경고 작업을 위한 보안 액세스 보안 프로파일 암호 해독 요구 사항

목차

문제

사용자는 액세스 정책 작업이 Warning(경고)으로 설정된 경우 보안 프로파일 설정에서 암호 해독을 활성화해야 하는지 여부와 관련하여 Cisco Secure Access에 대한 컨피그레이션 지침이 필요합니다. 특정 질문은 이러한 보안 프로필 기능에 적용됩니다.

- 위협 범주
- 파일 검사
- Cisco Secure Malware Analytics
- 파일 형식 차단
- 안전 검색

이 질문은 이러한 보안 기능이 제대로 작동하기 위한 액세스 정책 경고 작업과 보안 프로필 해독 요구 사항 간의 관계를 이해하는 데 중점을 둡니다.

환경

- 제품: Cisco Secure Internet Access Advantage
- 기술: 보안 액세스
- 소프트웨어 버전: 모두
- 설정: 다양한 보안 기능이 포함된 보안 프로파일
- 정책 구성: Warning 작업 설정이 있는 액세스 정책

해결

랩 검증을 통해 보안 프로필에서 암호 해독만 사용하도록 설정되어 있고 다른 모든 기능이 사용하지 않도록 설정된 경우에도 액세스 정책 경고 작업이 정상적으로 작동함을 확인했습니다. 즉, 이러한 보안 프로파일 기능의 경우 Warning 작업을 사용할 때 각 개별 기능에 대해 특별히 암호 해독을 활성화할 필요가 없습니다.

- 위협 범주
- 파일 검사
- Cisco Secure Malware Analytics
- 파일 형식 차단
- 안전 검색

컨피그레이션 지침

경고 작업으로 액세스 정책을 구성하는 경우:

1단계: 원하는 정책 규칙에 대해 Warning(경고)으로 액세스 정책 작업을 구성합니다.

2단계: Security Profile 설정에서 Decryption이 프로파일 레벨에서 활성화되어 있는지 확인합니다.

3단계: 개별 보안 기능(위협 범주, 파일 검사, Cisco Secure Malware Analytics, 파일 유형 차단, 안전 검색)은 특정 암호 해독 설정에서 비활성화한 상태로 유지되지만 경고 조치에서는 정상적으로 작동할 수 있습니다.

이 컨피그레이션 접근 방식을 사용하면 보안 프로파일 기능 관리의 유연성을 유지하면서 경고 조치가 올바르게 작동할 수 있습니다.

원인

액세스 정책의 경고 작업은 개별 보안 프로파일 기능 암호 해독 요구 사항과 다른 수준에서 작동합

니다. Warning 작업은 각 특정 보안 기능에 대해 개별 암호 해독 활성화를 요구하지 않고 보안 프로파일 레벨에서 활성화된 기본 암호 해독 설정만 사용하여 작동할 수 있습니다.

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.