EDR을 통한 제로 트러스트 아키텍쳐

2019. 12. 11

Genians

1. 보안 전략의 변화

Zero Trust Architecture

어떤 것도 신뢰할 수 있는 것은 없다.

1. 보안 전략의 변화

Zero Trust Architecture

검증된 것 이외에는

어떤 것도 신뢰할 수 있는 것은 없다.

2. 신뢰에 대한 고찰

검증

검증된 것만 신뢰할 수 있으며,

- 비즈니스의 효용성을 위해서는 모두 동일한 레벨의 검증 절차와 시간이 소요 되서는 안된다.

A type.

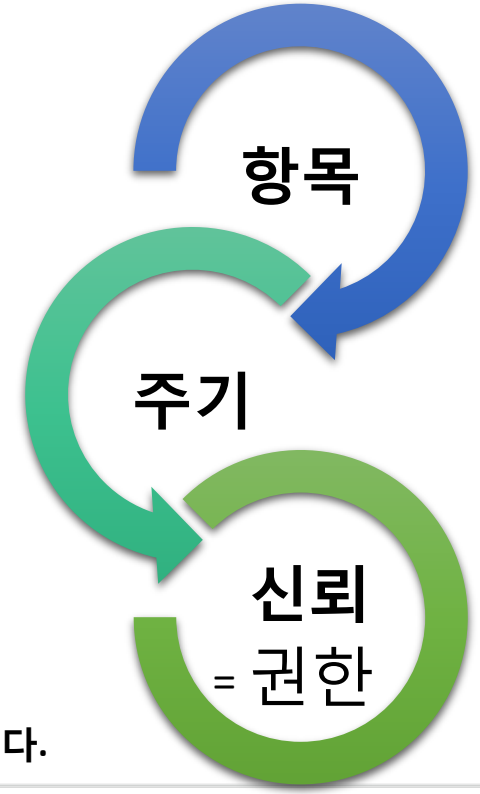
- 방문 기자
업무 목적 : 인터넷 업로드 및 메시지를 적기 위한 Tablet 이용 및 PC 이용

B type.

- 정 직원
인터넷 단말 : 외부 자료 송수신용 단말 : 망연계 솔루션 접근
인트라넷 단말 : 업무 자료 작성 및 내부 기간망 시스템 접근

C type.

- 개인정보 관리자 및 회계 업무 관리자
인트라넷 단말 : 업무 자료 작성 및 기간 시스템 접근



신뢰성이 확보된 단말은 사용 목적에 맞는 적절한 권한 할당 및 관리가 이루어져야 한다.

2. 신뢰에 대한 고찰

검증의 사례

조직내부에 많이 볼 수 있는 검증 사례 및 이슈

검증 사례 1.
단말 실 사용자에 대한 검증
[비-인가자 통제]

- 대다수의 고객사 내부 정직원은 최소 한번 이상의 인증을 거쳐 단말을 사용함.
- 대다수의 고객사는 인증 받은 이력에 대해 솔루션을 통해 기록하고 있으며, 감사로그에 대해 제출이 가능함.
- 본점을 제외한 지점 및 공용 PC에 대한 인증체계는 개인 단말보다 점검이 미흡함.

검증 사례 2.
필수 소프트웨어 설치 유무에 대한 검증
[필수 소프트웨어 통제]

- 대다수의 고객사 내부 정직원 대상으로 필수 소프트웨어의 현황에 대해 관리함
- 대다수의 고객사는 예외 처리시에 그에 대해 사유 및 요청자에 대한 기록을 표하고 있음
- 프로젝트 및 미러구성을 통해 식별하는 솔루션의 경우 누락되는 단말들이 존재함.

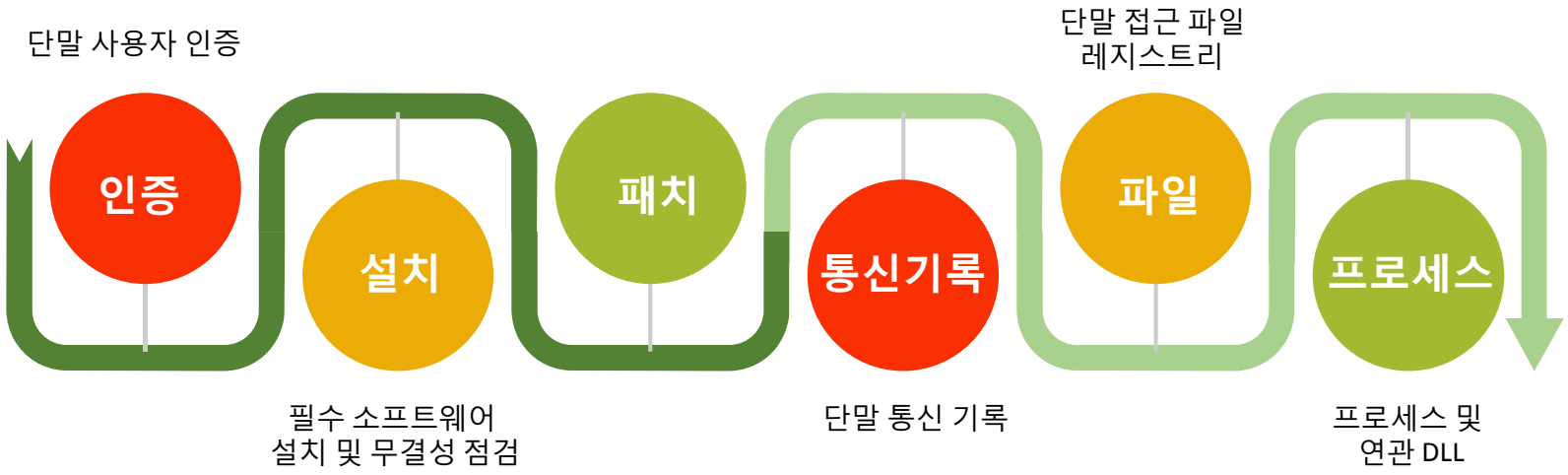
검증 사례 3.
이상 행위에 대한 검증
[단말 행위 분석]

- 일부 고객사 내부 인트라넷 단말 위주로 단말 내부 행위에 대한 정보 수집하고 있음
- 대다수의 고객사는 네트워크 기반으로 사용자 위협 행위를 분석하고 있음
- APT와 같은 보안 위협에 대하여, 네트워크 및 OS 로그를 기반으로 분석하고 있음.

