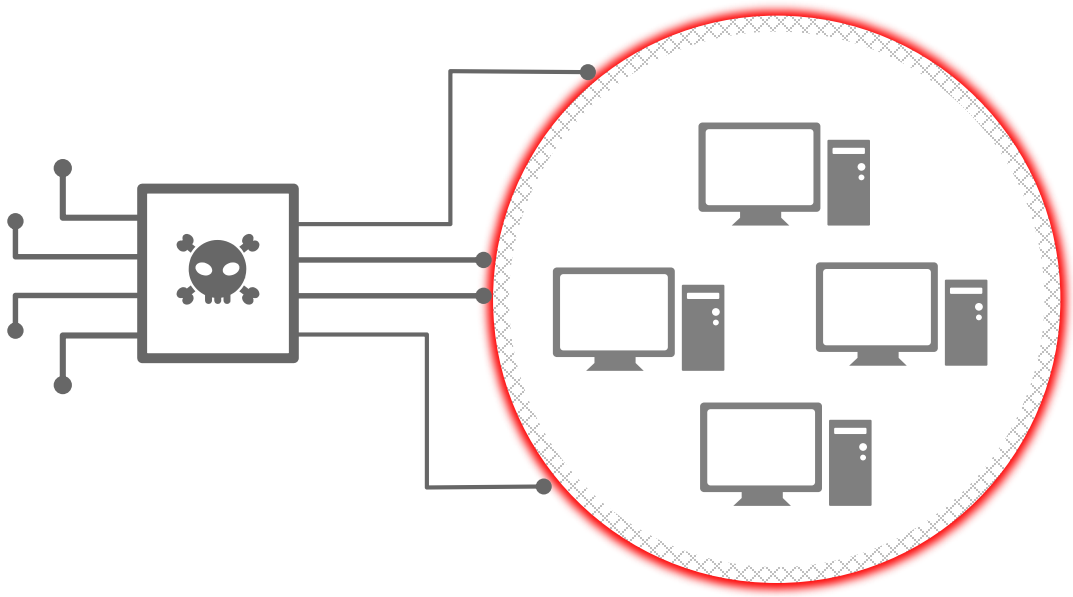
숨어있는 1% 위협을 찾아내는 EDR 보안전략

시스코 정관진 부장
Sep, 2018

Security Today

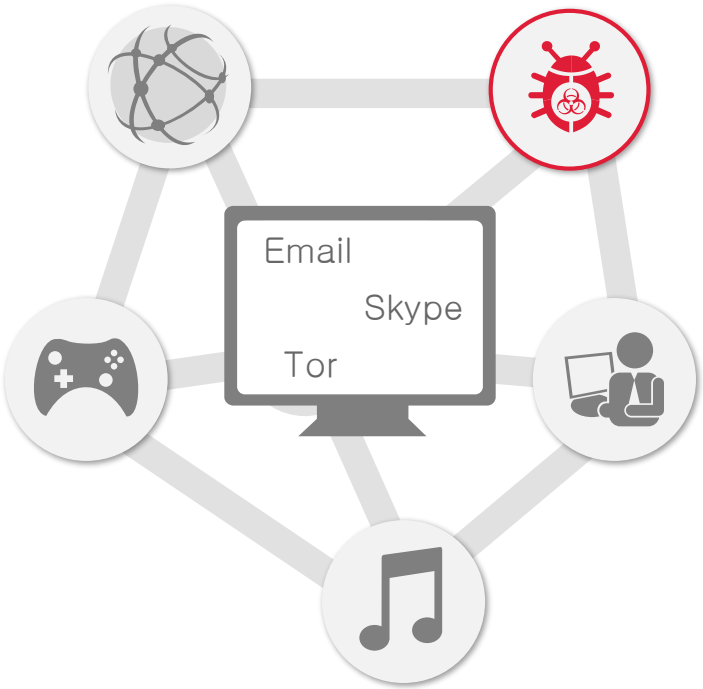
지능형 위협 탐지는 더욱 어려워 지고 있습니다.

과거 악성코드



Malware propagating across network likely to be caught

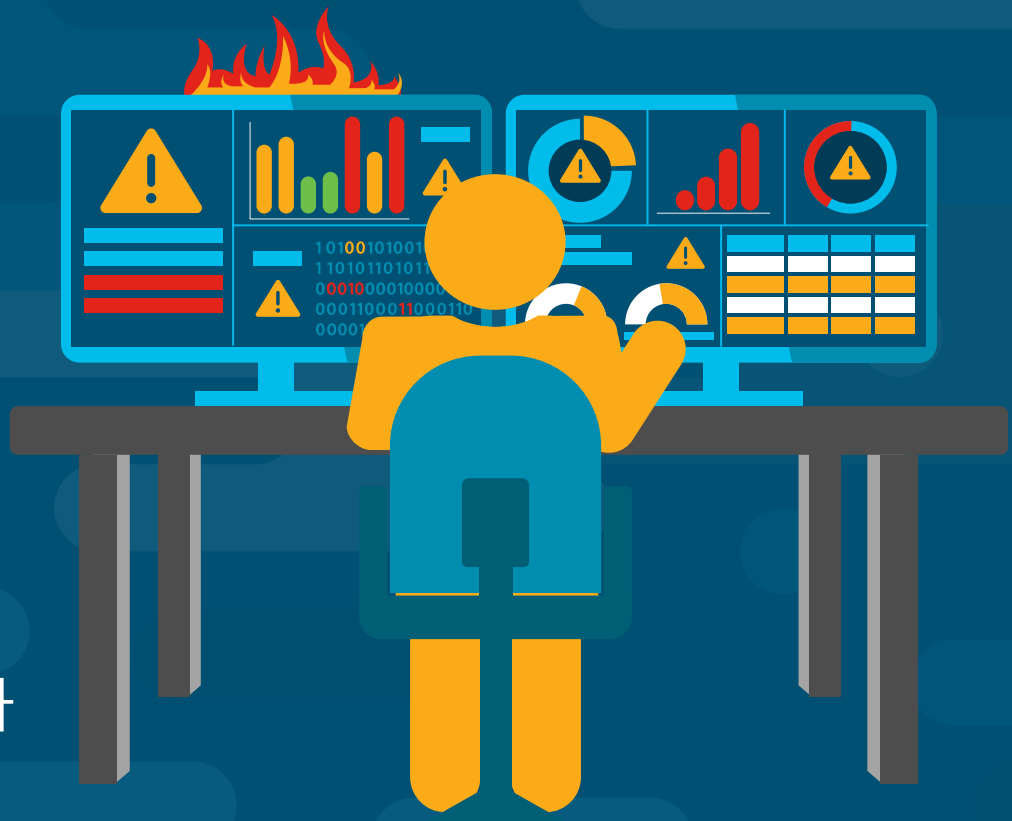
현재



Modern malware uses legitimate channels to infect host

도전과제

- 전문적 기술 및 인력 부족
- 대응 프로세스 및 도구의 부족
- 현재의 위협에 대응하기에는 어려움 증가



EDR 지금 우리에게 필요한 것은 ?

계속 진화하는 위협

현실적인 한계

빠르게 인지 하고 대응

99%의 위협
을 막을 수 있다고 말합니다.

