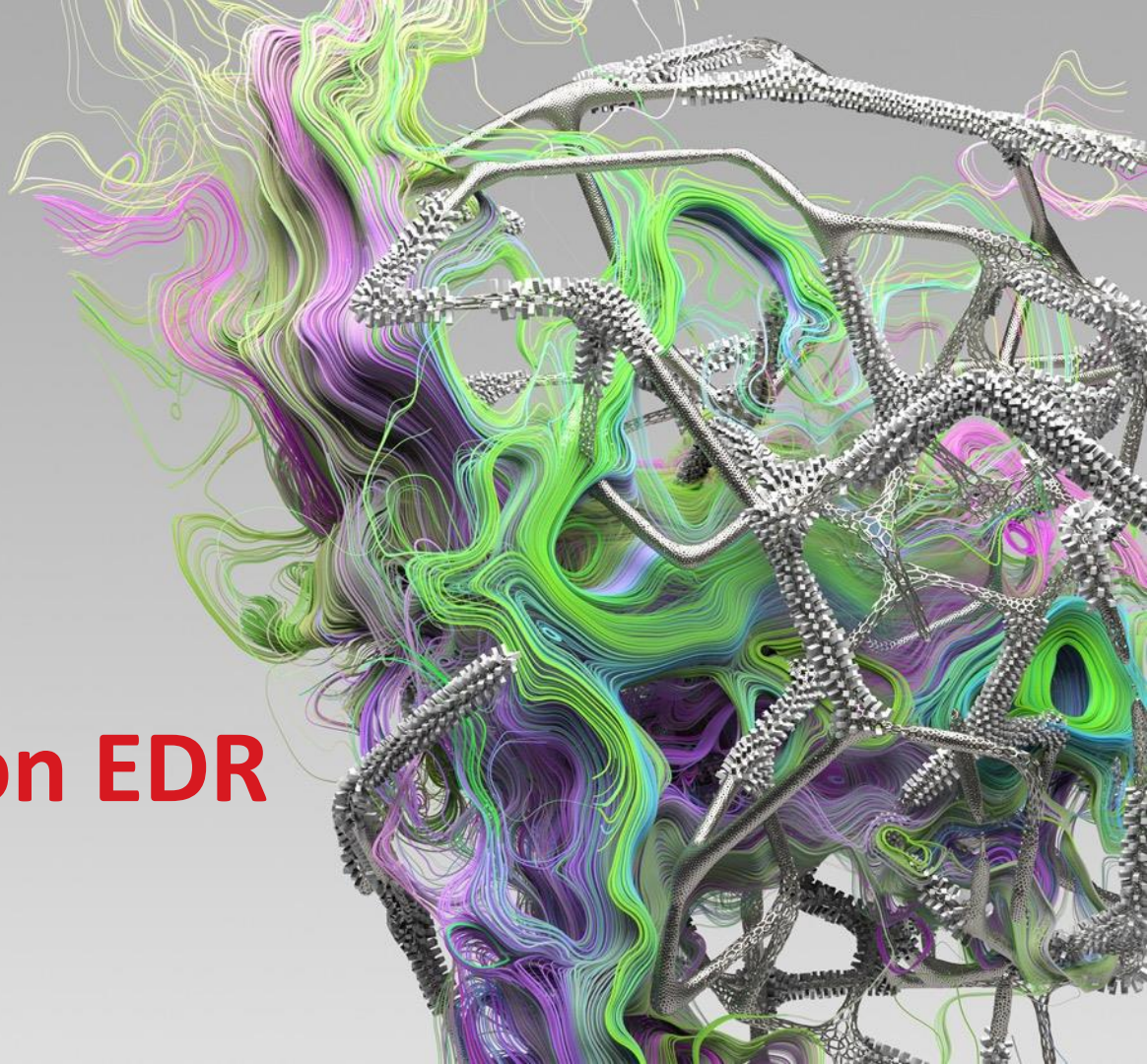
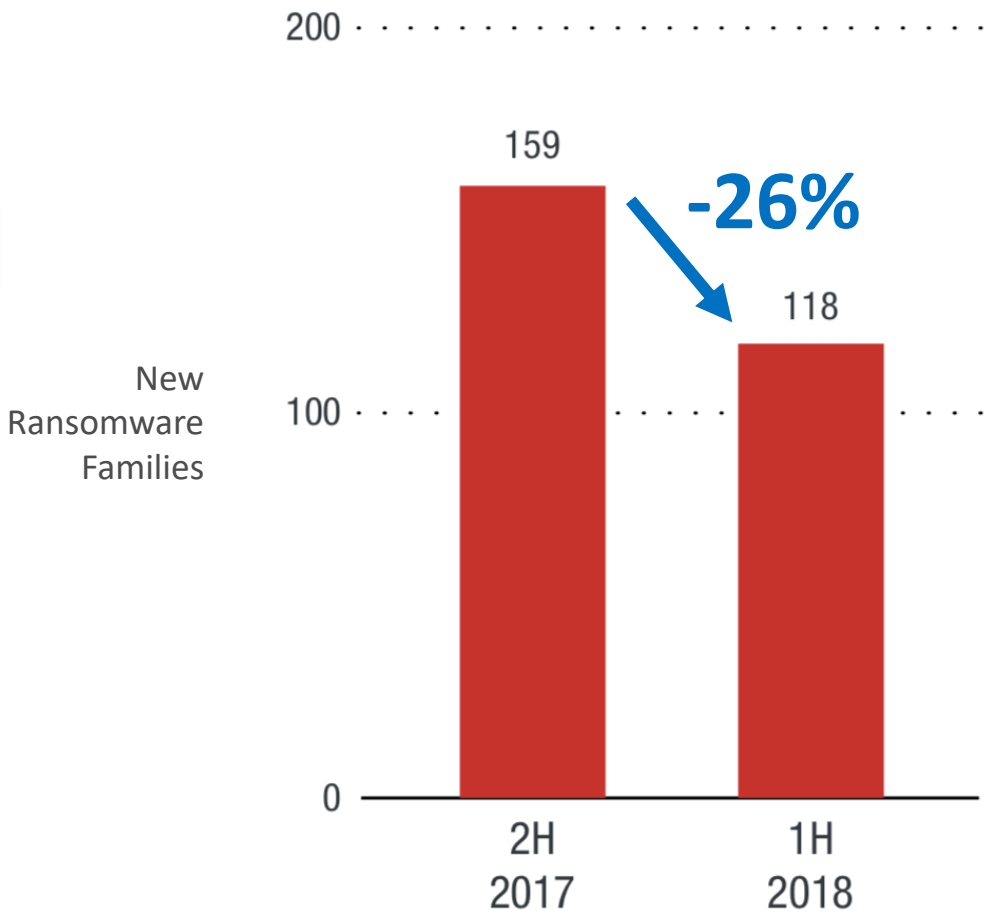
Next Generation EDR

