통합 보안 플랫폼 기업, 지니언스

PC 가시성의 모든 것

Genian EDR v2.0

Brand New 2023

Genians

Table of Contents

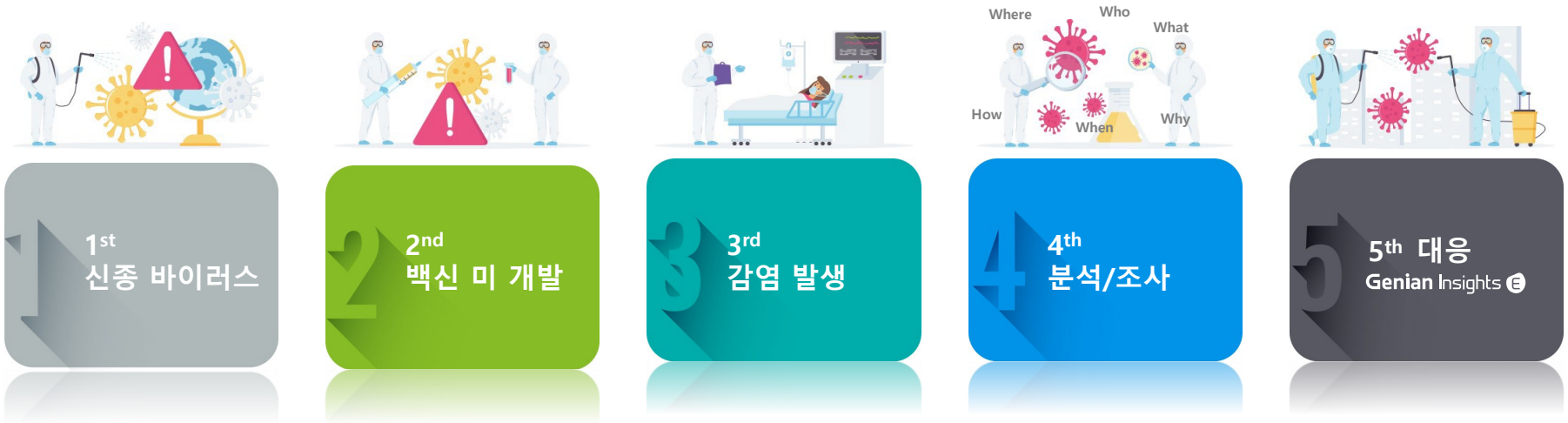
01.

배경 및 필요성

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.

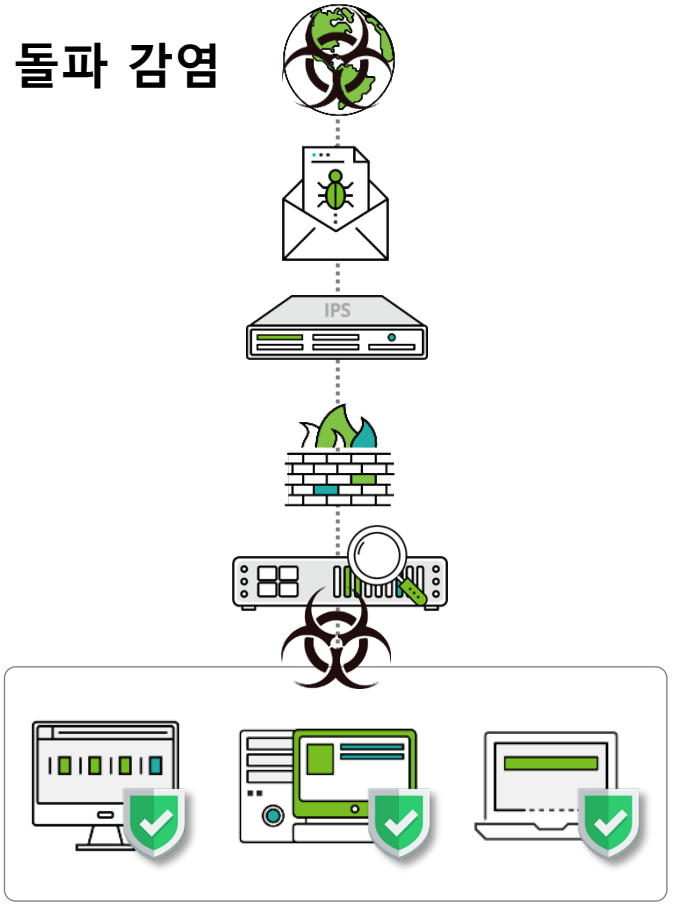
네트워크 경계에 있는 대부분의 보안 솔루션은 내부 자산을 보호하기 위해 구성되어 있으나 엔드포인트의 위협은 계속 증가하고 있습니다.

사용자에게 보내지는 악성 메일, 피싱 사이트, 위/변조 된 홈페이지 접속 등을 통한 악성코드 감염 및 APT 침해는 네트워크 보안 솔루션의 한계를 보여주고 있습니다.