그러면 우리가 놓치고 있었던 위협은 무엇일까요?

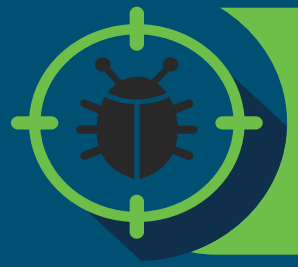
1%의 위협은 어디를 통해서 발생될까요?

탐지하지 못한 신종 악성 또는

우회 기법을 사용하는:

- 파일로 존재하지 않는 악성코드
- 동작 환경을 인지
- 다형성 악성코드
- 취약점을 이용한 공격
- 새로운 악성코드 유포 방법

지금 우리에게 필요한 건

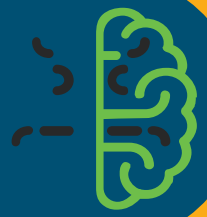


그리고 빠른 대응

Cisco Threat Response

더 많은 차단

AMP for Endpoints



더 많이 보고

Cisco Talos

마지막 방어 라인

악성코드 차단

다양한 탐지 차단 메카니즘

보이지 않는 위협요소 제거

네트워크,웹,이메일 그리고 엔드포인트까지 통합적인 관점의 대응 필요

Unknown 위협발견

선제적 위협 대응

악성코드 차단

다양한 탐지 차단 메카니즘

어떻게 위협을 막을까요...

차단

- 안티바이러스
- 메모리 기반 악성코드 탐지
- 시스템 프로세스 보호
- 클라우드 평판 (1:1, 1:many)
- 클라이언트 IOC

탐지

- 정적 분석
- 동적 분석 샌드박싱
- 랜섬웨어 보호 기능 (Malicious Activity Protection)
- 머신 러닝
- 디바이스 플로우
- 클라우드 IOC 위협지표

위협 감소

- 취약점 소프트웨어 검사
- 의심스러운 파일 자동 동적검사
- 프록시 로그 분석
- 타임라인 추적
- 위협 인텔리전스 활용 (Threat Response 를 통한 사고조사)

위협에 대응하기 위한 인텔리전스 조직

다양하고 방대한 데이터 수집은 다른 결과를 만들어 냅니다.

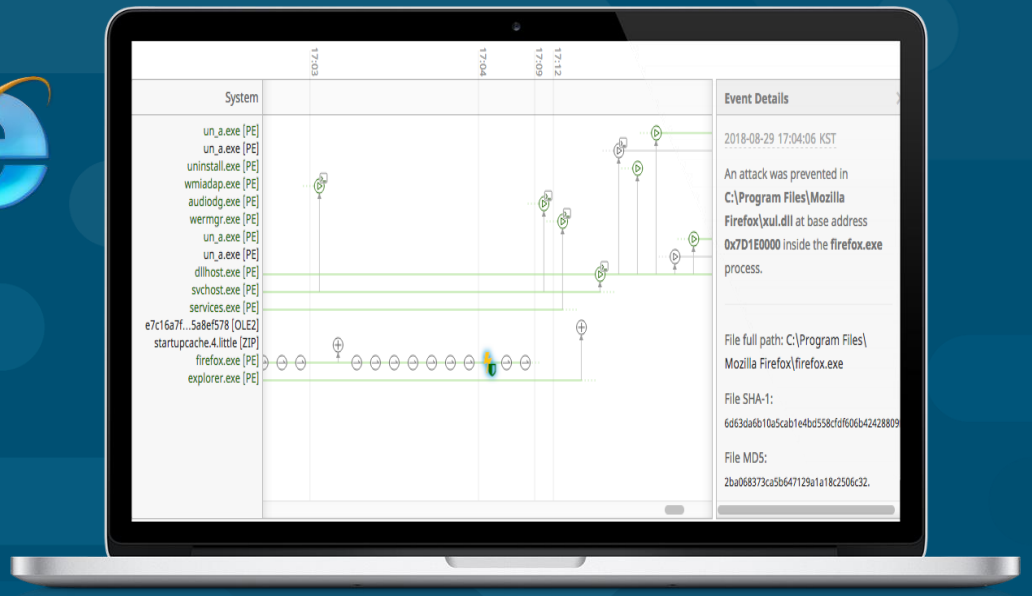
클라우드 기반의 분석

AMP 클라우드는 지속적으로
최신 위협 인텔리전스 데이터를
반영하여 지능형 위협에
효과적으로 대응

Fileless 악성코드 방어

취약점 공격에 대한 선제적 대응

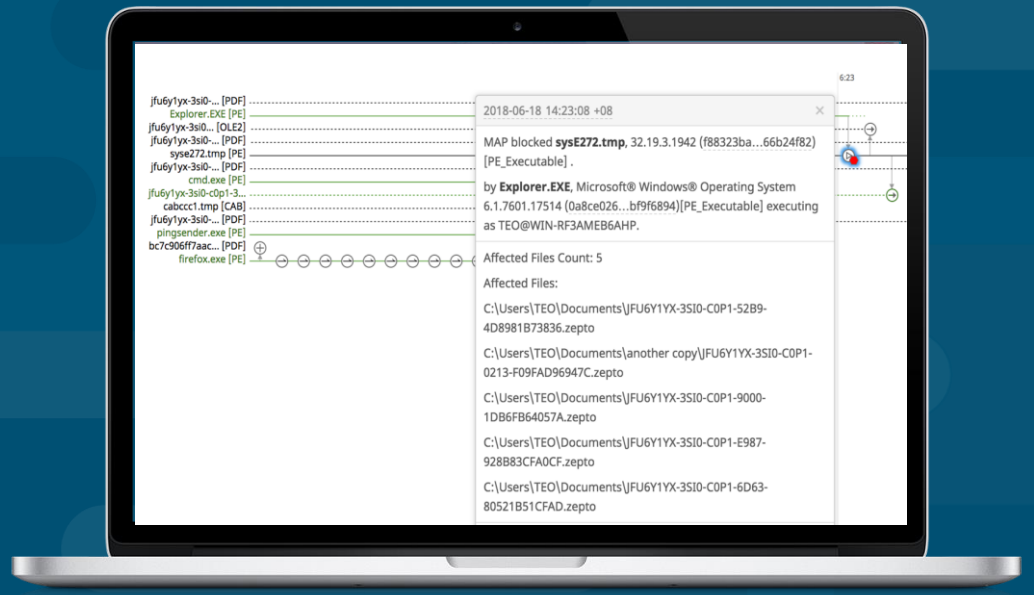
프로세스 활동을 모니터링하고 정상적인 애플리케이션에
메모리 인젝션 실행 행위를 차단



랜섬웨어에 대응하다

MAP(Malicious Activity Protection)

