Intelligent EDR, Intelligent Visibility

Genian Insights E v2.0 제품소개서

2021.02 / 지니언스

Genians

목 차

- 배경 및 필요성
- Genian Insights E 제품 소개
- 도입 효과

배경 및 필요성

배경 및 필요성

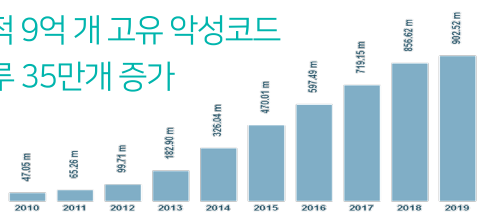
현재 도입/운영 중인 보안 솔루션으로는 더 이상 지능형 위협을 탐지 및 통제할 수 없습니다.

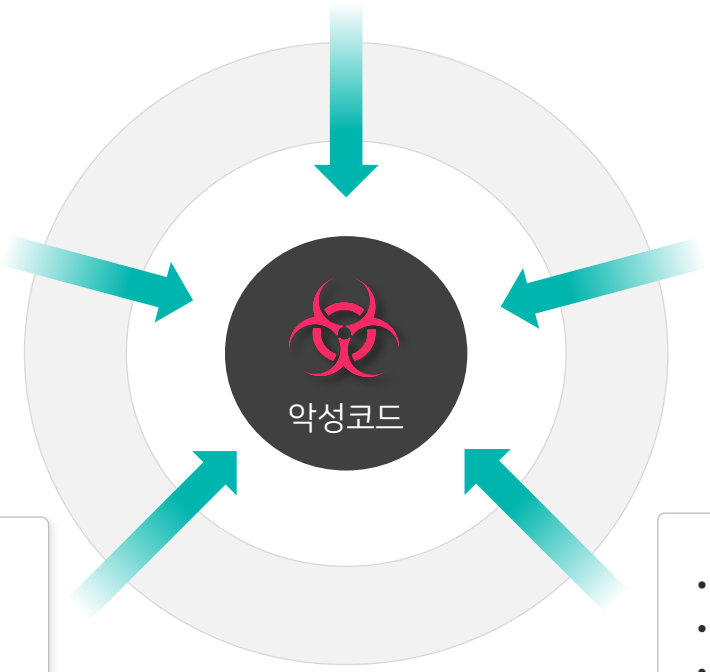
보안 담당자 관점의 현황 파악 어려움

- 악성파일 존재 여부 및 피해현황 파악의 한계
- 관리 감독 기관의 피해 상황 보고 요청 대응에 한계

10년간 고유 악성코드 수

누적 9억 개 고유 악성코드
하루 35만개 증가





APT 대응 솔루션(샌드박스)

- 암호화된 공격 탐지 불가
- 가상화 환경 내 파일 조합 불가
- 대용량 파일 분석 불가
- 다수의 샌드박스 회피 기법 존재

지능화·고도화 공격 패턴

- 파일 없는 악성행위
- 잠복/은닉형 악성행위
- 소프트웨어 취약점 공격
- 웹 취약점 공격

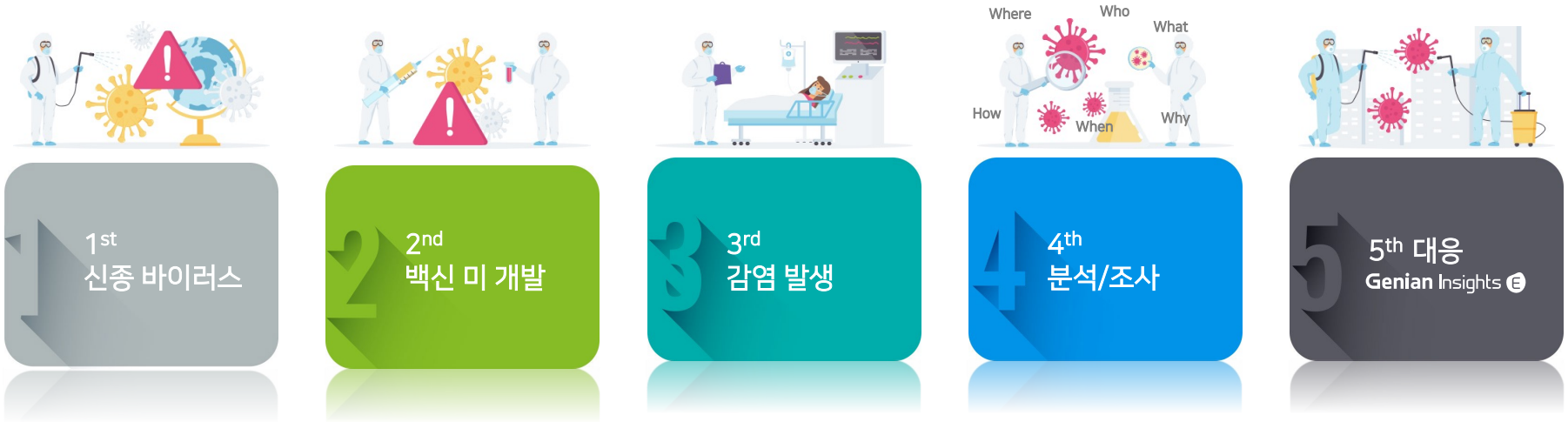
Anti-Virus의 한계

- 시그니처 기반 블랙리스트 방식
- 신종 악성 코드 및 지능형 지속공격 탐지불가
- 다수의 안티바이러스 회피 기법 존재

배경 및 필요성

점점 다변화, 고도화되고 있는 사이버 공격을 모두 막는 것은 불가능합니다.

의심스러운 활동에 대한 빠른 인지와 행적을 분석하여 감염의 대응책을 마련하고
확산을 막아 피해를 최소화하고 동일 형태의 피해가 발생하지 않도록 할 수 있는 솔루션이 필요합니다.



최종 공격 대상은 결국 엔드포인트 입니다.

네트워크 경계에 있는 대부분의 보안 솔루션은 내부 자산을 보호하기 위해 구성되어 있으나 엔드포인트의 위협은 계속 증가하고 있습니다.
사용자에게 보내지는 악성 메일, 피싱 사이트, 위/변조 된 홈페이지 접속 등을 통한 악성코드 감염 및 APT 침해는 네트워크 보안 솔루션의 한계를 보여주고 있습니다.

Genian Insights E
제품 소개

1.개요

Genian Insights E는
단말에 대한 지속적인 모닝터링 및 정보 수집을 통해 위협의 탐지 및 분석, 대응을 제공하는
단말 이상행위 탐지 및 대응 (Endpoint Detection & Response) 솔루션입니다.

2. Genian Insights E 구성

Genian Insights E는 Insights E 분석 서버, PC에 설치되는 Agent로 구성됩니다.

Insights E Server

- E Module에서 전달된 Event Raw Data의 저장 및 백업
- Data 분석을 통한 위협 및 이상 징후의 탐지
- 탐지된 위협의 상세 내용 분석
- Event 통합 분석 및 시계열 분석, 근원 분석 등
- 분석 내용의 보고서, 위젯, 대시보드 등 시각화 및 표출
- 타 시스템 연동을 위한 Syslog, REST API 제공
- 보안이 강화된 자체 OS 사용

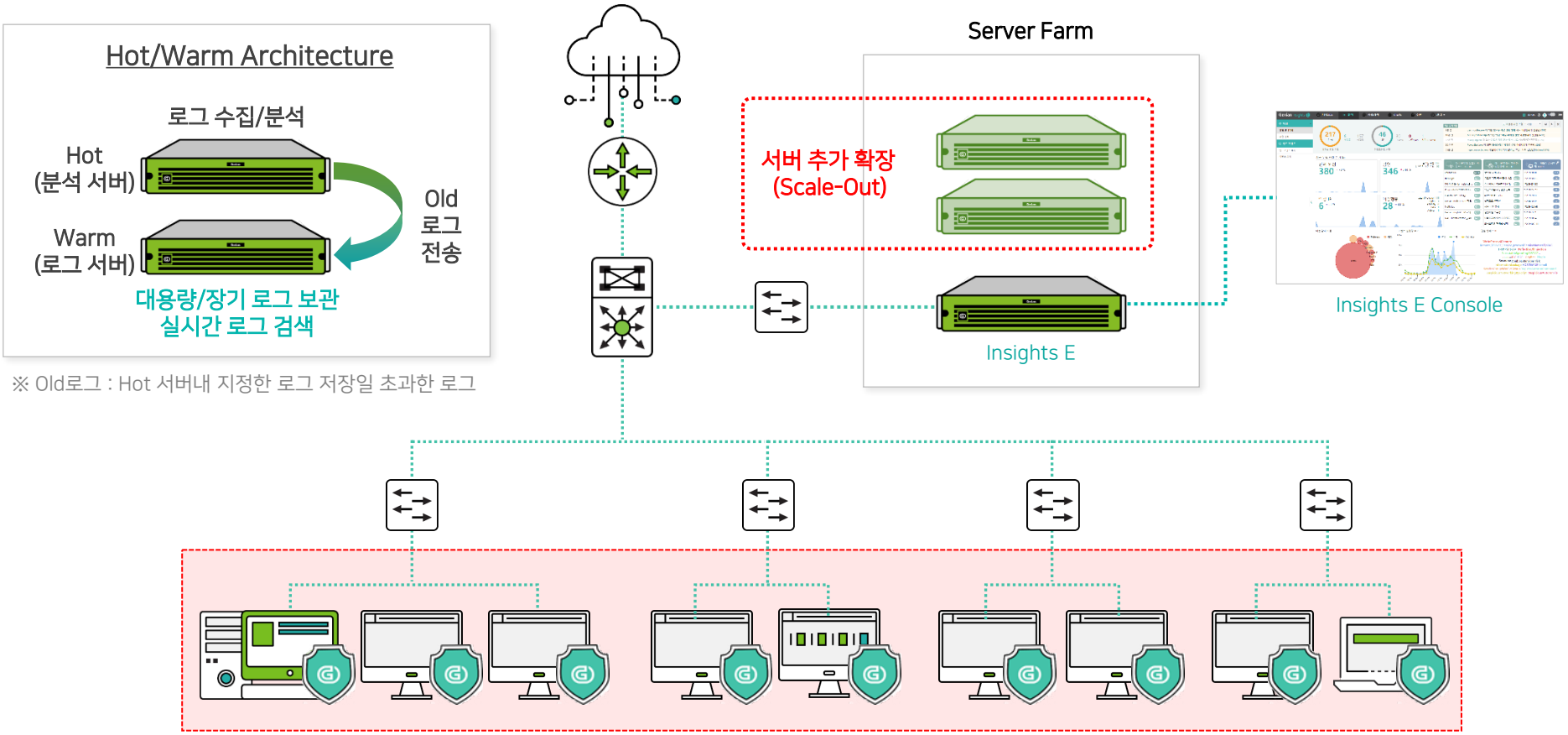
Insights E Agent

- 단말 주요 행위(파일, 프로세스, 네트워크, 레지스트리 등)의 모니터링 및 수집
- 수집된 정보 Server로 전송
- Off-line 에서 수집된 로그 임시 보관 (on-line 에서 서버로 전송)
- 위협 탐지 시 고지, 차단, 종료 등 단말 수준의 대응
- 위협 대상(파일 등)의 격리 및 삭제
- 가벼운 Agent

❖ Genian NAC 사용 시 NAC Agent 에 모듈(plug-in)을 추가함으로서 EDR Agent 설치 완료

2. Genian Insights E 구성

Genian Insights E 서버, Agent의 간단한 구성입니다.
Scale-Out 기능을 제공하여 확장을 쉽게 할 수 있습니다.



※ Old로그 : Hot 서버내 지정한 로그 저장일 초과한 로그

※ Genian NAC 사용 시, NAC Agent 에 플러그인(모듈)을 배포하는 형태로 구출 가능

3. 단말의 부하를 최소화한 수집 및 탐지

Agent는 서버로 로그 전송 역할만 수행, 분석 및 탐지는 서버에서 수행합니다.

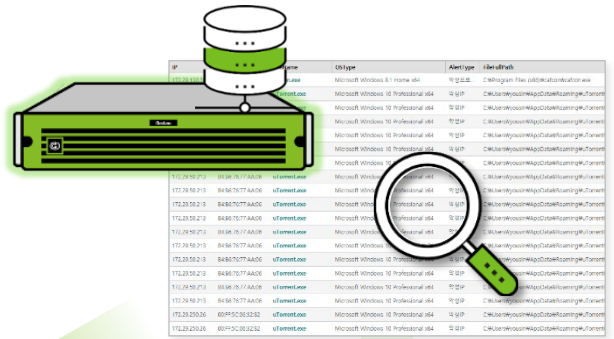
- File -
Name
Route
File Features
Size
Hash
Code Sign
Print

- Process -
Name
Route
Size
Hash

- Module -
Name
Additional info.

