FMC 상관관계 정책 허용 목록 이벤트를 사용하려면 네트워크 검색 정책을 사용하도록 설정해야 함

목차

문제

Cisco FMC(Secure Firewall Management Center)에서 허용 목록을 사용하여 상관관계 정책을 구성할 때, 대상 네트워크 IP에 네트워크 검색 정책을 구성하지 않는 한 허용 목록 이벤트 및 허용 목록 위반은 생성되지 않습니다. 이 컨피그레이션이 없으면 Analysis > Correlation > Allow List Events and Analysis > Correlation > Allow List Violations 아래에 이벤트가 표시되지 않습니다.

실험실 테스트 중 다음과 같은 동작이 관찰되었습니다.

- 상관관계 이벤트는 구성된 대상 네트워크에 대해 올바르게 생성됩니다.
- No Allow List Events 또는 Allow List Violations는 대상 네트워크 호스트가 규정을 준수하지 않을 때 생성됩니다.

환경

- FMC(Secure Firewall Management Center)에서 관리되는 Cisco FTD(Firepower Threat Defense)
- 특정 IP 주소를 대상으로 하는 허용 목록으로 구성된 상관관계 정책
- 특정 웹 애플리케이션, 애플리케이션 또는 프로토콜을 허용하도록 구성된 허용 목록

해결

개발 팀과 광범위한 랩 테스트 및 협의를 거친 결과, Allow List Events(목록 이벤트 허용) 및 Allow List Violations(목록 위반 허용)가 생성되기 위한 전제 조건으로 네트워크 검색 정책을 활성화해야 합니다.

해결에는 다음 단계가 포함됩니다.

1단계: 네트워크 검색 정책 사용

FMC 인터페이스에서 Policies(정책) > Network Discovery(네트워크 검색)로 이동하고 규칙이 없는 경우 규칙을 생성합니다.

2단계: 네트워크 검색 규칙 구성

적절한 소스 네트워크 설정으로 네트워크 검색 규칙을 구성합니다.

- 소스 네트워크를 내부 네트워크 범위로 지정합니다.
- 또는 모든 트래픽 소스를 모니터링하는 경우 모든 네트워크(0.0.0.0/0)를 사용합니다.
- 규칙이 Allow List Events를 생성할 것으로 예상되는 네트워크를 포함하는지 확인합니다.

3단계: 상관관계 정책 규칙 활성화

상관관계 정책 규칙이 활성 상태이고 비활성 상태가 아닌지 확인합니다.

4단계: 허용 목록 이벤트 생성 확인

네트워크 검색을 활성화하고 상관관계 정책 규칙을 활성화한 후:

1.- 브라우저를 사용하여 구성된 대상 네트워크에서 웹 사이트에 액세스합니다(호스트를 비준수 상태로 설정).

2.- Monitor Analysis(분석 모니터링) > Correlation(상관관계) > Allow List Events(이벤트 목록 허용) 및 Analysis(분석) > Correlation(상관관계) > Allow List Violations for event generation(이벤트 생성을 위한 목록 위반 허용)

3.- 호스트가 규정을 준수하지 않을 때 이벤트가 채워졌는지 확인합니다.

실험실 테스트에서 네트워크 검색이 활성화되면 규정을 준수하지 않는 호스트에 대해 허용 목록 이벤트 및 허용 목록 위반이 성공적으로 생성되었음을 확인했습니다.

원인

근본 원인은 네트워크 검색 정책이 FMC 상관관계 정책에서 허용 목록 이벤트를 생성하기 위한 필수 전제 조건이기 때문입니다. 활성 네트워크 검색 정책이 없으면 시스템은 구성된 허용 목록에 대해 호스트 규정 준수를 제대로 평가할 수 없으므로 대상 네트워크 호스트가 규정을 준수하지 않을 때 허용 목록 이벤트가 생성되지 않습니다.

관련 콘텐츠

- Cisco FMC Correlation Compliance Lists 설명서
- Cisco 기술 지원 및 다운로드

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.