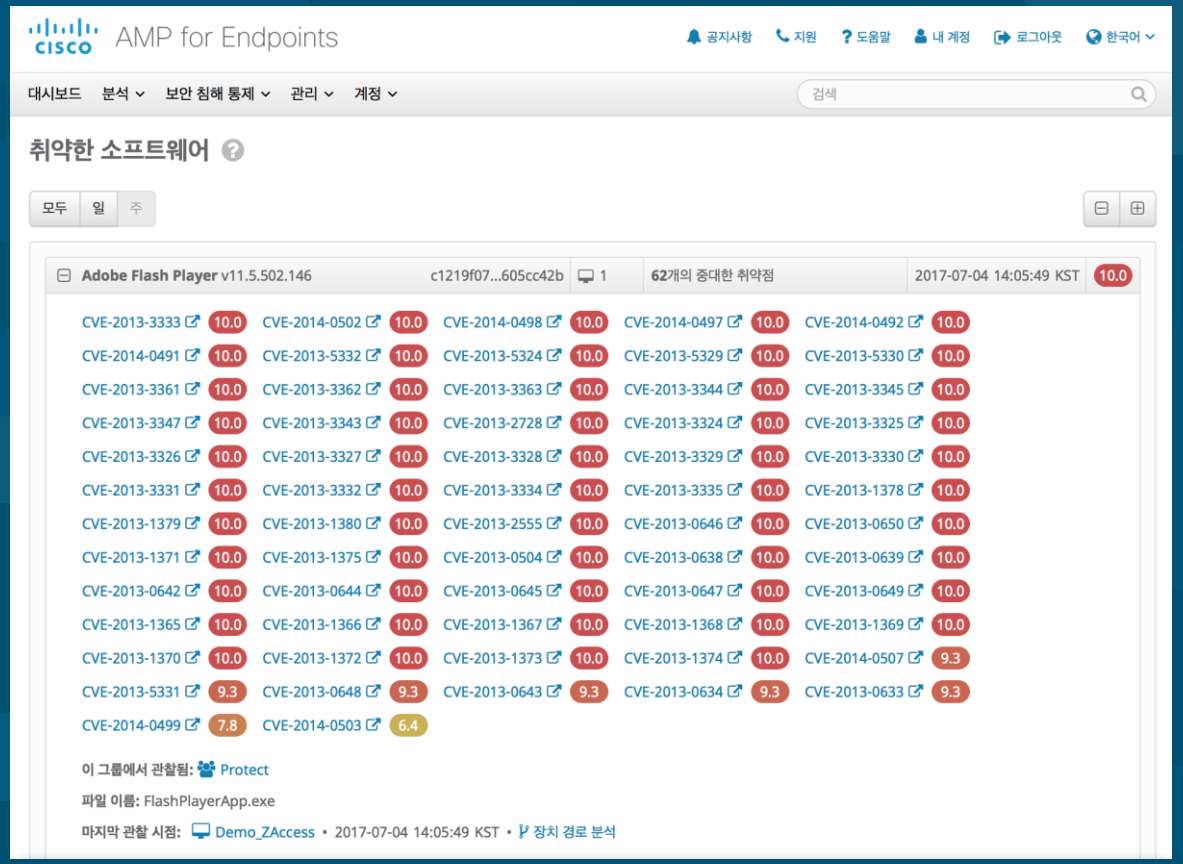
- 실행시점의 프로세스의 행동 모니터링
- 랜섬웨어의 형태의 행동 탐지
- 연관된 파일의 검역소 이동 및 프로세스 종료
- 파일에 대한 암호화 시도시 탐지



취약한 소프트웨어 현황

근본원인을 찾아 대응

- 악성코드의 감염 예방을 위한 소프트웨어 취약점 사전 대응
- 위협의 근본 원인 제거
- 탐지되는 프로세서와 매핑되는 취약한 소프트웨어
- CVE 세부 정보와 링크



보이지 않는 위협 요소 제거

네트워크, 웹, 이메일 그리고 엔드포인트까지 통합적인 관점에서의 대응 필요

한번 들여다 보고 전체에서 차단하다

인텔리전스를 공유하여 네트워크,웹, 이메일 그리고 엔드포인트까지 한번에 대응

가시성을 넓히다

데스크탑 부터 서버 그리고 모바일 디바이스 까지

에이전트 없는 프록시 기반 분석

네트워크 상에서 발생하는 어노멀리 트래픽 탐지

CTA (Cognitive Threat Analytics)