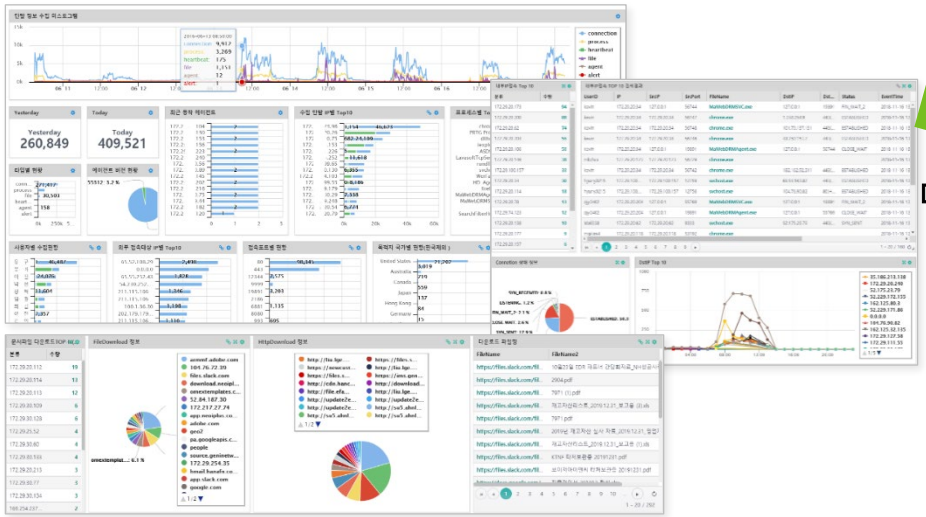
- Network -
IP
Status
Port
Connected Process

- Registry -
Name / Path
Modification
Additional info.



Malicious File / Threat Behavior

다양한 분석

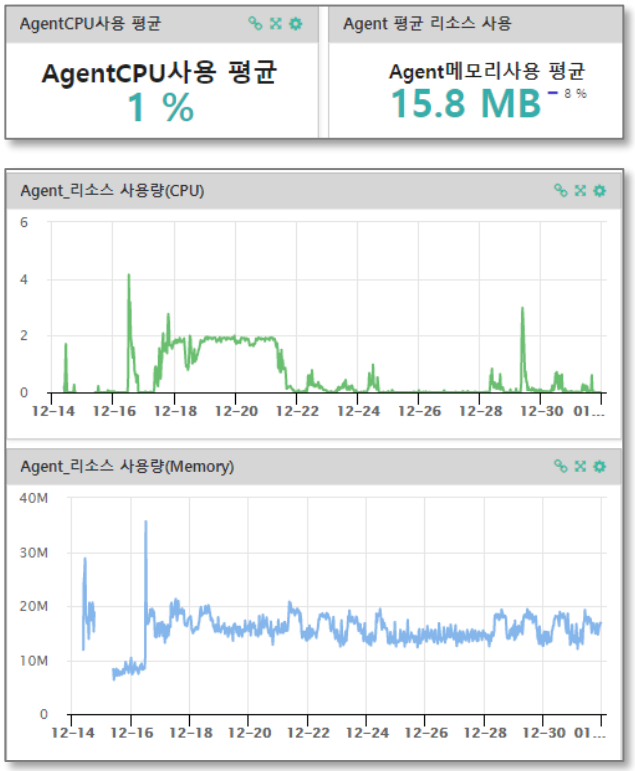


3. 단말의 부하를 최소화한 수집 및 탐지

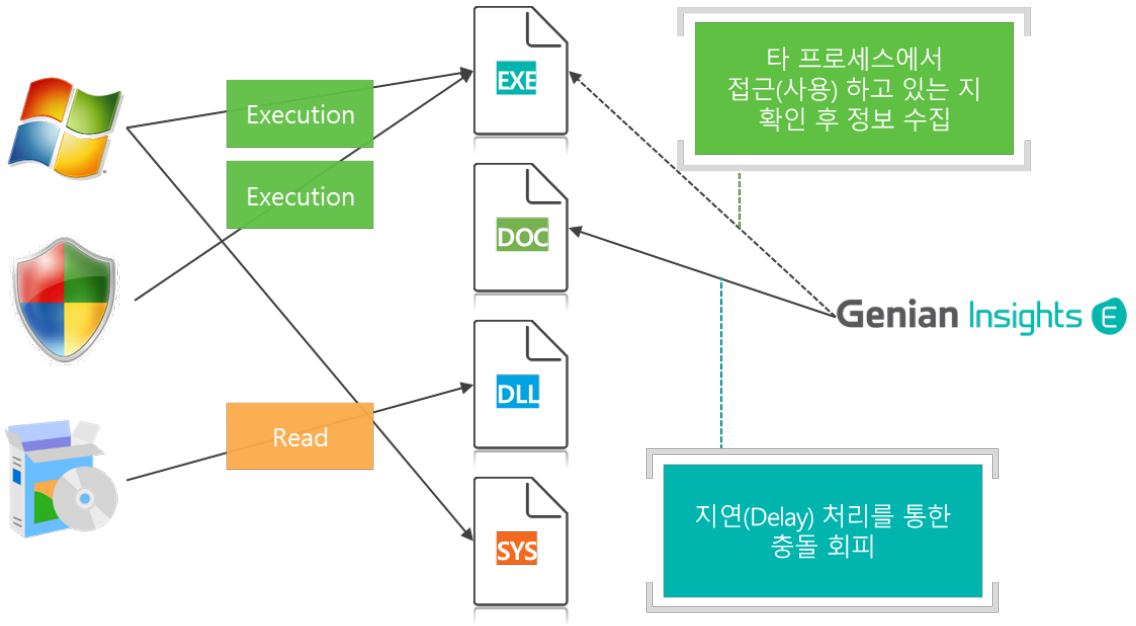
Agent는 충돌을 방지하기 위한 충돌 회피 기술이 적용되어 있으며, 최소의 리소스를 사용합니다.

확인 처리 기술(타 프로세스의 접근 확인 후 처리), 지연 처리 기술(지연처리하는 기술) 적용으로 타 프로그램의 동작에 영향을 주지 않는 기술 적용

CPU, MEMORY 사용을 최소화하여 동작하는 Agent

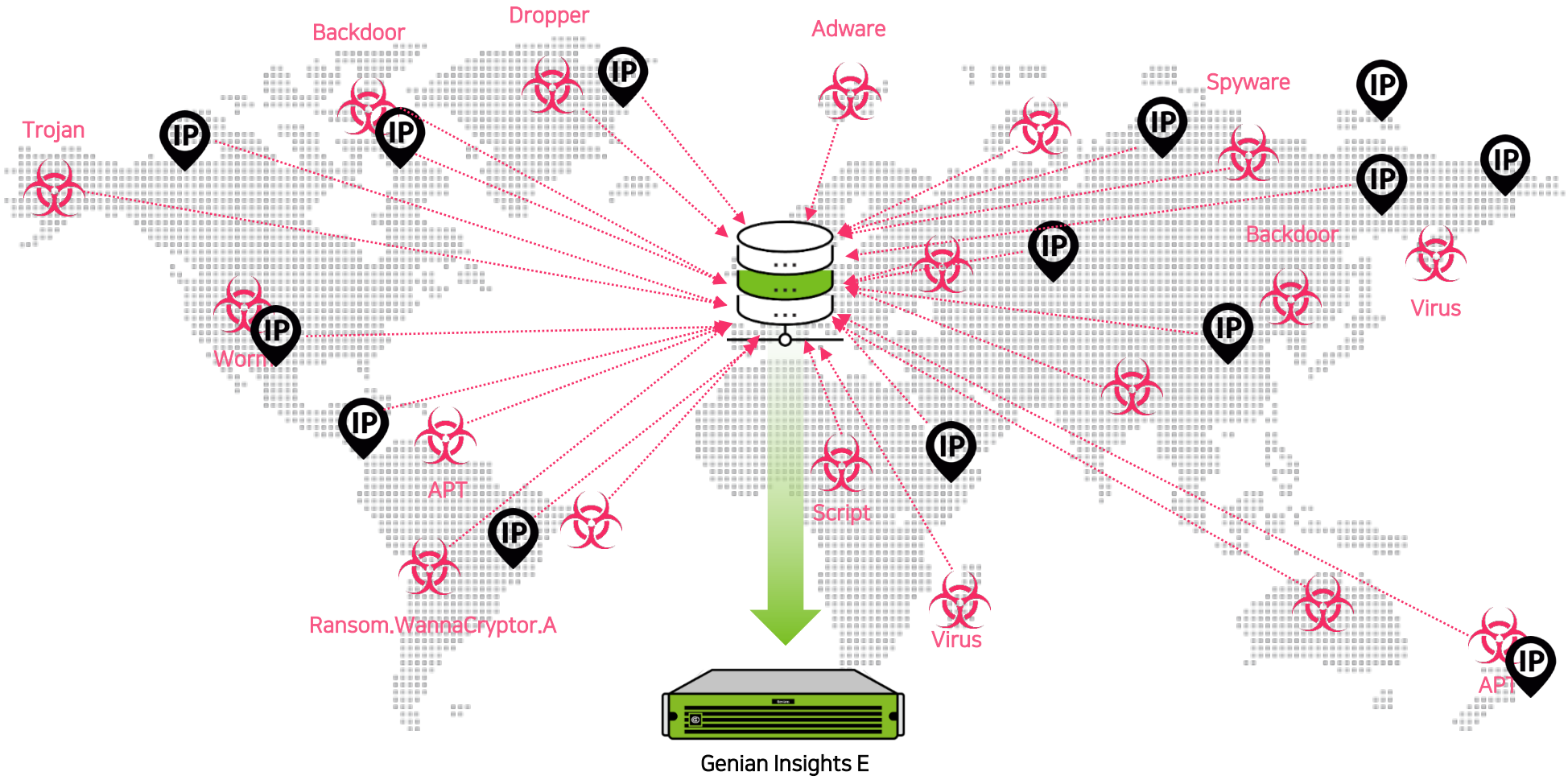


※ 제조사 내부 TEST 결과, 에이전트 100대 평균 리소스 사용률



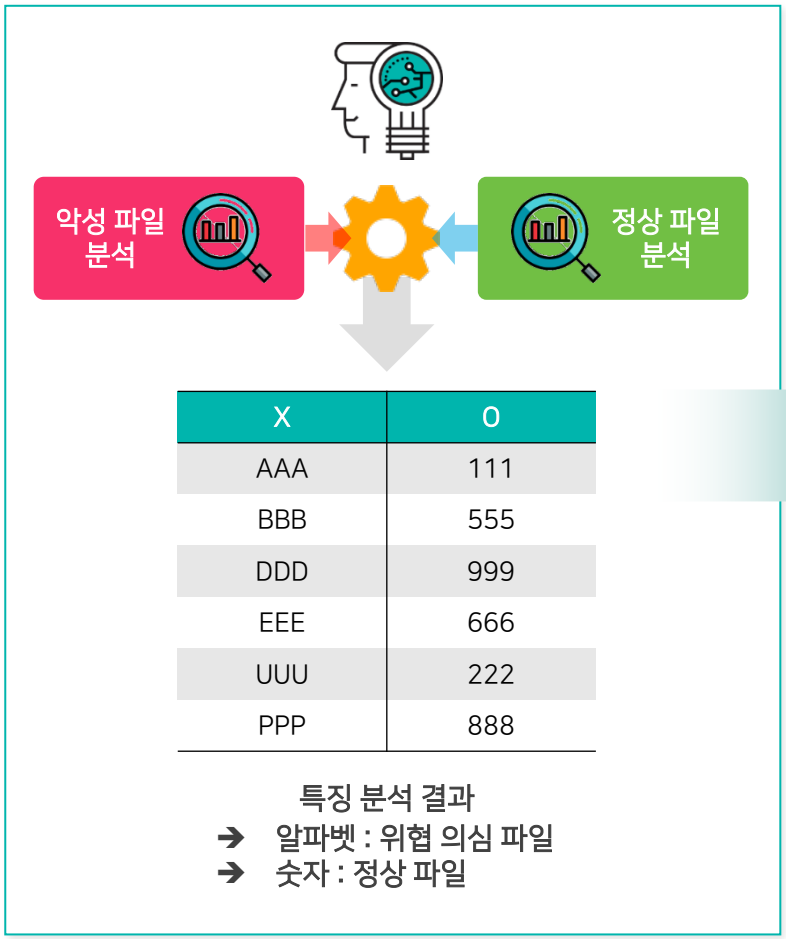
4. 탐지 기술

IOC(Indicator Of Compromise, 침해 지표) : 전 세계에서 탐지된 악성 파일/IP 정보를 DB화하여 알려진 위협을 탐지합니다.



