AMP(Advanced Malware Protection) 오탐 또는 미탐 이벤트로 작동

목차

소개

Cisco는 항상 AMP(Advanced Malware Protection) 기술의 위협 인텔리전스를 개선하고 확장하려고 노력합니다. AMP 제품이 실시간으로 알림을 트리거하지 않았다면 환경에 더 이상 영향을 주지 않도록 몇 가지 작업을 수행할 수 있습니다. 이 문서에서는 해당 작업 항목에 대한 지침을 제공합니다.

설명

즉각적인 조치

AMP 솔루션이 위협으로부터 네트워크를 보호하지 않았다고 생각되면 즉시 다음 조치를 취하십시오.

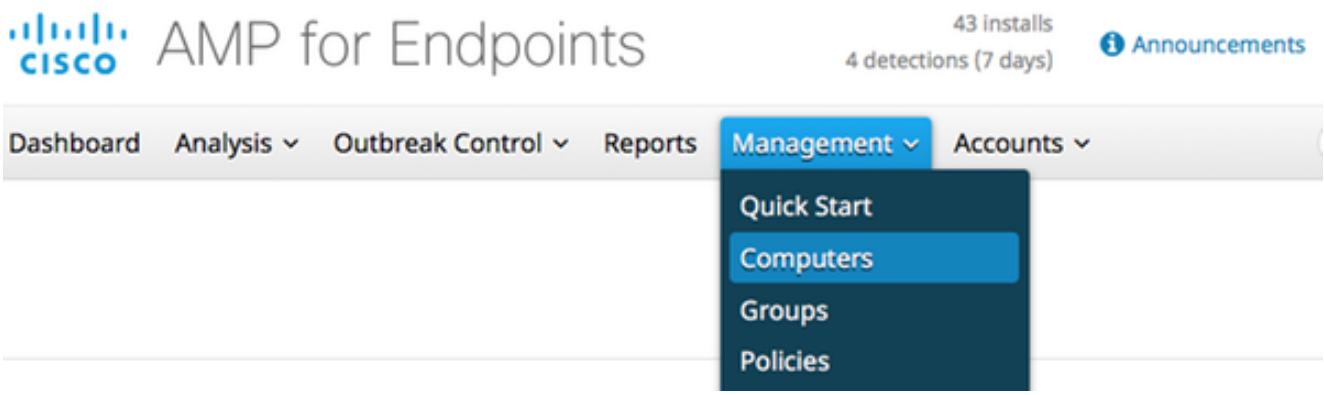
1. 네트워크의 나머지 부분에서 의심스러운 머신을 분리합니다. 분리 방법으로는 머신을 끄거나 네트워크에서 물리적으로 연결을 끊는 방법 등이 있습니다.
2. 머신의 감염 추정 시간, 의심스러운 머신에서 이루어진 사용자 작업 등 감염에 관한 중요한 정보를 기록합니다.

   경고: 머신을 초기화하거나 재설정하지 마십시오. 그렇게 하면 포렌식 조사나 문제 해결 프로세스 중에 문제를 일으키는 소프트웨어나 파일을 찾아낼 가능성이 없어집니다.

분석

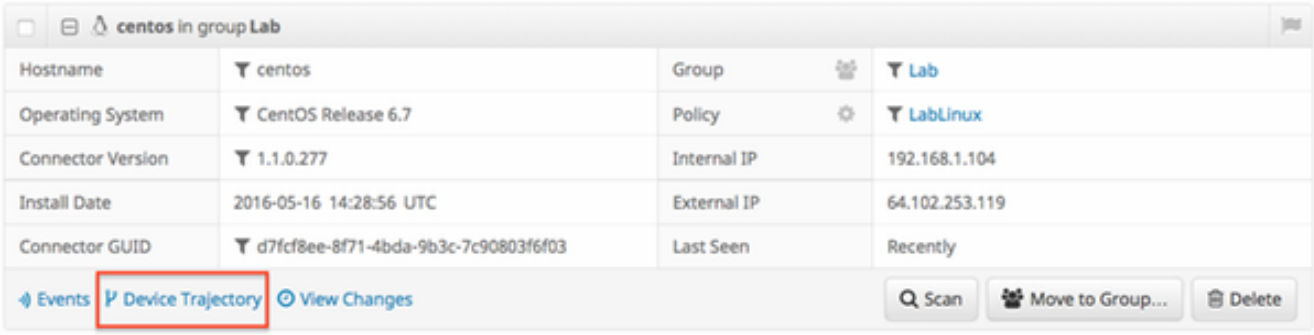
1. **Device Trajectory(디바이스 경로 분석)** 기능을 사용하여 자체 조사를 시작합니다. 디바이스 경로 분석에서는 약 9백만 개의 최신 파일 이벤트를 저장할 수 있습니다. AMP for Endpoints 디바이스 경로 분석은 감염을 유발하는 파일이나 프로세스를 추적하는 데 매우 유용합니다

   대시보드에서 **Management(관리) > Computers(컴퓨터)**로 이동합니다.



의심스러운 머신을 찾아 해당 머신에 대한 기록을 확장합니다. **Device Trajectory(디바이스 경로 분석)**를 클릭합니다

.



2. 의심스러운 파일 또는 해시가 있으면 맞춤형 탐지 목록에 추가합니다. AMP for Endpoints는 맞춤형 탐지 목록을 사용하여 파일이나 해시를 악의적인 것으로 처리할 수 있습니다. 이는 임시 대체 커버리지를 제공하여 더 이상의 영향을 방지하는 효과적인 방법입니다.

Cisco에서 분석

1. 동적 분석을 위해 의심스러운 모든 샘플을 제출합니다. 대시보드의 **Analysis(분석) > File Analysis(파일 분석)**에서 수동으로 제출할 수 있습니다. AMP for Endpoints에는 Threat Grid에서 파일의 행동에 대한 보고서를 생성하는 동적 분석 기능이 포함되어 있습니다. 또한, Cisco 연구팀에서 추가 분석이 필요할 경우 Cisco에 파일을 제공하는 이점이 있습니다.

2. 네트워크에서 *오탐* 또는 *미탐*이 발생한 것으로 의심되는 경우, AMP 제품에 대한 맞춤형 블랙리스트 또는 화이트리스트 기능을 활용하는 것이 좋습니다. Cisco TAC(Technical Assistance Center)에 문의할 때는 분석을 위해 다음 정보를 제공하시기 바랍니다.파일의 SHA256 해시파일의 복사본(가능한 경우)파일의 출처 및 사용 환경에 파일이 필요한 이유 등 파일에 대한 정보오탐 또는 미탐이라고 판단하는 근거 설명
3. 위협을 완화하거나 환경의 Triage(분류)를 수행하는 데 도움이 필요할 경우, 전문적으로 실행 계획을 세우고, 감염된 머신을 연구하고, 고급 툴이나 기능을 활용하여 악성코드의 전파 문제를 해결하는 CSIRT(Cisco Emergency Response Team)에 의뢰해야 합니다.
참고: Cisco TAC(Technical Assistance Center)에서는 이런 방식의 지원을 제공하지 않습니다.CSIRT 팀에 의뢰하려면 전화번호 +1-844-831-7715로 연락하십시오. 이들은 해당 서비스에 대한 보다 자세한 정보를 제공하고, 해당 사건에 대한 케이스를 엽니다. 프로세스에 대한 자세한 지침을 제공할 수 있도록 Cisco 어카운트 매니저와 후속 작업을 진행하십시오.

관련 기사

- Windows FireAMP Connector
- FireAMP Connector