AMP 엔드포인트 사용자에게 무료로 제공되는 클라우드 기반의 위협탐지

- 어노멀리 탐지
- 다양한 모델링 기반의 지능형 위협 탐지
- 가시성 증가
- 장시간에 걸친 위협 감지

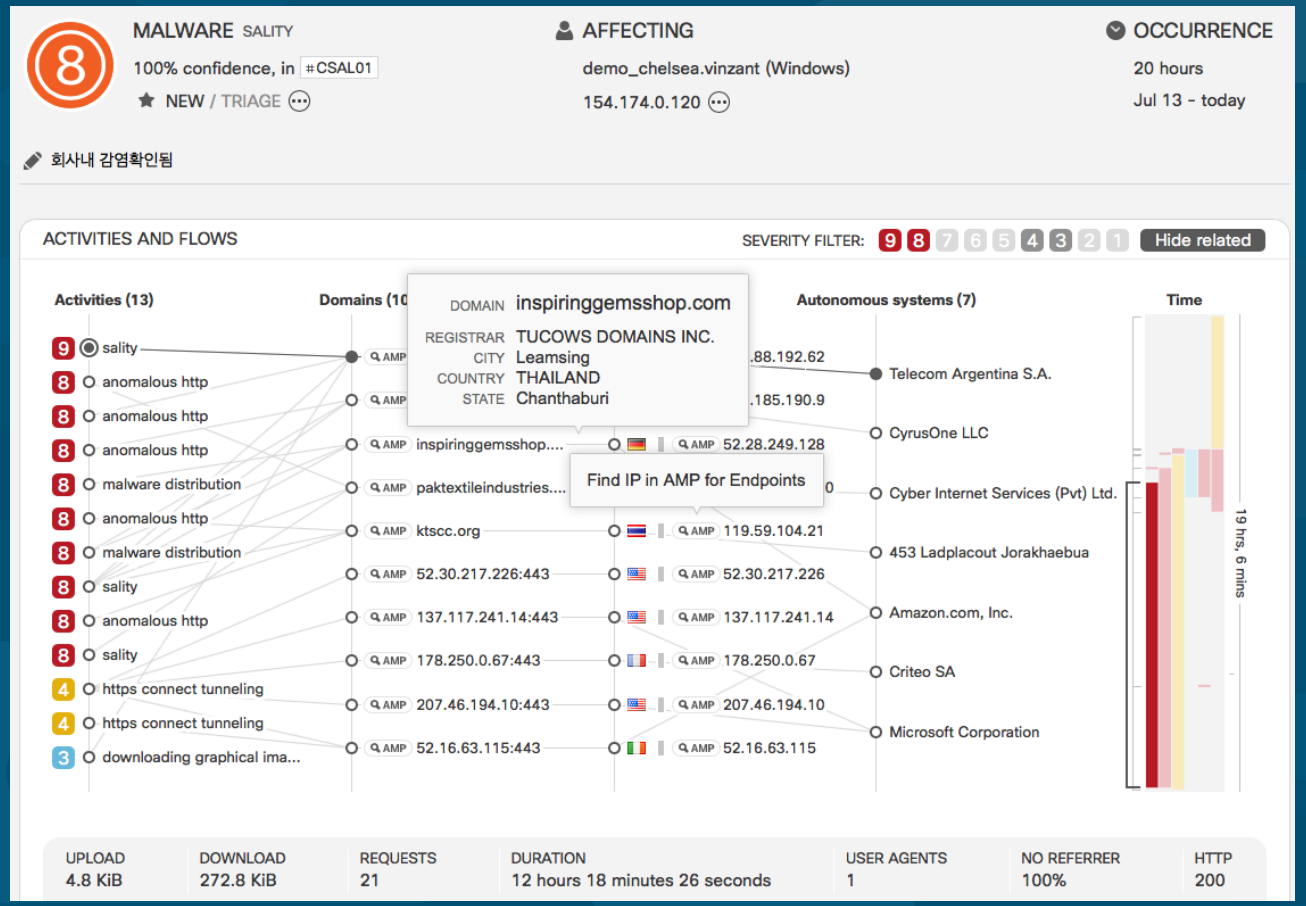
데이터 유출

C&C 통신

DGAs

익스플로잇 키트

HTTP(S) 터널링



Unknown 위협 발견

선제적 위협 대응

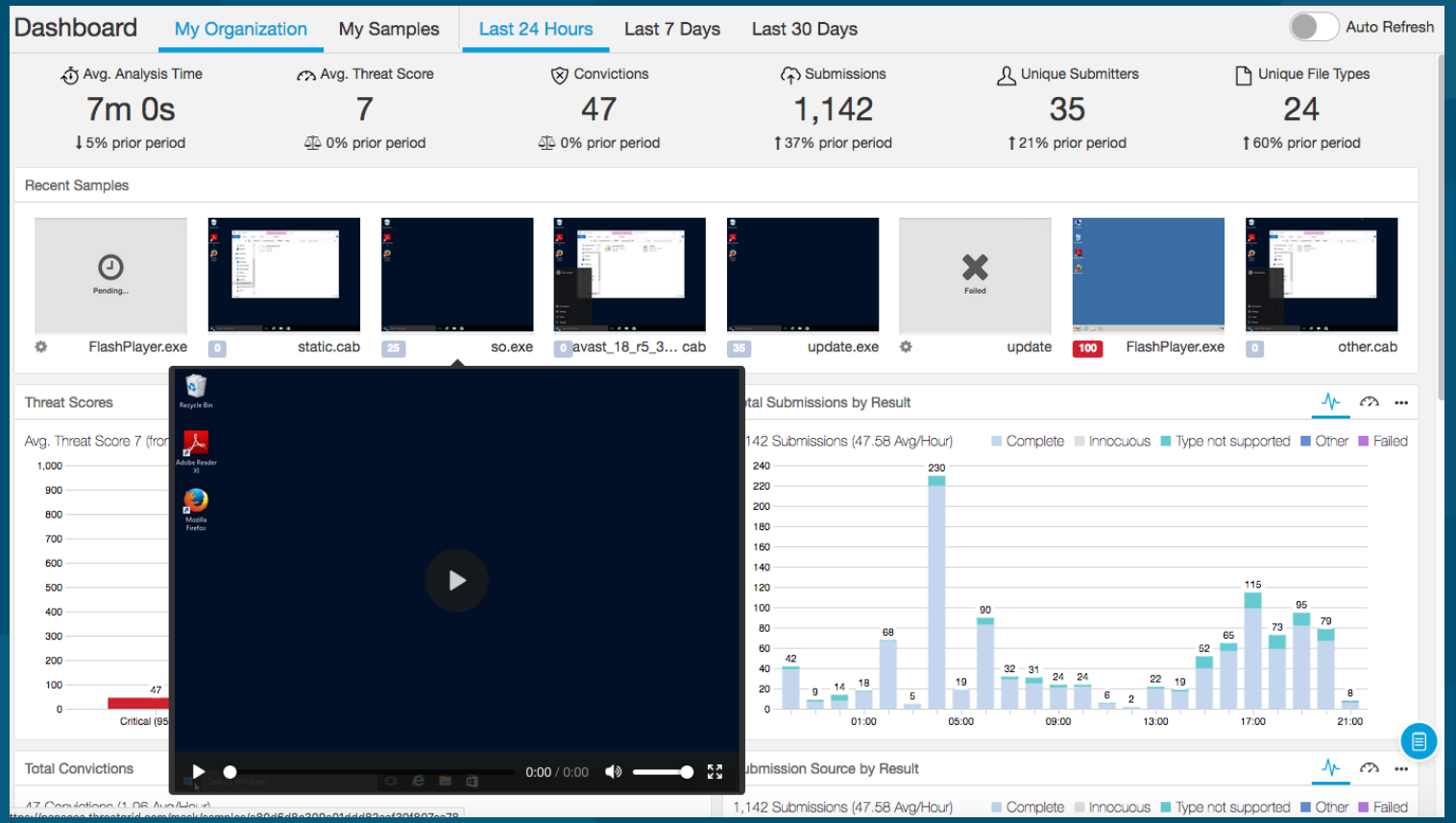
동적분석 샌드박싱

알려져 있지 않은 제로데이 위협 발견을 위한 악성코드 행위 분석

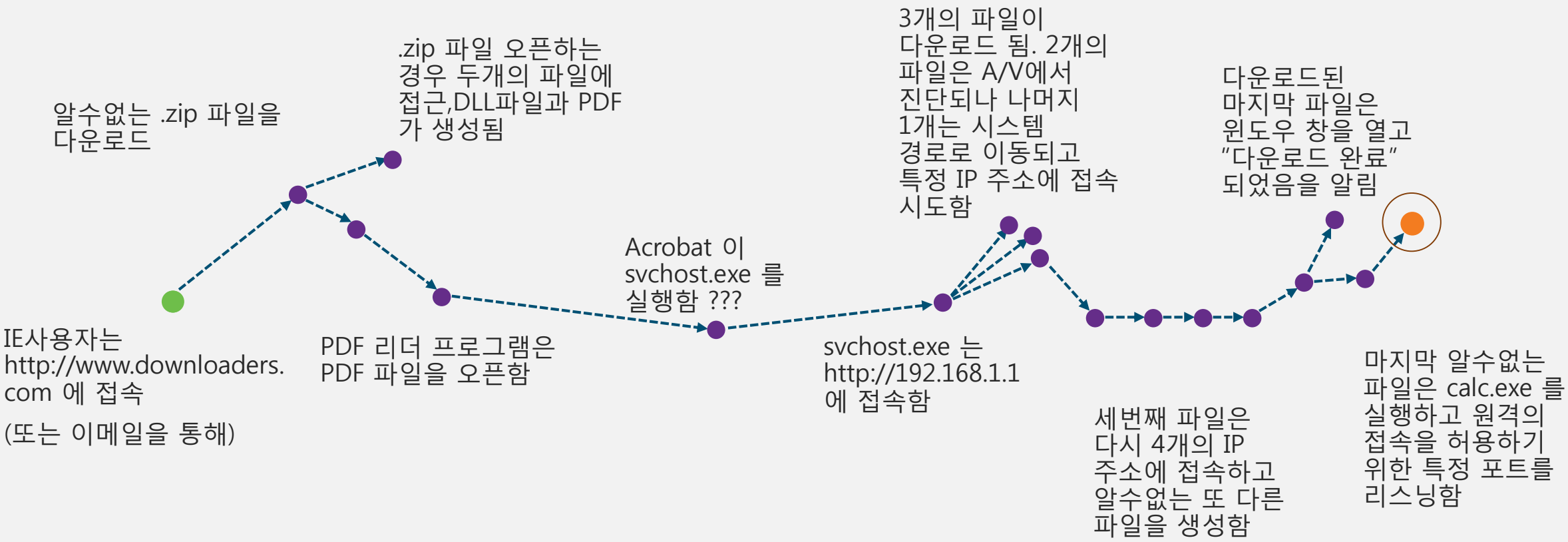
동적분석 샌드박싱 – Threat Grid

단순한 악성코드의 분석이 아니라 각 샘플과 과거 악성코드간의 상관관계 분석을 통해 위협요소를 판단하고 시각화를 통한 근거 데이터 제공