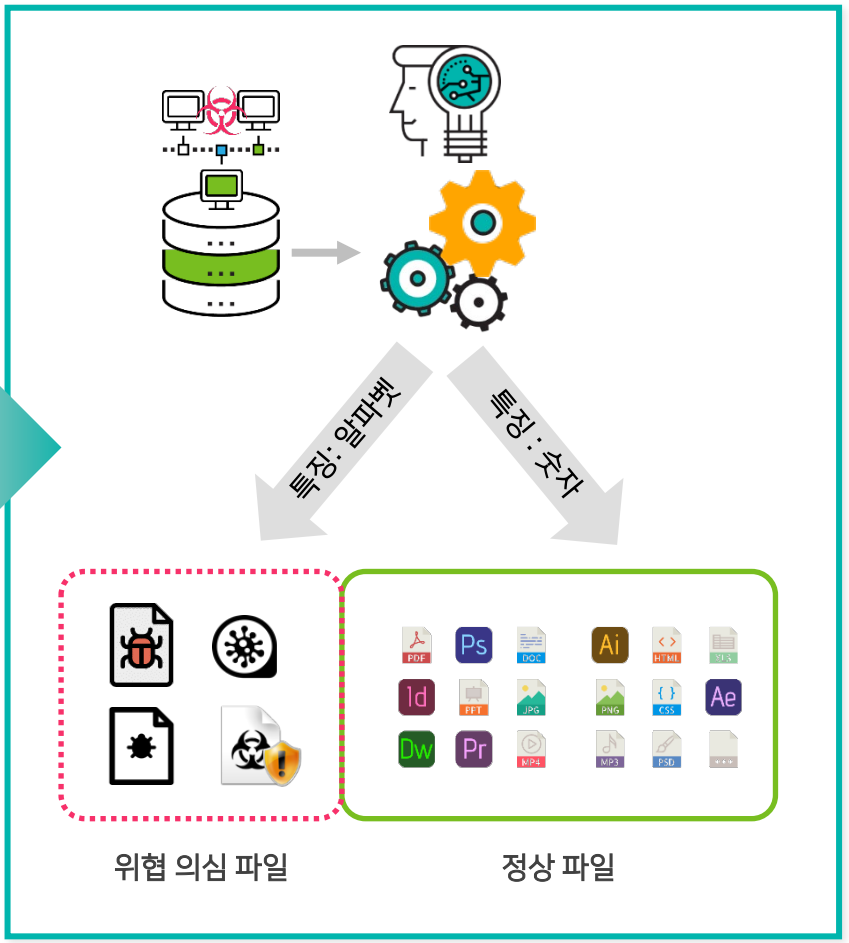
4. 탐지 기술

ML (Machine Learning) : 악성파일/정상 파일의 특징을 학습/분석하여 위협이 의심되는 파일을 탐지합니다.



X	O
AAA	111
BBB	555
DDD	999
EEE	666
UUU	222
PPP	888

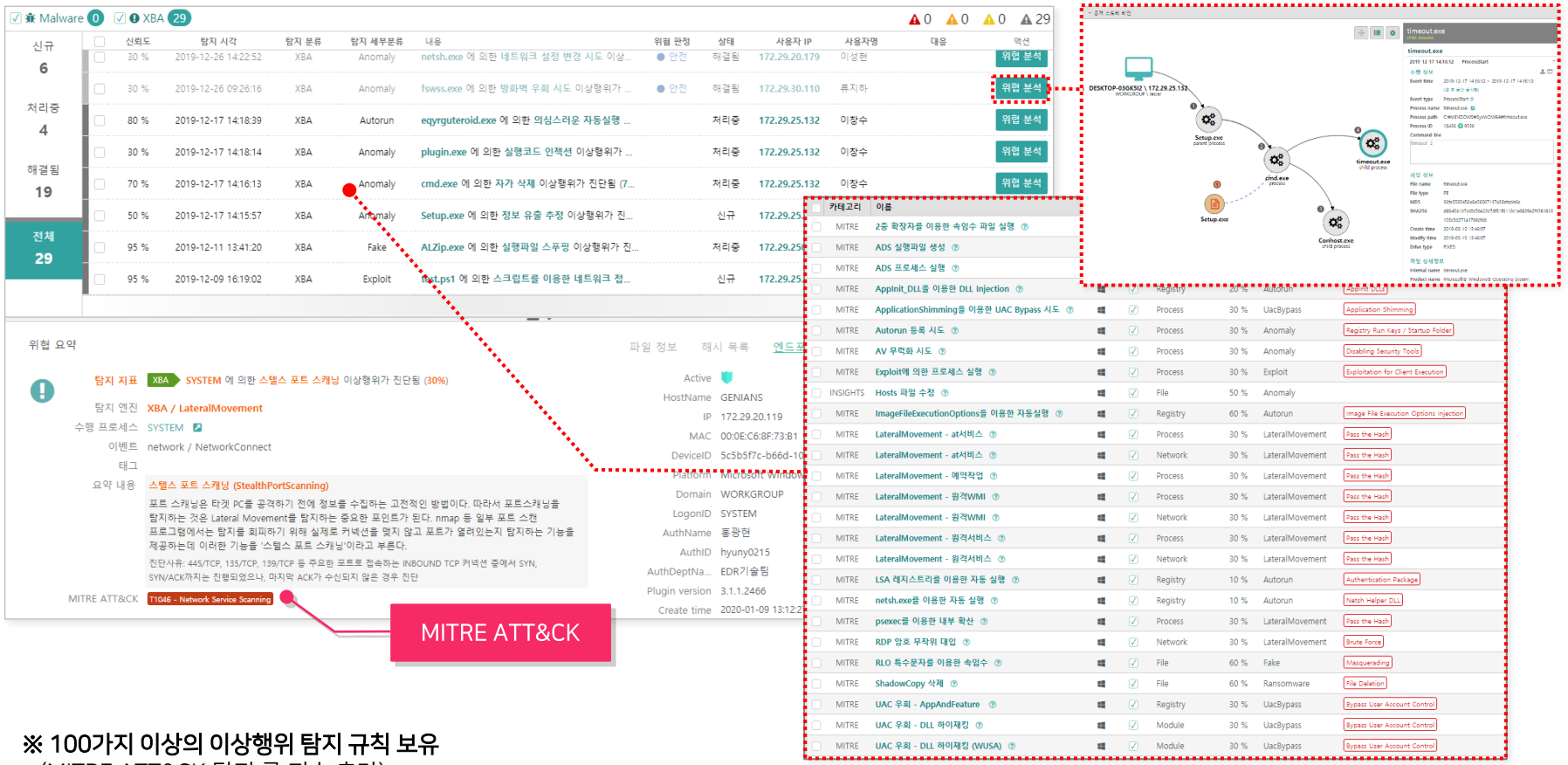
특징 분석 결과
➔ 알파벳 : 위협 의심 파일
➔ 숫자 : 정상 파일



※ 분기 1회 최신의 머신러닝 모델(파일) 제공

4. 탐지 기술

XBA(X Behavior Analysis) : Fileless 공격 등 비 정상적인 행위를 탐지하는 기술이 적용되어 있습니다.



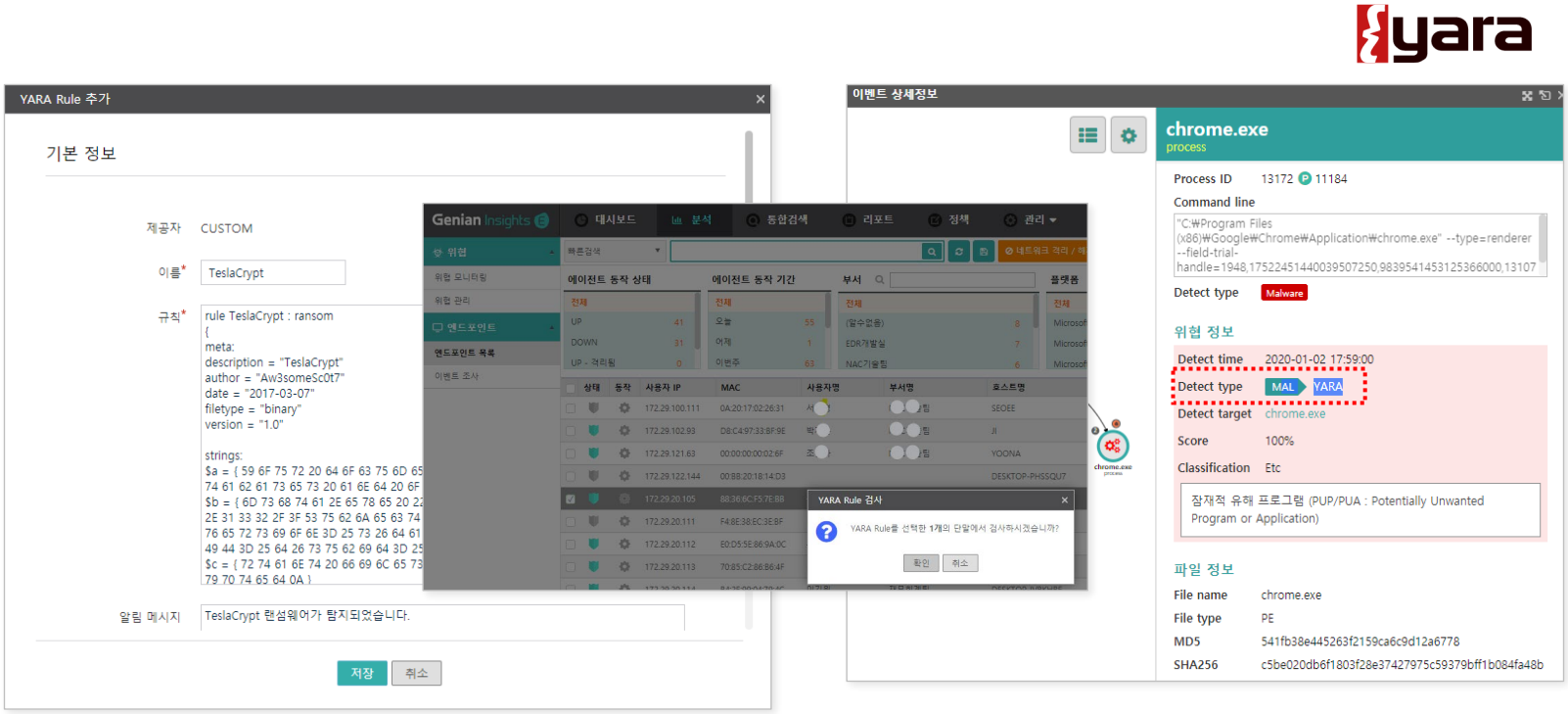
※ 100가지 이상의 이상행위 탐지 규칙 보유
(MITRE ATT&CK 탐지 룰 지속 추가)

4. 탐지 기술

YARA : 관리자가 직접 생성한 패턴 매칭 탐지 기술이 적용되어 있습니다.

YARA – 문자열이나 바이너리 패턴(Hex string)을 기반으로 미리 정의된 시그니처로 악성코드를 분류할 수 있게 하는 도구
: 백신 등 endpoint 에서도 활용하고 있는 탐지 기법

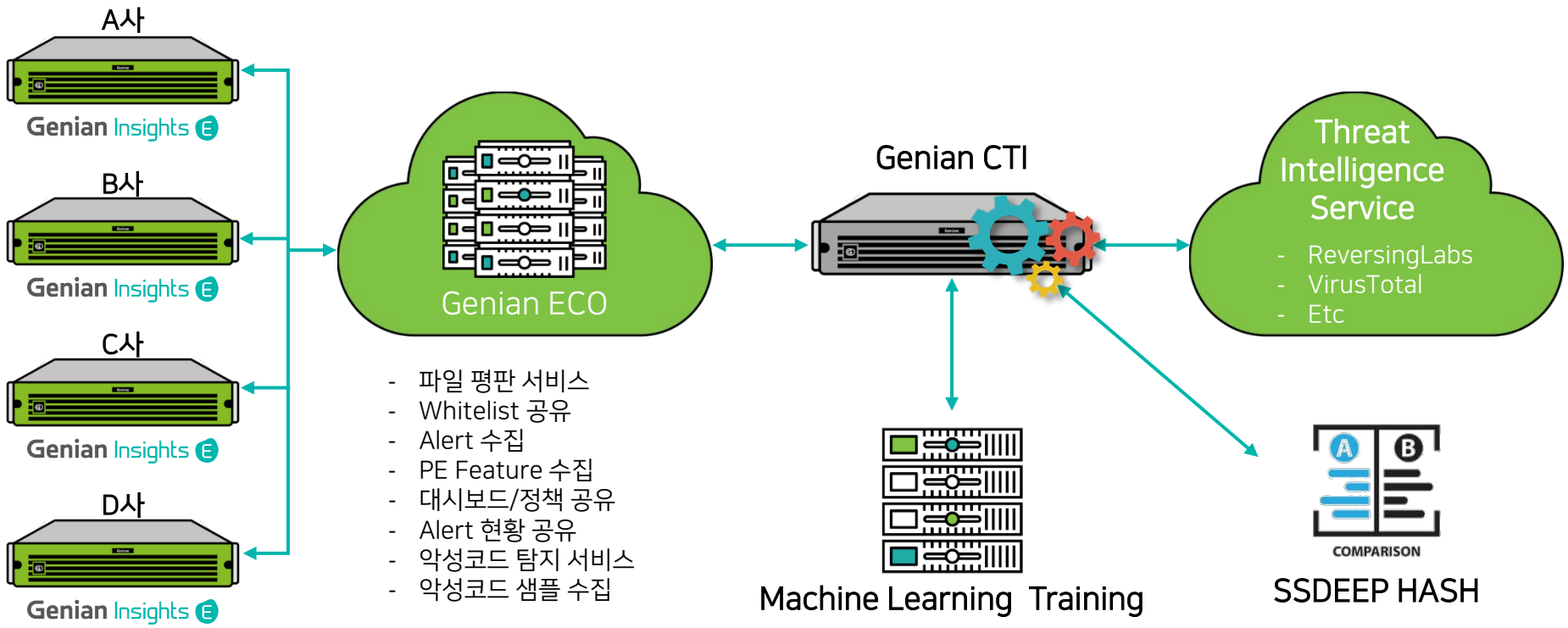
모든 파일, 프로세스에 대해 행위 기반 탐지를 적용하기 위해서는 자원 소모가 많고 무겁게 동작
➔ 먼저 YARA와 같은 정적 시그니처 또는 평판을 가지고 판단
➔ 탐지 시 별도의 자원 소모 없이 즉각 차단하거나 삭제 ➔ 효율적



4. 탐지 기술

Ecosystem : Genian 자체의 평판시스템을 제공합니다.

