AMP for Endpoints에서 오탐 파일 분석 트러블슈팅

목차

소개

이 문서에서는 AMP(Advanced Malware Protection) for Endpoints에서 오탐 파일 분석을 수집하는 방법에 대해 설명합니다.

기고자: Jesus Javier Martinez, Cisco TAC 엔지니어

사전 요구 사항

요구 사항

Cisco에서는 다음 주제에 대해 알고 있는 것이 좋습니다.

- AMP 콘솔 대시보드
- 관리자 권한이 있는 계정

사용되는 구성 요소

이 문서의 정보는 Cisco AMP for Endpoints 버전 6.X.X 이상을 기반으로 합니다.

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

배경 정보

AMP for Endpoints는 특정 파일/프로세스/SHA(Secure Hash Algorithm) 256에 대해 과도한 알림을 생성할 수 있습니다. 네트워크에 오탐(False Positive) 탐지가 있다고 생각되면 진단 팀이 심층적인 파일 분석을 진행할 수 있습니다. Cisco TAC에 문의할 때 다음 정보를 제공해야 합니다.

·파일 SHA 256 해시
·파일 샘플 사본
·AMP 콘솔에서 경보 이벤트 캡처
·AMP 콘솔에서 이벤트 세부 정보 캡처
·파일에 대한 정보(파일의 출처 및 환경에 있어야 하는 이유)
·파일/프로세스가 오탐이 될 수 있다고 생각하는 이유 설명

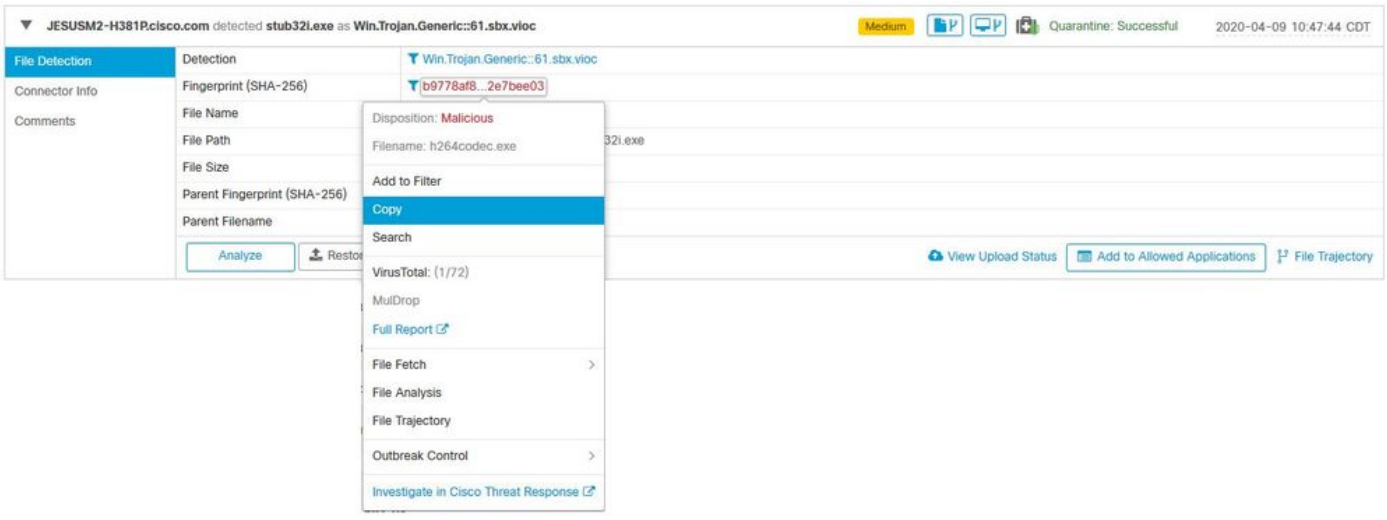
AMP for Endpoints에서 오탐 파일 분석 트러블슈팅

이 섹션에서는 Cisco TAC에서 오탐(False Positive) 티켓을 여는 데 필요한 모든 세부 정보를 얻는 데 사용할 수 있는 정보를 제공합니다.