2. 신뢰에 대한 고찰

단말에 대한 검증

주기적 검증 요소



실시간 검증

* 관련 소프트웨어

IT AM
Asset Management

NAC
Network Access Control

MS AD
Active Directory

* 관련 소프트웨어

DLP
Data Loss Prevention

EDR
EndPoint Detection & Response

EndPoint Forensics

3. 주기적 단말의 검증

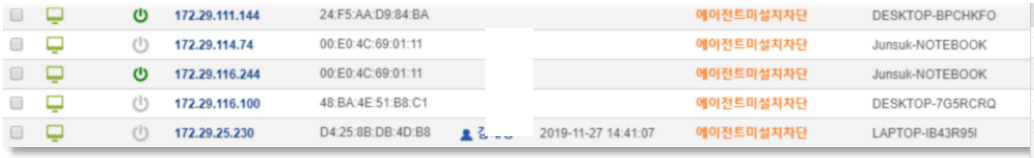
주기적 검증 항목의 결과물

IP의 실명제 (ID가시성 제공)

[감사로그]

- 단말의 IP/하드웨어 주소에 대한 ID 매핑

단말 주기적 보안 상태 현황 관리

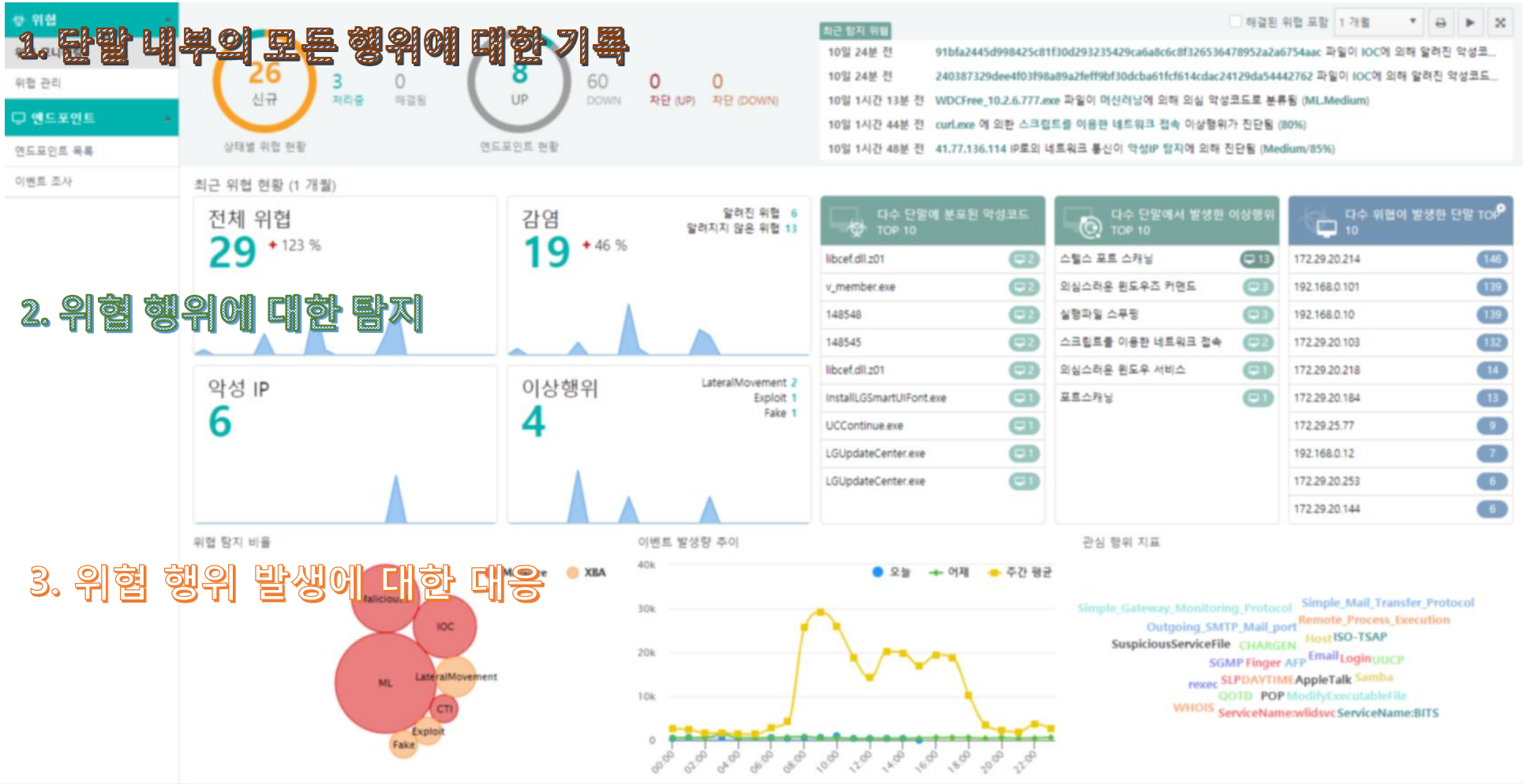


- 조직내부의 필수 소프트웨어 및 패치 상태값 식별 및 미 – 설치 단말에 대한 조치 (예제)

[감사로그]