Trend Micro



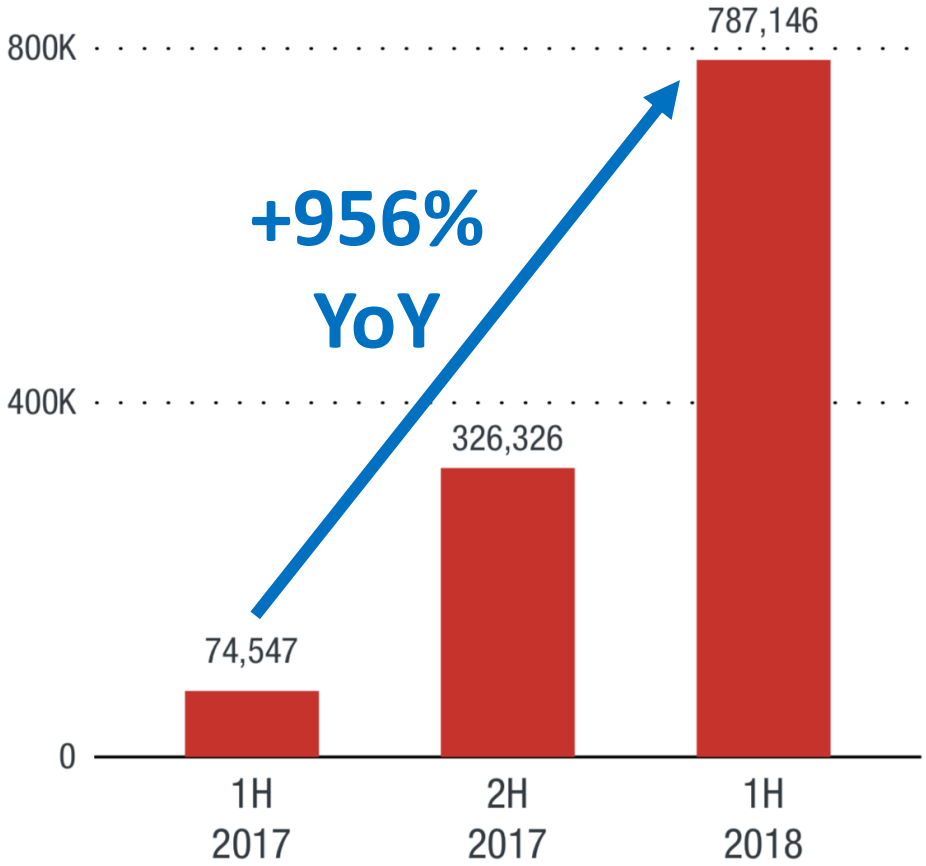
랜섬웨어 패밀리의 감소 추세



요구 금액과 피해액은 증가

Source: “Unseen Losses, Imminent Losses”, Trend Micro, August 2018

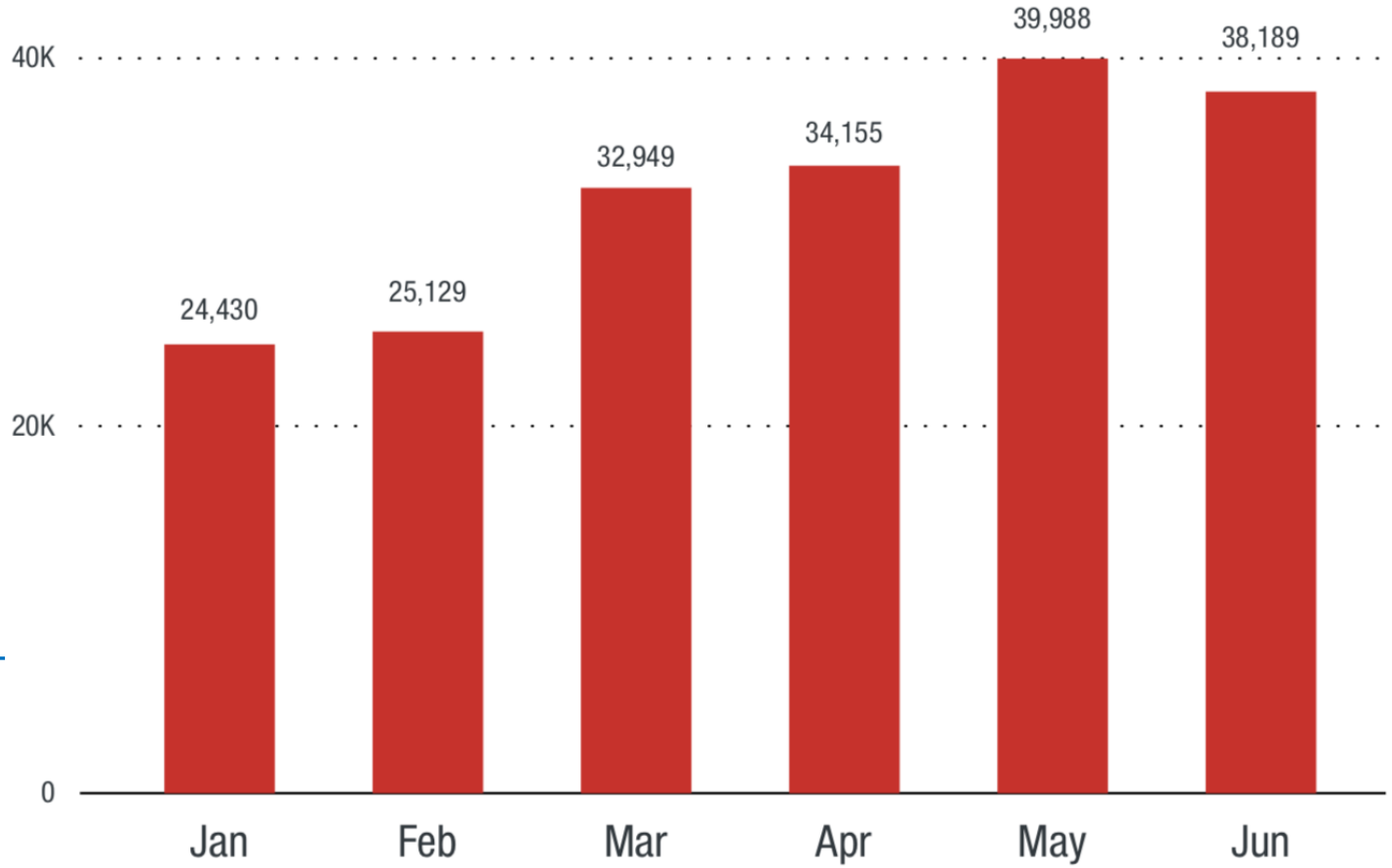
코인 마이너 위협의 증가



Source: “Unseen Losses, Imminent Losses”, Trend Micro, August 2018

파일리스 악성코드 증가

현재 추세로는 2019년 중반에 랜섬웨어의 위협 이상으로 증가할 것으로 예상



Endpoint Detection and Response (EDR)

Advanced Threats

- 지능적 공격들과 파일리스에 대한 탐지의 어려움
- 탐지 시 필요한 데이터, 범위 및 문제 해결 방법을 이해하기가 어렵다

EDR

- 엔드포인트의 시스템 레벨에서의 행위와 이벤트를 기록 (ie. user, file, process, registry, memory and network events)
- 알려진 IOC 데이터베이스 및 행동 분석 기법과 비교하여 이러한 공격을 식별하고 대응
- EDR은 공격에 대한 범위, 특성 및 대응 정보를 신속하게 제공

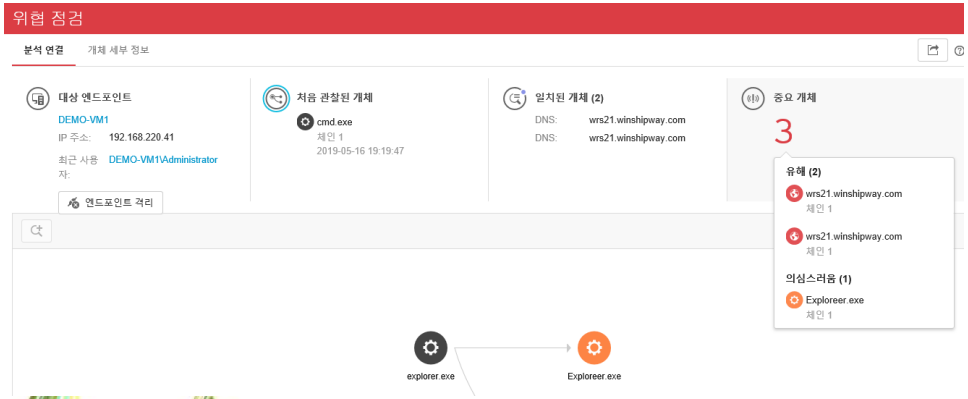
Endpoint Detection & Response(EDR)

Why EDR? Detection!!!

- 평판기술, 샌드박스 솔루션으로 확보한 위협 지표(IoC)의 활용 확장
  - EDR 대시보드, APT솔루션으로 위협지표(IoC)를 확인 및 탐지
  - 위협지표가 활동 중인 엔드포인트를 찾아서 조치
  - 아직 조치되지 않고 있는 엔드포인트는? 최초 근원지는?
    - EDR은 비활동 상태로 잠재하고 있는 위협지표 엔드포인트 추적

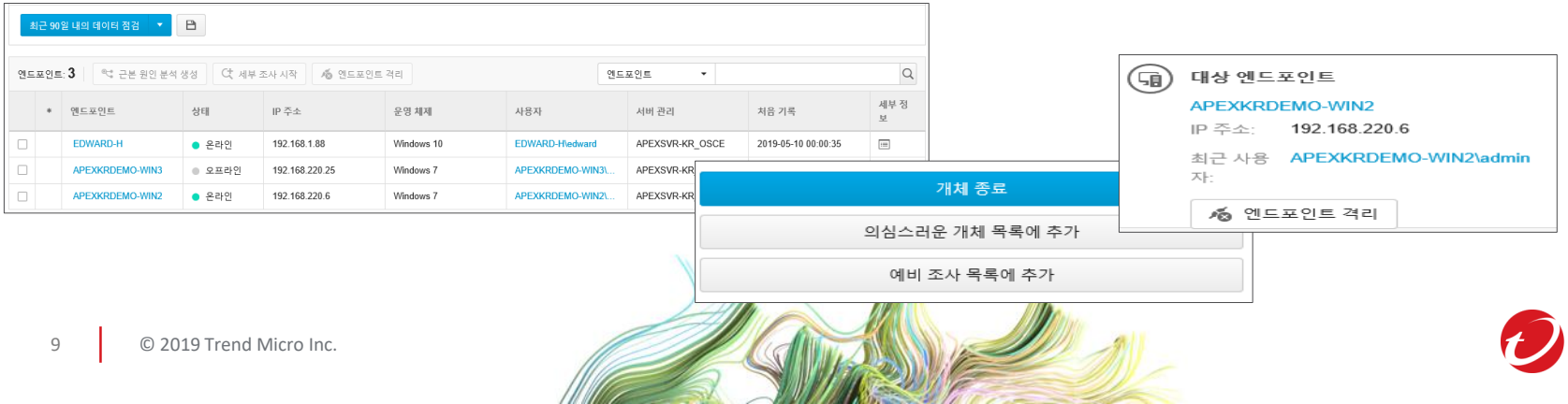
Why EDR? Analysis!!!

- 위협 지표의 상관 관계 분석
  - 특정 파일이 악성으로 판단되었다면 그 파일은 어떠한 경로로 다운로드 또는 복사되었는가?
  - 이 파일이 최초의 숙주 파일이 맞는가? C&C로부터 다운로드된 것은 아닌가? 어떤 파일이 C&C에 최초 접속하게 되었는가…?
    - 위협 체인을 제시하여 위협지표의 유입 경로, 시도한 행동 내역, 해당 엔드포인트에서 변경한 내역 등을 포함한 감염근원 파악



Why EDR? Response!!!

- 위험 엔드포인트에 대한 적절한 조치
  - 탐지와 분석을 통해 찾아낸 엔드포인트에 백신이 설치되어 있지 않다면?
  - 새로이 찾아낸 위협지표에 대해서 백신의 패턴과 평판 정보가 반영되어 있지 않다면?
  - 이번에 찾아낸 엔드포인트 외에 다른 엔드포인트들도 동일한 위협 지표를 내포하고 있다면?
    - 위협 지표 악성코드 프로세스 강제종료, 위협지표 C&C로의 접속 차단
    - 내부 엔드포인트로의 확산(Lateral Movement) 방지
    - 동일한 위협지표를 내포한 다른 엔드포인트 검색 & 동일한 조치