- 독자적 기술의 정적, 동적 분석
- 분석된 데이터와의 상관관계
- VM 밖에서 모니터링하는 접근 방식
- 행동지표를 통한 손쉬운 위협 판단
- 상세분석 보고서 및 표준화된 포맷 제공
- 웹 기반의 실제 동작 화면 제공
- 프로세스 시각화
- 강력한 검색 및 API 제공

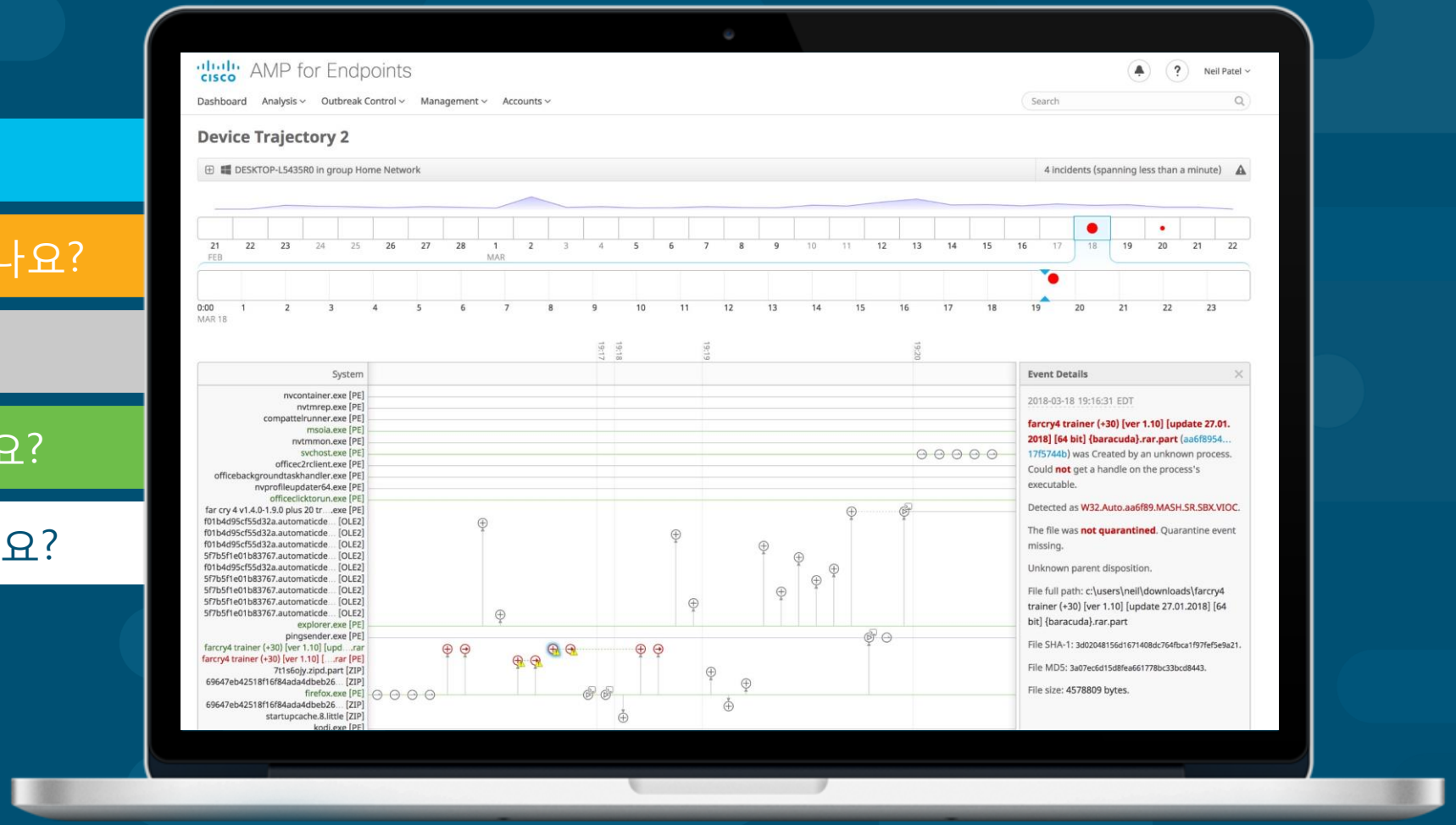


위협의 전체 스토리를 볼 수 있으면 어떨까요 ?



지속적 분석이 왜 필요한가 ?

- 무슨 일이 발생 했나요?
- 악성코드가 어디서 시작 되었나요?
- 악성코드는 어디에 있었나요?
- 악성코드가 무슨 행동을 하나요?
- 어떻게 위협을 차단할 수 있나요?



유입이 어디서 부터 시작되었는가 ?

무슨 일이 발생 했나요?

악성코드가 어디서 시작 되었나요?