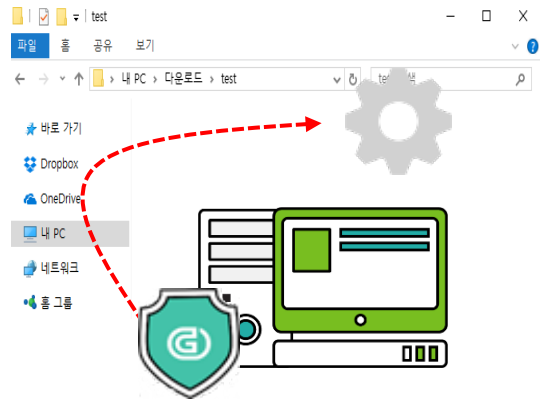
- 오탐 및 최신 악성코드 분석 결과를 고객에게 공유하기 위한 Genian Insights E ECO-SYSTEM 구성
- 파일의 근거 (해당 파일이 어떤 역할을 하는 파일인가? 정말 악성인가?) / 오탐 자동 예외 처리
- 지니언스 고객을 통해 수집된 위협과 예외 처리된 데이터를 수집, 가공하여 Genian Insights E를 사용하는 모든 고객에게 재배포합니다.
- 이를 통해 Genian Insights E를 사용하는 고객들의 오탐을 줄여주며, 위협 혹은 파일 세부 정보 식별이 필요할 때 그 정보를 알려줍니다.



5. 대응

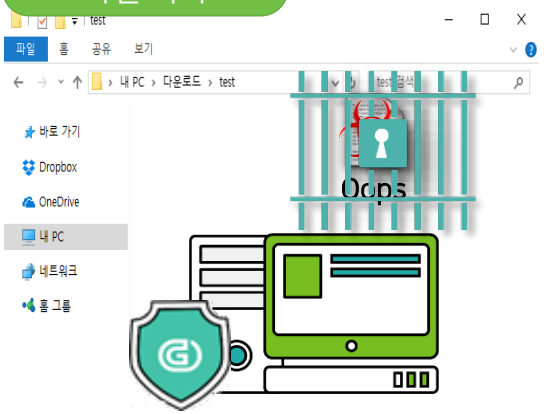
악성 파일에 대한 프로세스 중지, 격리, 사용자/관리자 알람, 네트워크 격리 등의 대응 기능을 제공합니다.

프로세스 종료

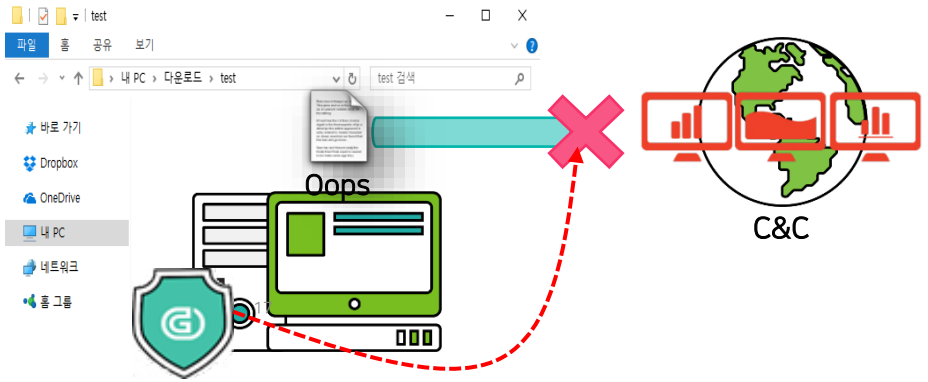


사용자/관리자 알람 경고

파일 격리



네트워크 격리



6. 분석

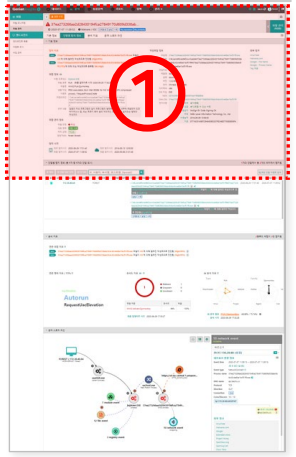
전체 위협에 대한 요약 정보를 보여주는 위협 모니터링화면을 제공합니다.

6. 분석

탐지된 파일의 위협 정보를 확인할 수 있으며,
이상 행위(Fileless) 탐지 시 연관된 MITRE ATT&CK 링크를 제공합니다.

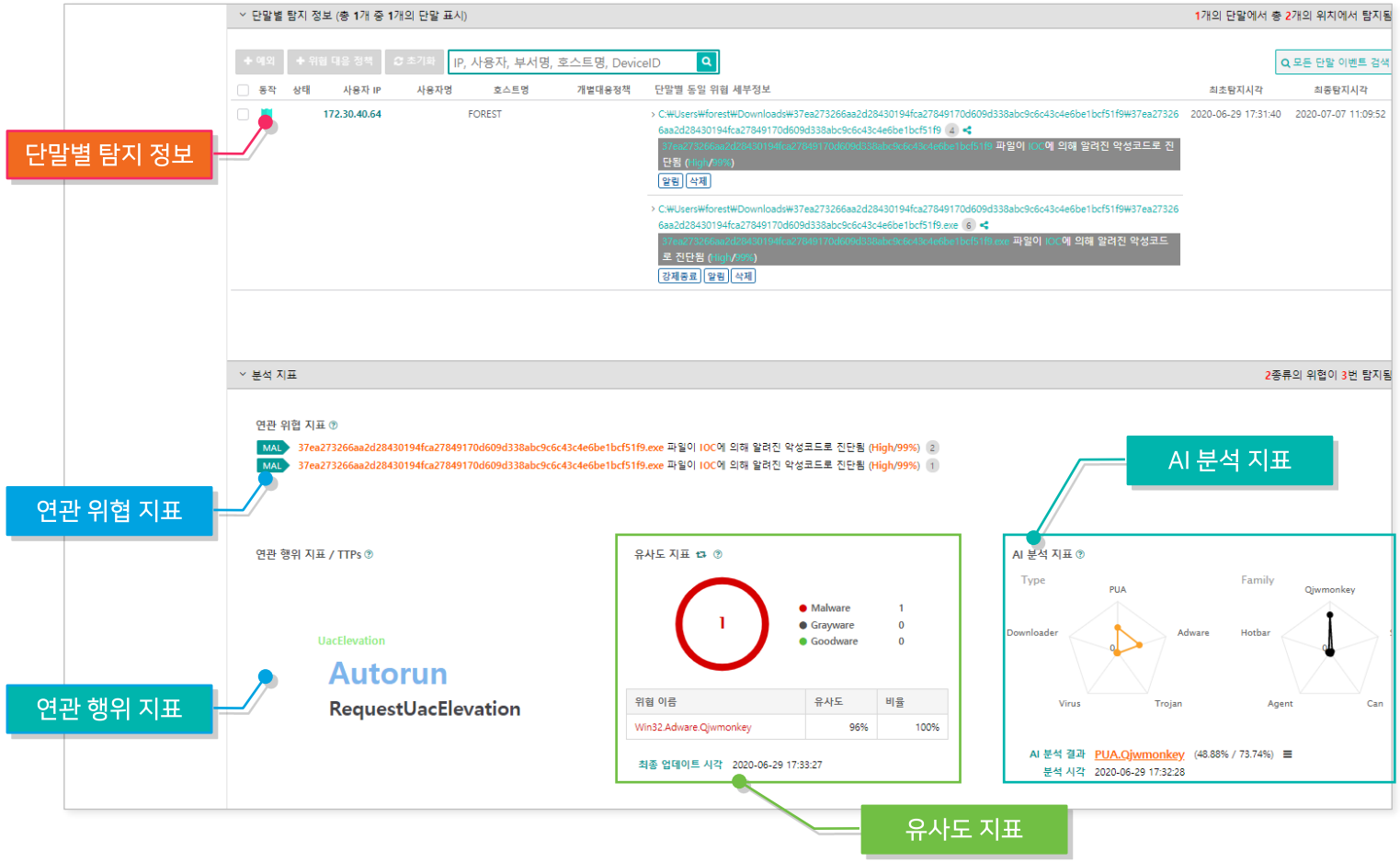
❖ MITRE ATT&CK : 공격의 기법들을 프로파일링하여, 카테고리별 목록화

위협 분석 전체 화면

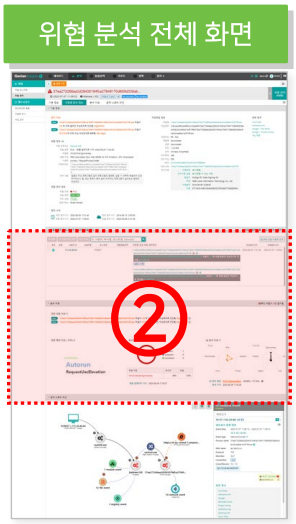


6. 분석

단말 별 탐지정보, 연관지표, 행위, 유사도 등 분석에 도움이 되는 다양한 정보를 제공합니다.

