Secure Endpoint Console에서 탐지 엔진 식별

목차

[소개](#)

[사전 요구 사항](#)

- [요구 사항](#)
- [사용되는 구성 요소](#)

[문제](#)

[솔루션](#)

소개

이 문서에서는 Secure Endpoint 콘솔에서 특정 탐지를 담당하는 엔진을 식별하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco Secure Endpoint 콘솔

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- Secure Endpoint Console v5.4.2025030619

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

문제

특정 탐지를 담당하는 올바른 엔진을 확인하는 것은 이벤트의 특성을 이해하고 효과적으로 이를 선별하는 초기 단계 중 하나입니다.

솔루션

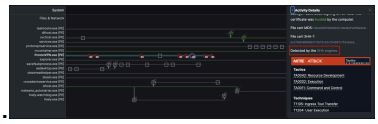
1. AMP 콘솔의 Events(이벤트) 페이지로 이동하여 더 자세히 조사할 이벤트를 찾습니다.
2. 강조 표시된 아이콘을 클릭하여 Device Trajectory(디바이스 전파 흔적 분석)를 엽니다. 

디바이스 전파 흔적 분석 아이콘

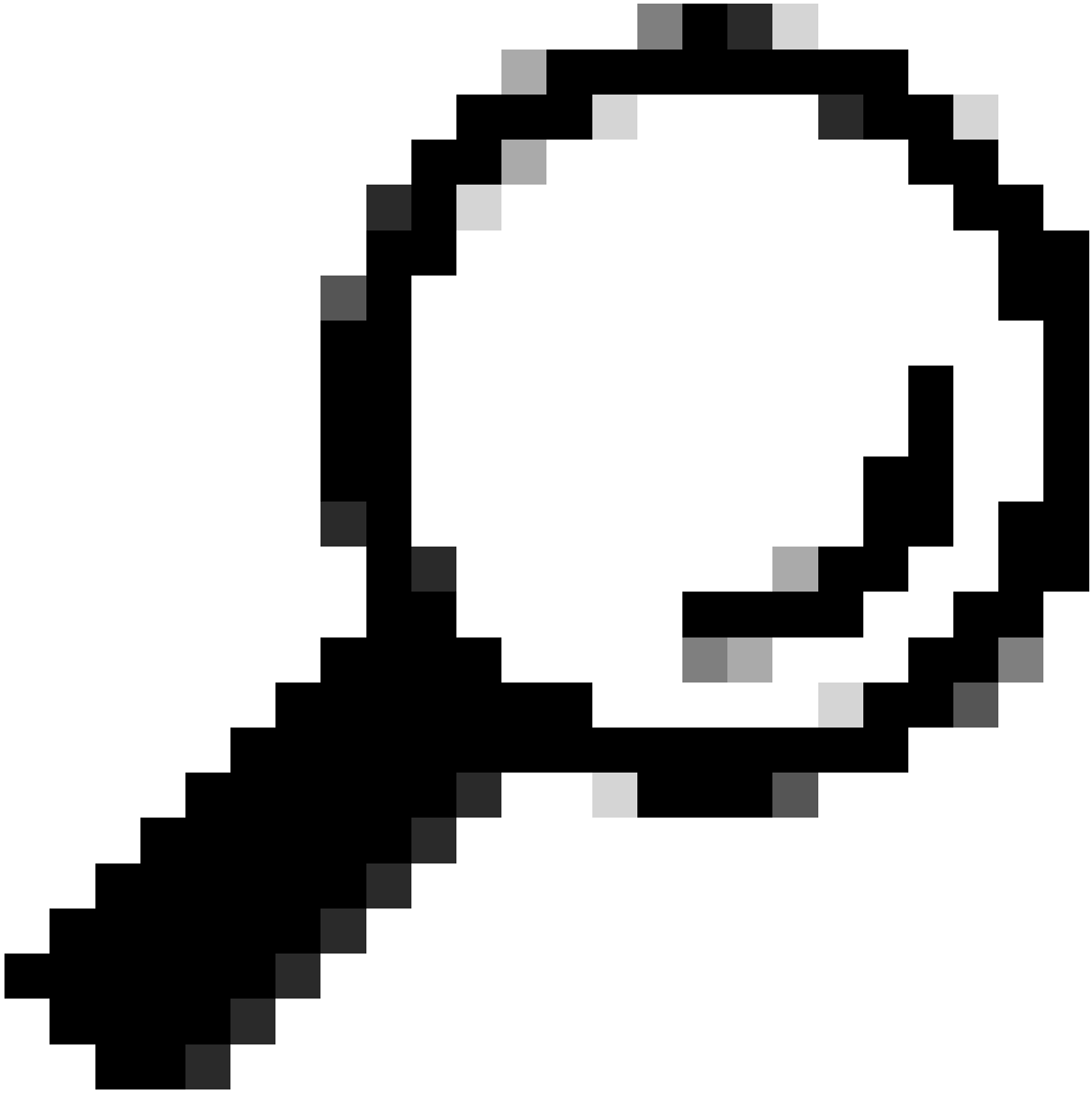
3. Activity Details(활동 세부사항) 아래의 오른쪽에 있는 이벤트 세부사항을 볼 수 있습니다.

디바이스 전파 흔적의 이벤트 세부 정보

4. 아래쪽으로 스크롤하여 Detected by(탐지된 사람) 섹션을 찾습니다.



섹션별로 탐지됨



팁: 이 정보를 이해하는 것은 위협의 특성을 평가하고 구성할 적절한 제외를 신속하게 결정하는 데 필수적입니다. 또한 오탐 조사를 위해 TAC에 케이스를 제출할 때 이러한 세부 정보를 제공하면 프로세스를 신속하게 진행할 수 있습니다.

Detected By(탐지자) 섹션을 볼 수 없거나 추가 지원이 필요한 경우 TAC에 문의하십시오.

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.