Endpoint Detection & Response

탐지

샌드박스 분석 결과, OpenIoC,

사용자 정의 정보 등의 사용 내역을 대입하여 영향도 조사

위협지표 흔적이 존재하는 엔드포인트들을 스위핑

분석

확보된 위협지표와 엔드포인트를 대상으로 Root Cause Analysis(RCA) 레포트 생성

위협 체인을 통해 침해 경로 확인

동일 위협이 존재하는 엔드포인트 리스트 확보

대응

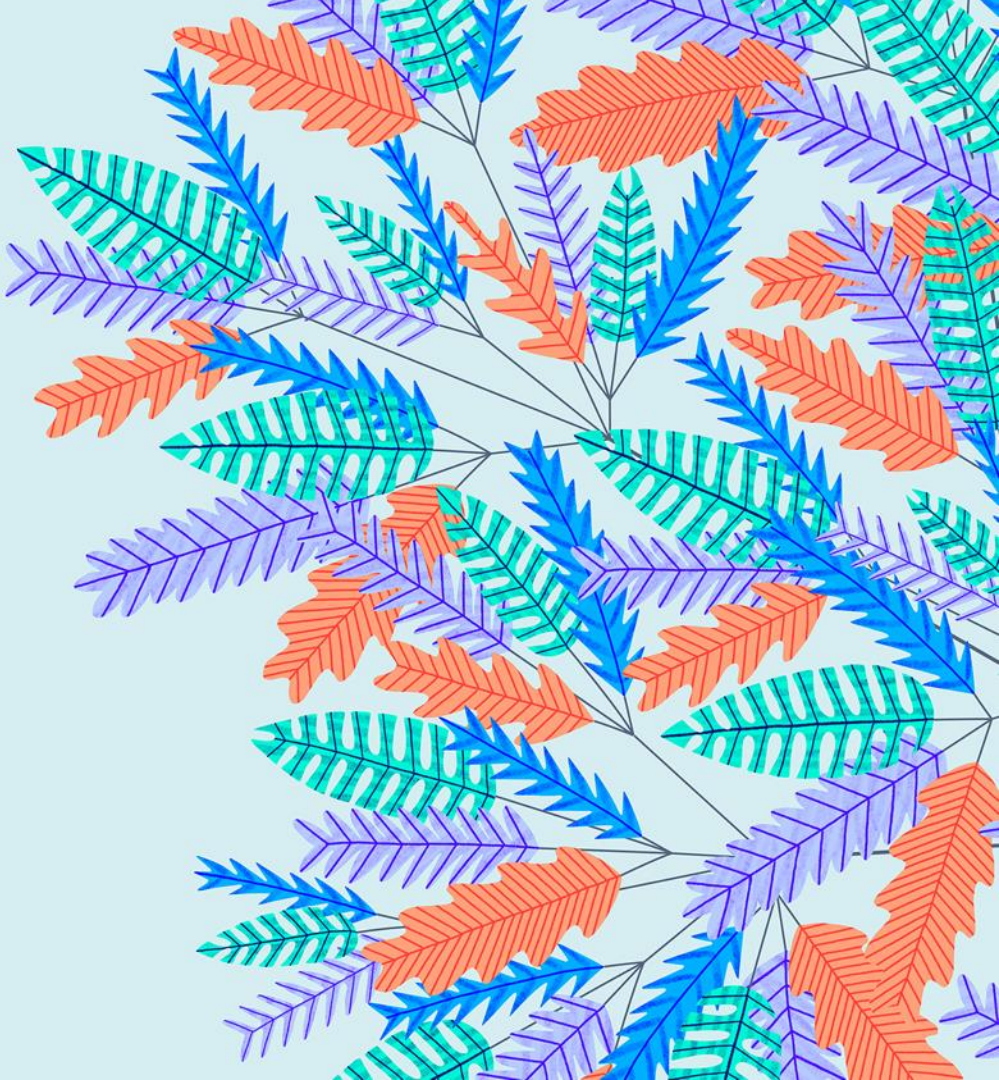
위협지표 강제 종료, 접속 차단

대상 엔드포인트 격리

위협을 내포하고 있는 모든 엔드포인트에 대해 효과적이고 신속한 대응(IoC 공유)

TREND MICRO™

EDR - 탐지

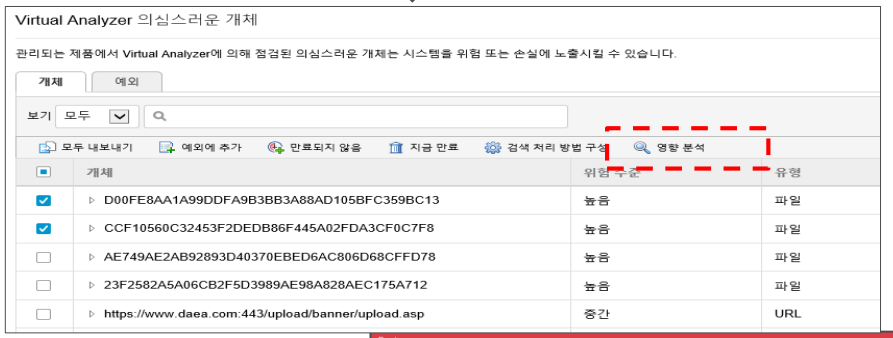


탐지 1. 샌드박스 분석 결과 활용 탐지

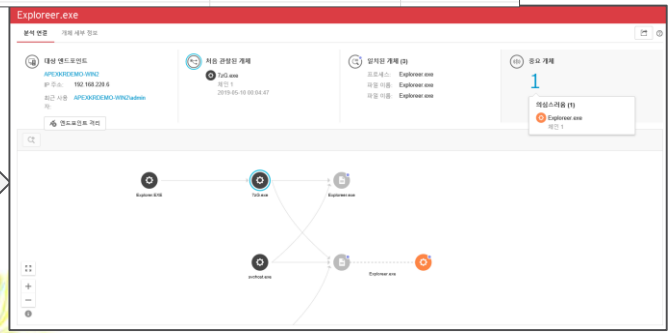
- 샌드박스 분석 결과를 대입하여 영향도 조사
  - 의심 파일
  - IP주소
  - URL
  - 도메인

- RCA를 통한 위협 체인 분석

Trend Micro Deep Discovery
(네트워크 APT, 이메일 APT)
샌드박스 분석 결과



Root Cause Analysis
(RCA)

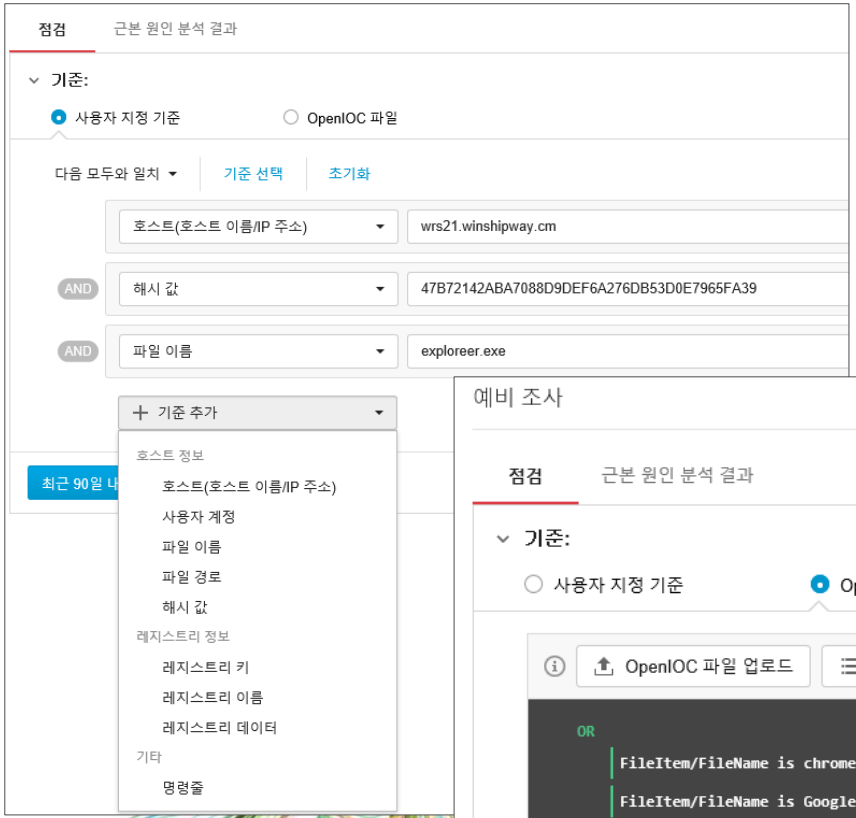


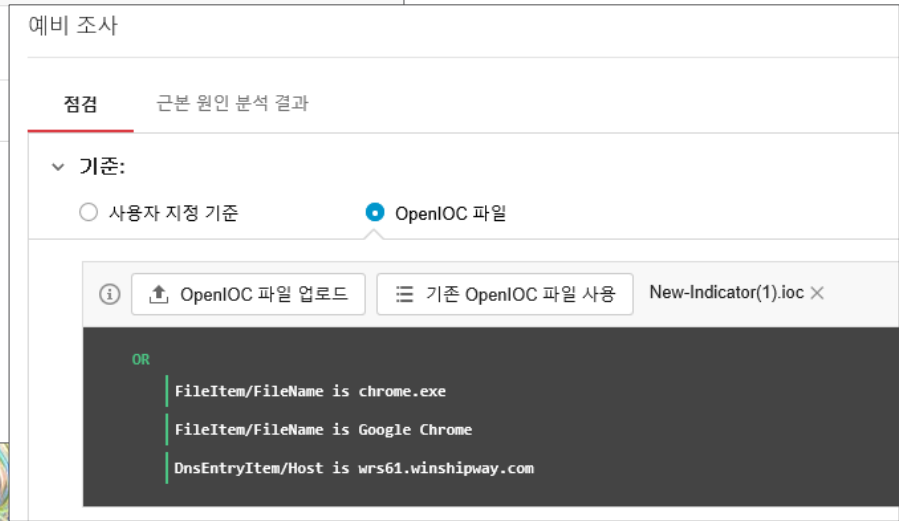
탐지 2. 사용자 지정 기준 및 IOC를 이용한 스위핑

검색 조건 및 입력값

- 호스트, IP주소
- 사용자 계정
- 파일명
- 파일경로
- 해시정보
- 레지스트리
- 명령어
- C&C콜백 이벤트

- OpenIOC 파일 활용





탐지 3. 운영센터 대시보드에서의 위협 영향도 조사

- APEX 대시보드
- 보안 정합성 상태 표시
- 탐지된 위협 표시
  - 랜섬웨어, APT, 소셜 엔지니어링 공격, C&C콜백, 수평 이동 위협, 취약점 공격 등의 위협 표시
  - 위협 탐지 정보를 쿼리하여 영향받은 엔드포인트 조회
  - 최초 감염 근원지 또는 위협 잠재 내포 엔드포인트(Patient Zero ID) 포착
  - 위협 분석 진행

대시보드 - 운영센터

Trend Micro Apex Central

admin

대시보드 | 디렉터리 | 정책

운영 센터 | 요약 | DLP 발생 건수 조사 | 데이터 손실 방지 | 규정 준수 | 위협 탐지 | Mac | 애플리케이션 제어 | +

62% 바이러스 백신 패턴 규정 준수

만료된 패턴을 사용하는 엔드포인트: 8

1 중요한 위협

영향을 받는 사용자: 1 (0)

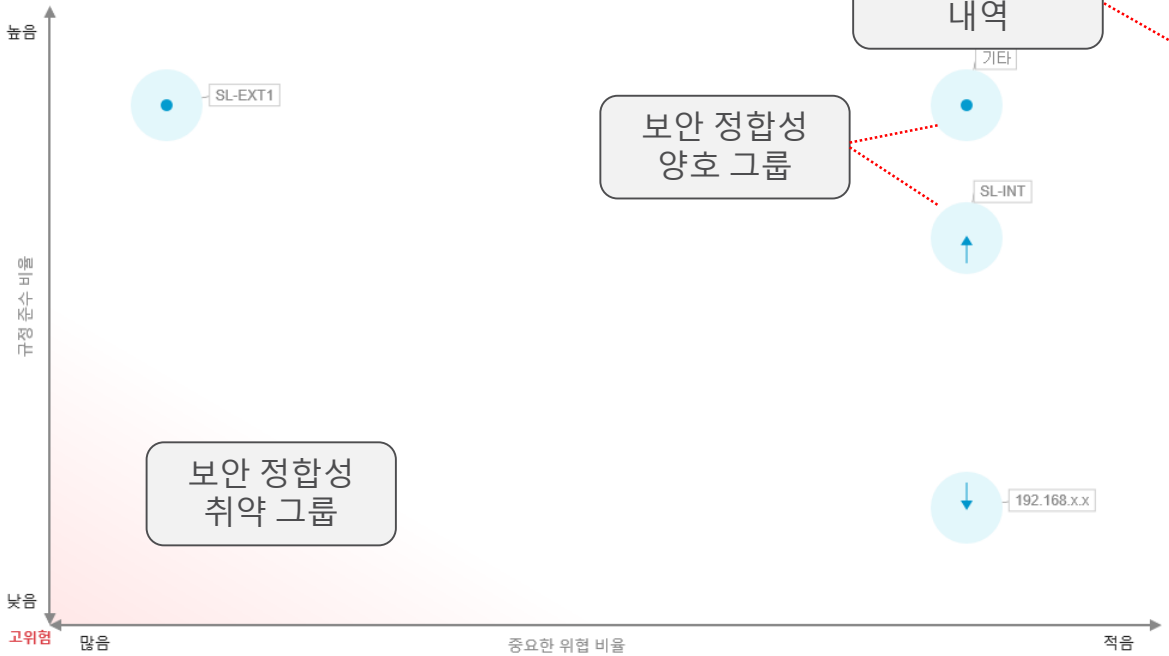
13 해결된 이벤트

0 해결되지 않은 이벤트의 영향을 받는 사용자: 0

위협 탐지 내역

보안 정합성 양호 그룹

보안 정합성 취약 그룹



모두

62% 바이러스 백신 패턴 규정 준수

평균 변화(30일 동안):		- 22%
관리되는 에이전트:	22	
호환 바이러스 패턴 사용	13	62%
만료된 바이러스 패턴 사용	8	38%
7일 동안 오프라인	1	
예외	0	
관리되지 않는 엔드포인트:	0	