파일 SHA 256 해시

1단계. SHA 256 해시를 가져오려면 **AMP Console > Dashboard > Events로 이동합니다.**

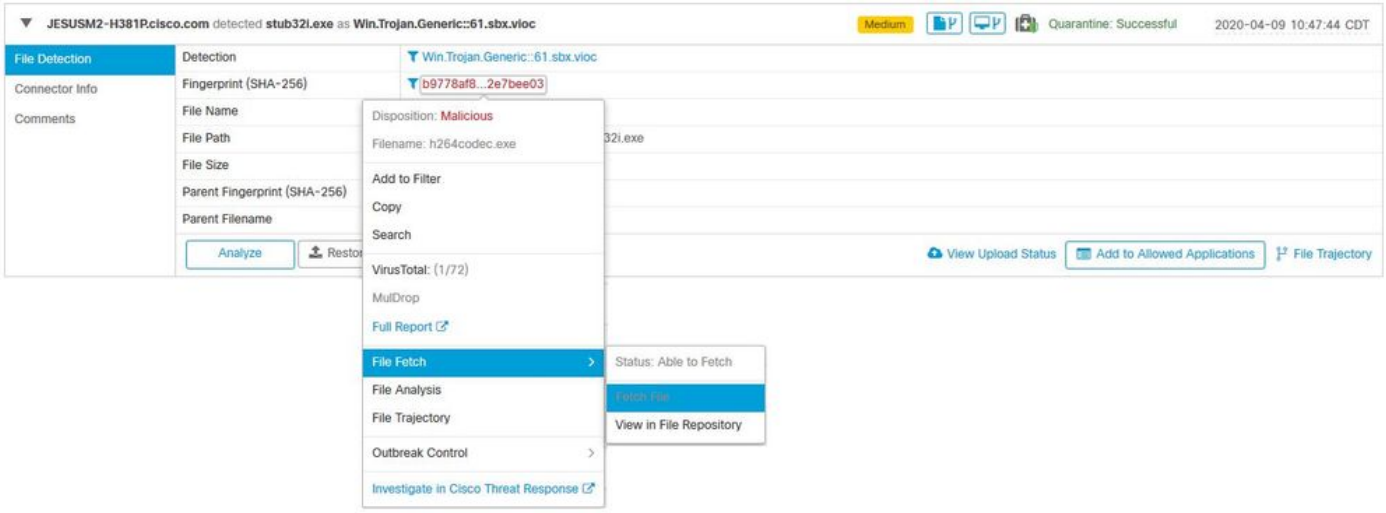
2단계. **Alert Event**(경고 이벤트)를 선택하고 **SHA256**을 클릭한 다음 이미지에 표시된 대로 **Copy(복사)**를 선택합니다.