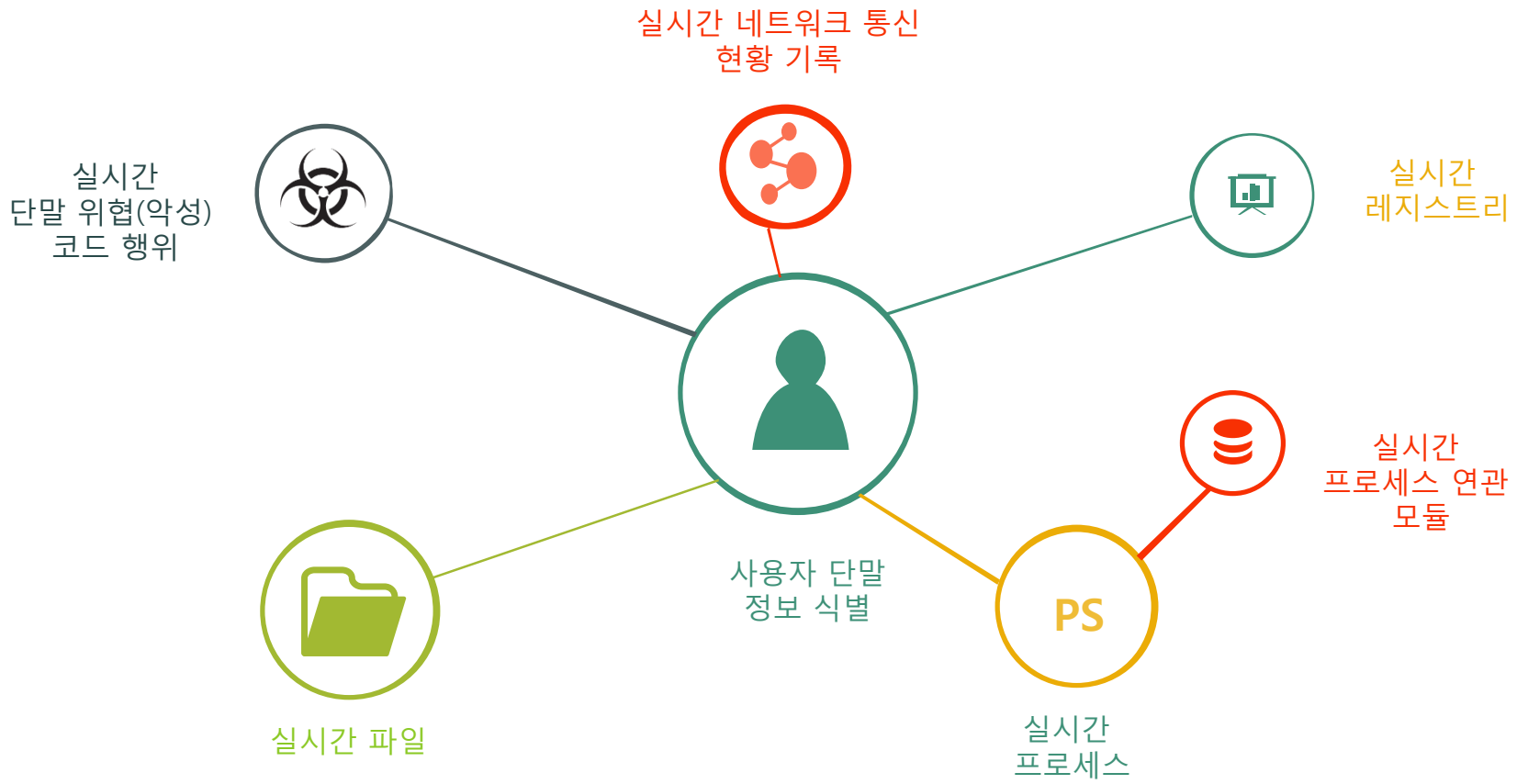
4. 실시간성 단말 검증

실시간성 검증 항목의 결과물



4. 실시간성 단말 검증

검증을 위한 기능



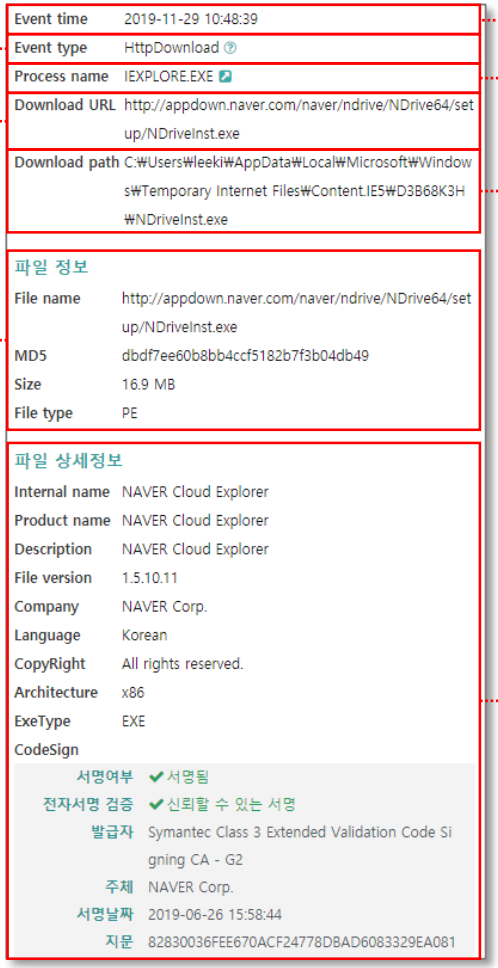
4. 실시간성 단말 검증

파일 : 상세정보, 유입/유출, 변경 정보

로그 타입

해당 파일의 원본 위치

- 파일 이름
- MD5 해시
- 크기
- 종류



로그 발생 시간(파일 생성 시간)

로그를 발생 시킨 프로세스

다운로드 받은 파일의 위치

파일 속성 정보

- 내부 이름
- 제품 이름
- 버전
- 제조사
- 언어
- 코드사인 정보
  - 서명 여부
  - 전자서명 검증
  - 발급자
  - 주체
  - 서명 날짜
  - 지문(해시)