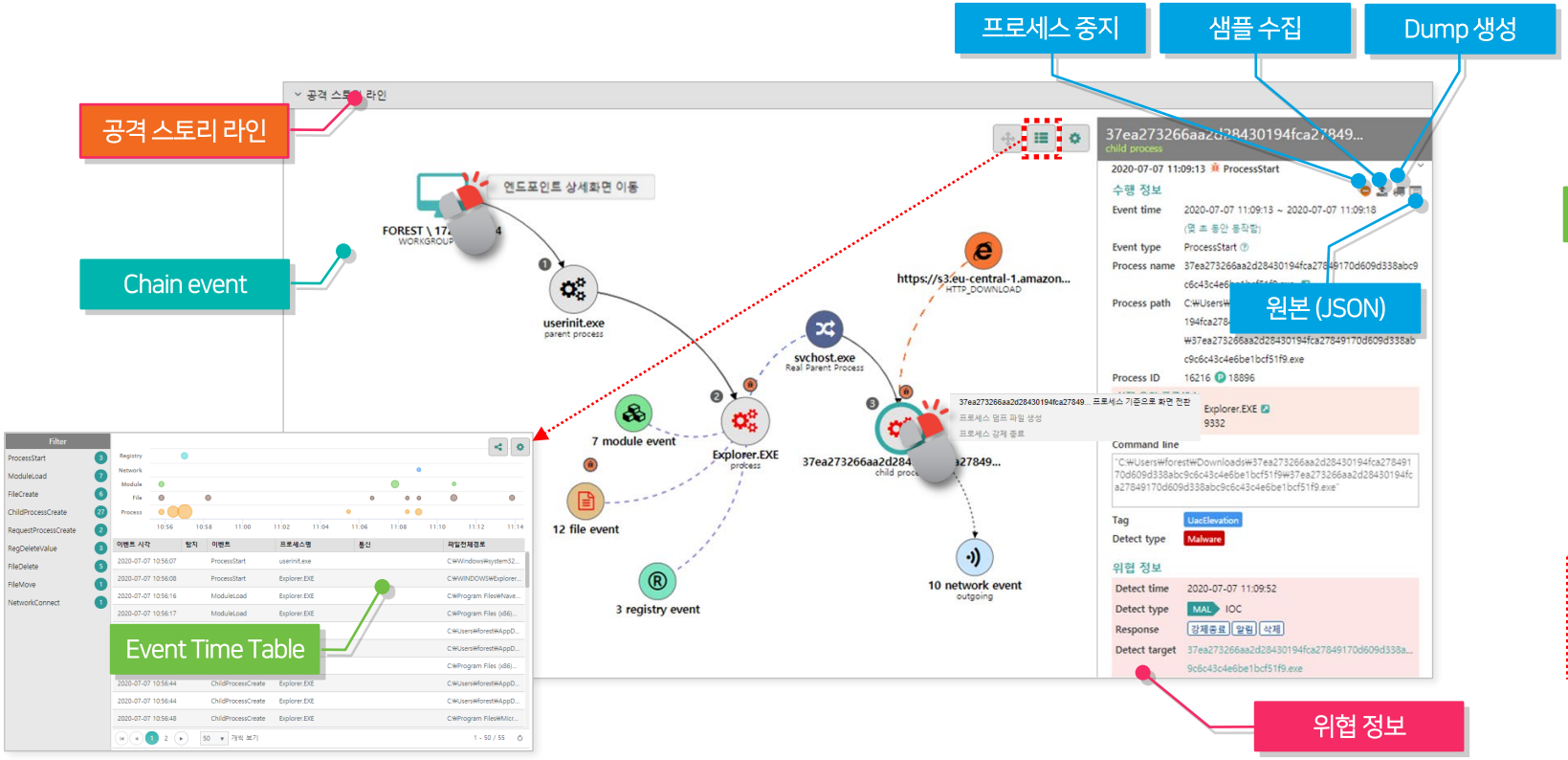


위협 분석 전체 화면



6. 분석

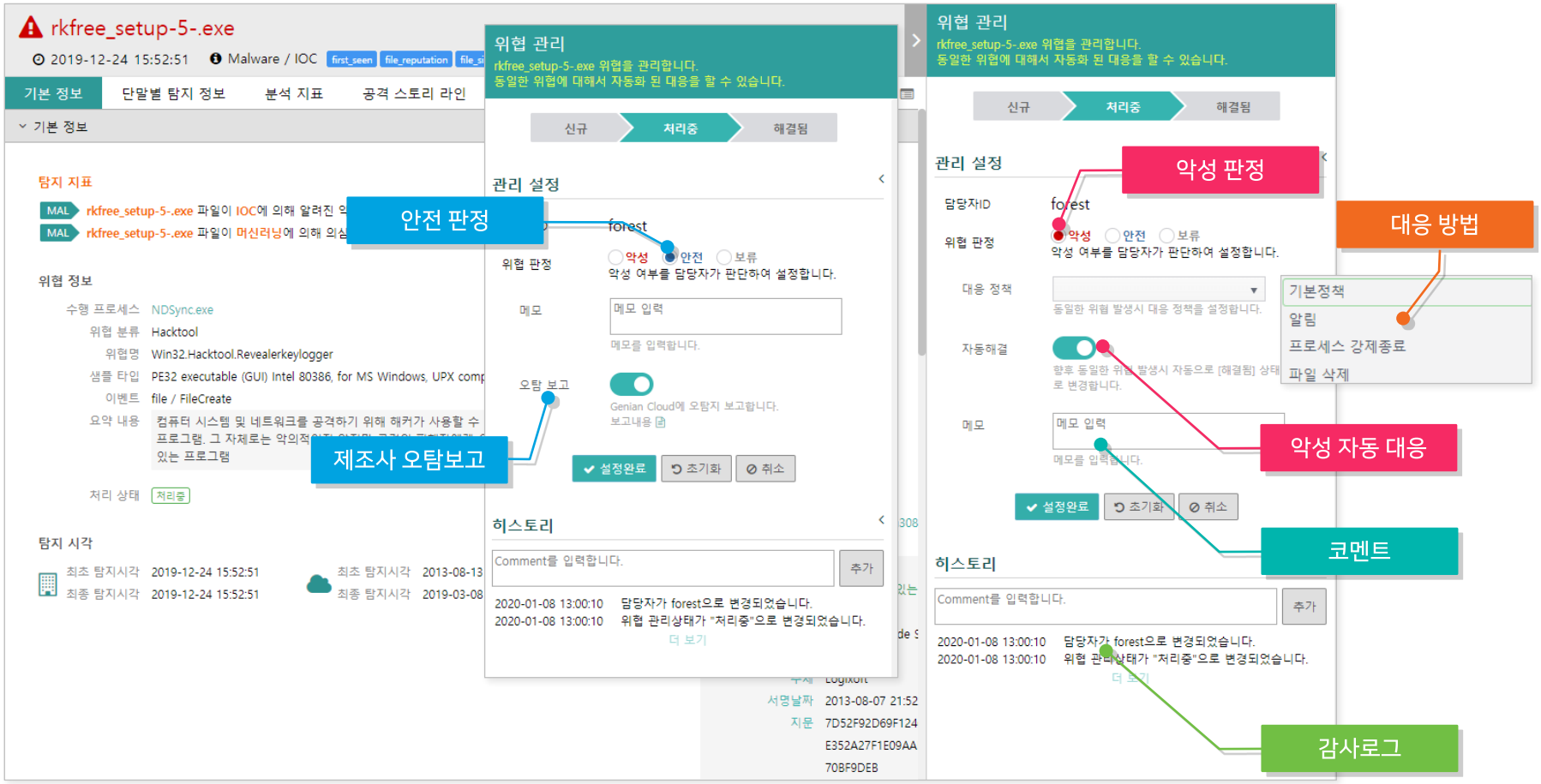
공격 스토리 라인에서는
파일/프로세스의 실행 관계를 표시하며, 프로세스 제어, 파일 수집 등의 제어 기능을 제공합니다.



※ 위협 탐지와 관계없이 수집한 모든 로그에 대해서 위와 같은 Chain Event를 제공합니다.

6. 분석

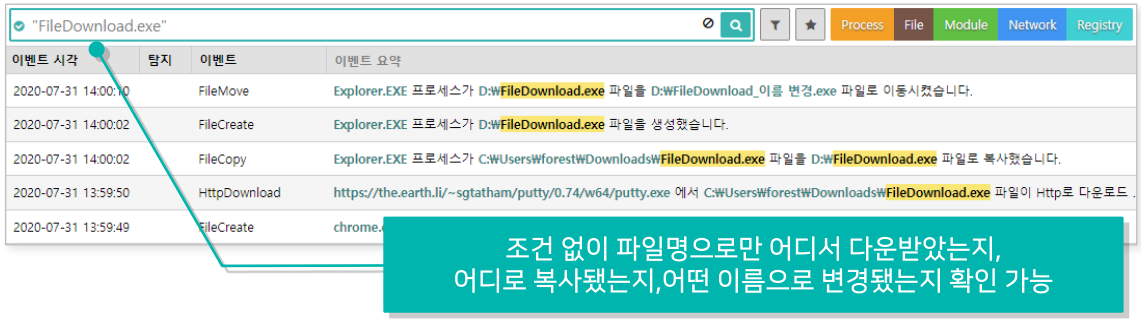
분석 후 위협에 대한 안전/악성 판단 후 자동 대응을 할 수 있습니다.



6. 분석

조건 없이 파일 명 하나만으로도 파일의 생성, 변경 정보를 확인할 수 있으며, 검색 기록 불러오기, 즐겨찾기 기능으로 동일한 검색을 쉽고 빠르게 할 수 있습니다.

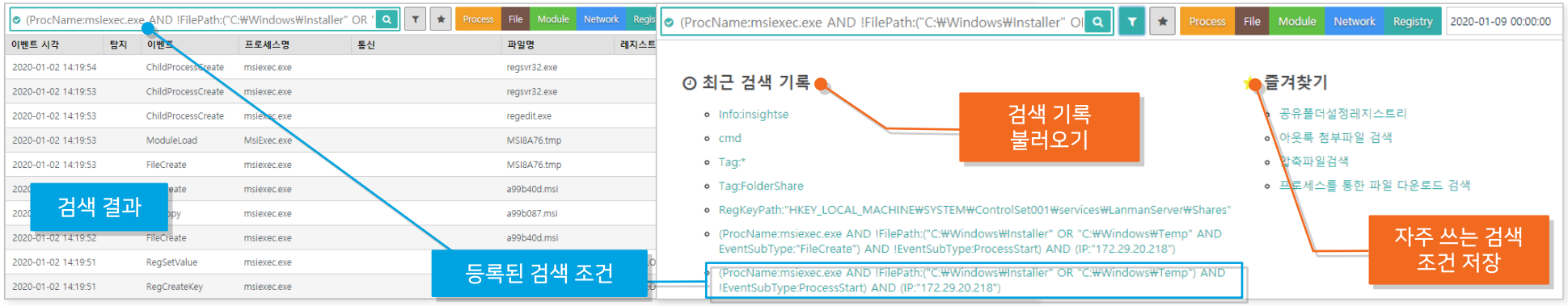
❖ FileDownload.exe 다운로드 ➔ C 에서 D 드라이브로 복사 ➔ D 드라이브에서 이름 변경



검색 조건	해석
IP:172.29.20.0/24 AND FileName:abc.exe OR NOT FilePath:windows AND FileSize:>100000 AND Score:[50 TO 100]	172.29.20.0/24 PC에서 파일 위치가 windows가 아니고 파일 크기가 1MB 이상이며, 파일 스코어가 50~100점 사이의 abc.exe 파일 존재 유무 검색

최근 검색을 한 기록은 별도로 보관되어 다시 불러오기로 검색이 가능하며, 자주 쓰이는 검색 조건은 " 즐겨찾기 " 로 등록, 재 검색 가능함

(ProcName:msiexec.exe AND !FilePath:("C:₩Windows₩Installer" OR "C:₩Windows₩Temp" AND EventSubType:"FileCreate") AND !EventSubType:ProcessStart) AND (IP:"172.29.20.218")

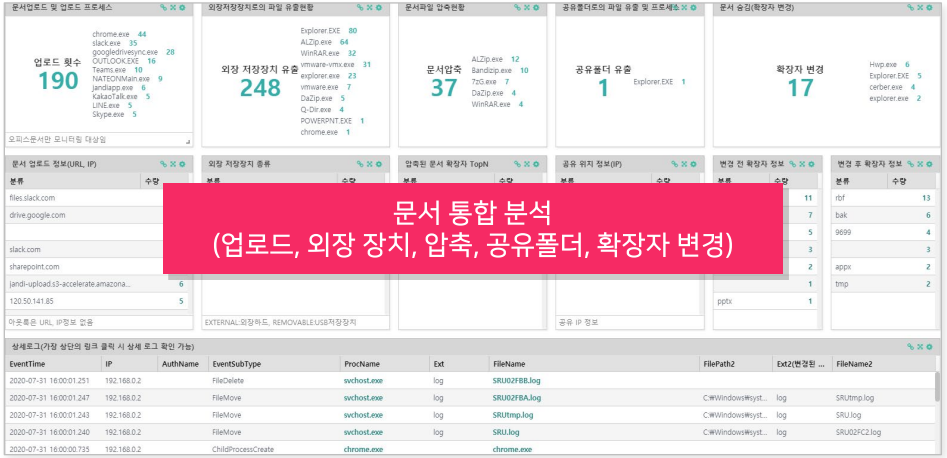


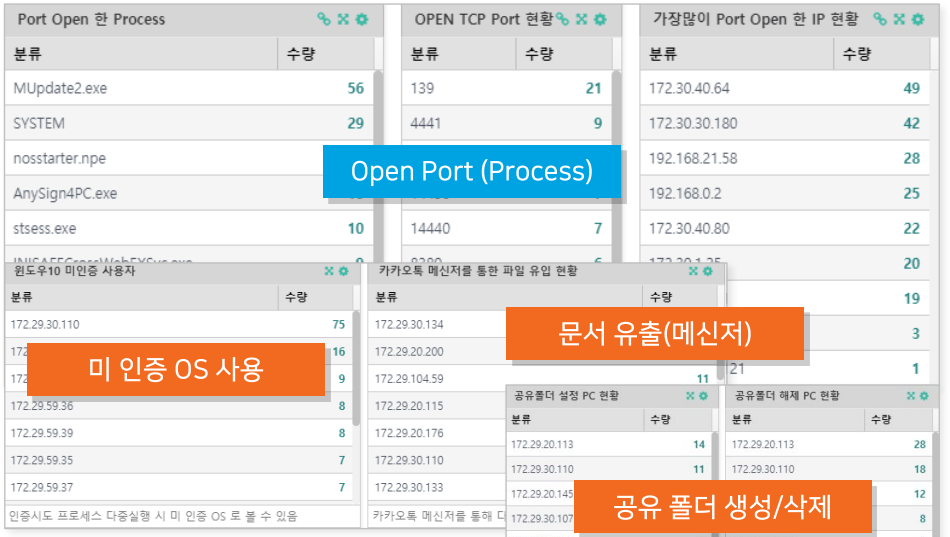
❖ 3개월 로그 39억 8천만 건 상황에서의 2가지 조건 검색 속도 : 약 3초

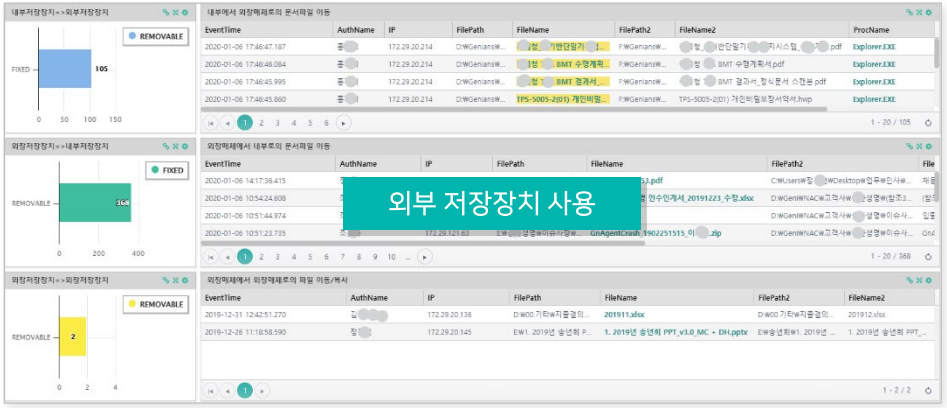
6. 분석

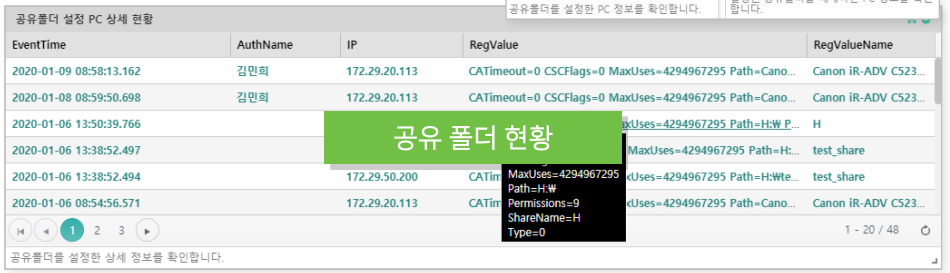
대시보드는 다양한 커스터마이징을 통해 엔드포인드의 가시성을 극대화 합니다. (Endpoint Discovery)