파일 샘플 복사본

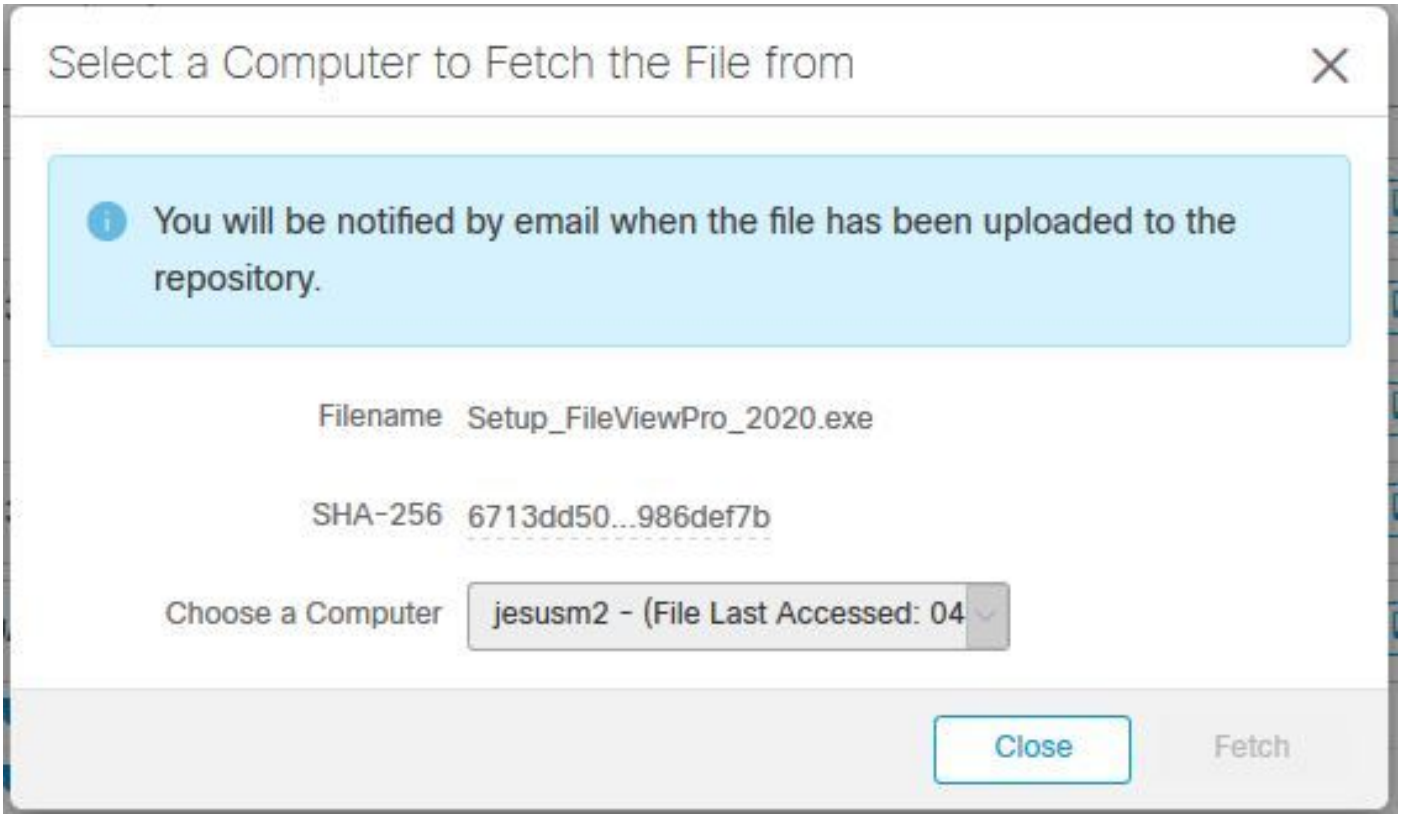
1단계. AMP Console에서 파일 샘플을 가져오고, **AMP Console > Dashboard > Events**(대시보드)로 **이동합니다.**

2단계. **Alert Event를** 선택하고 **SHA256**을 클릭한 다음 이미지에 표시된 대로 **File Fetch(파일 가져오기) > File Fetch(파일 가져오기)로** 이동합니다.