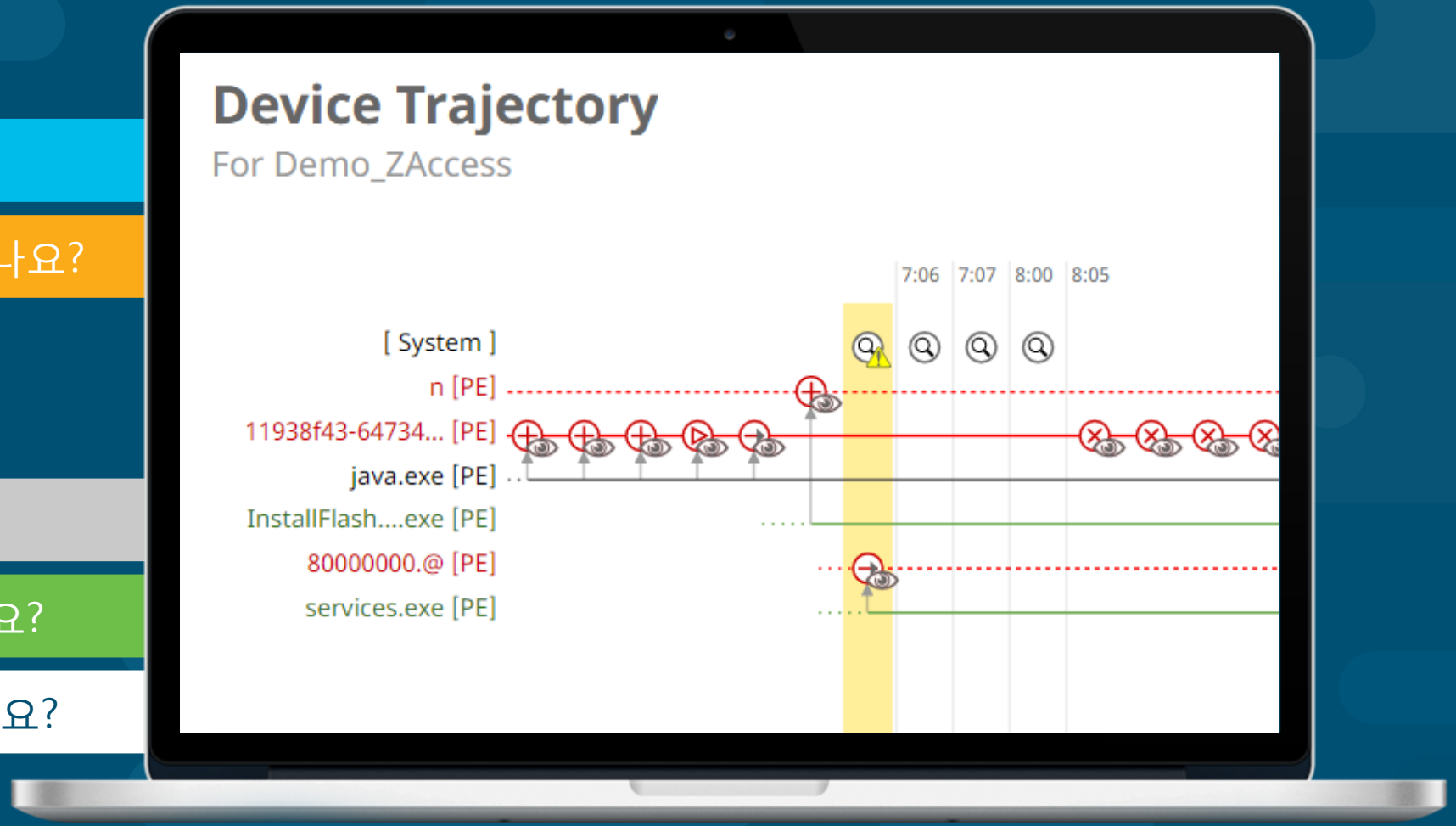
위협의 시작 점 및 진행 추적 :

- 시스템에 어떻게 유입이 되었는가
- 초기 유입지점은 무엇인가
- 어떤 공격을 이용하여 침투하였나

악성코드는 어디에 있었나요?

악성코드가 무슨 행동을 하나요?

어떻게 위협을 차단할 수 있나요?



감염된 영역 추적

무슨 일이 발생 했나요?

악성코드가 어디서 시작 되었나요?

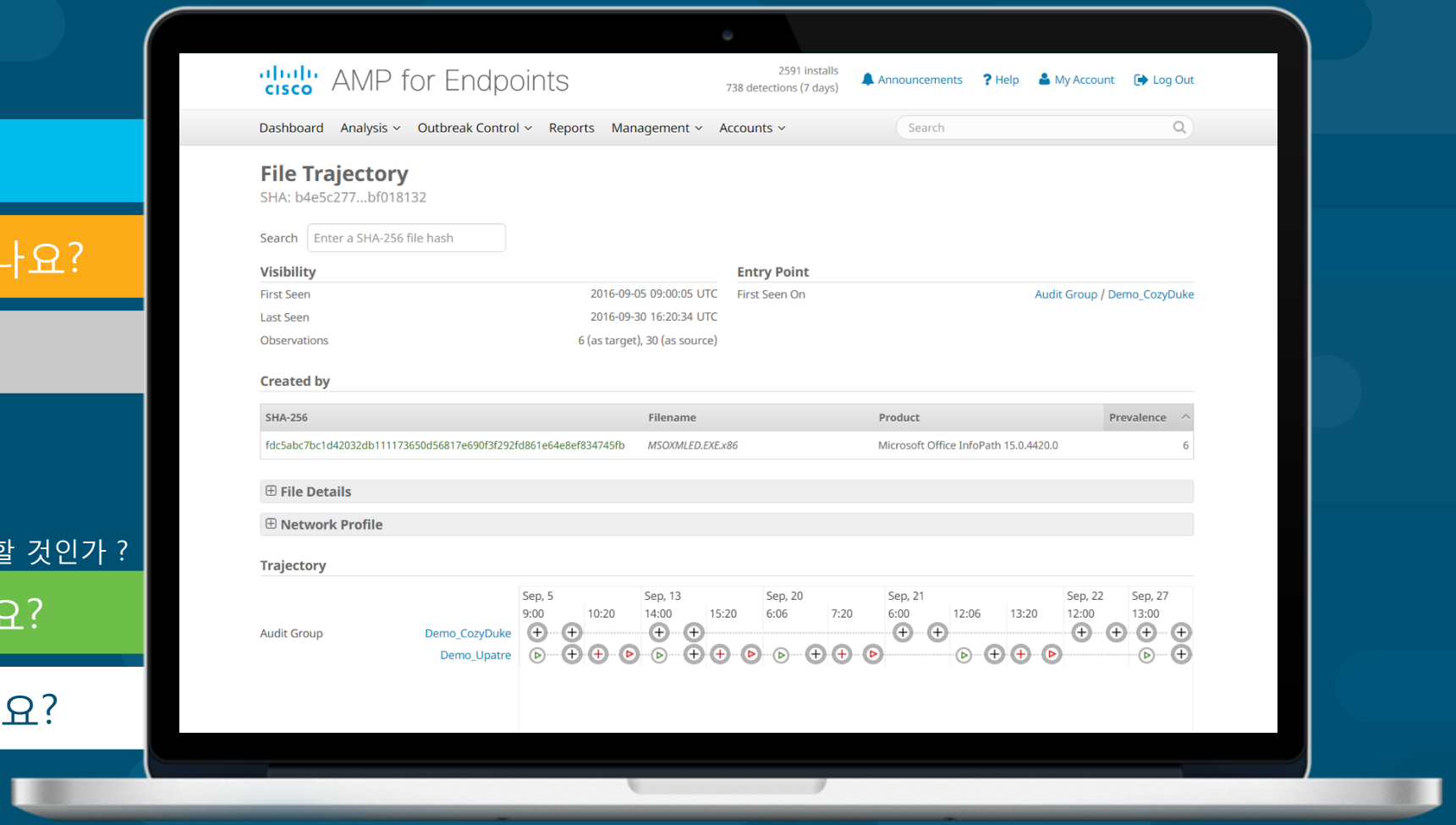
악성코드는 어디에 있었나요?

시스템의 감염된 영역의 추적:

- 현재 공격의 시작점은 어디인가
- 다른 엔드포인트에서도 탐지하는가
- 대응을 위해 어느지점부터 시작을 해야 할 것인가 ?