1 중요한 위협

랜섬웨어	0
알려진 APT(Advanced Persistent Threat)	0
소셜 엔지니어링 공격	0
취약점 공격	0
수평적 이동	0
알 수 없는 위협	0
C&C 콜백	1

wrs21.winshipway.com

1 영향을 받는 사용자

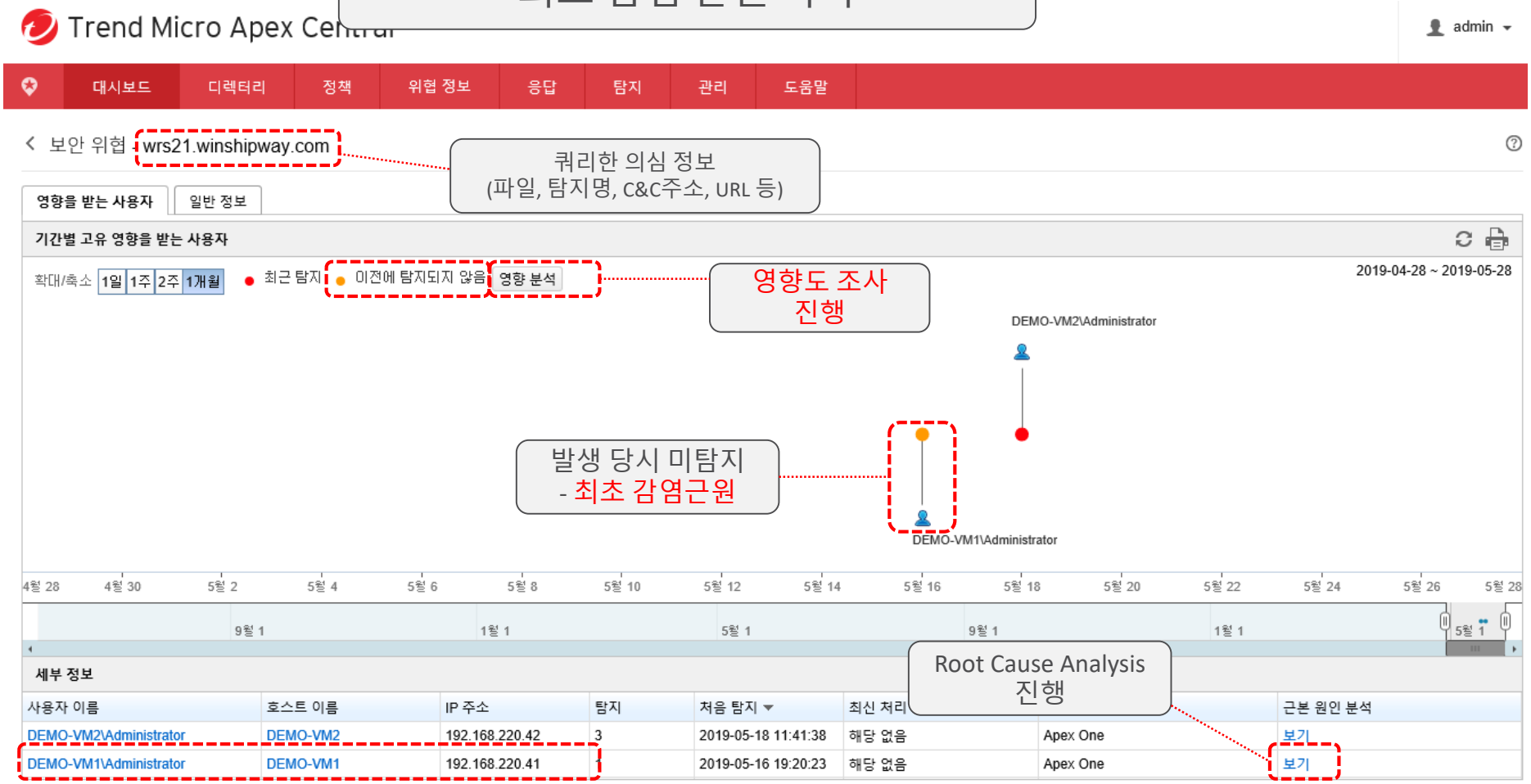
APEXKRDEMO-WIN1\Administrator

1 영향을 받는 엔드포인트

APEXKRDEMO-WIN1

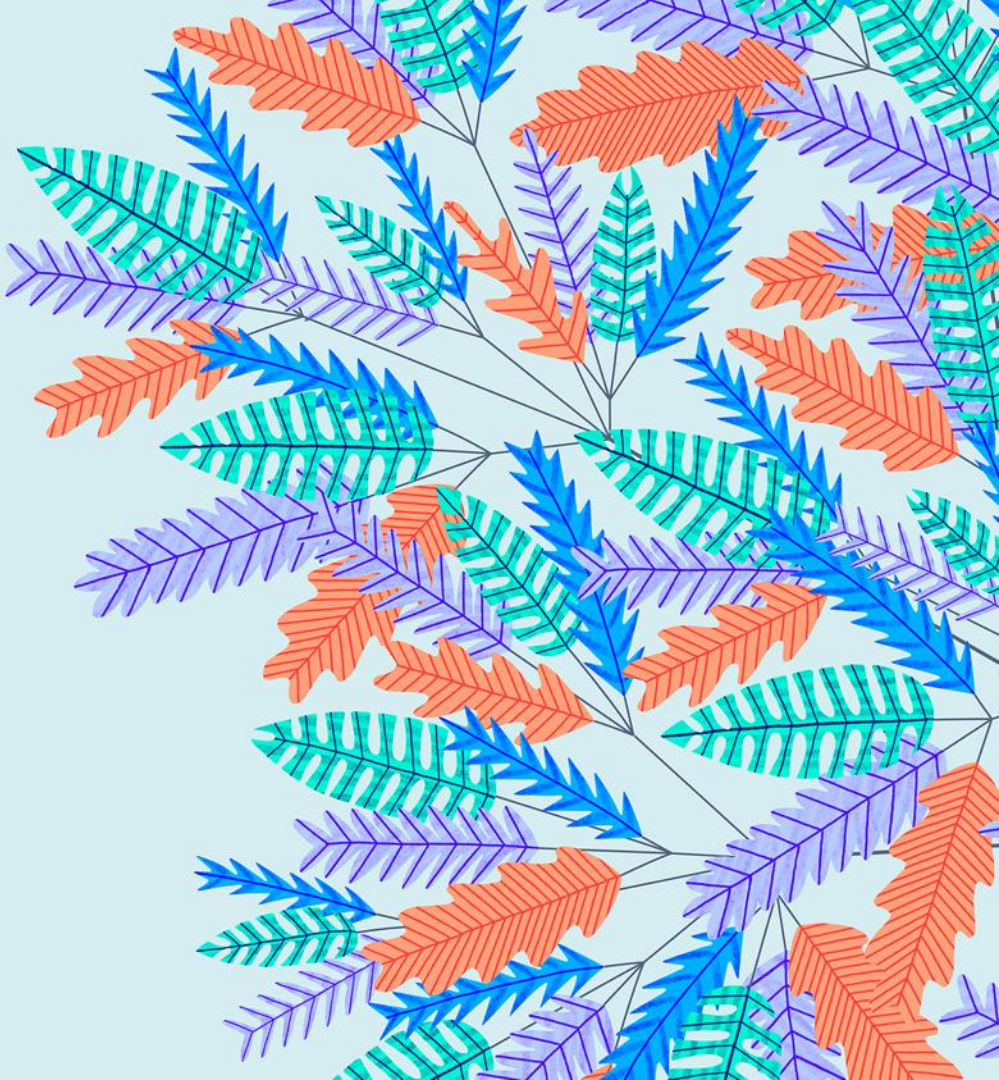
*지난 30일 동안의 중요한 위협 및 탐지를 표시합니다.