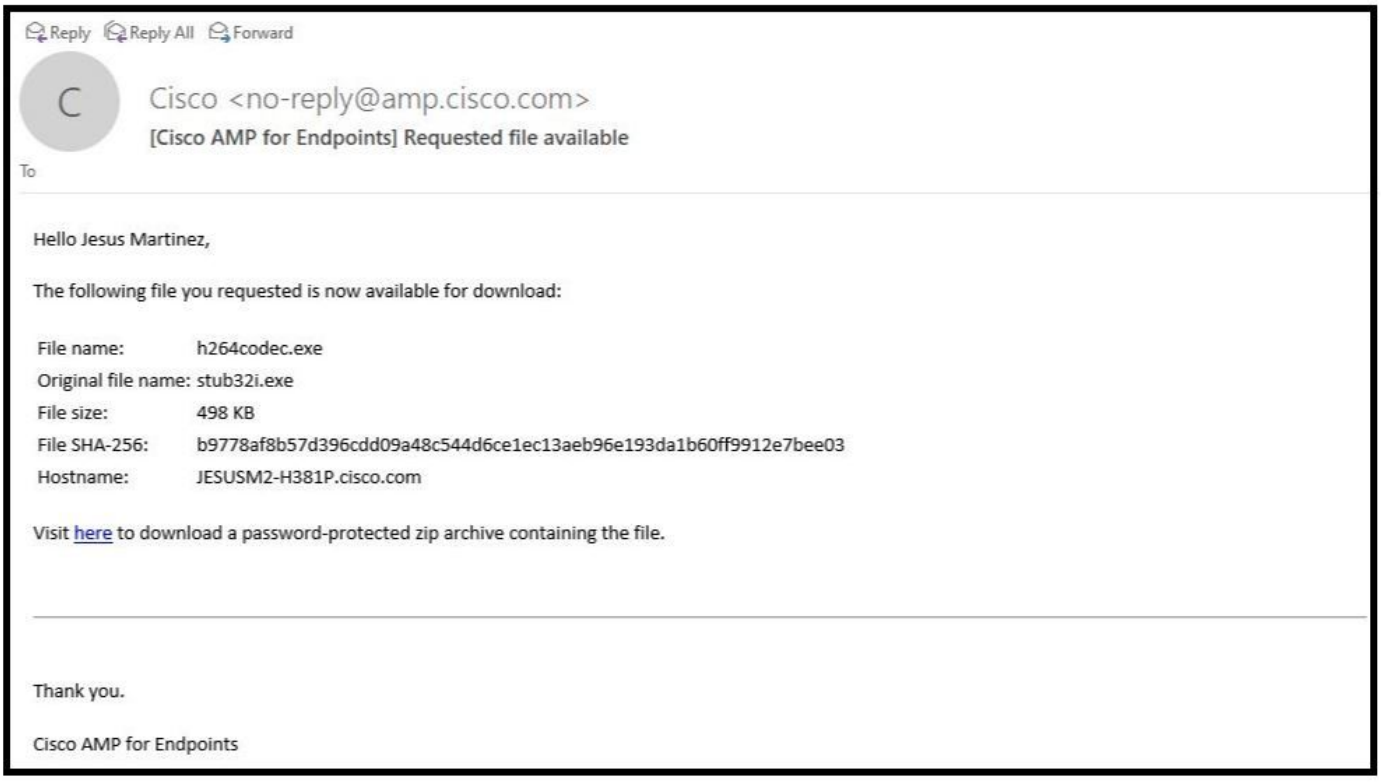


3단계. 파일이 탐지된 디바이스를 선택하고 이미지에 표시된 대로 **Fetch(가져오기)를** 클릭합니다 (디바이스가 **ON으로** 설정되어야 함).

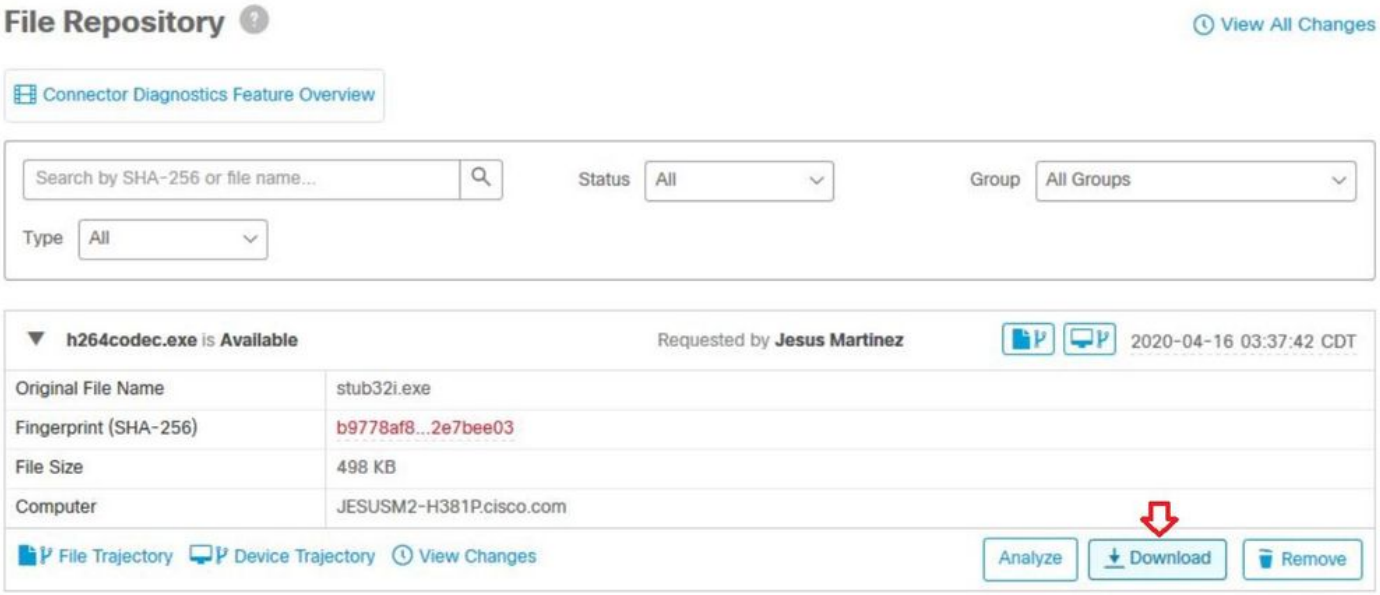
4단계. 이미지에 표시된 메시지를 수신합니다.