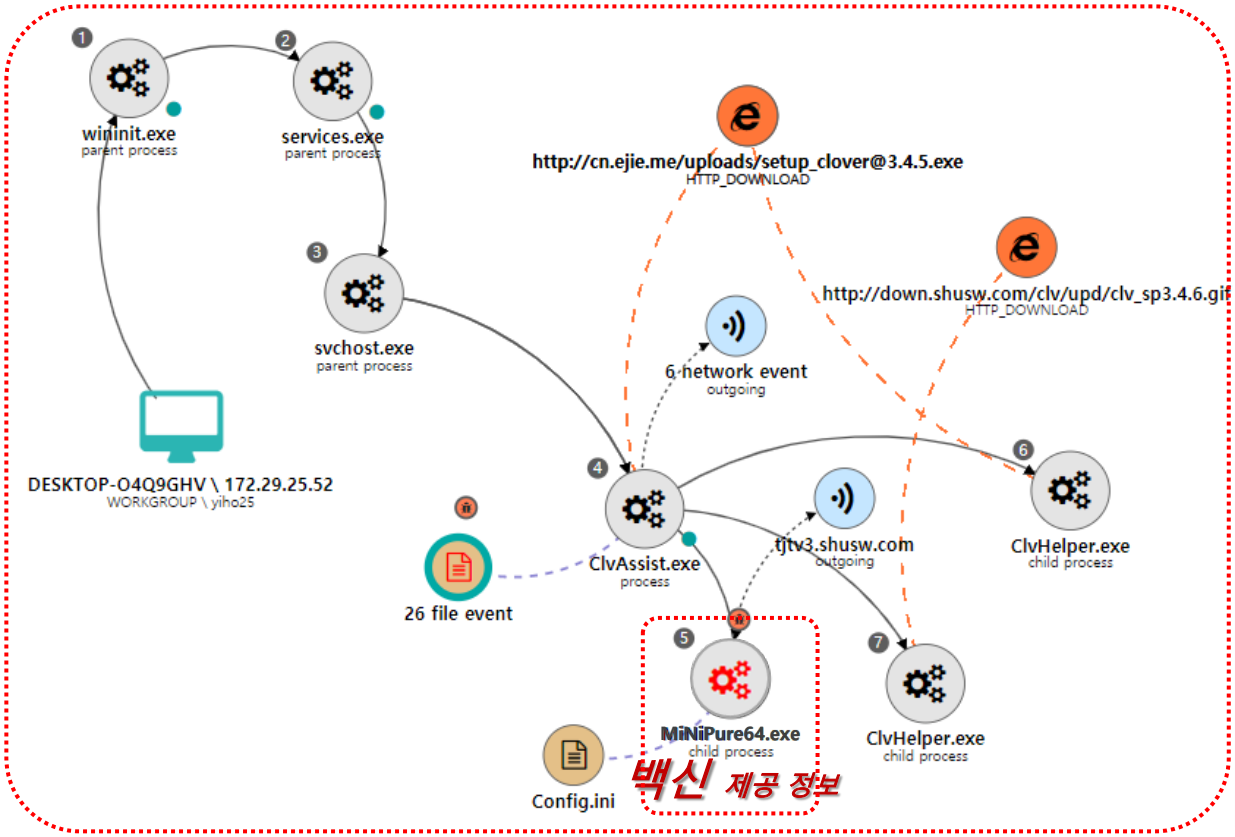
배경 및 필요성

코로나 바이러스의 돌파감염처럼 많은 보안 솔루션이 있음에도 해킹 사고는 줄지 않고 있으며, 백신으로는 역부족인 상황입니다. 백신으로 탐지를 했어도 해당 파일이 언제부터 있었는지, 다른 PC에도 해당 파일이 있는지, 어떤 정보가 유출이 됐는지, 어떤 파일을 생성했는지 알 수 없습니다.