문서에 대한 업/다운로드, 아웃룩 메일 첨부 문서 송/수신, 공유 폴더를 통한 파일 유출, 공유 폴더 현황(설정, 삭제), 윈도우 미 인증 PC, 메신저를 통한 문서 유입/유출, 외장 저장장치를 통한 문서 유입/유출 등





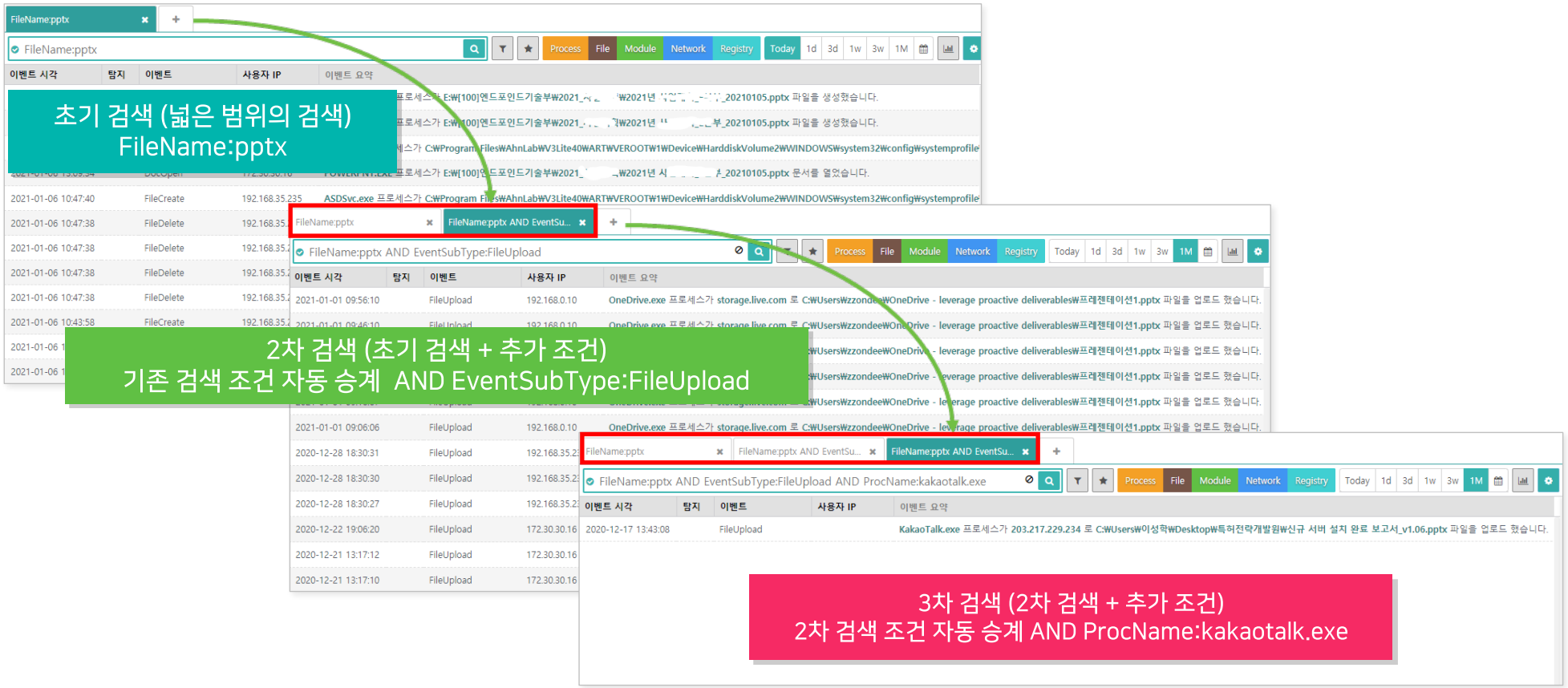




6. 분석

편리하고 유용한 로그 검색

한번 검색한 결과에 다시 **검색 탭을 추가**해서 단계별 상세 검색을 할 수 있습니다.



정확한 정보를 모르는 상태에서의 특정 로그를 확인하기 위해 범위를 좁혀 가면서 검색을 해야 합니다.
여러 번 검색을 한다면 기존 검색 결과를 지우고 재 검색을 하는 게 아닌 기존 검색결과도 같이 보면서 검색을 해야 효율적으로 사용할 수 있습니다.

6. 분석

Into the unknown : TAGs

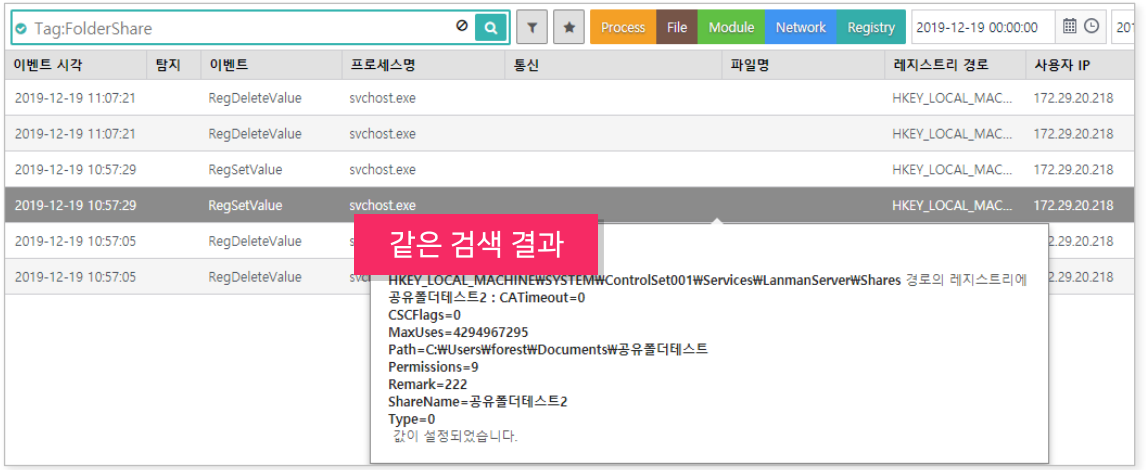
수집한 로그의 의미를 알 수 있도록 Tag를 설정하여 원하는 Tag 검색으로 복잡한 파일 경로, 레지스트리 등의 검색을 쉽고 빠르게 할 수 있습니다.

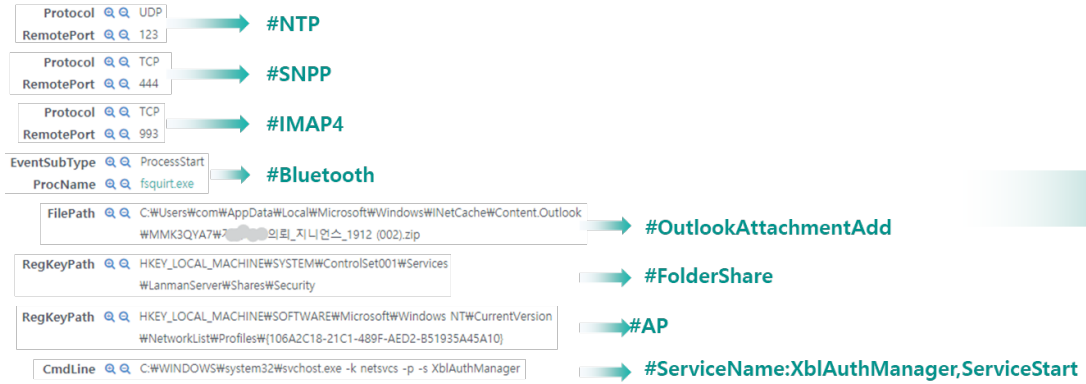
검색조건 (Raw data 검색)

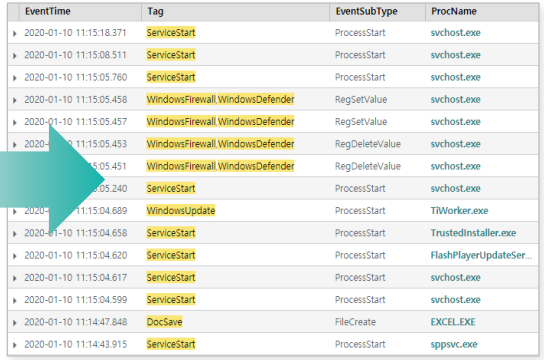
RegKeyPath:"HKEY_LOCAL_MACHINE₩SYSTEM₩ControlSet001₩services₩LanmanServer₩Shares"

검색조건 (tag 검색)

Tag:FolderShare



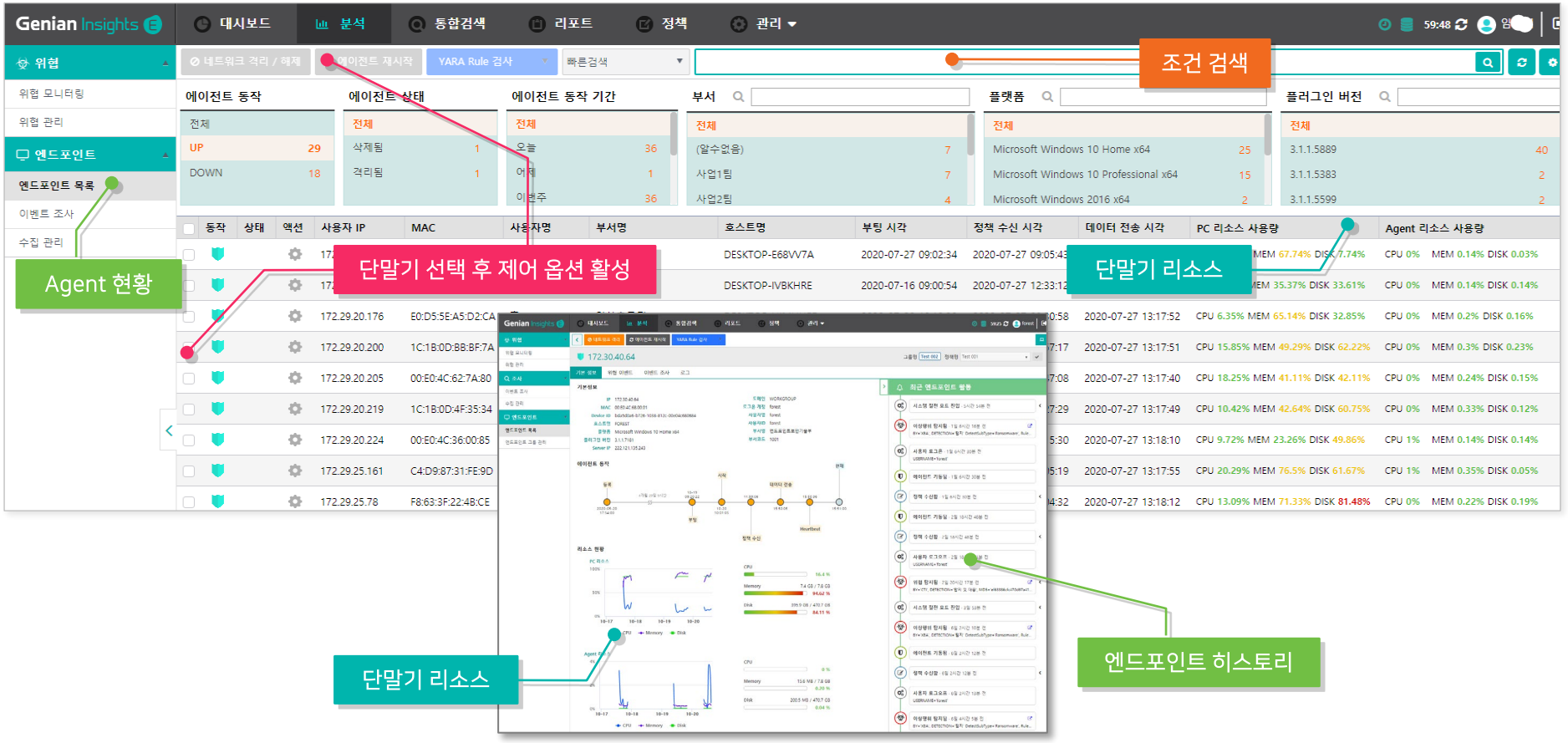




7. Agent 관리

설치된 Agent 현황을 파악할 수 있습니다.