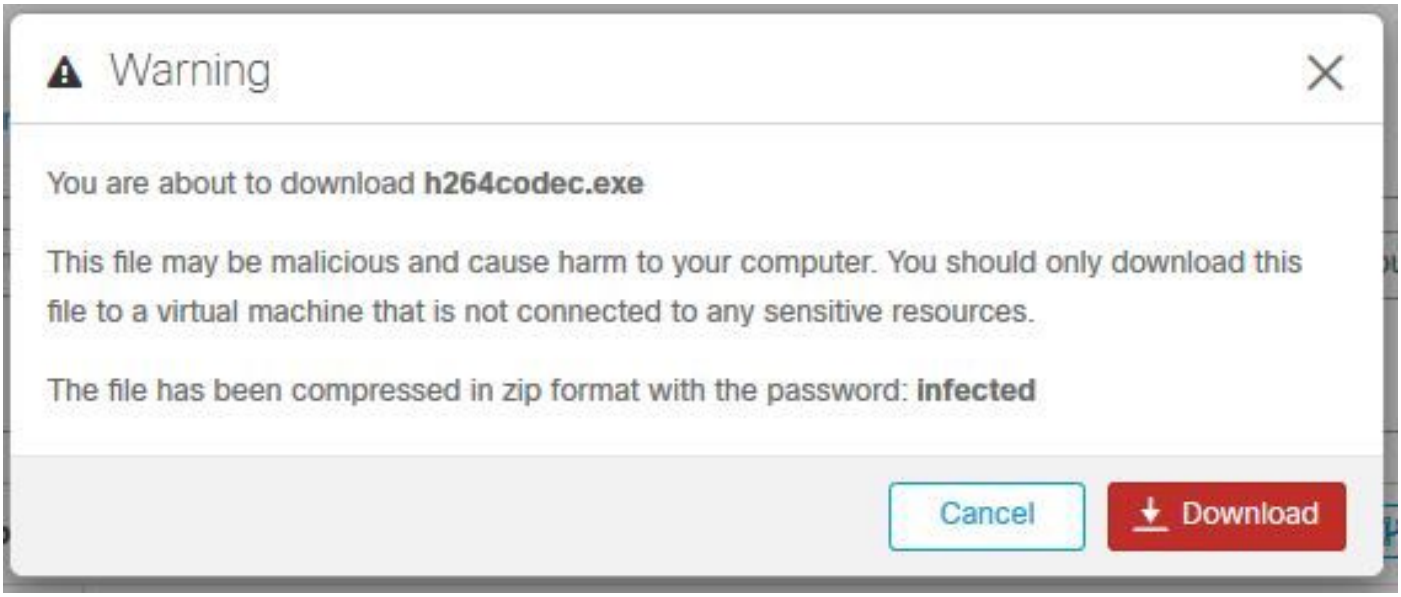
몇 분 후에 이미지에 표시된 대로 파일을 다운로드할 수 있는 경우 이메일 알림을 받게 됩니다.



5단계. **AMP Console > Analysis > File Repository로 이동하여** 파일을 선택하고 이미지에 표시된 대로 **Download**를 클릭합니다.