돌파 감염

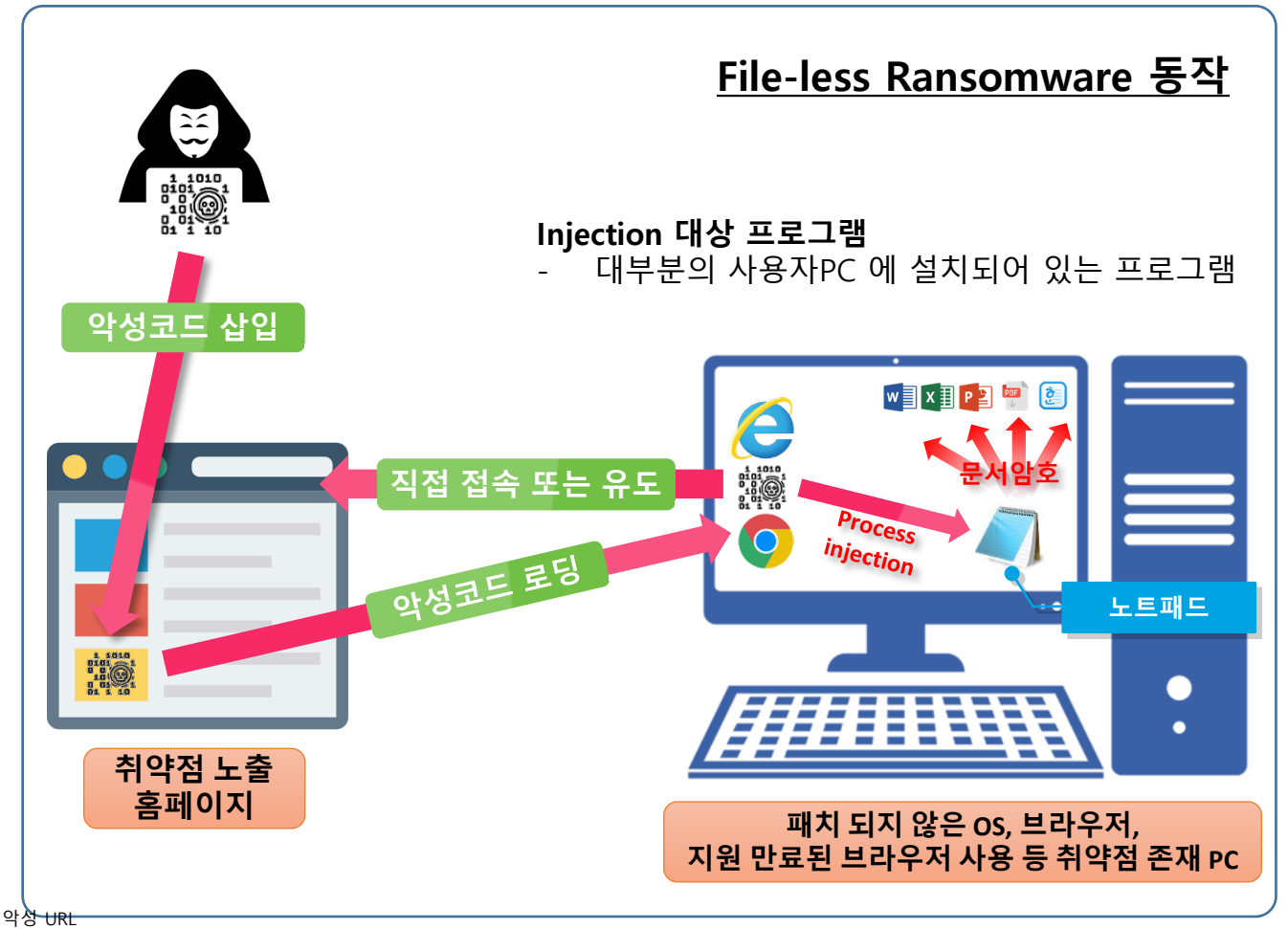


EDR 제공 정보



배경 및 필요성

파일만 탐지/대응 하는 시대는 지났습니다. 정상 파일(프로세스)에 의한 이상행위도 탐지할 수 있어야 합니다.



1. 유포지 : 악성코드를 직접 유포하는 악성 URL
2. 경유지 : 악성코드를 유포하는 유포지로 연결하는 악성스크립트가 삽입된 악성 URL
3. Mozi : 2016년 유행한 미라이(Mirai) 악성코드 변종으로 IoT 기기를 감염시켜 DDoS 공격을 수행하는 악성코드
4. Emotet : 2014년 독일, 오스트리아, 스위스 등에서 처음으로 발견된 악성코드로 금융 정보 탈취를 목적으로 한 악성코드
5. Folina : 원격 템플릿 기능을 활용, MSDT(Microsoft 진단도구) URL을 통해 파워쉘을 실행시키는 취약점

02.

Genian EDR 제품 소개

1) 개요

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

1. 단말 행위 모니터링/수집

- File, Module, Process, Connection, Registry 정보
- 사용자 및 단말에서 발생하는 이상 행위
- 외부 저장매체의 파일 정보
- 윈도우 이벤트 수집 (옵션)
- 다양한 대시보드 제공

2. 위협의 탐지

- 침해사고지표(IOC) 기반의 알려진 위협 탐지
- 머신러닝(ML)기반의 알려지지 않은 위협 탐지
- 행위 기반의 File-less 위협 탐지
- 야라(YARA)를 이용한 사용자 설정 기반의 심층조사

