Secure Endpoint Cloud Console에서 IP 허용 및 차단 목록 구성

목차

소개

이 문서에서는 Cisco Secure Endpoint의 IP 허용/차단 기능에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco는 Cisco Secure Endpoints 포털에 액세스할 수 있는 것을 권장합니다.

사용되는 구성 요소

이 문서의 정보는 Secure Endpoint 콘솔을 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

보안 엔드포인트로 IP 허용/차단 목록 구성

IP Allow/Block List란?

IP 차단 및 허용 목록은 디바이스 흐름 상관관계와 함께 사용되어 맞춤형 IP 주소 탐지를 정의합니다. 목록을 생성한 후, Cisco 인텔리전스 피드와 함께 또는 단독으로 사용하도록 정책에서 정의할 수 있습니다. 개별 IP 주소, CIDR 블록 또는 IP 주소와 포트 조합을 사용하도록 목록을 정의할 수 있습니다. 목록을 제출하면 중복 주소가 백엔드에서 결합됩니다.

IP 주소 예

이러한 항목을 목록에 추가하는 경우

- 192.0.2.0/24
- 192.0.2.15
- 192.0.2.135
- 192.0.2.200

목록은 다음과 같은 결과로 처리됩니다.

- 192.0.2.0/24

그러나 포트도 포함할 경우 결과는 달라집니다.

- 192.0.2.0/24
- 192.0.2.15:80
- 192.0.2.135
- 192.0.2.200

목록은 다음과 같은 결과로 처리됩니다.

- 192.0.2.0/24
- 192.0.2.15:80

IP 허용 목록이란?

IP 허용 목록을 사용하면 탐지하지 않을 IP 주소를 지정할 수 있습니다. IP 허용 목록의 항목은 IP 차단 목록 및 Cisco 인텔리전스 피드에서 재정의를 생성합니다. 단일 IP 주소, 전체 CIDR 블록을 추가하거나 포트 번호를 사용하여 IP 주소를 지정하도록 선택할 수 있습니다.

IP 차단 목록이란?

IP 차단 목록을 사용하면 컴퓨터 중 하나가 IP 주소에 연결될 때마다 탐지할 IP 주소를 지정할 수 있습니다. 단일 IP 주소, 전체 CIDR 블록을 추가하거나 포트 번호를 사용하여 IP 주소를 지정하도록 선택할 수 있습니다. 컴퓨터가 목록의 IP 주소에 연결할 때 수행되는 작업은 정책의 Network 섹션에서 지정한 내용에 따라 달라집니다.

격리 IP 허용 목록이란 무엇입니까?

격리 IP 허용 목록은 격리 중에 차단되지 않은 IP 주소를 지정합니다. 격리 IP 허용 목록은 격리 IP 허용 목록이 규칙의 포트 번호를 지원하지 않는다는 점에서 IP 허용 목록과 다릅니다.

IP 허용/차단 목록 만들기

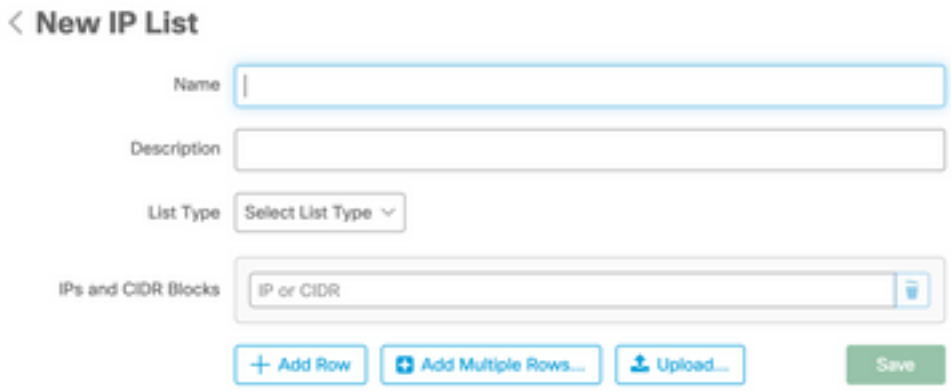
1단계. IP 목록을 생성하려면 이미지에 표시된 대로 Secure Endpoint 포털에서 **Outbreak Control**로 이동하고 **IP Block & Allow Lists**(**IP 차단 및 허용 목록**) 옵션을 클릭합니다.

IP 차단 및 허용 목록

2단계. 이미지에 표시된 대로 **Create IP List** feature(**IP 목록** 기능 생성)를 선택합니다.

IP 목록 생성

3단계. New IP List(새 IP 목록) 페이지가 표시됩니다. 새 목록의 이름과 설명을 입력하고 이미지에 표시된 대로 List Type 드롭다운 목록에서 **Allow**, **Block** 또는 **Isolation Allow**를 선택합니다.



IP 목록 컨피그레이션

4단계. 행당 하나의 IP 주소 또는 CIDR 블록을 입력할 수 있습니다. IP 주소를 입력할 수 있는 옵션은 다음과 같습니다.

- 행 추가**를** 클릭하여 단일 행을 추가할 수 있습니다.
- Add Multiple Rows(여러 행 추가)를 선택한 경우 여러 IP 주소 및 CIDR 블록을 빠르게 **추가할 수도 있습니다**.
- 그런 다음 IP 주소와 CIDR 블록의 목록을 입력하거나 대화 상자에 붙여 넣은 다음 완료되면 **Add Rows(행 추가)**를 클릭합니다.
- 또한 IP 주소 및 CIDR 블록을 포함하는 CSV 파일을 새 줄 문자로 구분하여 업로드할 수 있습니다. 파일을 업로드하려면 Upload(**업로드**)를 클릭한 다음 Browse(찾아보기)를 클릭하여 CSV 파일을 선택하고 **Upload(업로드)**를 클릭합니다. 목록 유형에서 허용 목록, 차단 목록 또는 격리 허용 중 어떤 것을 사용할지 선택합니다.

5단계. 완료되면 IP 주소 목록 컨피그레이션을 저장합니다.

추가 컨피그레이션 예

IP 주소와 상관없이 차단 또는 허용 목록에 포트를 추가하려면 적절한 목록에 두 개의 항목을 추가합니다. 여기서 XX는 차단할 포트 번호입니다.

- 0.0.0.1/1:XX
- 128.0.0.1/1:XX

참고: 업로드된 IP 목록은 최대 100,000개의 행을 포함하거나 최대 2MB 크기일 수 있습니다. 현재 IPv4 주소만 지원됩니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.