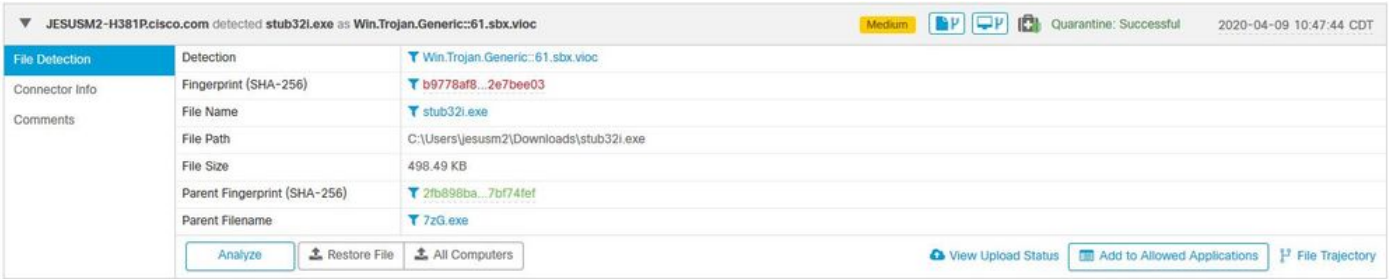
6단계. 알림 상자가 나타나면 이미지**에** 표시된 대로 다운로드를 클릭하고 파일이 ZIP 파일에 다운로드됩니다.



AMP 콘솔에서 알림 이벤트 캡처

1단계. **AMP Console > Dashboard > Events로 이동합니다.**

2단계. Alert **Event**를 선택하고 이미지에 표시된 대로 캡처를 수행합니다.