3. 위협의 대응

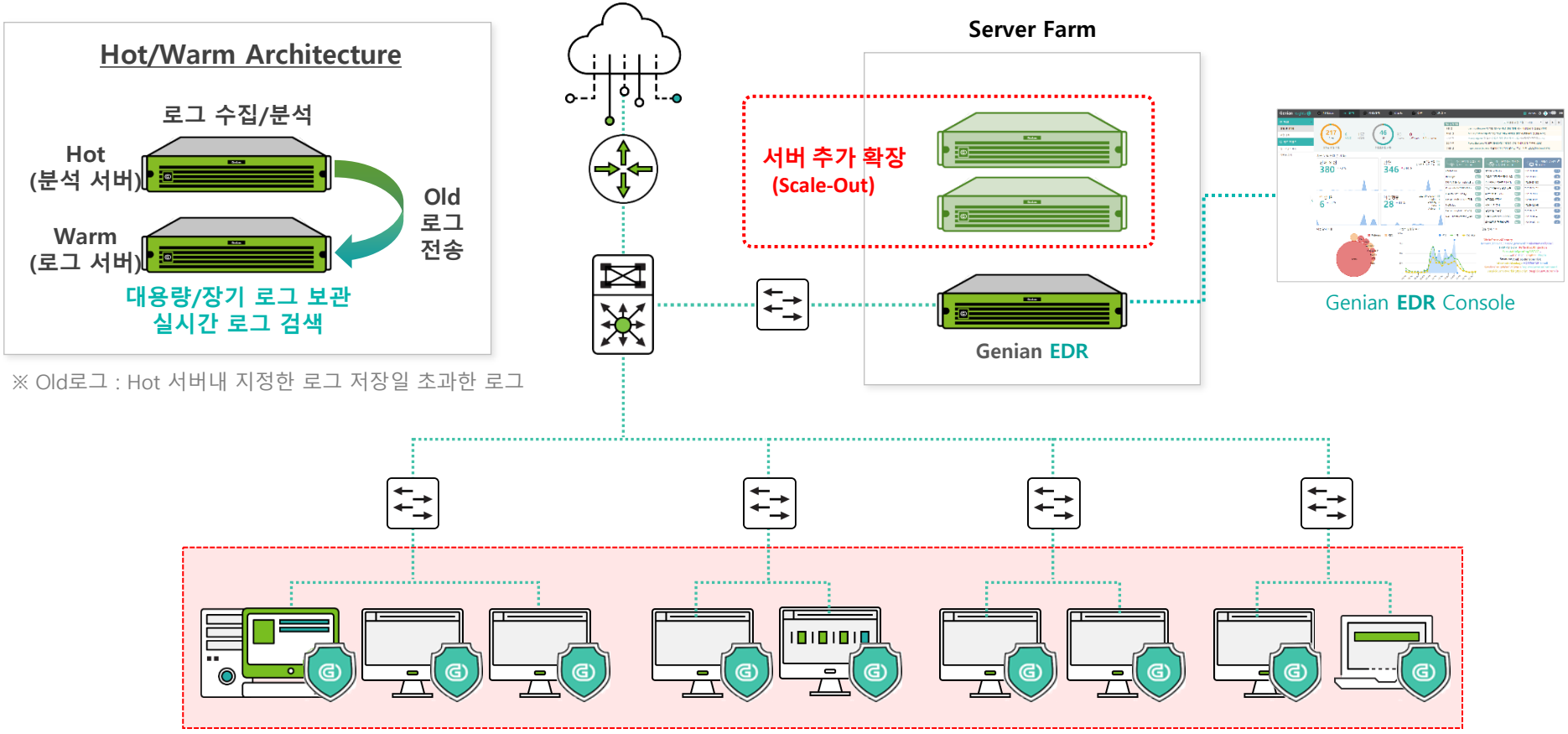
- 탐지된 위협 대상의 고지, 종료, 삭제, 네트워크 격리
- 알려진 위협 사전 대응
- 분석 후 대응 (대응 시 동일 이벤트 자동 대응)
- 샌드박스, SIEM 등 기존 보안 솔루션 연동

4. 탐지 위협의 조사/분석

- 탐지된 위협의 상세 정보 제공, 의심 파일 수집
- 통합 검색 및 연관 검색
- 이벤트 타임라인 및 연관 분석(Chain of Event)
- Ecosystem(평판서비스) 제공

2) Genian EDR 구성

Genian EDR 서버, Agent 의 간단한 구성입니다.
Scale-Out 기능을 제공하여 쉽게 확장 할 수 있습니다.