최초 감염 근원 파악

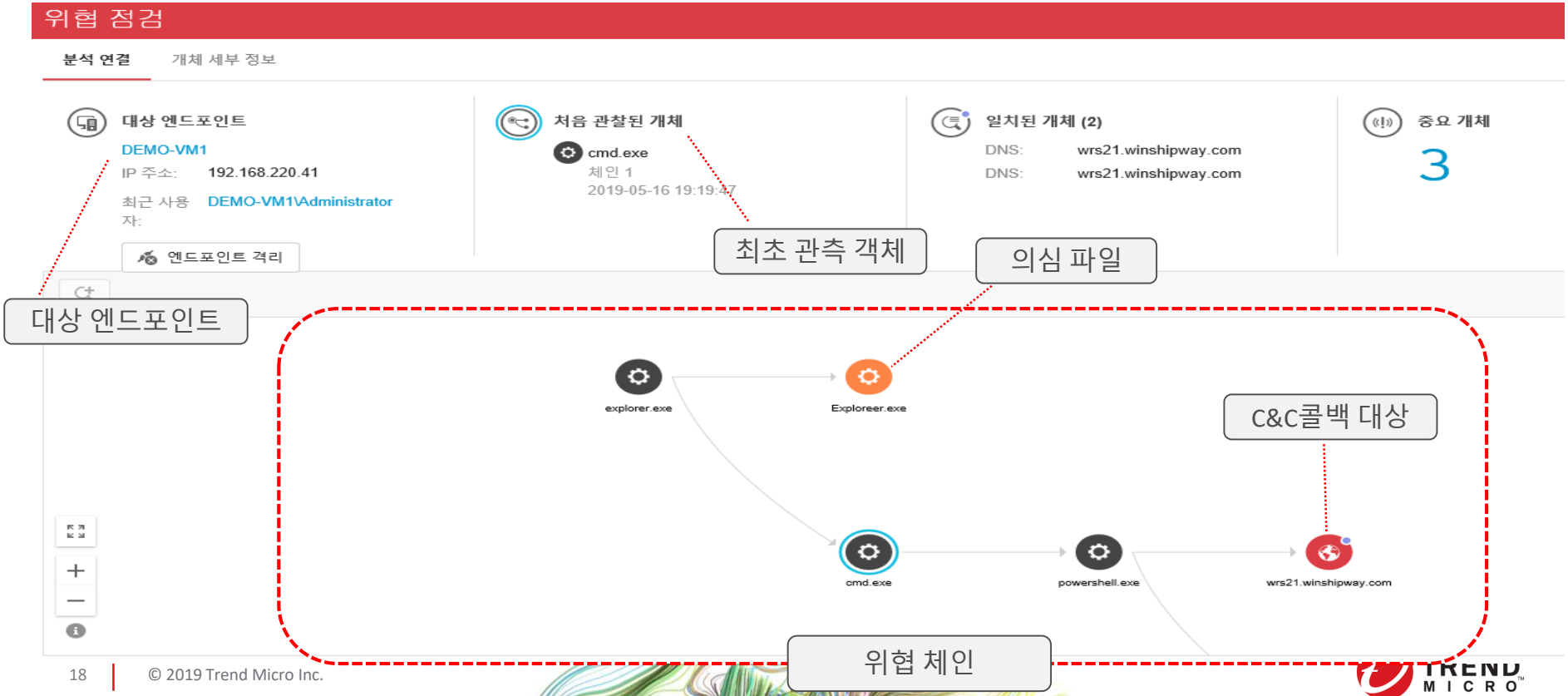

Trend Micro Apex Central
admin
대시보드
디렉터리
정책
위협 정보
응답
탐지
관리
도움말
보안 위협 wrs21.winshipway.com
쿼리한 의심 정보
(파일, 탐지명, C&C주소, URL 등)
영향을 받는 사용자
일반 정보
기간별 고유 영향을 받는 사용자
확대/축소 1일 1주 2주 1개월
최근 탐지
이전에 탐지되지 않음
영향 분석
영향도 조사
진행
2019-04-28 ~ 2019-05-28
DEMO-VM2\Administrator
발생 당시 미탐지
- 최초 감염근원
DEMO-VM1\Administrator
4월 28 4월 30 5월 2 5월 4 5월 6 5월 8 5월 10 5월 12 5월 14 5월 16 5월 18 5월 20 5월 22 5월 24 5월 26 5월 28
9월 1 1월 1 5월 1 9월 1 1월 1 5월 1
세부 정보
Root Cause Analysis
진행
사용자 이름 | 호스트 이름 | IP 주소 | 탐지 | 처음 탐지 | 최신 처리 | | 근본 원인 분석
DEMO-VM2\Administrator | DEMO-VM2 | 192.168.220.42 | 3 | 2019-05-18 11:41:38 | 해당 없음 | Apex One | 보기
DEMO-VM1\Administrator | DEMO-VM1 | 192.168.220.41 | 1 | 2019-05-16 19:20:23 | 해당 없음 | Apex One | 보기