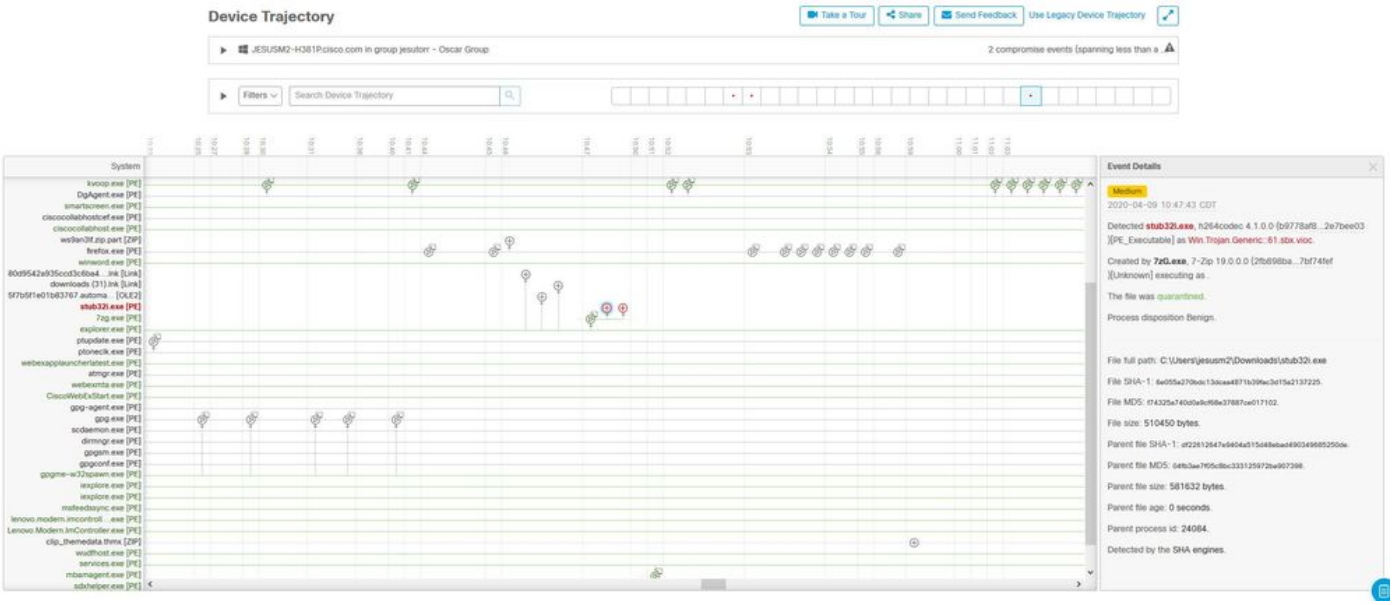


AMP 콘솔에서 이벤트 세부 정보 캡처

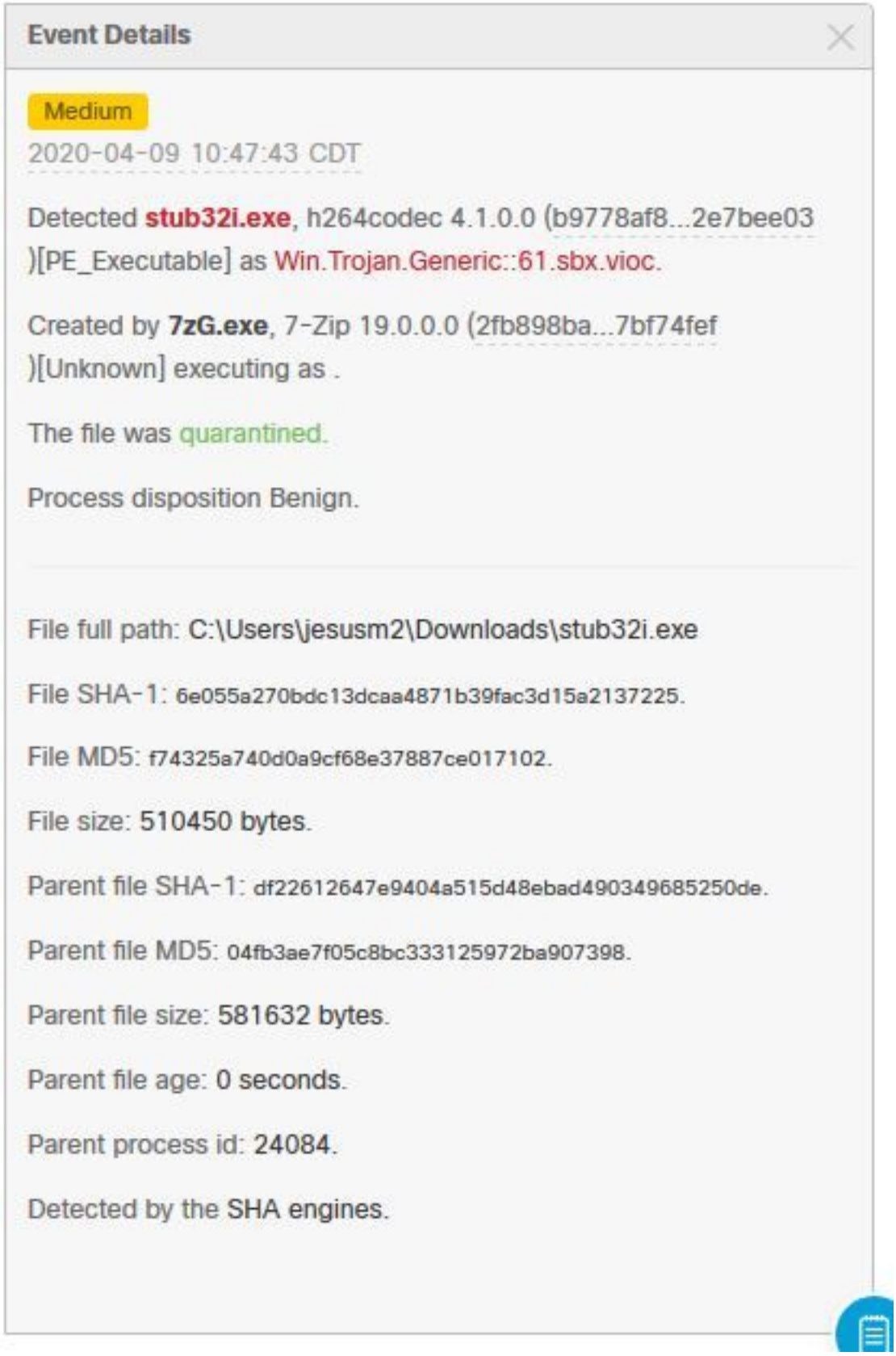
1단계. **AMP Console > Dashboard > Events로 이동합니다.**

2단계. Alert Event(경고 이벤트)를 선택하고 이미지**에** 표시된 대로 Device Trajectory(디바이스 전파 흔적 분석) 옵션을 클릭합니다.

