Secure Access Webhook 통합을 위한 IP 범위 및 방화벽 구성

문제

서드파티 통합은 Cisco SSE(Secure Access) 대시보드에서 성공적으로 로드되지만 SIEM 통합을 위한 온프레미스 HTTP 커넥터에서 Webhook 기반 보안 이벤트가 수신되지 않습니다. 조직에서는 방화벽 규칙을 올바르게 구성하고 Webhook 이벤트 전달을 활성화하기 위해 Cisco SSE 소스 IP 범위(지역별 IP 포함)에 대한 설명이 필요합니다.

환경

- 제품: Cisco SSE(Secure Access)
- 기술: 솔루션 지원 - 보안 액세스 보고 및 로깅
- 통합 유형: Webhook 기반 서드파티 통합
- 대상 커넥터: 온-프레미스 HTTP 커넥터 서버

해결

Cisco Secure Access Integrations의 Webhook 전달 문제를 해결하려면 지정된 SSE 소스 IP 범위에서 온-프레미스 커넥터로의 인바운드 HTTPS 트래픽을 허용하도록 방화벽 규칙을 구성합니다.

Cisco SSE 소스 IP 범위

다음과 같은 Cisco SSE 소스 IP 범위에서 인바운드 HTTPS 연결을 허용하도록 방화벽을 구성합니다.

```
146.112.161.0/24
```

```
146.112.163.0/24
146.112.165.0/24
146.112.167.0/24
```

방화벽 컨피그레이션 단계

1단계: 서드파티 통합 상태 확인

SSE 대시보드에서 Admin(관리) > Third Party Integrations(서드파티 통합)로 이동하여 조직에 맞게 통합이 로드되고 있는지 확인합니다.

2단계: 방화벽 규칙 구성

SSE 소스 IP 범위에서 온-프레미스 커넥터 서버로의 인바운드 HTTPS 트래픽(포트 443)을 허용하는 방화벽 규칙을 만듭니다. 네트워크 방화벽 및 인터넷과 커넥터 서버 사이의 모든 중간 방화벽에 규칙이 적용되었는지 확인합니다.

3단계: Webhook 이벤트 전달 확인

방화벽 변경 사항을 구현한 후 온-프레미스 HTTP 커넥터를 모니터링하여 Cisco SSE에서 Webhook 이벤트를 수신하고 있는지 확인합니다.

지역 IP 정보

Cisco SSE는 EU 및 미국 지역의 공유 IP 범위만 사용합니다. 제공된 IP 범위는 두 지역 구축을 모두 포괄하며 조직이 속한 기본 지역에 관계없이 구성해야 합니다.

원인

Cisco Secure Access의 Webhook 이벤트는 SSE 소스 IP 주소에서 온-프레미스 HTTP 커넥터 서버로의 인바운드 HTTPS 연결을 허용하지 않는 방화벽 규칙에 의해 차단됩니다. SSE 대시보드에 통합 로드가 성공적으로 표시되지만, 실제 Webhook 전달에는 Cisco 인프라의 트래픽이 사용자 커넥터 엔드포인트에 도달할 수 있도록 특정 방화벽 컨피그레이션이 필요합니다.

관련 콘텐츠

- Cisco Secure Access 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.