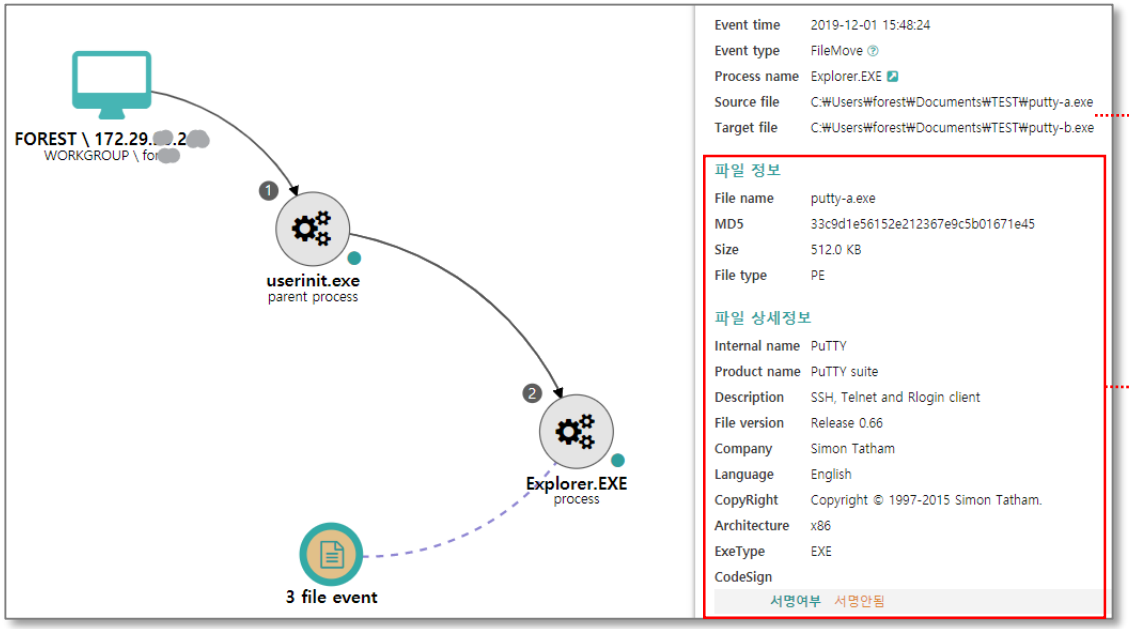
4. 실시간성 단말 검증

파일 : 상세정보, 유입/유출, 변경 정보

이벤트 시각	탐지	이벤트	프로세스명	통신	파일명
2019-12-01 15:48:27		FileMove	Explorer.EXE		putty-b.exe
2019-12-01 15:48:24		FileMove	Explorer.EXE		putty-a.exe
2019-12-01 15:48:20		FileMove	Explorer.EXE		putty.exe

파일명 변경

파일명 변경



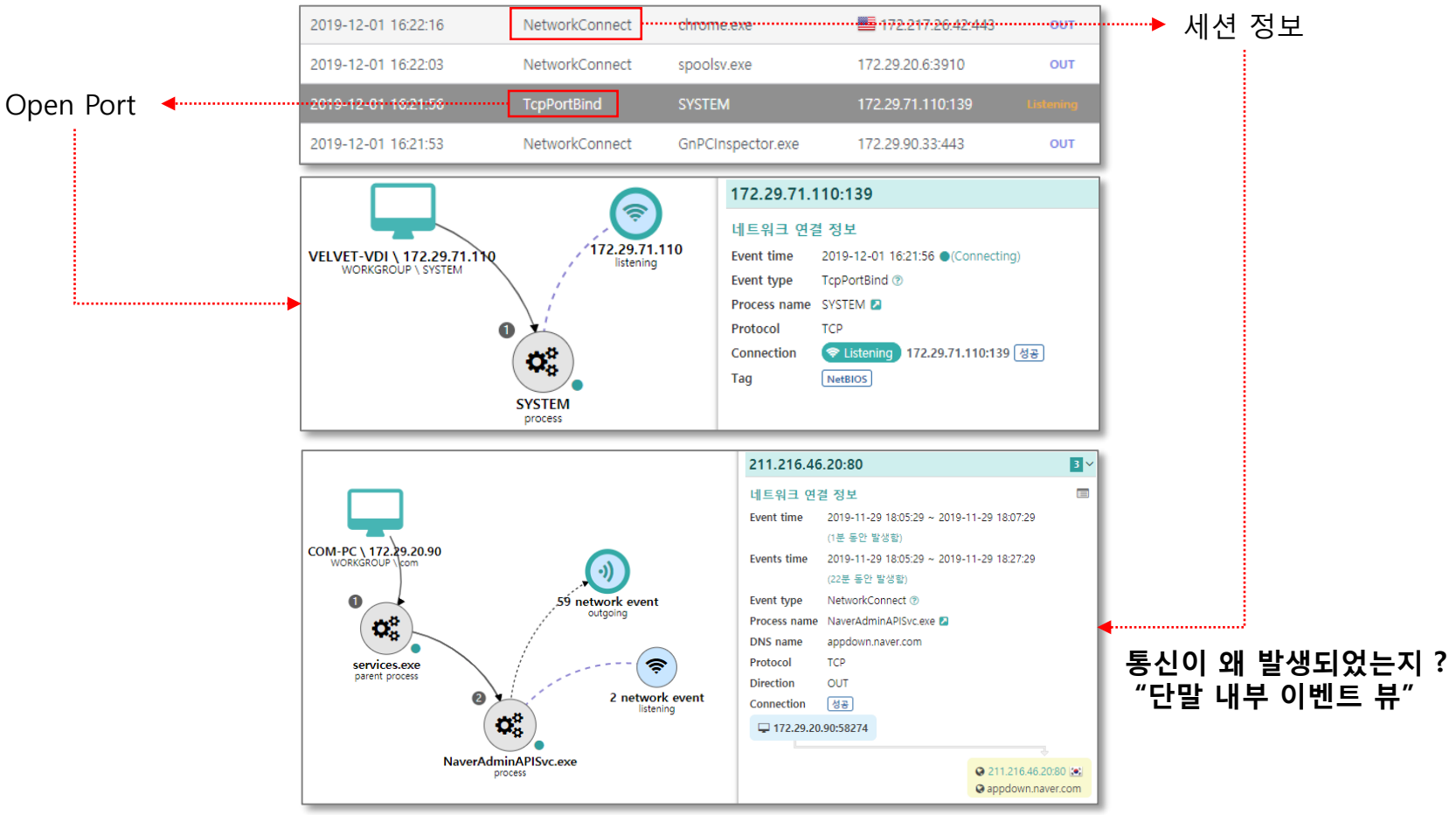
파일명 변경

파일 속성 정보
- 내부 이름
- 제품 이름
- 버전
- 제조사
- 언어
- 코드사인 정보

파일 변경 전후의 어떤 일이 발생되었는가?
"단말 내부 이벤트 뷰"