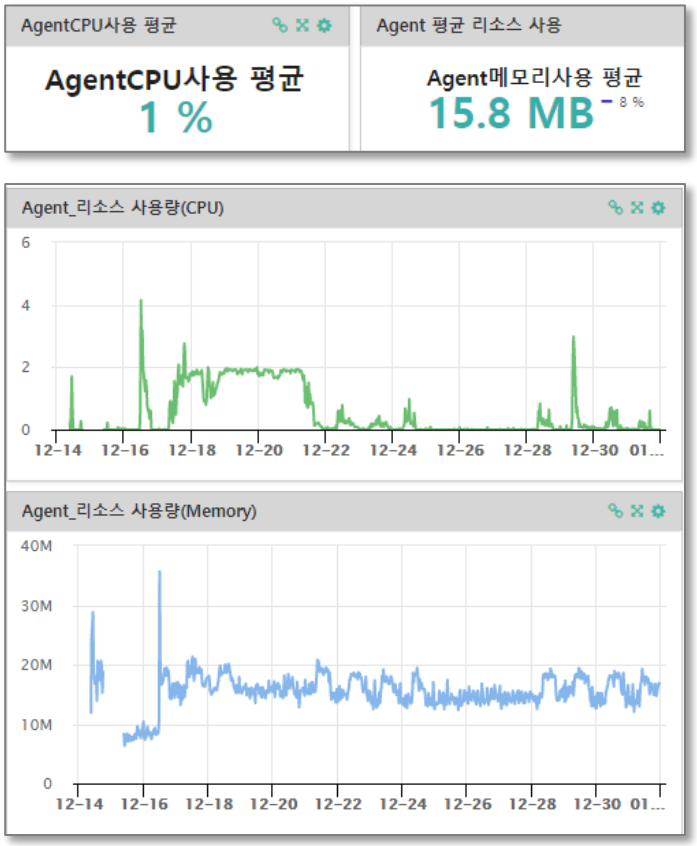
※ Old로그 : Hot 서버내 지정한 로그 저장일 초과한 로그

※ Genian NAC 사용 시, NAC Agent 에 EDR 플러그인(모듈) 형태의 간단한 배포와 인증 정보 자동 연동 기능 제공

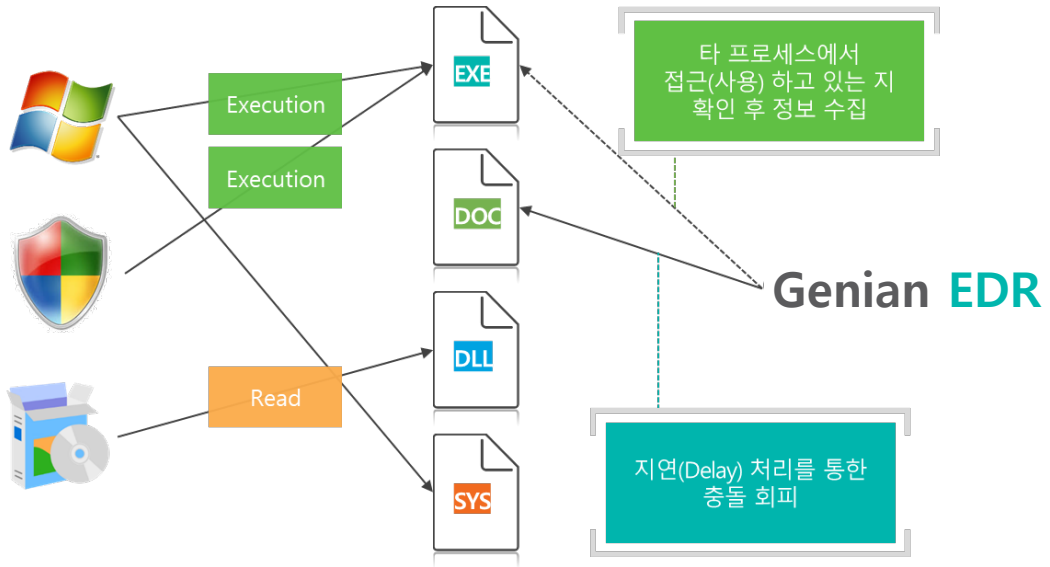
3) Light Agent

Agent는 최소의 리소스를 사용하며, 충돌을 방지하기 위한 충돌 회피 기술이 적용되어 있습니다.

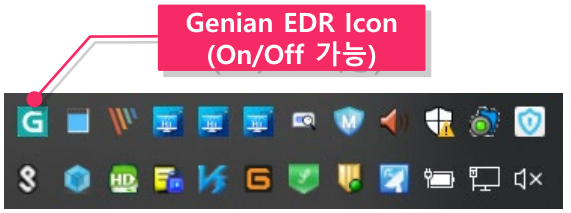
- CPU, MEMORY 최소 사용 동작 및 CPU, Memory 사용률 제한 기능이 있는 Agent
- 확인 처리 기술(타 프로세스의 접근 확인 후 처리), 지연 처리 기술(지연처리하는 기술) 적용으로 타 프로그램의 동작에 영향을 주지 않는 기술 적용



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



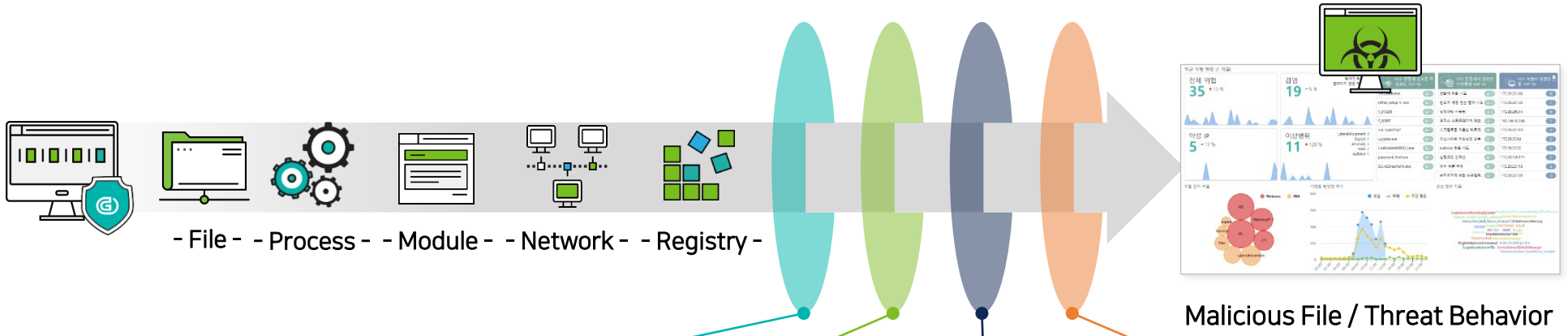
프로그램명	개요
NAC	Network 접근제어 에이전트
백신관리	백신 중앙관리 에이전트
백신	00000에서 제공하는 백신 프로그램
DLP	000000에서 제공하는 정보유출방지프로그램
WPM	자료 영구 삭제 프로그램
SW관리	미 인증 소프트웨어 차단 프로그램
Print0000	출력물보안솔루션
매체제어	000000에서 제공하는 매체제어프로그램



