결의 최종 허용/삭제 여부는 연결과 일치하는 액세스 제어 규칙에 따라 결정됩니다. 또한, 액세스 규칙에 따라 연결에 침입 또는 악성코드 검사를 적용할지도 결정됩니다.

보안 인텔리전스 피드 카테고리

다음 표에서는 Cisco Talos Intelligence Group(Talos) 피드에서 사용할 수 있는 카테고리에 대해 설명합니다. 이러한 범주는 네트워크와 URL 차단에 모두 사용할 수 있습니다.

이러한 범주는 시간이 지남에 따라 변경될 수 있으므로 새로 다운로드한 피드에 범주 변경 사항이 포함될 수 있습니다. 보안 인텔리전스를 구성할 때 범주 이름 옆의 정보 아이콘을 클릭하여 설명을 볼 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

보안 인텔리전스 카테고리	설명
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. 주의 현재 이 범주는 활성 피드를 갖지 않으며 나중에 사용하기 위해 예약되어 있습니다.
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
tor_exit_node	Tor Anonymizer 네트워크에 대한 종료 노드 서비스를 제공하는 것으로 알려진 호스트

보안 인텔리전스를 위한 라이선스 요건

보안 인텔리전스를 사용하려면 **IPS** 라이선스를 활성화해야 합니다. 선택 가능한 라이선스 활성화 또는 비활성화의 내용을 참조하십시오.

보안 인텔리전스 구성

보안 인텔리전스 정책을 사용하면 소스/대상 IP 주소 또는 대상 URL을 기준으로 원치 않는 트래픽을 미리 삭제할 수 있습니다. 모든 허용된 연결은 계속해서 액세스 제어 정책을 통해 평가되고 결과적으로 삭제될 수도 있습니다. 보안 인텔리전스를 사용하려면 IPS 라이선스를 활성화해야 합니다.

프로시저

단계 **1** **Policies(**정책**)** > **Security Intelligence(**보안 인텔리전스**)**를 선택합니다.

단계 **2** 정책이 활성화되지 않은 경우 **Enable Security Intelligence(**보안 인텔리전스 활성화**)** 버튼을 클릭합니다.

Security Intelligence(보안 인텔리전스**)** 토글을 클릭하여 **Off(**끄기**)**로 전환하면 언제든지 정책을 비활성화할 수 있습니다. 컨피그레이션은 보존되므로 정책을 다시 활성화할 때 다시 구성할 필요가 없습니다.

단계 **3** 보안 인텔리전스를 구성합니다.

네트워크(IP 주소) 및 URL에 대한 별도의 차단 목록이 있습니다.

a) **Network(**네트워크**)** 또는 **URL** 탭을 클릭하여 구성할 목록을 표시합니다.

b) 차단/드롭 목록에서 **+**를 클릭하여 연결을 즉시 삭제할 개체 또는 피드를 선택합니다.

개체 선택기는 유형별로 별도의 탭에서 개체 및 피드를 구성합니다. 원하는 개체가 아직 없는 경우 목록 하단에서 **Create New Object(**새 개체 생성**)** 링크를 클릭하여 바로 생성합니다. Cisco Talos Intelligence Group(Talos) 피드에 대한 설명을 보려면 피드 옆에 있는 **i** 버튼을 클릭합니다. 보안 인텔리전스 피드 카테고리, 2 페이지도 참조하십시오.

참고 보안 인텔리전스는 /0 넷마스크를 사용하는 IP 주소 블록을 무시합니다. 여기에는 any-ipv4 및 any-ipv6 네트워크 개체가 포함됩니다. 네트워크 차단용으로 이러한 개체를 선택하지 마십시오.

c) Do Not Block(차단 안 함) 목록에서 **+**를 클릭하고 차단 목록에 예외 사항을 선택합니다.

이러한 목록을 구성하는 유일한 이유는 차단 목록에 있는 IP 주소 또는 URL에 대한 예외 사항을 만드는 것입니다. 제외된 연결은 나중에 액세스 제어 정책을 기준으로 평가되고 어떤 식으로든 삭제될 수 있습니다.

d) 다른 차단 목록을 구성하려면 이 프로세스를 반복합니다.

단계 **4** (선택 사항). **Edit Logging Settings(**기록 설정 수정**)** 버튼()을 클릭하여 기록을 컨피그레이션합니다.

로깅을 활성화하면 차단 목록 항목과 일치하는 항목이 로깅됩니다. 로깅이 활성화된 상태에서 제외된 연결이 액세스 제어 규칙과 일치하는 경우에는 로그 메시지를 받더라도 예외 항목과 일치하는 항목은 로깅되지 않습니다.

다음 설정을 구성합니다.

- **Connection Events Logging(**연결 이벤트 로깅**)** - 로깅을 활성화 또는 비활성화하려면 토글을 클릭합니다.
- **Syslog** - 외부 syslog 서버로 이벤트의 복사본을 전송하려는 경우 이 옵션을 선택하고 syslog 서버를 정의하는 서버 개체를 선택합니다. 필요한 개체가 아직 없으면 **Add Syslog Server(Syslog** 서버 추가**)**를 클릭하여 개체를 생성합니다.

  디바이스의 이벤트 스토리지는 제한되어 있으므로 외부 syslog 서버로 이벤트를 전송하면 더 장기적으로 저장할 수 있으며 이벤트 분석 성능이 개선됩니다.

보안 인텔리전스 모니터링

보안 인텔리전스 정책에 대해 로깅을 활성화한 경우 시스템에서는 차단 목록의 항목과 일치하는 각 연결에 대해 보안 인텔리전스 이벤트를 생성합니다. 이러한 연결에는 일치하는 연결 이벤트가 있습니다.

삭제된 연결에 대한 통계가 Monitoring(모니터링) 페이지에서 사용할 수 있는 다양한 대시보드에 표시됩니다.

Monitoring(모니터링**)** > **Access and SI Rules(**액세스 및 **SI** 규칙**)** 대시보드에는 트래픽과 가장 많이 일치하는 액세스 규칙 및 보안 인텔리전스 규칙에 상응하는 규칙이 표시됩니다.

또한, **Monitoring(**모니터링**)** > **Events(**이벤트**)**를 선택한 다음 **Security Intelligence(**보안 인텔리전스**)** 보기를 선택하여 **Connection(**연결**)** 탭에서 관련 연결 이벤트뿐만 아니라 보안 인텔리전스 이벤트를 볼 수 있습니다.

- 이벤트의 SI 범주 ID 필드는 네트워크 또는 URL 개체나 피드와 같이 차단 목록에서 일치하는 개체를 나타냅니다.
- 연결 이벤트의 Reason(이유) 필드에서는 이벤트에 표시된 작업이 적용된 이유에 대해 설명합니다. 예를 들어 IP 차단 또는 URL 차단과 같이 이유와 페어링된 차단 작업은 보안 인텔리전스가 연결을 삭제했음을 나타냅니다.

보안 인텔리전스의 예시

사용 사례 장에는 보안 인텔리전스 정책을 구현하는 예시가 포함되어 있습니다. 위협을 차단하는 방법의 내용을 참조하십시오.