SIEM 통합을 위한 웹 후크 기반 보안 이벤트 수신 온프레미스 HTTP 커넥터 수신 SIEM 통합

목차

문제

Webhook 기반 보안 이벤트는 SIEM 통합을 위한 온-프레미스 HTTP 커넥터에서 수신되지 않습니다.

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
- 대시보드 상태: Admin(관리) > Third Party Integrations(서드파티 통합)에서 서드파티 통합이 성공적으로 로드되었습니다.

해결

Cisco Secure Access 서드파티 통합으로 인한 웹후크 전달 문제를 해결하려면 이러한 Cisco SSE 소스 IP 범위에서 인바운드 HTTPS 트래픽을 허용하도록 방화벽 규칙을 구성합니다.

필수 방화벽 구성

다음 Cisco SSE 소스 IP 범위에서 온-프레미스 커넥터로 향하는 인바운드 HTTPS 트래픽을 허용합니다.

```
146.112.161.0/24

146.112.163.0/24

146.112.165.0/24

146.112.167.0/24
```

이러한 IP 범위는 Cisco SSE가 EU 및 미국 지역 모두에서 Webhook 전달을 위해 사용하는 공유 IP 주소를 나타냅니다.

확인 단계

1단계: SSE 대시보드에서 서드파티 통합 상태를 확인합니다.

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

2단계: 방화벽 규칙을 구성합니다.

제공된 SSE IP 범위에서 온-프레미스 커넥터 서버로의 인바운드 HTTPS 연결을 허용하도록 네트워크 방화벽 및 중간 방화벽을 업데이트합니다.

3단계: Webhook 이벤트 전달 모니터링

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

추가 트러블슈팅

방화벽 규칙을 구성한 후에도 webhook 이벤트가 여전히 수신되지 않는 경우:

- 온-프레미스 커넥터가 올바르게 구성되어 있고 예상 포트에서 수신 대기 중인지 확인합니다.
- SSE 소스 IP와 커넥터 엔드포인트 간의 네트워크 연결을 확인합니다.
- SSE 대시보드에서 Webhook 통합 컨피그레이션을 검토합니다.
- 실시간 Webhook 제공을 검토하기 위해 실시간 문제 해결 세션 예약을 고려하십시오.

원인

네트워크 방화벽이 Cisco SSE 소스 IP 주소에서 온-프레미스 HTTP 커넥터로의 인바운드 HTTPS 연결을 차단할 경우 웹 후크 전달 오류가 발생합니다. Cisco SSE는 EU 및 미국 지역의 공유 인프라에서 특정 IP 범위를 사용하여 웹후크 이벤트를 전달하며, 성공적인 이벤트 전달을 위해서는 방화벽 구성을 통해 이러한 범위를 명시적으로 허용해야 합니다.

관련 콘텐츠

- 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.