다양한 프로그램이 설치된
고객사 PC 환경에서 안정적인 동작

4) 탐지 기술

Multi-layer의 탐지 엔진으로 구성이 되어 File 과 이상행위(file-less) 탐지와 함께 분석에 필요한 상세 정보를 제공합니다.



IOC 탐지 (파일)

알려진 악성파일 탐지
전세계에서 탐지 됐던 파일의 패턴 매칭

ML 탐지 (파일)

악성파일과 유사한 특징(features*)을 가진 파일

XBA 탐지 (행위)

파일은 정상이나
이상행위에 대한 탐지
(내부 파일 유출, 자동 실행 등록 등 MITRE ATT&CK 기반 및 커스텀 룰)

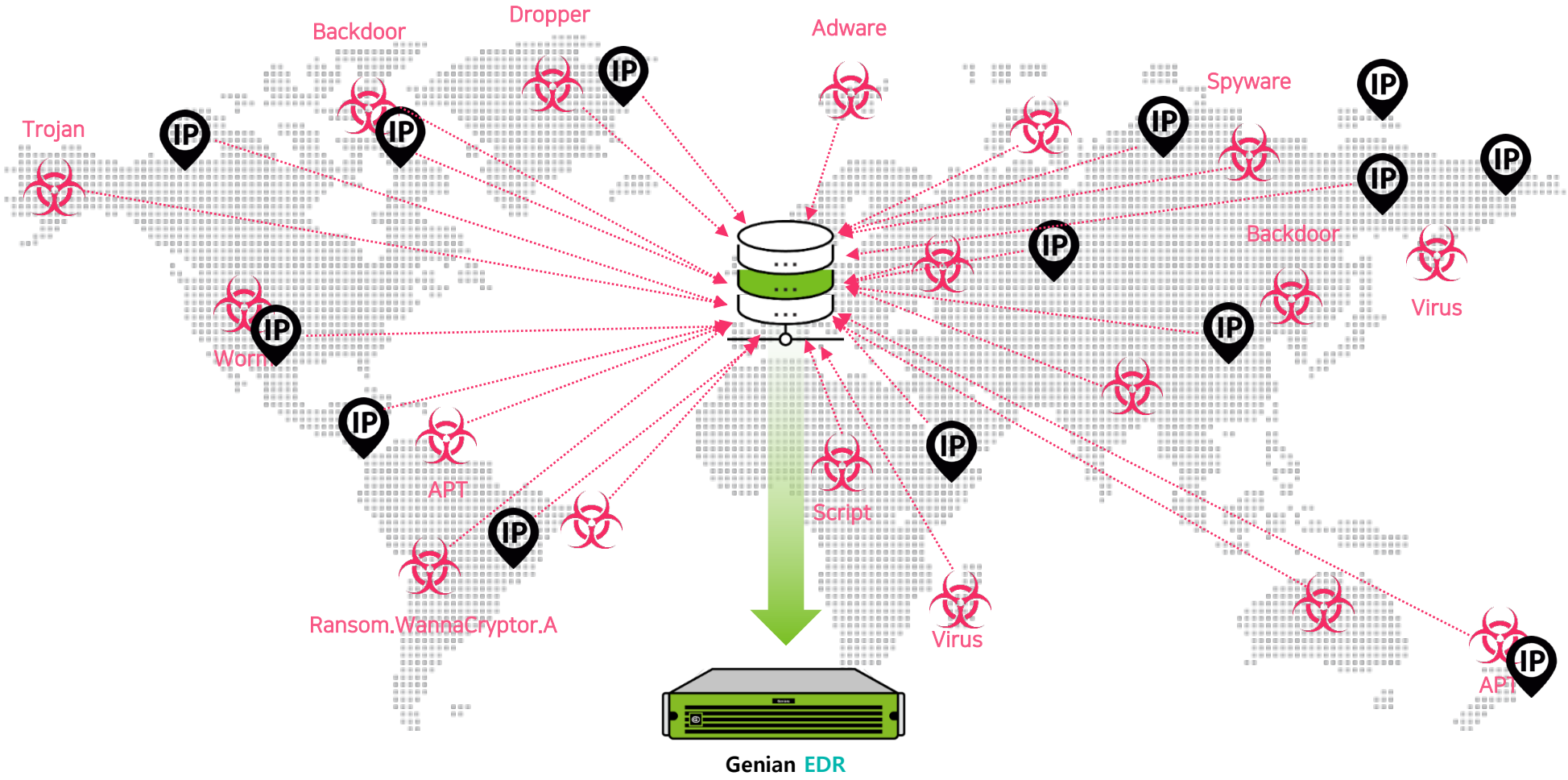
CTI (평판조회, 유사도)