TREND MICRO™

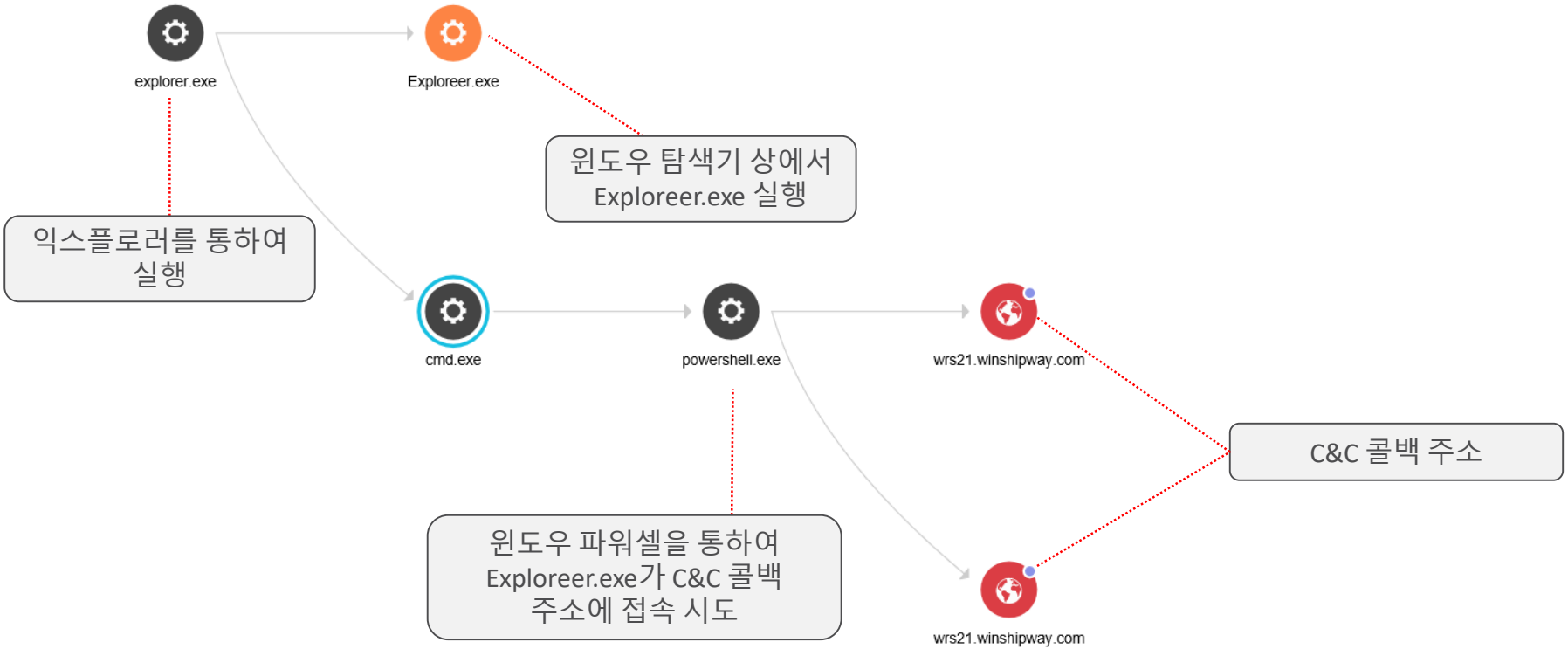
EDR - 분석



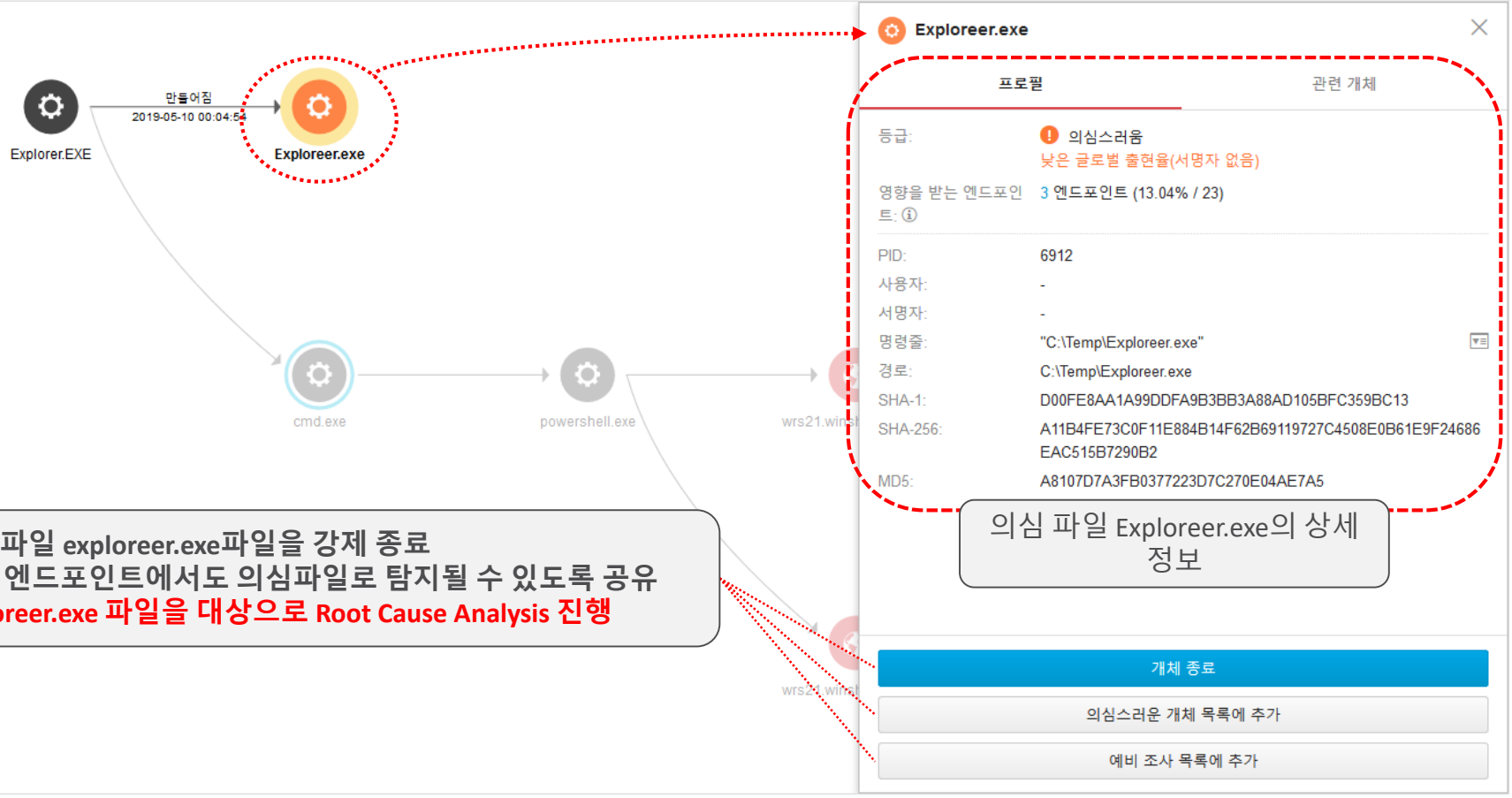
Root Cause Analysis 결과



Root Cause Analysis 결과



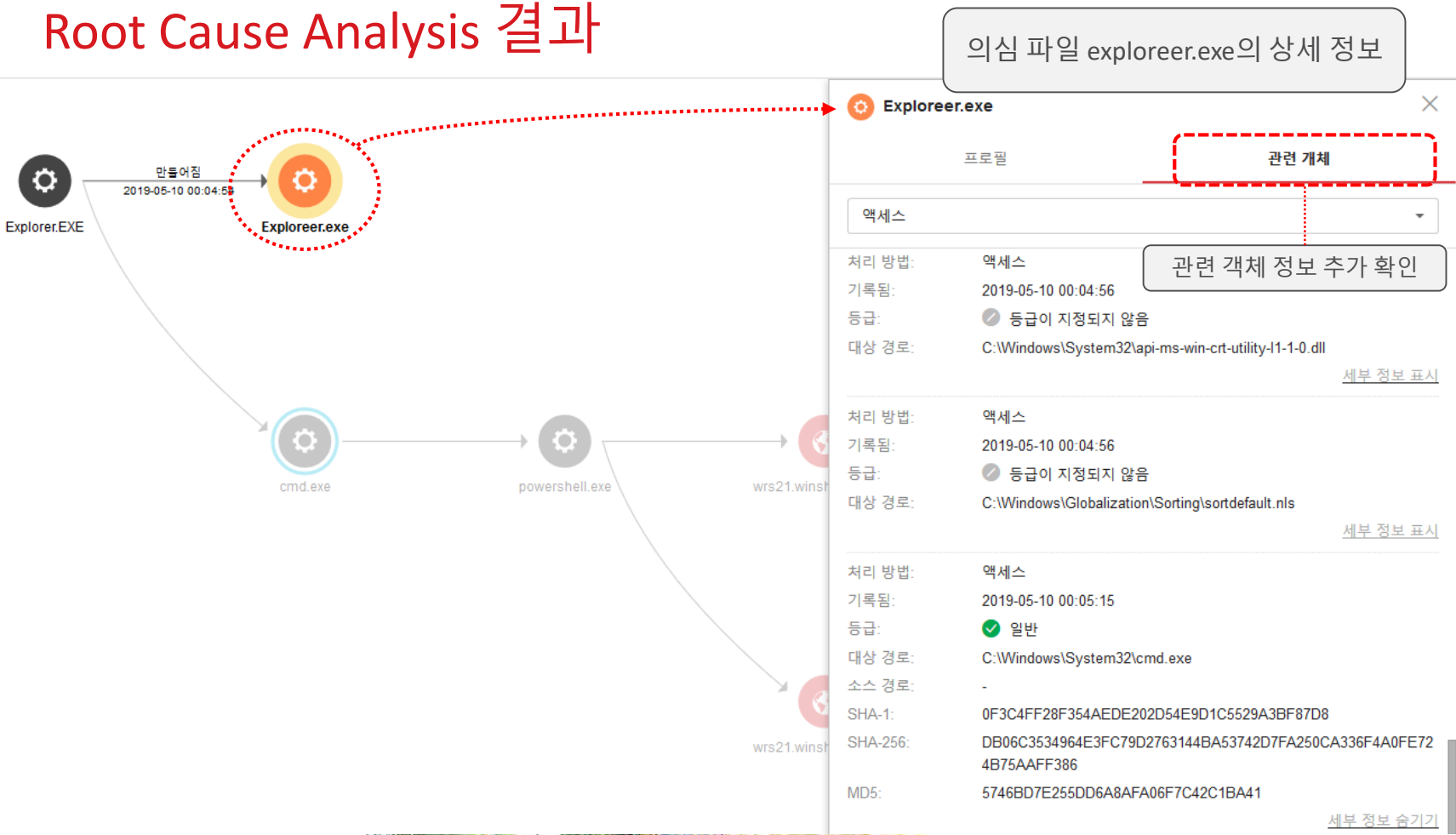
Root Cause Analysis 결과



의심 파일 Exploreer.exe의 상세 정보

- 의심파일 exploreer.exe파일을 강제 종료
- 다른 엔드포인트에서도 의심파일로 탐지될 수 있도록 공유
- **exploreer.exe 파일을 대상으로 Root Cause Analysis 진행**

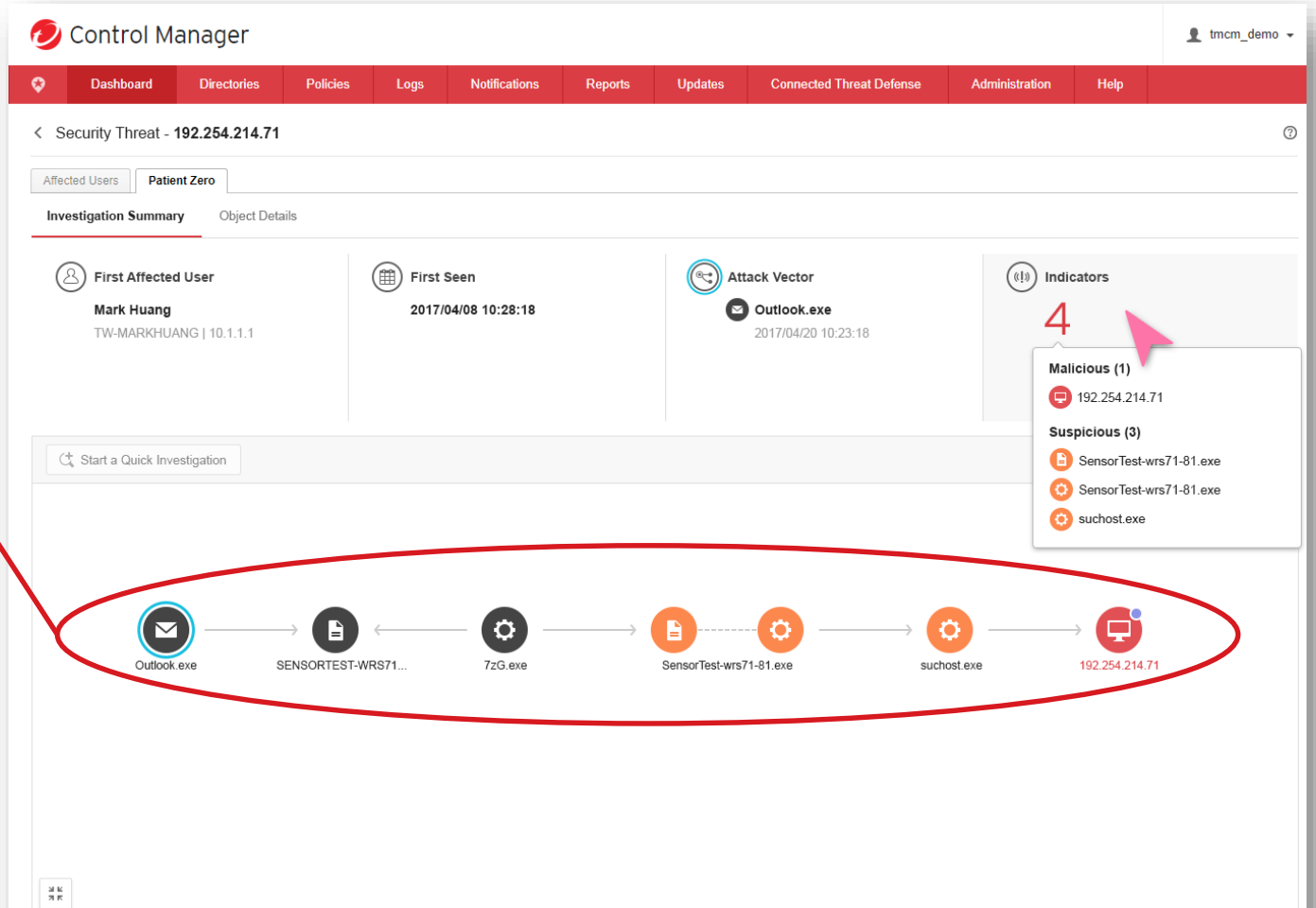
Root Cause Analysis 결과



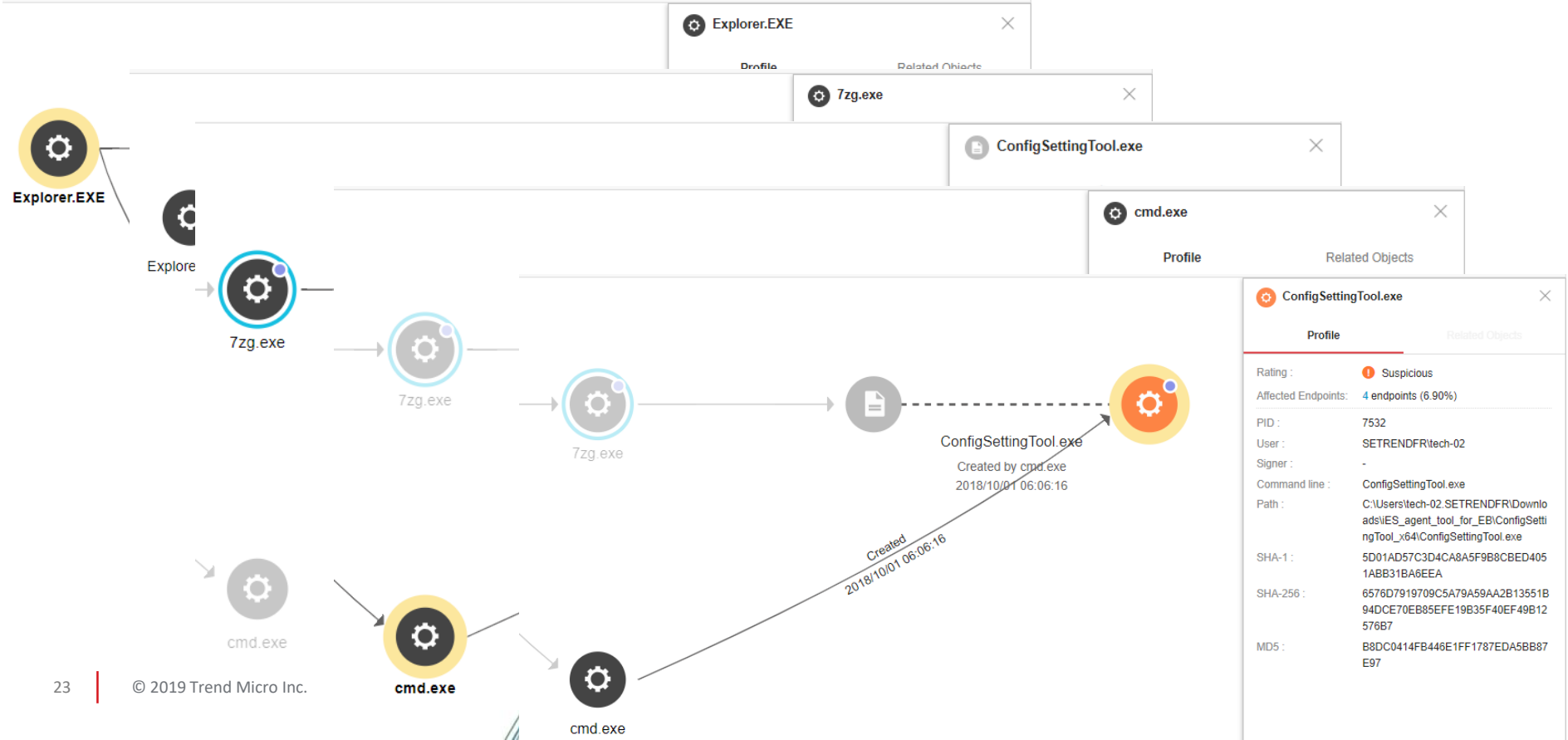
Root Cause Analysis 결과

"How did this happen?"

