Cisco XDR의 알려진 문제

목차

소개

이 문서에서는 Cisco XDR에 대해 현재 알려진 기술 문제를 다룹니다.

Cisco는 검토 중, 해결 중 또는 예상대로 작동하는 것으로 간주하여 기술적인 문제를 승인할 수 있습니다.

알려진 문제:

사고

1.- 작업 표시 해당 없음 옵션은 XDR 인시던트 생성에만 고려되고 인시던트 업데이트에는 고려되지 않습니다.

> 상태: 문제 식별 및 해결 보류 중
>
> 세부 정보: Cisco XDR 안내 응답 플레이북 숨기기 옵션 제공 현재 인시던트에 적용되지 않는 작업 2024년 10월, Cisco는 적용 가능한 Observables가 없는 작업을 자동으로 숨기도록 Cisco XDR을 개선했습니다. 이 개선 사항은 인시던트가 생성될 때 작동하지만 업데이트 시 적용 가능한 작업은 평가하지 않습니다.
>
> 다음 단계: Cisco는 이 문제를 해결하기 위해 노력하고 있습니다.
>
> 예상 해결 방법: 2024년 12월

조사

현재 이 XDR 기능에 대해 알려진 문제가 없습니다.

Cisco 통합

현재 이 XDR 기능에 대해 알려진 문제가 없습니다.

서드파티 통합

1.- G-type 라이센스가 있는 Microsoft 고객은 XDR Microsoft 통합을 사용할 수 없습니다.

상태: 설계대로 작업

세부 정보: Microsoft G-type 자격은 정부 기관의 제한된 환경에서만 액세스를 프로비저닝합니다.

다음 단계: Cisco는 Microsoft와 협력하여 요구 사항 파악 수신 통합 Microsoft GCC 환경에서 Microsoft G-type 자격 부여 제공됨. 가능하다면 Cisco XDR은 Microsoft Defender for Endpoint, O365 및 Entra용 Microsoft G-type 라이센스와 통합하려고 합니다.

자산

현재 이 XDR 기능에 대해 알려진 문제가 없습니다.

XDR 자동화

1.- XDR 인시던트 자동화 규칙이 예기치 않게 중지됩니다.

상태: 문제 식별 및 해결 보류 중

세부 정보: 인시던트 자동화 규칙 제공 워크플로 및 트리거 예기치 않게 실행이 중지됩니다. 이 표시되지 않음 XDR 사용자 인터페이스에서 검토 시 제외 다음에 대한 메트릭 워크플로는 시간이 지남에 따라 실행됩니다. 이렇게 하면 문제가 지속된 기간에 따라 워크플로가 축소되거나 전혀 실행되지 않습니다.

다음 단계: Cisco에서는 이 문제를 XDR 백 엔드에서 문제로 식별했으며 이를 해결하기 위해 노력하고 있습니다. 또한 Cisco는 향후 이 문제가 발생하지 않도록 추가적인 모니터링 및 상태 추적 기능을 구현할 계획입니다.

해결 방법: 규칙을 비활성화하고 다시 활성화하여 워크플로 규칙 트리거 및 처리의 재시작을 시작합니다.

예상 해결 방법: 2025년 1월

XDR 분석

현재 이 XDR 기능에 대해 알려진 문제가 없습니다.

보안 클라이언트

1.- 보안 클라이언트/엔드포인트 배포는 Microsoft Intune/Microsoft Defender for Endpoint 업데이트

의 영향을 받아 제대로 설치되지 않습니다.

상태: 설계대로 작업

세부 정보: 지속적: 이 문제는 Cisco XDR 고객이 Cisco XDR에서 Cisco Secure Client for Network Visibility Module(NVM) 사용을 설치하는 데 영향을 줍니다. Intune을 통해 구성된 Microsoft Defender for Endpoint 설정은 Secure Client가 제대로 설치되지 않도록 제한합니다. Microsoft Defender for Endpoint Attack Surface Reduction에서 현재 미리 보기 중인 피쳐가 있는 경우 공격 표면 감소 - 복사 또는 가장된 시스템 도구 사용 차단(미리 보기)이(가) 비활성화되어 있으면 설치가 수행될 수 있습니다.

다음 단계: Cisco Secure Client는 설치를 시도할 때 예상대로 동작합니다. 그러나 Microsoft Defender for Endpoint/Microsoft Intune으로 인해 설치에 예기치 않은 간섭이 발생합니다. Cisco는 이 문제를 겪고 있는 고객을 위한 해결 방법을 찾아냈습니다.

해결 방법: 이 기능에 대한 컨피그레이션은 애플리케이션 개발자에게 문의하거나 이 기능을 통해 이 기능에 대해 자세히 설명하는 것이 좋습니다 기술 자료. 즉각적인 교정을 위해 Intune에서 관리되는 끝점을 덜 제한적인 정책으로 이동하거나 적절한 조치가 취해질 때까지 이 기능을 명시적으로 일시적으로 해제할 수 있습니다. Intune 관리 포털의 이 설정은 보안 끝점 연결을 복원하는 임시 측정값으로 사용되었습니다.

이 문제에 대한 자세한 내용은 다음을 참조하십시오. 기사.

Cisco 지원에 문의해야 하는 경우 이 링크에 제공된 지침을 따릅니다.

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.