악성코드가 무슨 행동을 하나요?

어떻게 위협을 차단할 수 있나요?



악성코드가 무슨일을 하는지 판단

무슨 일이 발생 했나요?

악성코드가 어디서 시작 되었나요?

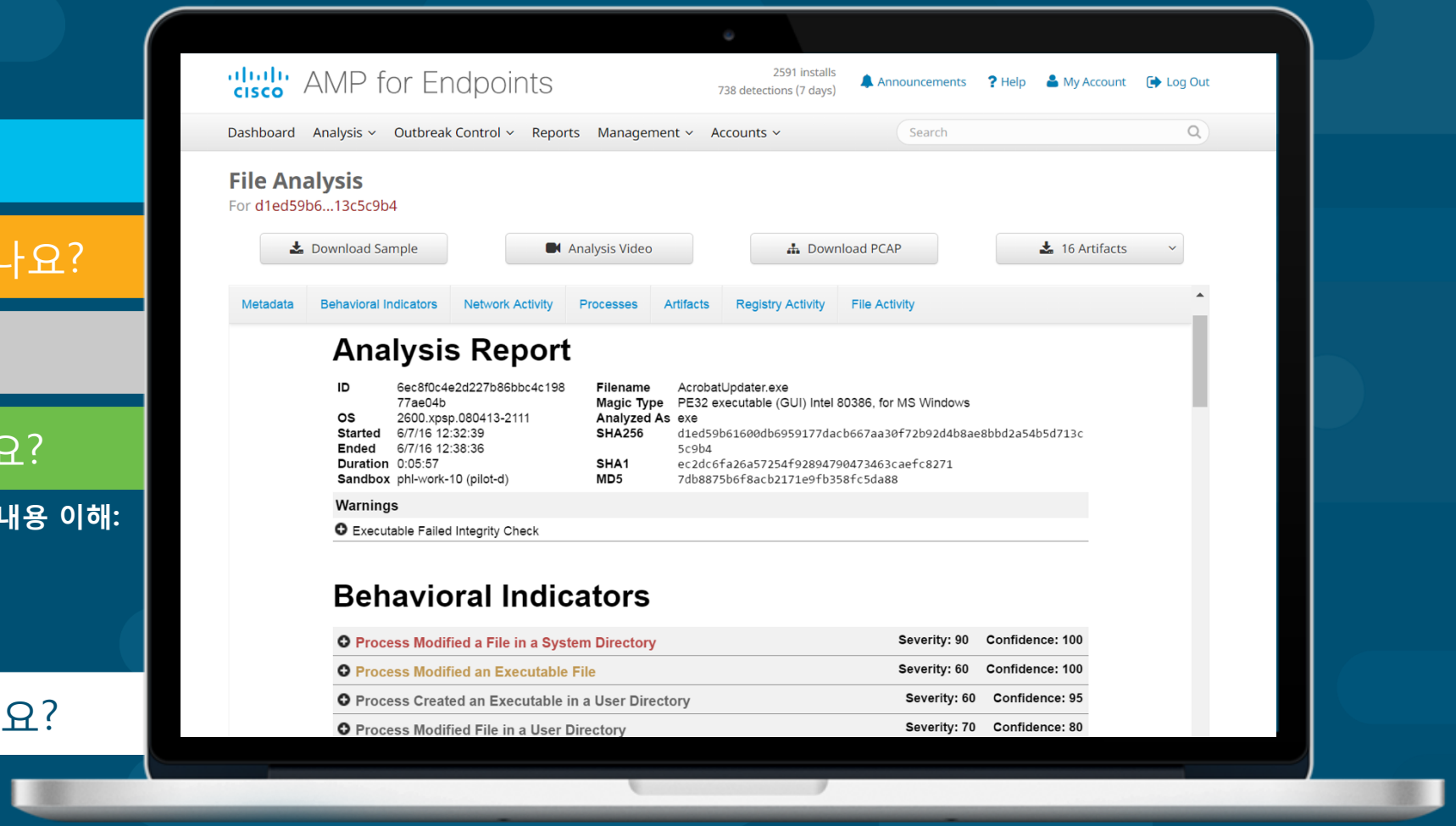
악성코드는 어디에 있었나요?

악성코드가 무슨 행동을 하나요?

악성코드가 어떻게 동작하는지 세부적인 내용 이해:

- 무엇을 시도하려고 하였는가
- 악성코드가 어떤 행동등을 보였는가
- 사고대응을 위해 세부적인 정보 획득

어떻게 위협을 차단할 수 있나요?



자동 또는 몇 번의 클릭으로 위협차단

무슨 일이 발생 했나요?

악성코드가 어디서 시작 되었나요?

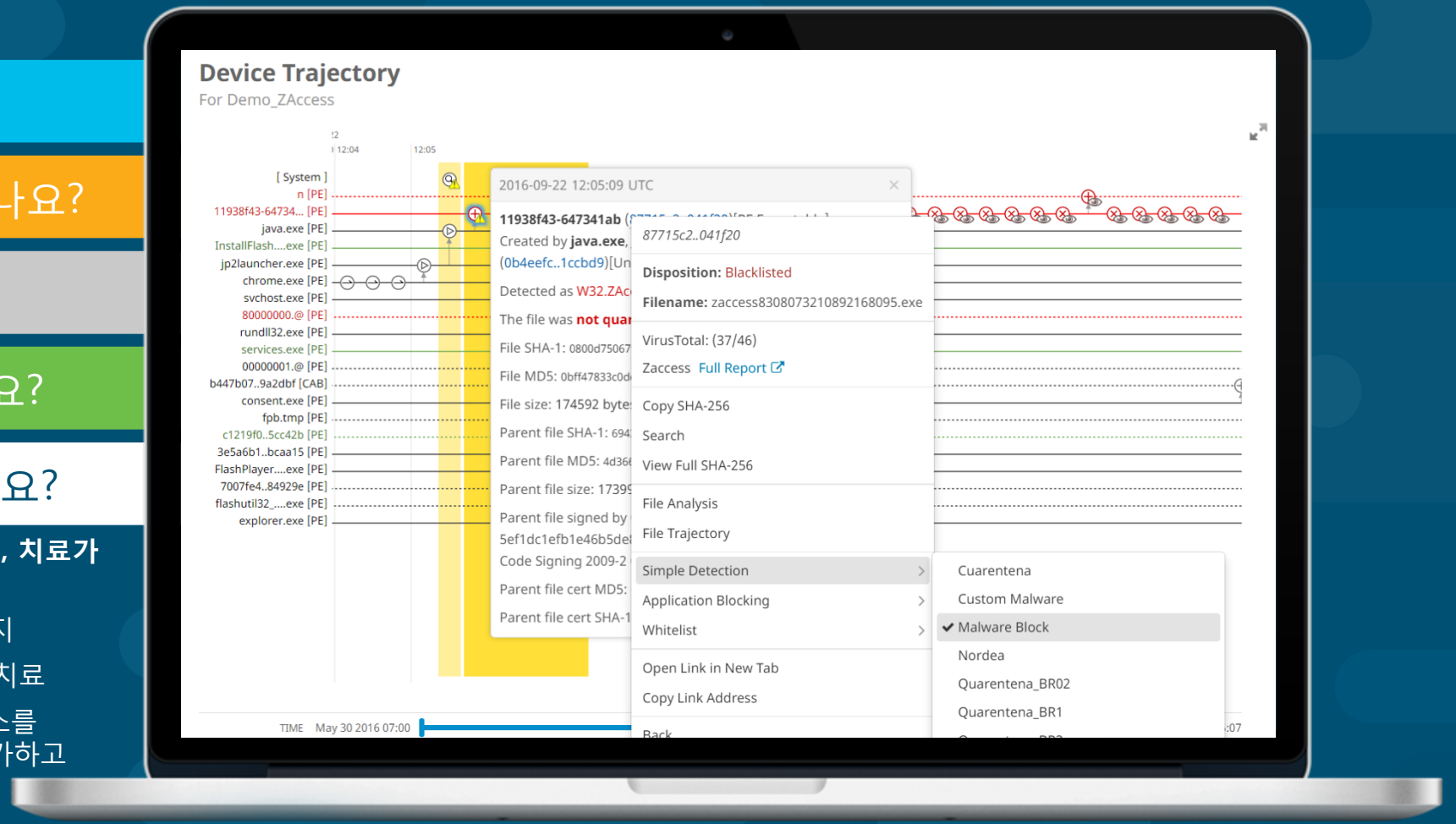
악성코드는 어디에 있었나요?