- **Root cause analysis** for simple or full "kill chain"
- Enhanced by Trend intelligence
  - Red (known bad)
  - Orange (suspicious)
  - Black (known good)

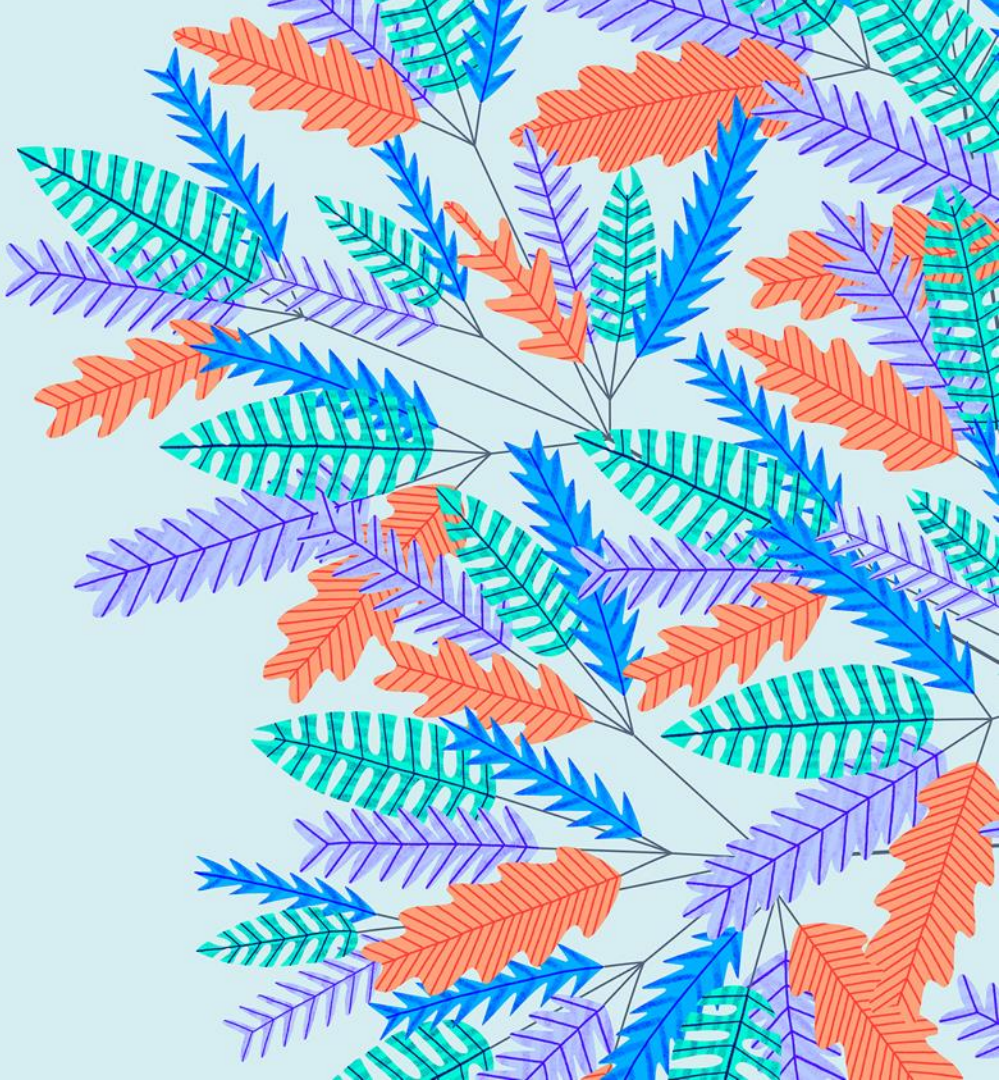


위협 체인 분석



TREND MICRO™

EDR - 대응

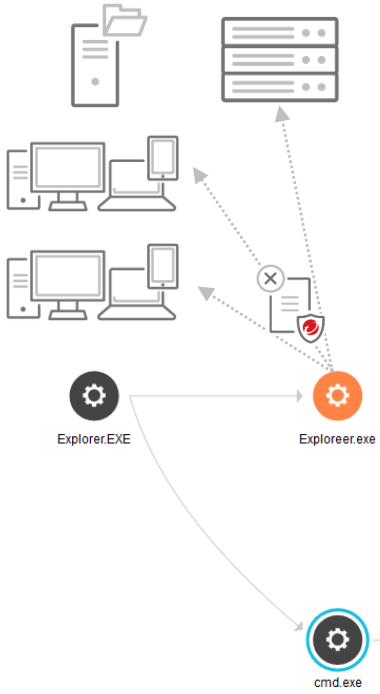


대응 1. 의심 프로세스 강제 종료

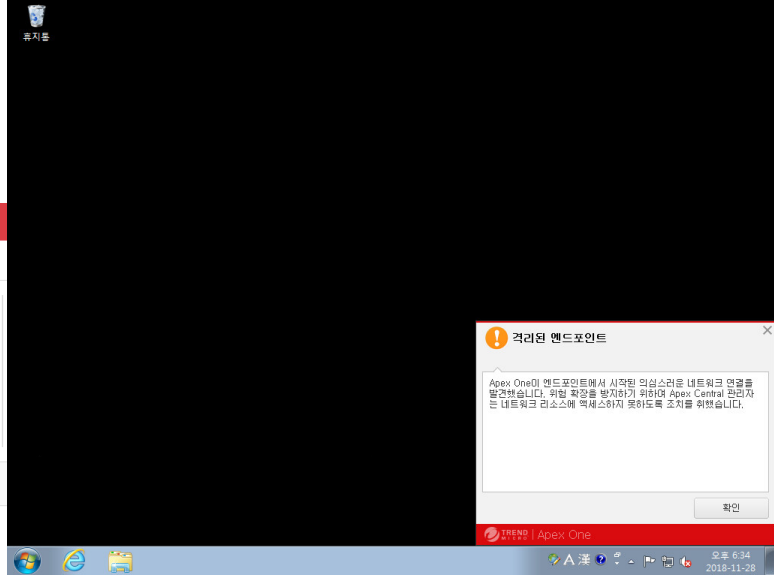
- RCA 분석결과를 통한 의심 파일 프로세스 강제 종료

대응 2. 의심 객체 정보 공유

- 다른 엔드포인트에 의심객체 정보를 공유
- 의심파일로 탐지되어 동일 파일 실행 차단
- 동일 URL, 도메인, IP주소인 경우 접속 차단



대응 3. 위험 엔드포인트 격리



위협 점검

분석 연결 | 개체 세부 정보

대상 엔드포인트
APEXKRDEMO-WIN2
IP 주소: 192.168.220.6
최근 사용자: APEXKRDEMO-WIN2\admin
엔드포인트 격리

처음 관찰된 개체
cmd.exe
체인 1
2019-05-10 00:04:56

대상 엔드포인트를
네트워크로부터 격리

Explorer.EXE
Exploreer.exe

위험 엔드포인트를
네트워크로부터 격리

EDR 중앙관리서버간에만 통신 가능(향후 격리해제 가능)

powershell.exe
wrs21.winshipway.com
wrs21.winshipway.com

대응 3. 위험 엔드포인트 일괄 격리

- 긴급 사안인 경우 동일한 위협 지표의 흔적이 발견된 엔드포인트들을 일괄적으로 격리 적용

엔드포인트: **3** | 근본 원인 분석 생성 (3) | 세부 조사 시작 (3) | 엔드포인트 격리 (3) | 엔드포인트

	*	엔드포인트	상태	IP 주소	운영 체제	사용자	서버 관리	처음 기록	세부 정보
☑		EDWARD-H	온라인	192.168.1.88	Windows 10	EDWARD-H\edward	APEXSVR-KR_OSCE	2019-05-10 00:00:35	
☑		APEXKRDEMO-WIN3	오프라인	192.168.220.25	Windows 7	APEXKRDEMO-WIN3\...	APEXSVR-KR_OSCE	2019-05-25 21:58:35	
☑		APEXKRDEMO-WIN2	온라인	192.168.220.6	Windows 7	APEXKRDEMO-WIN2\...	APEXSVR-KR_OSCE	2019-05-10 00:04:48	

EDR 도입 기대 효과

TREND MICRO™

EDR 워크 플로우 구현

탐지

Trend Micro Deep Discovery
(네트워크 APT, 이메일 APT)

샌드박스 분석 결과
의심 객체

Custom Intelligence
사용자 정의 의심 객체
Yara Rule
Open IOC

운영센터 대시보드
위협 탐지 객체

Attack Discovery Engine
ADE 탐지 결과

분석

Root Cause Analysis

영향도 조사
위협 내포 엔드포인트 추적
Patient Zero ID(최초 감염 근원)
위협 체인 분석
의심파일 연관 객체
프로세스 인젝트
.....

