악성 IP

악성 IP

추가 보안 보호 기능을 활성화하여 알려진 악성 IP와의 통신을 차단할 수 있습니다. 이러한 악성 IP는 TrustWave에서 정의하며 보안 프로파일 규칙 집합으로 멀티 클라우드 방어에 통합됩니다. 규칙 집합은 TrustWave에서 업데이트를 제공하므로 자주 업데이트됩니다. 악성 IP 프로파일의 자동 업데이트 설정을 사용하여 업데이트를 정책 규칙 집합에 동적으로 적용할 수 있습니다.

Note TrustWave는 학습된 다양한 동작을 기반으로 악성 IP를 식별합니다.

- 웹 허니팟에서 악의적인 공격자 식별
- 봇넷 C&C 호스트
- Tor 출구 노드
- 기타 학습된 행동

악의적인 IP 프로파일 생성

단계 **1** **Manage(**관리**)** > **Profiles(**프로파일**)** > **Malicious IP(**악성 **IP)**로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

단계 **3** 이름과 설명을 제공합니다.

단계 **4** IP Reputation(IP 평판)을 활성화하려면 확인란을 선택합니다.

단계 5 TrustWave 규칙 집합 버전 선택에 대해 수동 또는 자동 모드를 클릭합니다.

단계 6 Manual(수동) 모드의 경우 드롭다운에서 *TrustWave Ruleset Version(TrustWave* 규칙 집합 버전*)*을 선택합니다. 선택한 규칙 집합 버전은 이 프로파일을 사용하는 모든 게이트웨이의 멀티 클라우드 방어 데이터 경로 엔진에 사용됩니다. 프로파일은 최신 규칙 집합 버전으로 자동 업데이트되지 않습니다.

단계 7 Automatic(자동) 모드의 경우, 멀티 클라우드 방어에서 규칙 집합 버전을 게시한 후 업데이트를 며칠 단위로 지연할지 선택합니다. 멀티 클라우드 방어에서는 새 규칙 집합을 자주 게시하며 이 프로파일을 사용하는 게이트웨이는 N일 이상의 최신 규칙 집합 버전으로 자동 업데이트됩니다. 여기서 N은 드롭다운에서 선택한 "delay by days(지연 일수)" 인수입니다. 예를 들어 2021년 1월 10일의 구축을 5일 연기하도록 선택하는 경우 멀티 클라우드 방어 컨트롤러는 1월 5일 또는 그 이전에 게시된 규칙 집합 버전을 선택합니다. 해당 규칙 집합 버전을 사용한 내부 테스트가 어떤 이유로 실패할 경우 멀티 클라우드 방어이(가) 게시되지 않을 수도 있습니다.

What to do next

악성 **IP** 프로파일 연결

이 문서를 확인하여 규칙을 생성/편집합니다.

IP 평판

IP Reputation(IP 평판) 확인란은 프로파일을 활성화 또는 비활성화하는 수단으로 사용됩니다. 프로파일을 선택하고 프로파일이 정책 규칙 집합 규칙에 첨부되면, 악성 IP 보호가 시행됩니다. 이 옵션을 선택하지 않고 프로파일이 정책 규칙 집합 규칙에 첨부된 경우, 악성 IP 보호가 시행되지 않습니다. 항상 프로파일의 IP Reputation(IP 평판) 확인란을 선택하여 프로파일이 활성화된 것과 같은 방법을 권장합니다. 악성 IP 프로파일을 비활성화하려면 확인란의 선택을 취소하는 대신 정책 규칙 집합 규칙에서 해당 연결을 제거합니다.

악성 IP 검사기

TrustWave는 IP 주소가 악성 IP로 나열되어 있는지 여부를 확인하는 데 사용할 수 있는 온라인 IP 평판 서비스(https://rbladmin.marshal.com/)를 제공합니다.