4. 실시간성 단말 검증

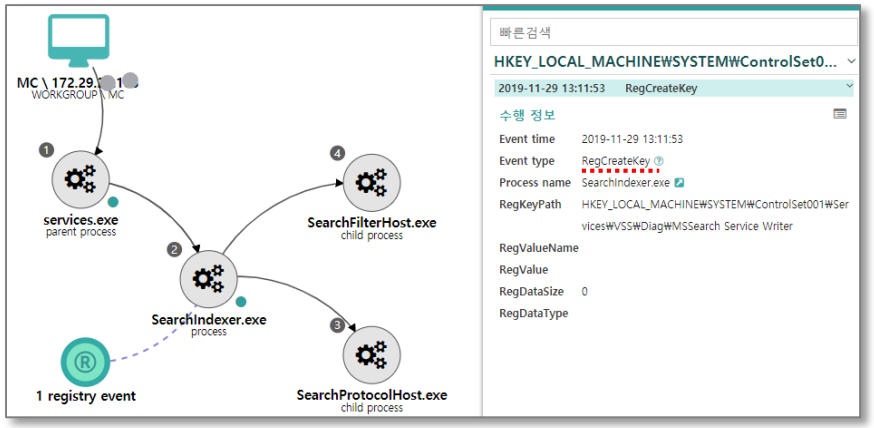
실시간 네트워크 접속 정보



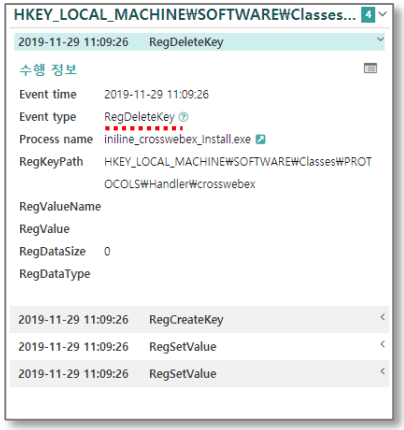
4. 실시간성 단말 검증

레지스트리

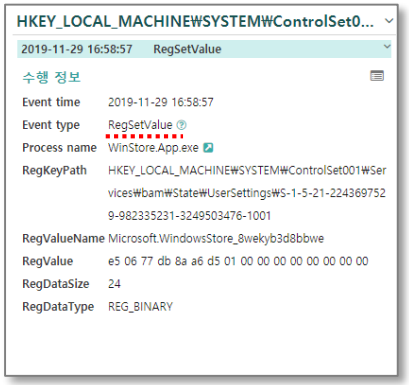
생성



삭제

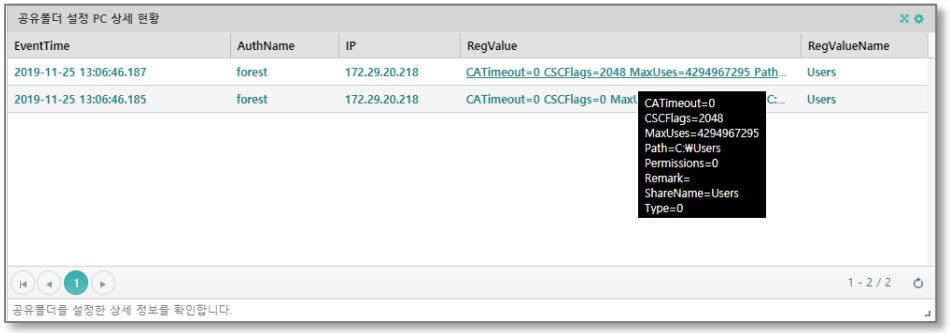


셋팅



*** 탐지되는 데이터 정보**

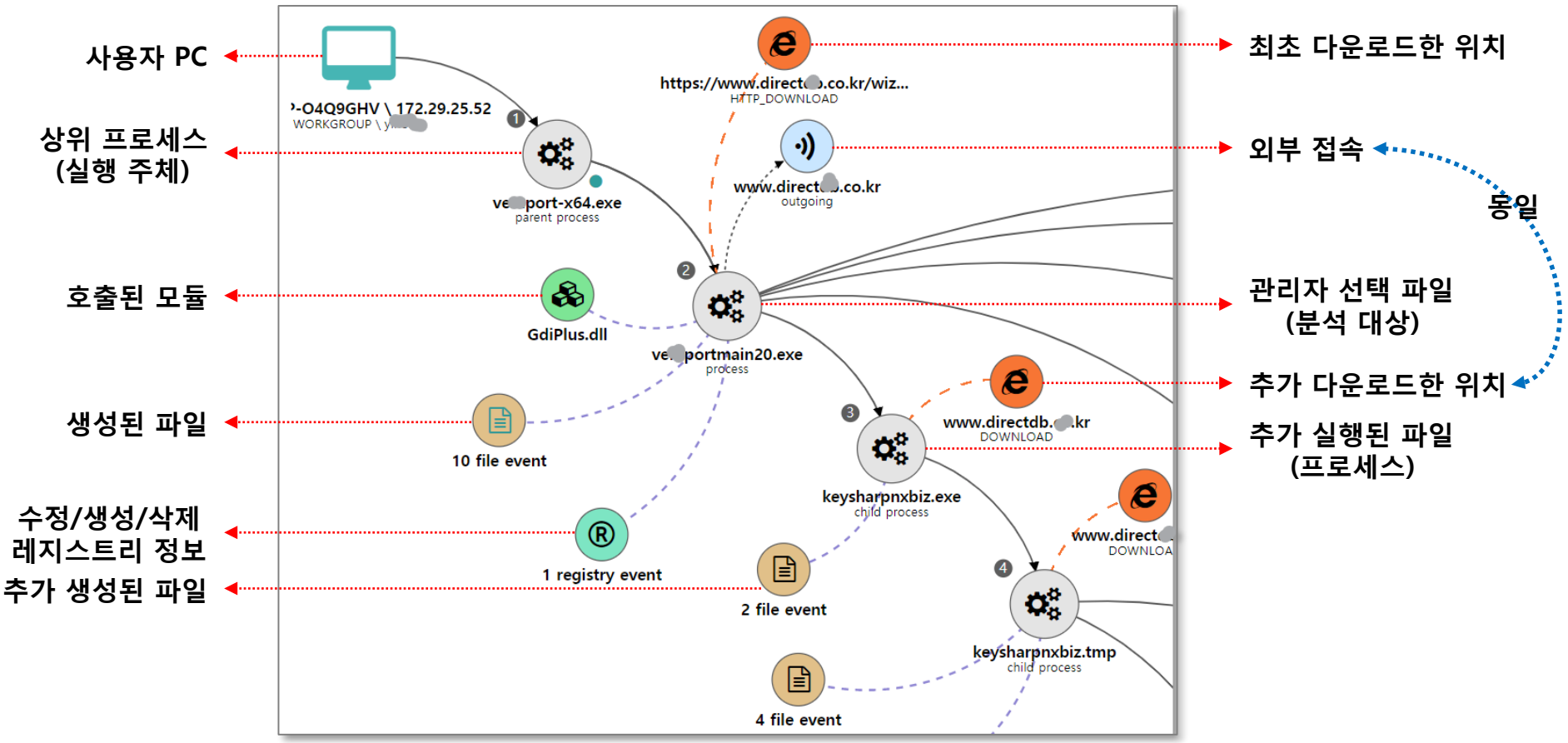
Event type : 레지스트리 생성/삭제/셋팅
Process name : 프로세스 명칭
RegKeyPath : 레지스트리 위치
RegValueName : 레지스트리 값 이름
RegValue : 설정 값
RegDataSize : 데이터 사이즈
RegDataType : 데이터 타입