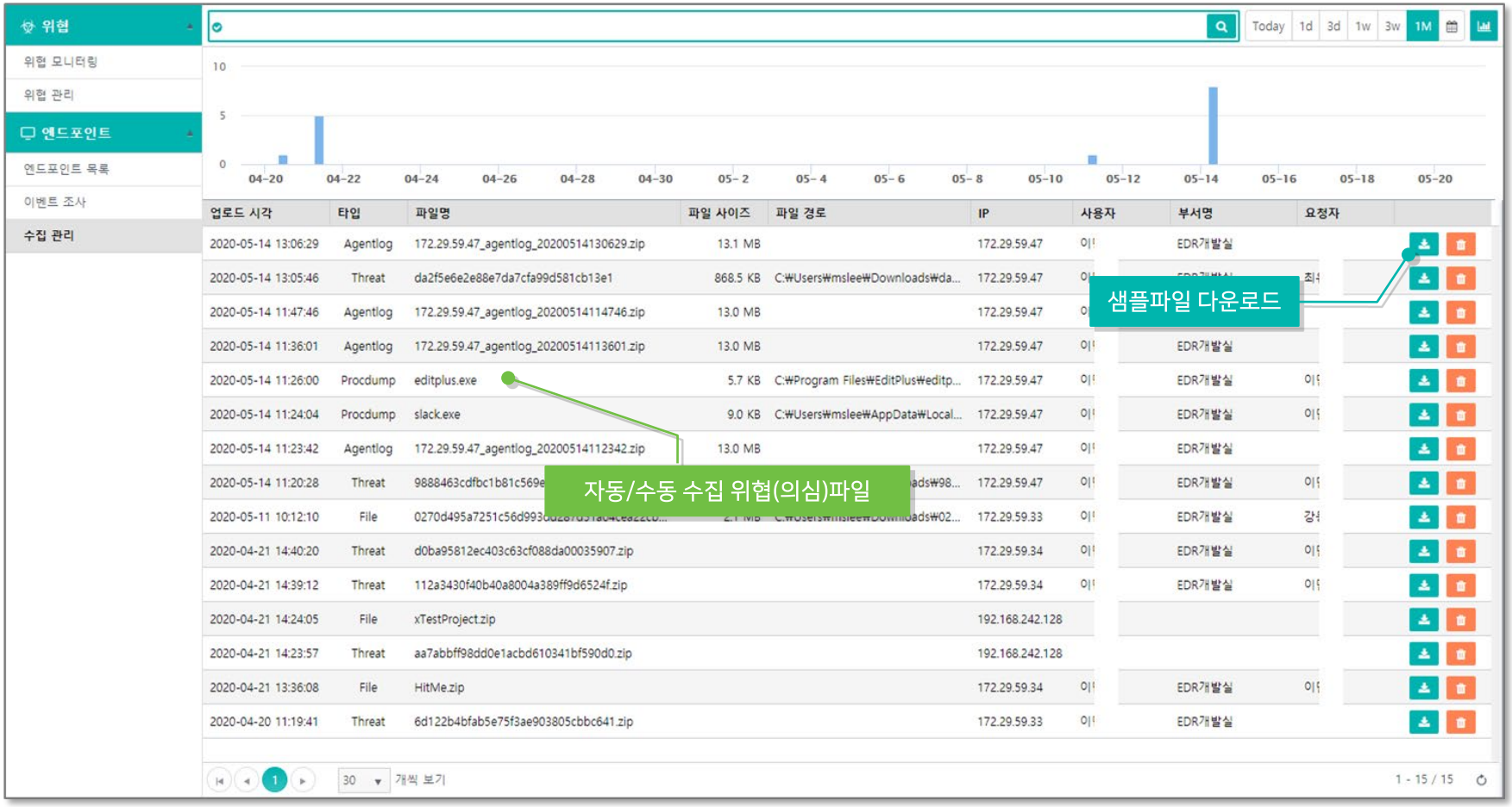
Agent On/Off 상태, IP, MAC, 사용자 정보, OS 정보, 부팅 시각, 정책 수신 시각, 데이터 전송 시각을 제공하며, 단말기 선택 후 네트워크 차단, Agent 재 기동, YARA Rule 검사를 수동으로 할 수 있습니다.



8. 수집관리

위협파일, 의심파일(PE)은 선택에 따라 자동/수동 수집하며, 관리자가 선택한 일반 PE 파일을 수동으로 수집할 수 있습니다.

탐지된 위협 파일은 추가 분석을 위해 사용자 PC 에서 EDR 서버로 파일을 전송, 관리할 수 있는 기능을 제공합니다.



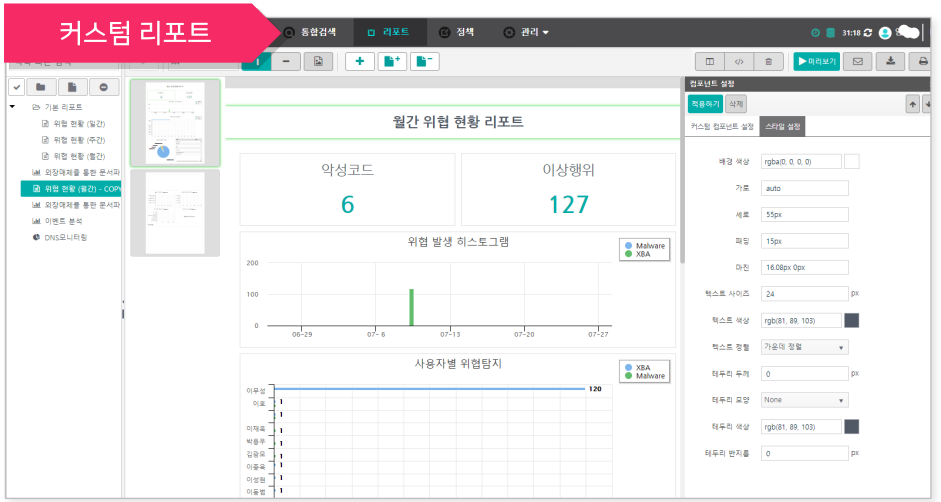
9. 리포트

관리자가 직접 생성할 수 있는 다양한 리포트를 제공합니다.

커스텀 리포트를 생성할 수 있도록 항목별 수정 옵션을 제공하며, HTML 수정을 통해 다양한 리포트를 생성할 수 있습니다.

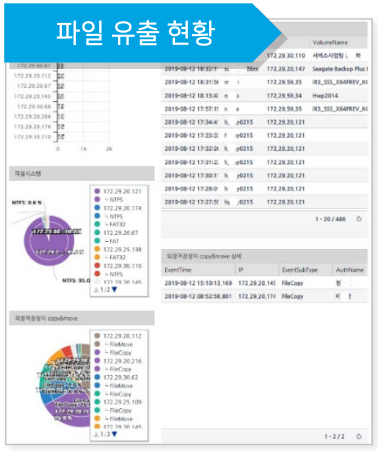
악성코드 탐지 현황

커스텀 리포트

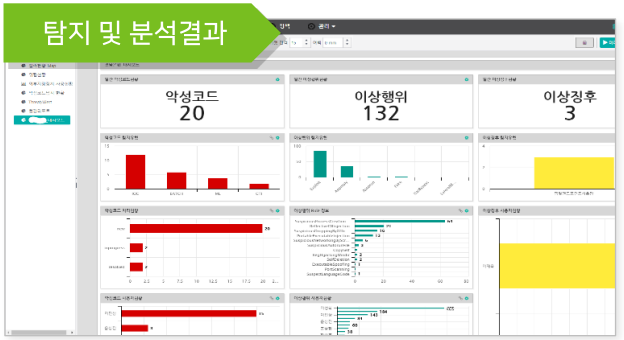


HTML 수정 가능

파일 유출 현황



탐지 및 분석결과

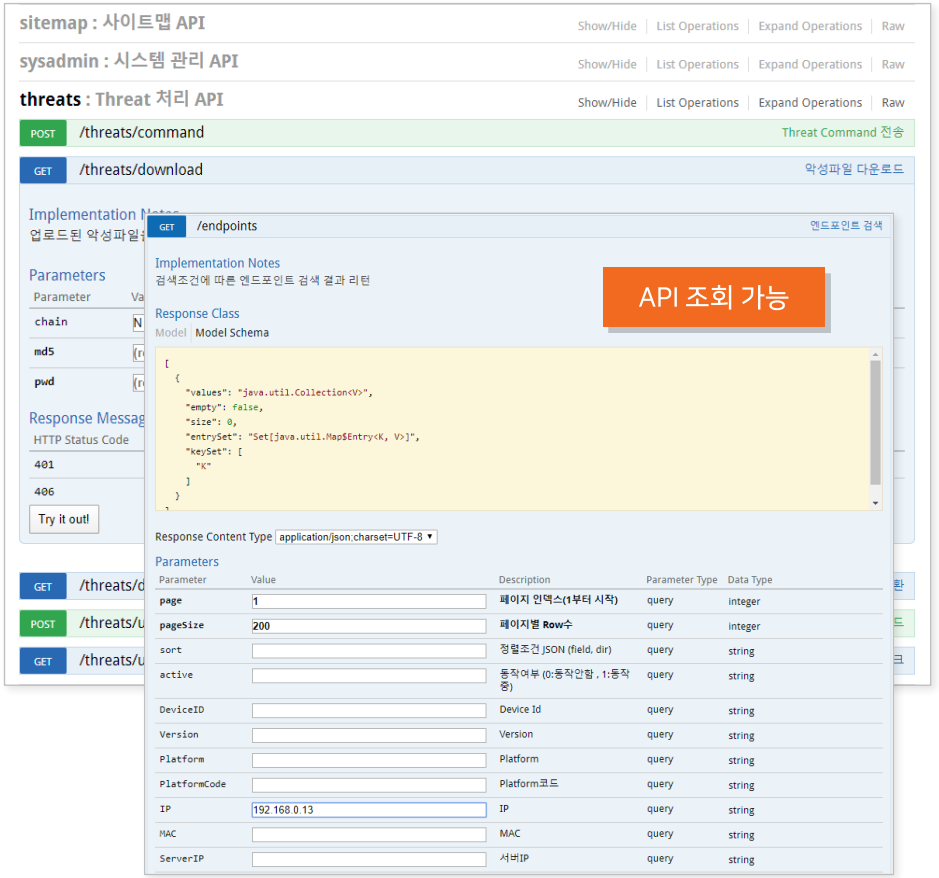


10. 연동

Syslog, SNMP, Rest API 를 지원하고 있어 타 시스템과의 연동을 다양하게 할 수 있습니다.

※ Syslog, SNMP 설정

※ REST API



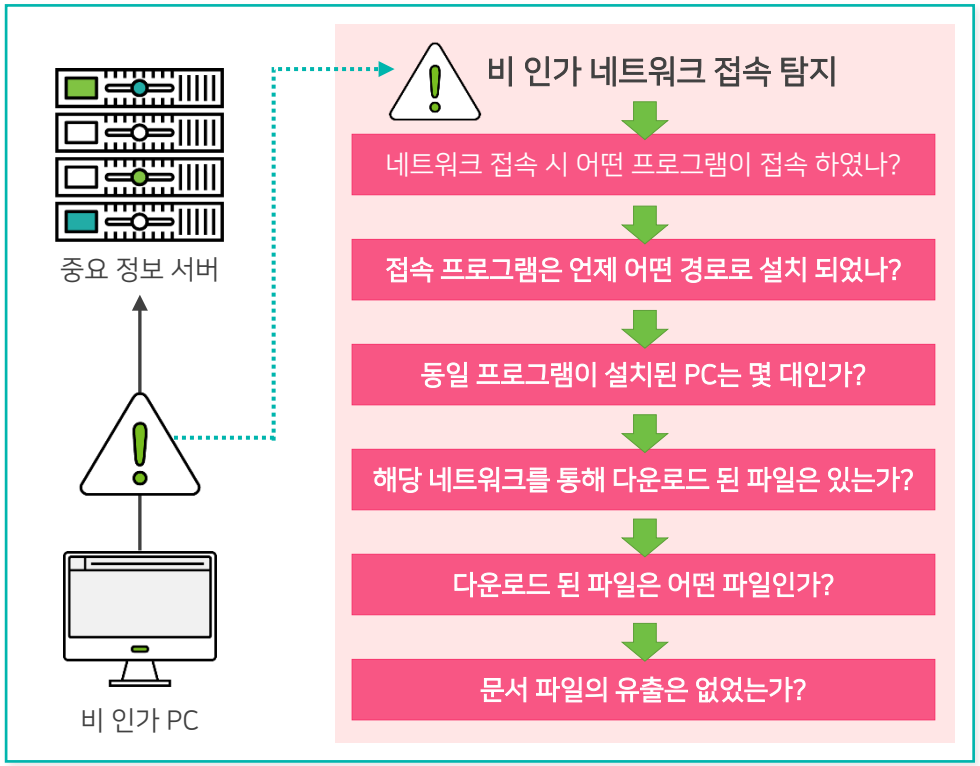
10. 연동

기타 다른 형태의 연동도 별도의 패치 작업 없이 플러그인 추가로 간단히 가능합니다.
(연동 플러그인 개발 후 패치 없이 적용)

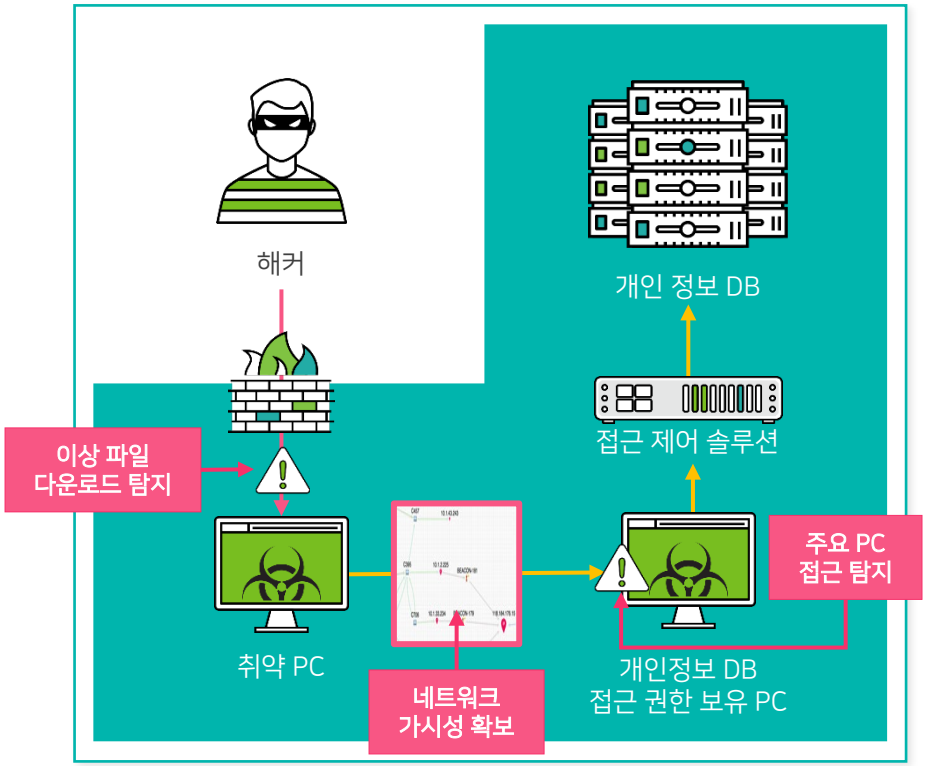
도입 효과

침투 경로와 행위에 대한 파악

단말에 침투한 파일이 언제, 어떻게 유입/실행이 됐으며, 어떤 네트워크 통신과 어떤 행위를 했는지에 대한 정보를 바탕으로 이상 파일/행위에 대한 탐지와 대응을 쉽게 할 수 있습니다.



