Impact=Unknown을 보여주는 FMC 침입 이벤트 문제 해결

목차

문제

새 FMC(Firewall Management Center)를 구축하고 버전 7.7.12로 업그레이드한 후, 모든 침입 이벤트는 예상 영향 값 대신 "Impact=Unknown"을 표시합니다. 그러면 경고 컨피그레이션에 영향 필드가 필요하므로 적절한 경고 메커니즘이 트리거되지 않습니다.

환경

- FMC 버전 7.7.12. 다른 소프트웨어 버전도 영향을 받을 수 있습니다.
- 방지 또는 탐지 모드의 침입 정책.

해결

이 문제를 해결하려면 침입 이벤트가 생성되는 모든 관련 IP 주소를 포함하도록 검색 정책 범위를 확인하고 구성합니다.

1단계. 영향을 받는 IP 주소 식별

"Impact=Unknown"이 표시된 침입 이벤트를 검토하고 이러한 이벤트와 관련된 특정 IP 주소를 식별합니다. 이러한 IP 주소를 문서화하여 현재 검색 정책 컨피그레이션과 비교합니다.

2단계. 현재 검색 정책 컨피그레이션 검토

FMC Policies(FMC 정책) > Network Discovery(네트워크 검색)로 이동하고(최신 버전에서는 Policies(정책) > Advanced(고급) > Network Discovery(네트워크 검색)) 현재 검색 정책 설정을 검토하여 검색 범위에 현재 포함된 IP 주소 범위 또는 서브넷을 확인합니다.

3단계. 검색 정책 범위 업데이트

침입 이벤트가 발생하는 모든 IP 주소를 포함하도록 검색 정책 컨피그레이션을 수정합니다. 적절한 영향 평가와 함께 침입 이벤트를 수신할 것으로 예상되는 모든 네트워크 세그먼트를 검색 정책 범위에 포함해야 합니다.

4단계. 컨피그레이션 변경 사항 구축

모든 관리되는 디바이스에 업데이트된 검색 정책 컨피그레이션을 구축하여 전체 보안 인프라에 변경 사항이 적용되도록 합니다.

5단계. 영향 필드 채우기 확인

새 침입 이벤트를 모니터링하여 영향 필드가 이제 "Unknown(알 수 없음)" 대신 적절한 값으로 채워지고 있는지 확인합니다.

원인

"Impact=Unknown"을 표시하는 침입 이벤트는 영향받는 IP 주소가 FMC의 검색 정책에 포함되지 않은 컨피그레이션 문제로 인해 발생했습니다. IP 주소가 구성된 검색 정책의 범위를 벗어나는 경우 FMC에서 해당 주소에 대한 침입 이벤트의 영향을 제대로 평가할 수 없으므로 영향 필드가

"Unknown(알 수 없음)" 값으로 채워집니다. 이는 소프트웨어 또는 하드웨어 결함이 아니라 컨피그레이션과 관련된 문제입니다.

관련 콘텐츠

- 침입 이벤트 영향 레벨
- 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.