탐지된 파일의 평판 정보
(외부 최초, 최종 탐지 시간, 악성코드 명 및 악성파일의 유사도* 정보) 추가 제공 (외부 통신 가능 환경)

※ PE features : PE 파일은 수십개의 섹션이 있으면 해당 섹션에 특징을 features 라 함
※ 유사도 : 탐지된 파일이 어떤 악성코드와 유사한 지에 대한 % 제공 (ssdeep hash)

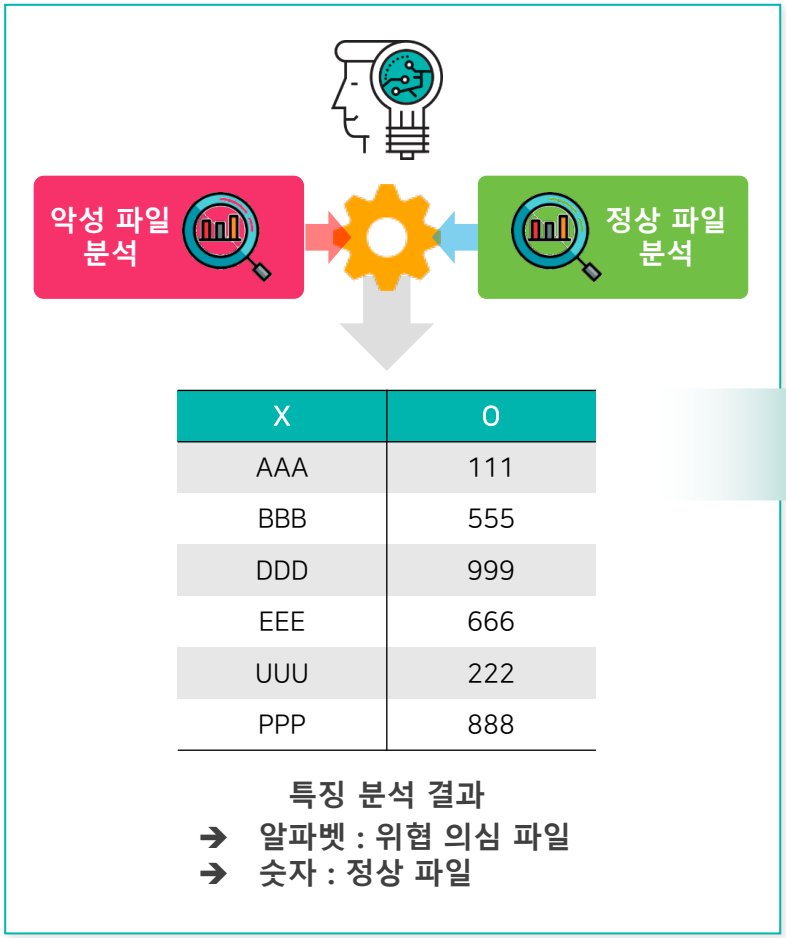
4) 탐지 기술

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