관리자가 지정한 이벤트 발생시에 관리자 위젯으로 실시간 식별 지원

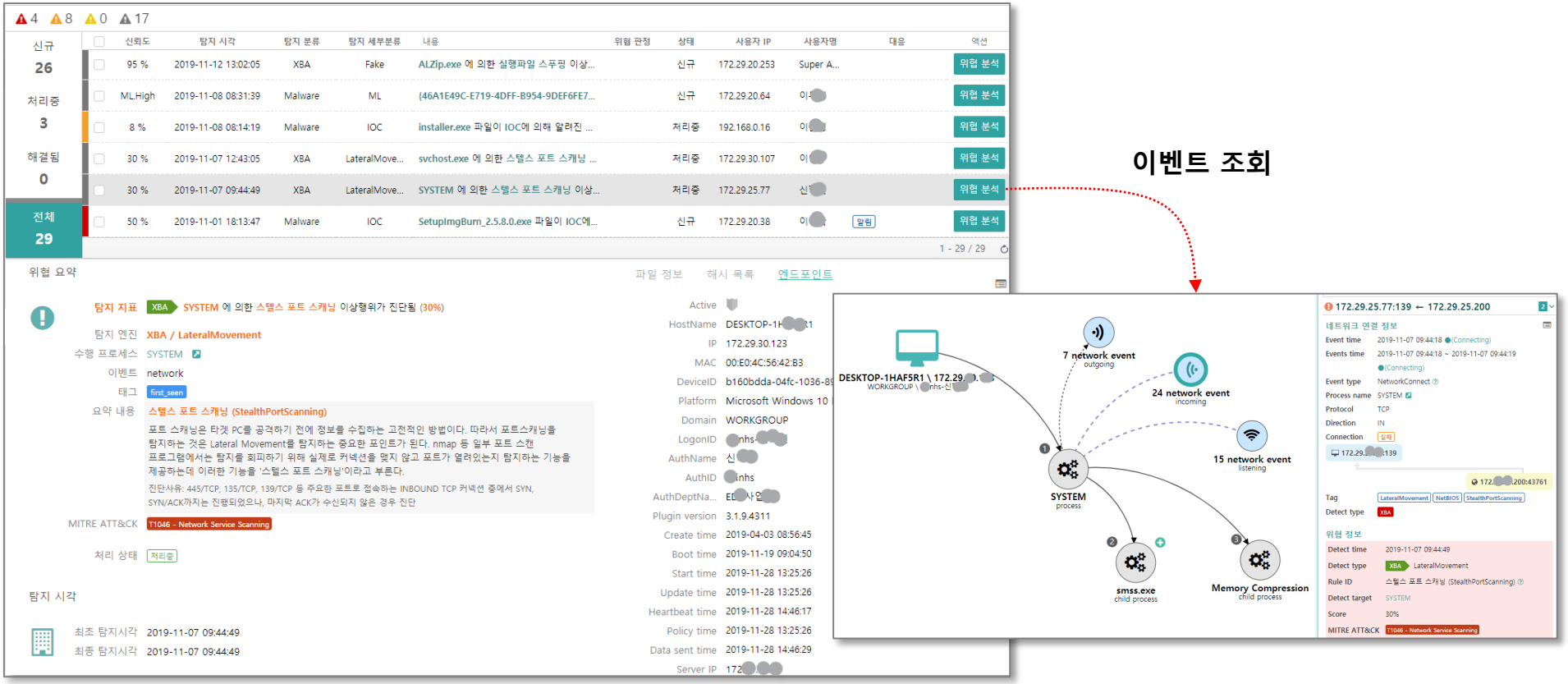
4. 실시간성 단말 검증

파일, 프로세스, 모듈, 네트워크 정보



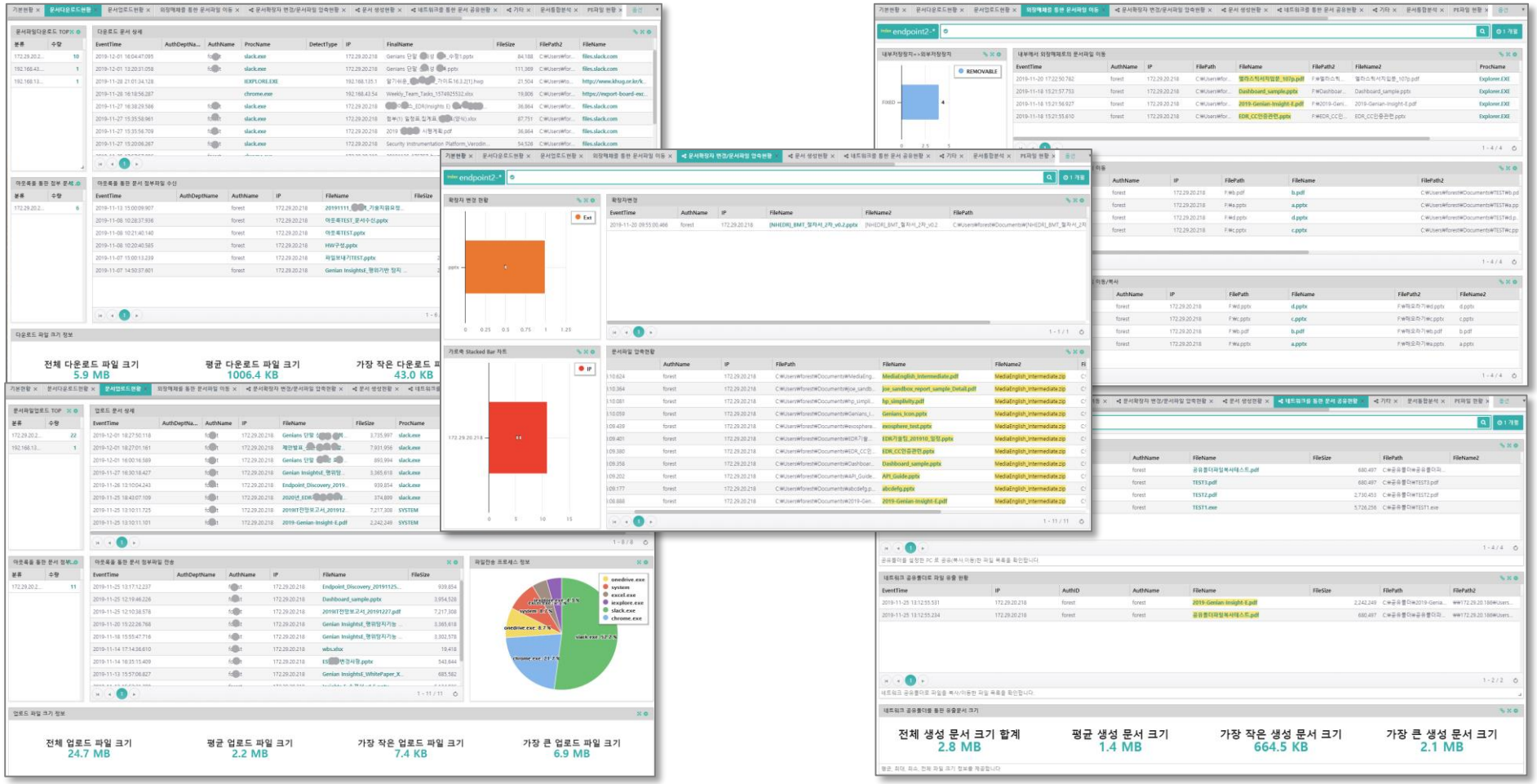