대응

의심 파일 강제 종료

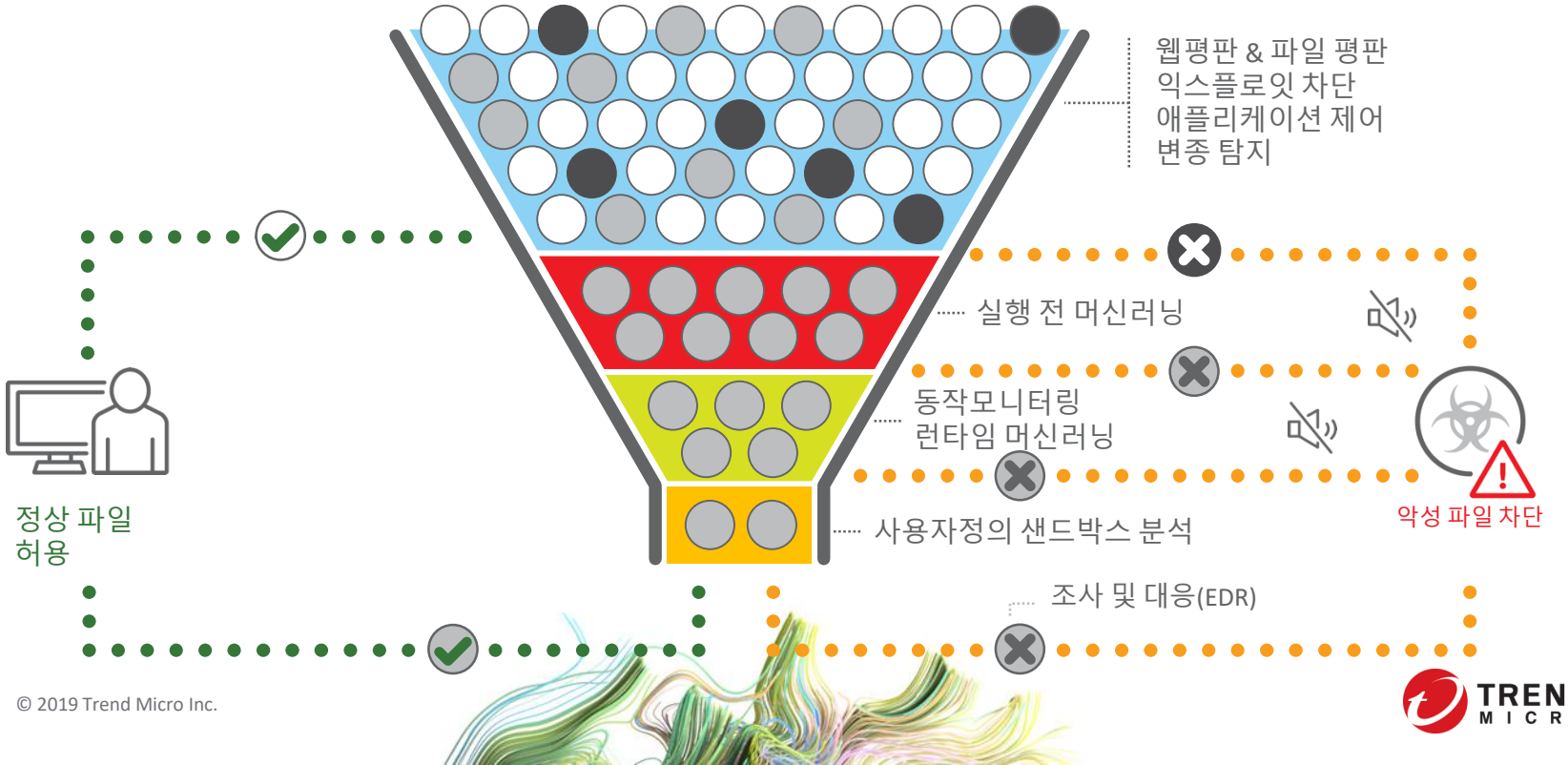
의심객체 정보 공유
의심 파일 실행 차단
의심 주소 접속 차단

위험 엔드포인트 격리

TREND MICRO

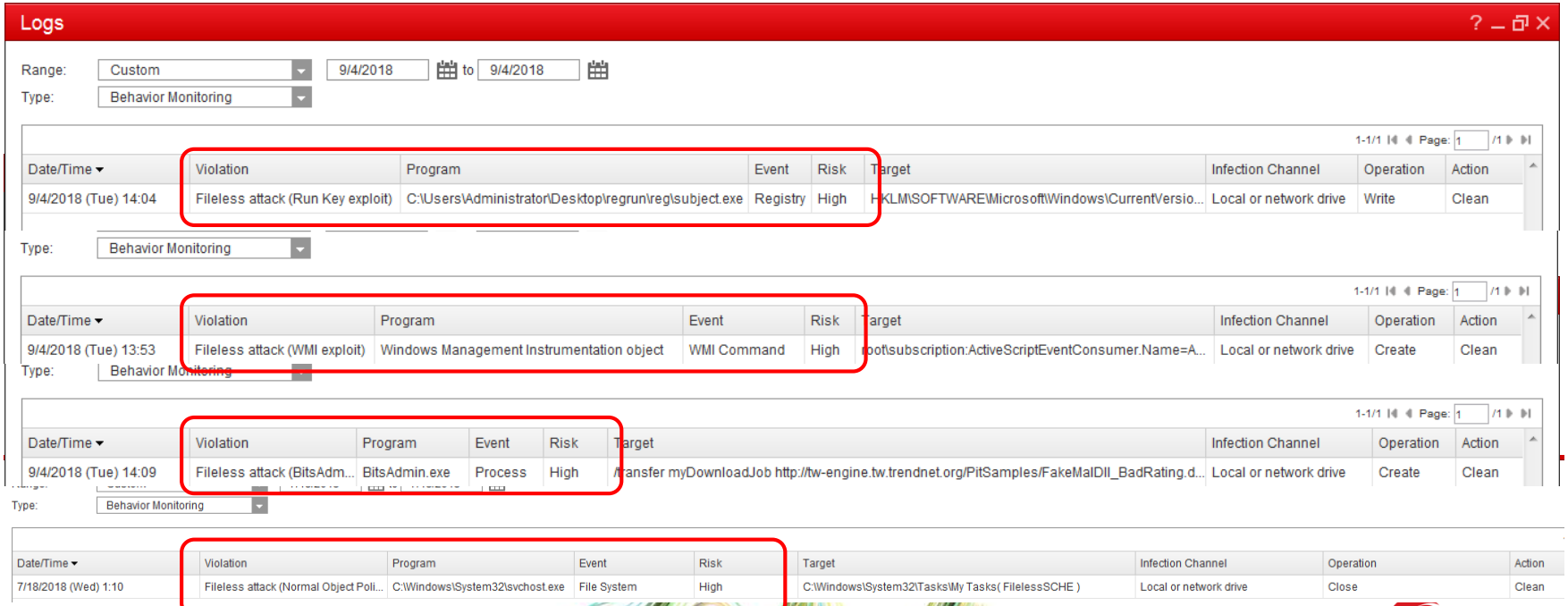
스마트: 상황 별 대응 기술

범례
- 알려진 정상 데이터
- 알려진 악성코드
- 알려지지 않은 데이타
- 노이즈 캔슬레이션



파일리스 악성코드 탐지

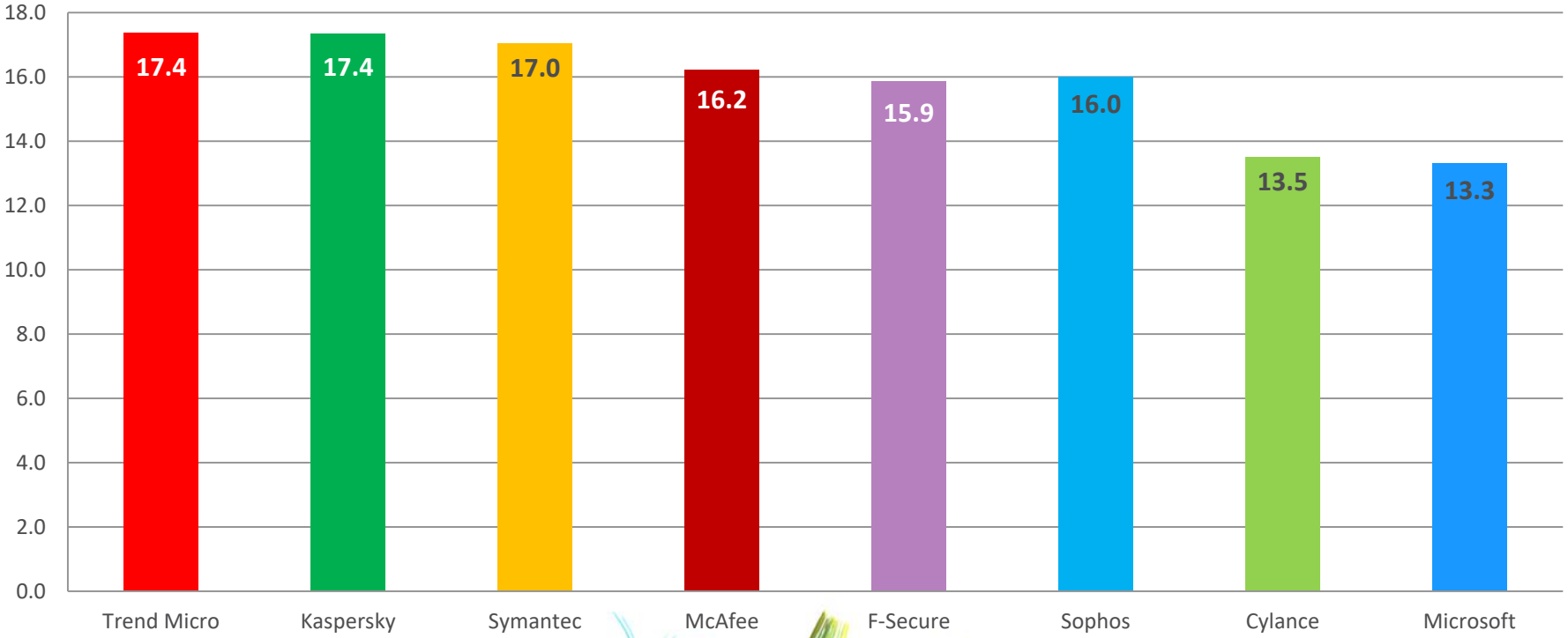
- RegRun, WMI, BitsJob, Scheduled Task 등의 파일리스 악성행위를 동작모니터링으로 탐지 및 제거




Trend Micro **Apex One™**
검증된 차세대 EDR 솔루션

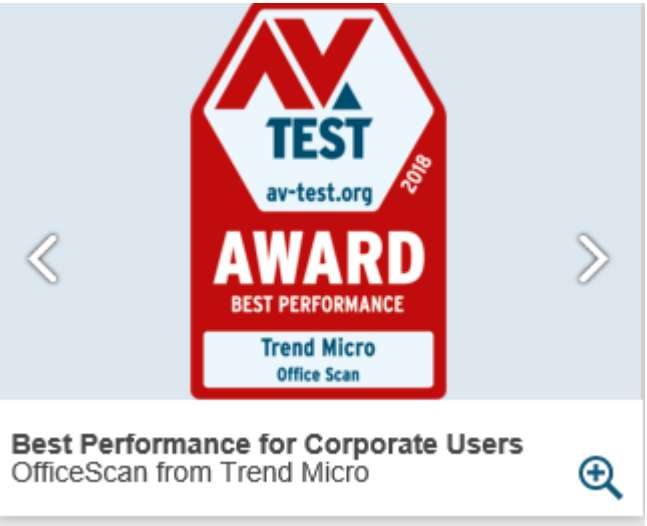
최근 3년 최고 점수 획득

Includes performance, protection (prevalent & 0-day) & usability



Source: av-test.org
Jan 2014 to Jun 2018

Awards 2018



Best Performance for Corporate Users
OfficeScan from Trend Micro

Best Protection for Consumer Users
Internet Security from Trend Micro

The AV-TEST Awards – a year of peak performance

In the daily fight against cyber attacks, an antivirus software manufacturer wages battle on many fronts. Thus, it is not only a question of ensuring that a product can match up against international competition, it is also about implementing a service-minded security promise made to the customer when the product is purchased. Only the most innovative research and development achievements can lead to consistent peak performance, which the AV-TEST Institute regularly puts to the test in its monthly side-by-side tests. With "Internet Security" and "OfficeScan", Trend Micro put two top contenders into the lineup in 2018 which were able to meet the high standards of the AV-TEST Institute in several categories.

In the area of consumers, Trend Micro receives recognition for best protection on Windows systems: The **Best Protection 2018** Award for outstanding protection goes to that manufacturer's "Internet Security" product.

In the corporate sector, AV-TEST is recognizing the product "Trend Micro OfficeScan" with the **Best Performance 2018** Award for its strong protection with minimal reduction of system performance.

TREND MICRO™

THE ART OF CYBERSECURITY

Unknown threats detected and stopped over time by Trend Micro. **Created with real data by artist Brendan Dawes.**