Unknown ➔ Known

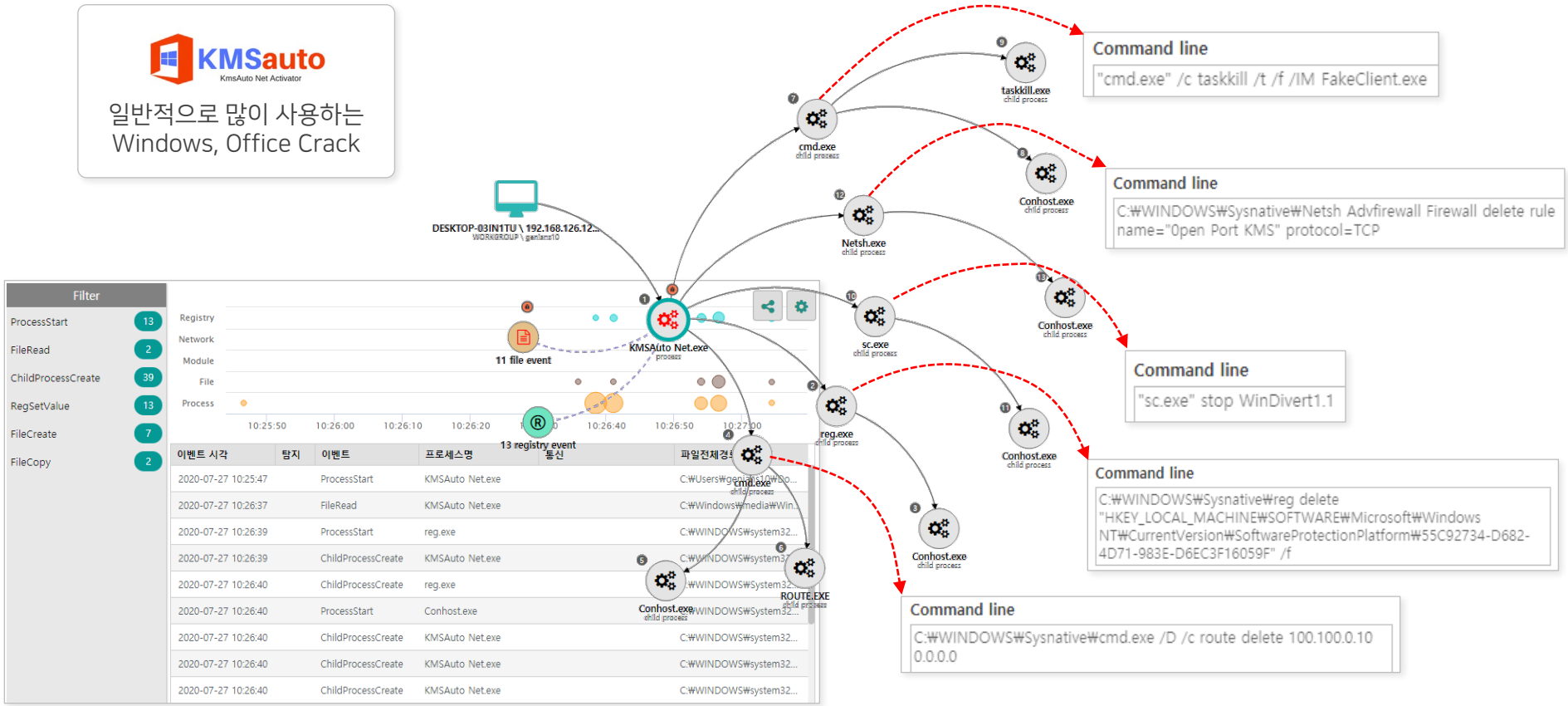


Unknown ➔ Known

침투 경로와 행위에 대한 파악

리버스 엔지니어링(Reverse Engineering)없이 프로그램의 동작을 확인할 수 있습니다.

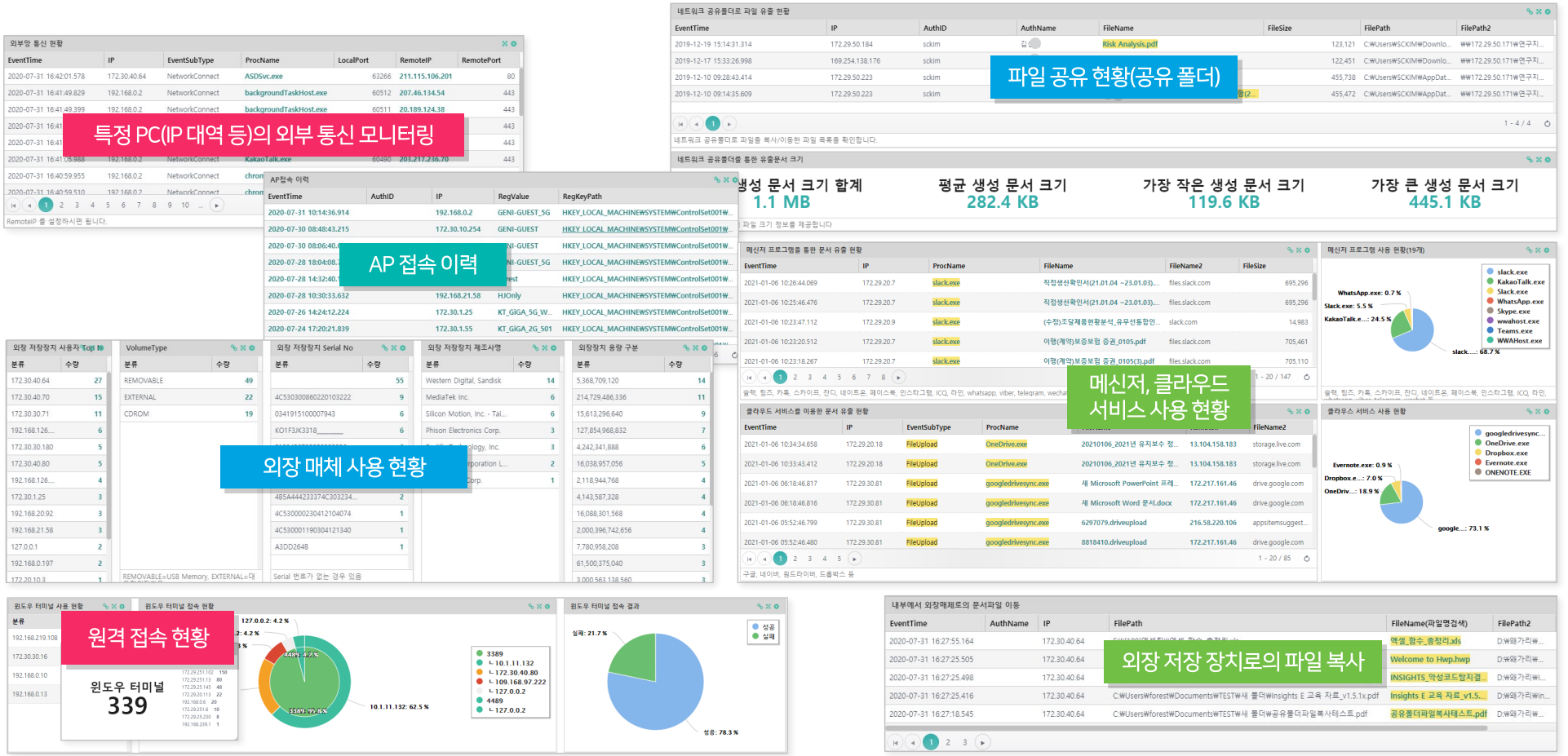
특정 프로세스 킬(KILL), 서비스 중지, 파일 생성, 방화벽 정책 삭제, 레지스트리 삭제, 라우팅 삭제 등



내부 보안 정책 점검

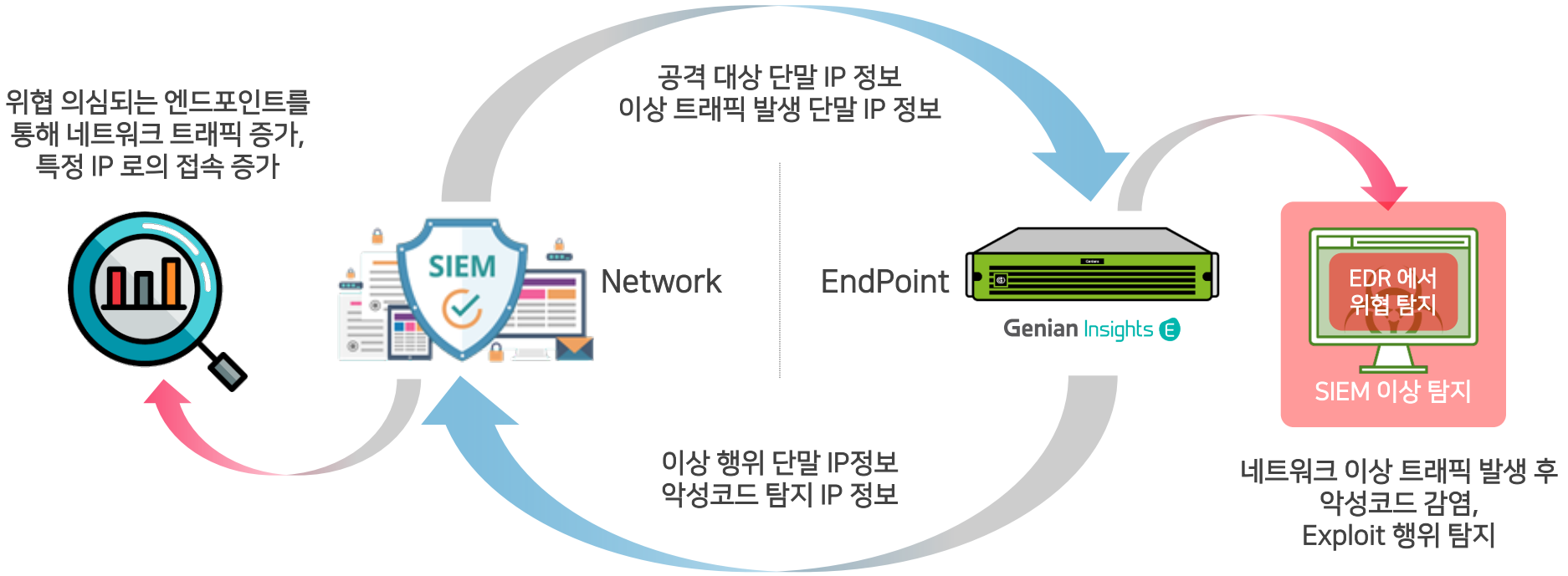
기존에 확인이 어려웠던 엔드포인트 보안 정책의 정합성을 확인할 수 있습니다.

폐쇄망 PC의 외부 통신, 내부 중요 시스템 접속 차단 PC의 통신 이력, USB 사용 금지 PC의 USB 사용 이력, 허용되지 않은 DNS 변경, 프록시 사용, 공유폴더 사용 여부, 테더링 사용, 개인 클라우드 사용 등 사용자 PC에서 적용되는 정책이 정상적으로 적용되고 있는지 확인 가능



네트워크와 엔드포인트의 연관성

네트워크 상의 위협 의심 정보를 연동하여, 네트워크 상의 이상 행위가 엔드포인트에서의 악성 행위나 악성파일 생성으로 이어졌는지 분석할 수 있습니다. 상호 연동으로 반대 상황도 분석이 가능합니다.



Thank you!