4. 실시간성 단말 검증

단말 위협 탐지



4. 실시간성 단말 검증

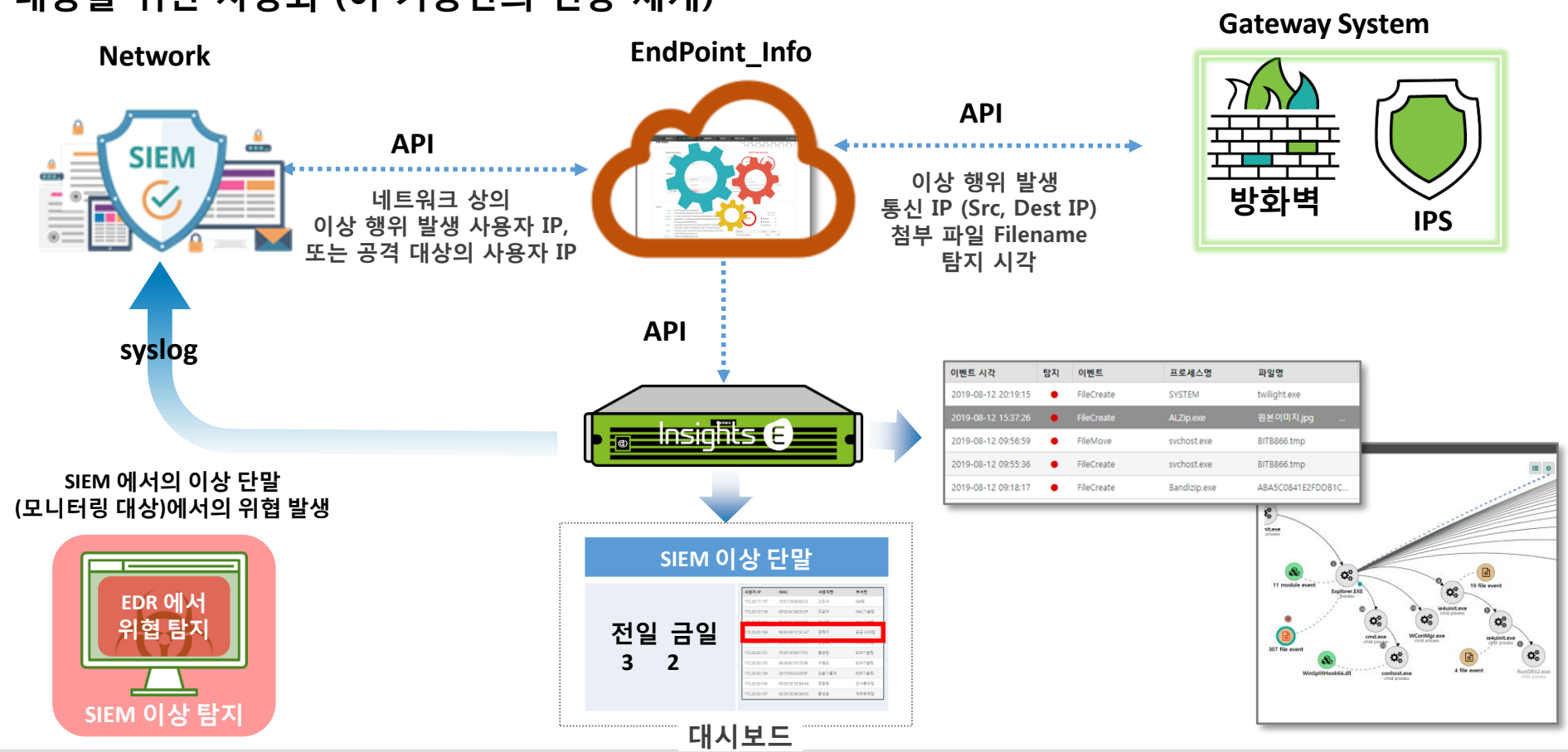
수집 자료 활용 : 자료(Data) 에서 정보(Information) 제공