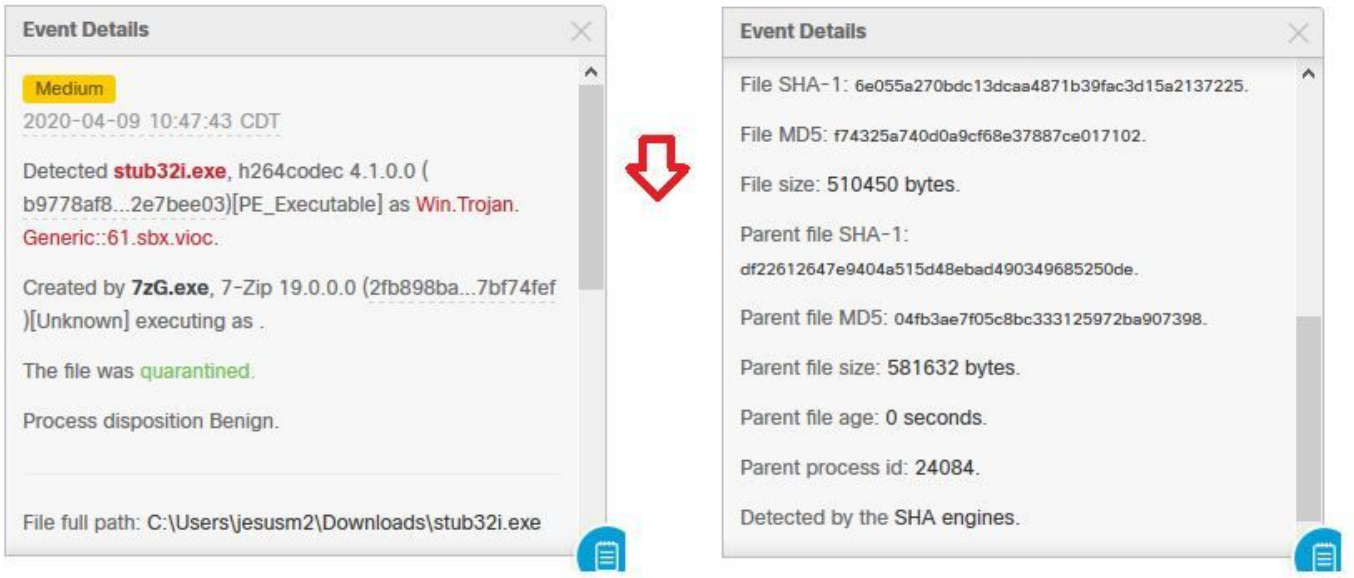
이미지에 표시된 대로 **Device Trajectory** 세부사항으로 리디렉션됩니다.



3단계. 이미지에 표시된 대로 **이벤트 세부 정보** 상자를 캡처합니다.



4단계. 필요한 경우 아래로 스크롤하여 일부 캡처를 수행하여 이미지에 표시된 모든 **이벤트 세부** 정보를 가져옵니다.



파일 정보

- 파일의 출처 정보.
- 파일이 웹 사이트에서 오는 경우 웹 URL을 공유합니다.
- 파일 설명을 공유하고 파일 기능을 설명합니다.

설명

- 파일 프로세스가 오탐일 수 있다고 생각하는 이유는 무엇입니까?
- 파일에서 신뢰하는 이유를 공유합니다.

정보 제공

- 모든 세부 정보를 수집하면 https://cway.cisco.com/csc/에 요청된 모든 정보를 업로드합니다.
- 서비스 요청 번호를 참조하는지 확인합니다.

결론

Cisco는 항상 AMP for Endpoints 기술을 위한 위협 인텔리전스를 개선하고 확장하기 위해 노력하지만, AMP for Endpoints 솔루션에서 잘못된 알림을 트리거할 경우, 환경에 더 이상 영향을 미치지 않도록 몇 가지 조치를 취할 수 있습니다.이 문서에서는 False Positive(오탐) 문제와 관련하여 Cisco TAC에서 케이스를 여는 데 필요한 모든 세부 정보를 얻을 수 있는 지침을 제공합니다.진단 팀 파일 분석을 기반으로, 파일 속성을 변경하여 AMP Console에서 트리거된 경고 이벤트를 중지하거나 Cisco TAC에서 해당 환경에서 문제 없이 파일/프로세스를 실행할 수 있는 적절한 수정 사항을 제공할 수 있습니다.