악성코드가 무슨 행동을 하나요?

어떻게 위협을 차단할 수 있나요?

위 내용들에 대해 세부적으로 알게된다면, 치료가 가능합니다:

- 출발지와 모든 감염된 호스트 확산 중지
- 위협이 발견되면 AMP 에서 자동으로 치료
- 수동 조치일 경우, 간단히 오른쪽 마우스를 클릭하여 해당파일을 블랙리스트에 추가하고 전체시스템에서 해당 파일을 제거



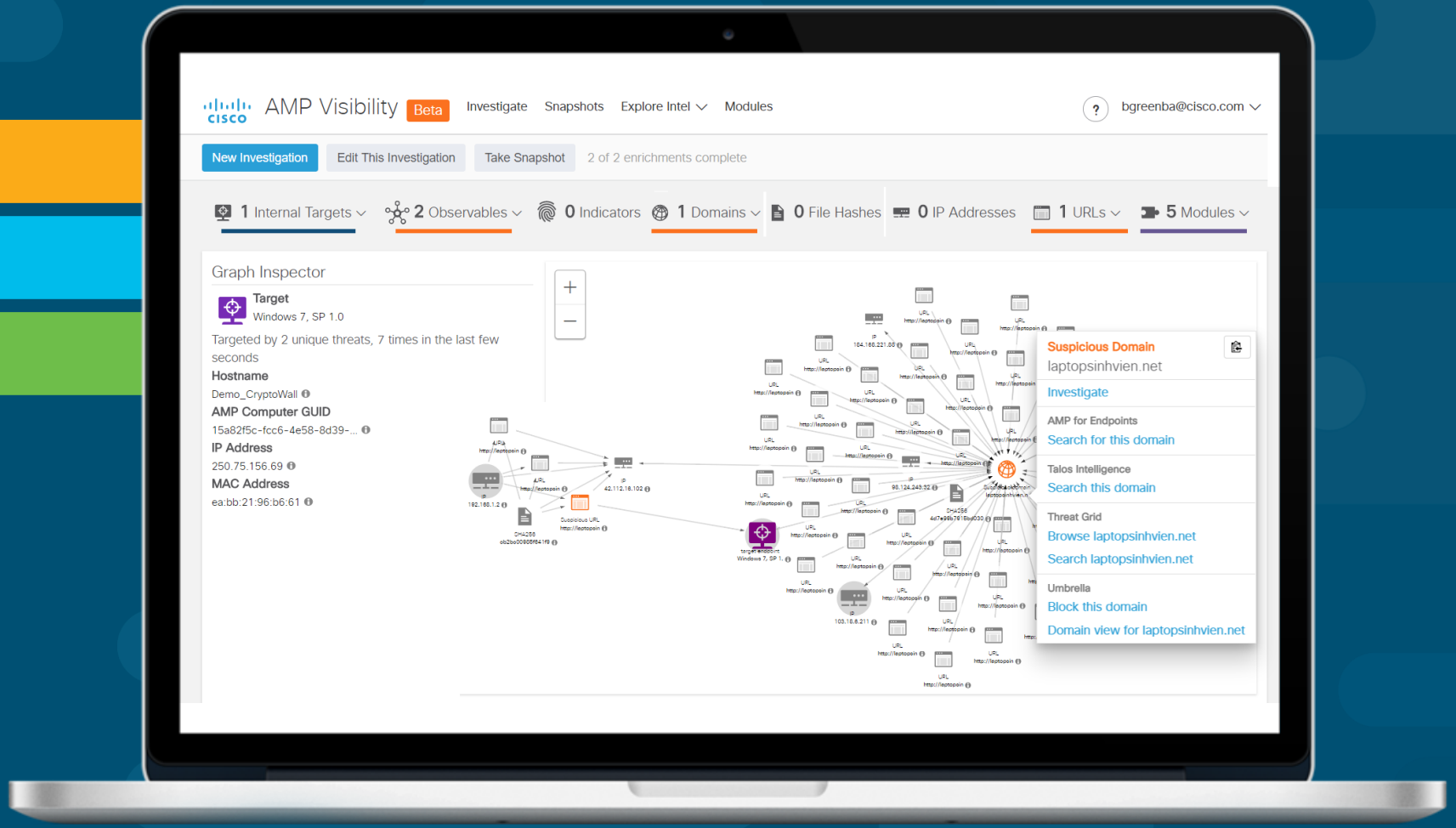
가시성 기반의 조사 및 대응 - Threat Response

위협 추적

원 클릭 차단

인텔리젼스 상관관계

인텔리젼스 가시성 도구로 IP, 해쉬 및 기타 공격과 연관된 데이터를 조회하여 각 인텔리젼스 데이터와 연계하여 한눈에 가시성을 제공해 줌.



관제 및 분석팀

Next-Gen Firewalls

Malware Detection

3rd party Sources

Endpoint Security

SIEM

Next-Gen IPS

Secure Internet Gateway

Email Security

Web Security

Network Analytics

Threat Intel

Identity Mgmt

CaseStudy : 보안팀의 인텔리전스 활용 예

알려져 있는 정보를 통한
Threat Hunting
- 감염된 시스템 확인
- 추가 IP 연결 확인
- 연관된 위협 정보 확인

AMP for Endpoints

차세대 엔드포인트 보안

1%

여러분이 놓쳤던 작은 부분까지

- 차단, 탐지 그리고 대응까지 한번에
- 못 보던 1% 까지 들여다 보다
- 클라우드 또는 프라이빗 환경의 빠른 구성
- 지속적인 파일 행동 분석 및 회귀적 보안
- 빠른 대응 : 한번 보고, 모든 곳에서 차단
- 다양한 플랫폼에서의 위협 차단 제공

cisco.com/go/ampendpoint