4. 실시간성 단말 검증

관리를 위한 기능

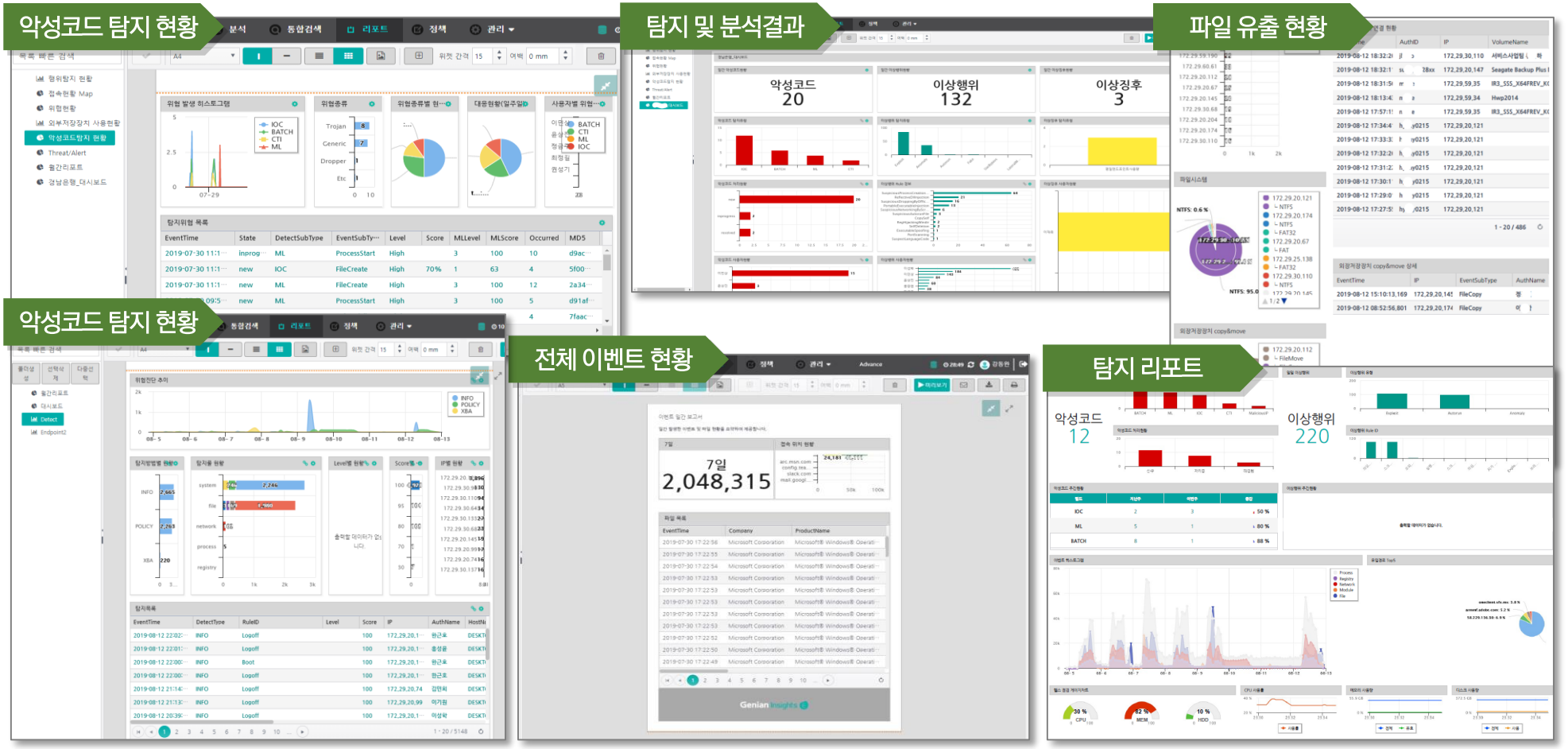
* 대응을 위한 자동화 (이 기종간의 연동 체계)



4. 실시간성 단말 검증

관리를 위한 기능

보고를 위한 리포트



5. 검증을 통한 단말의 신뢰성 회복

검증을 통한 내부 단말의 신뢰 회복 및 보안 아키텍쳐 확립

자산 손실 및 유출에 대한 리스크

자산을 이용하는 사람들은
누구이며, 어떻게 접근하는가 ?

접근 권한 세분화

권한부여를 위한
점검사항

단말 보안
점검 사항

설정된 보안 아키텍쳐
옳바름에 대한 관찰

필요에 따른 업데이트
수정체계

Thank you!

스타워즈 4편 1977년 개봉
스타워즈 1편 1999년 개봉