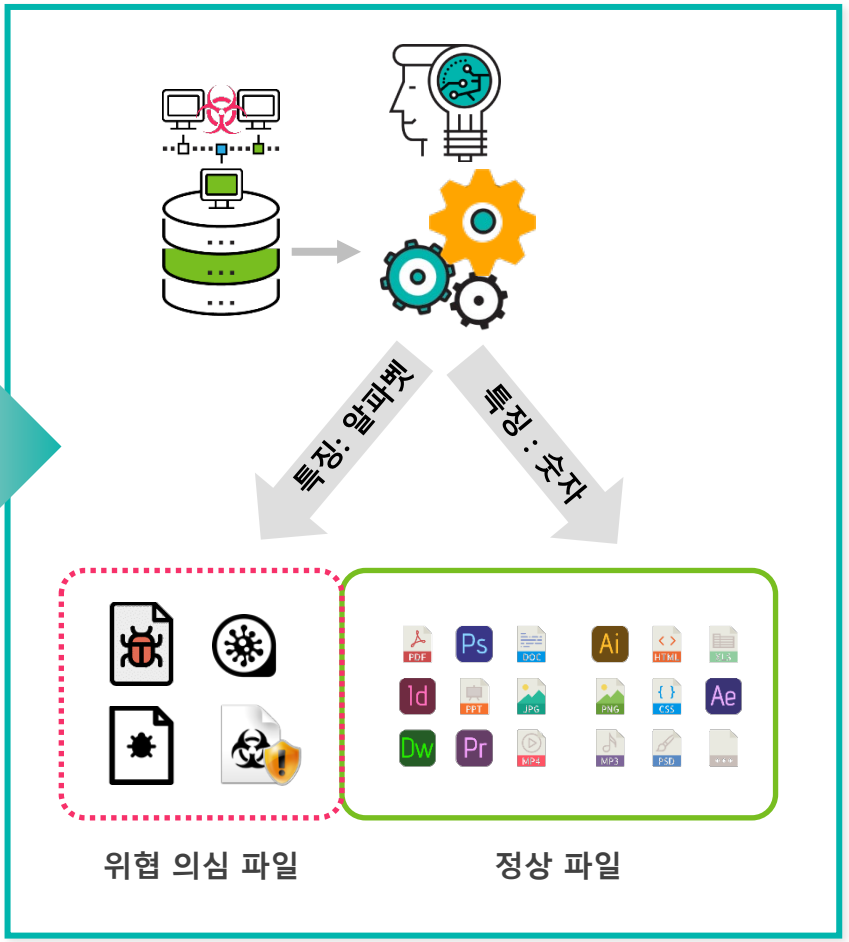
4) 탐지 기술

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



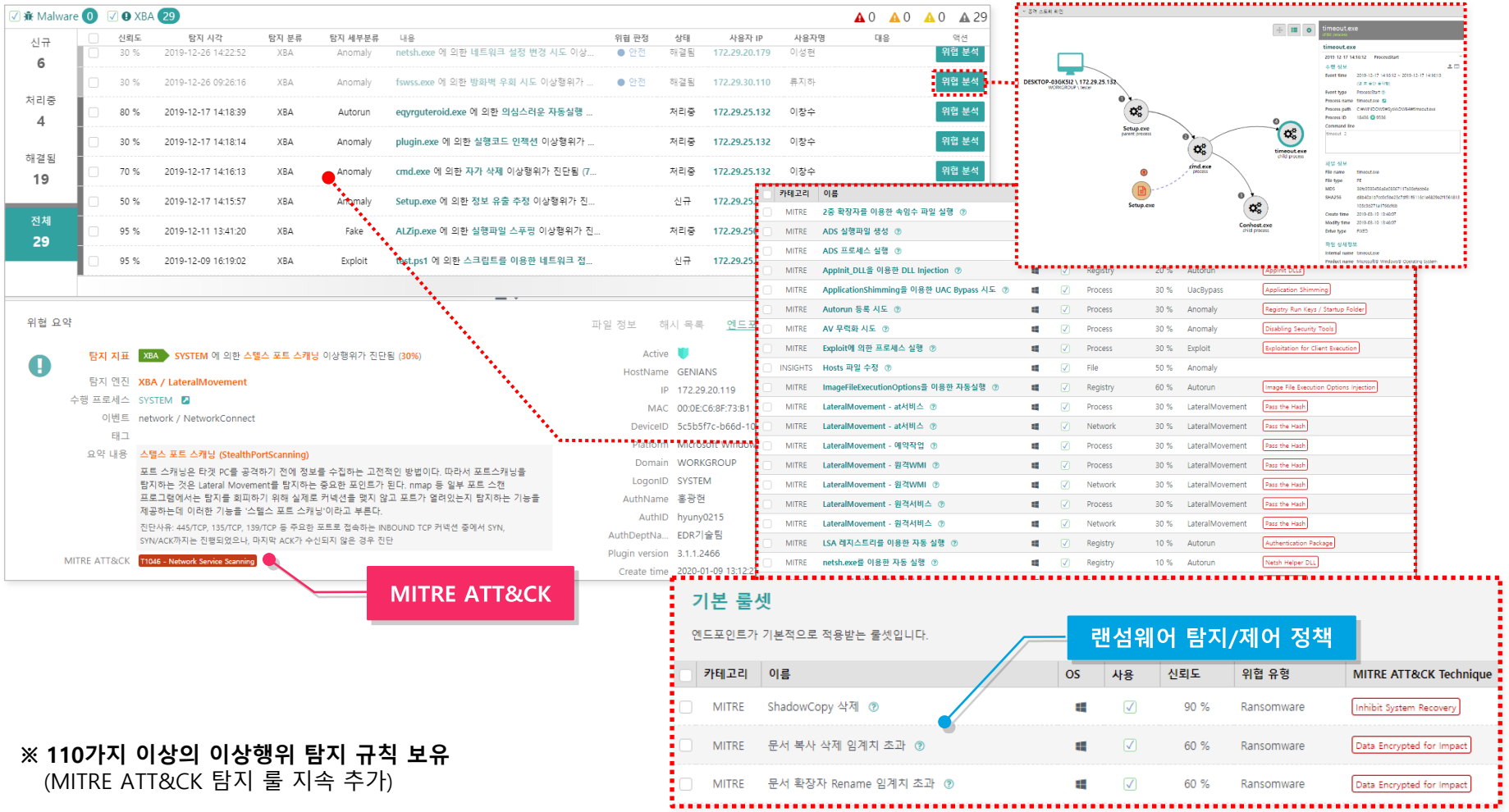
X	O
AAA	111
BBB	555
DDD	999
EEE	666
UUU	222
PPP	888

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



4) 탐지 기술

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

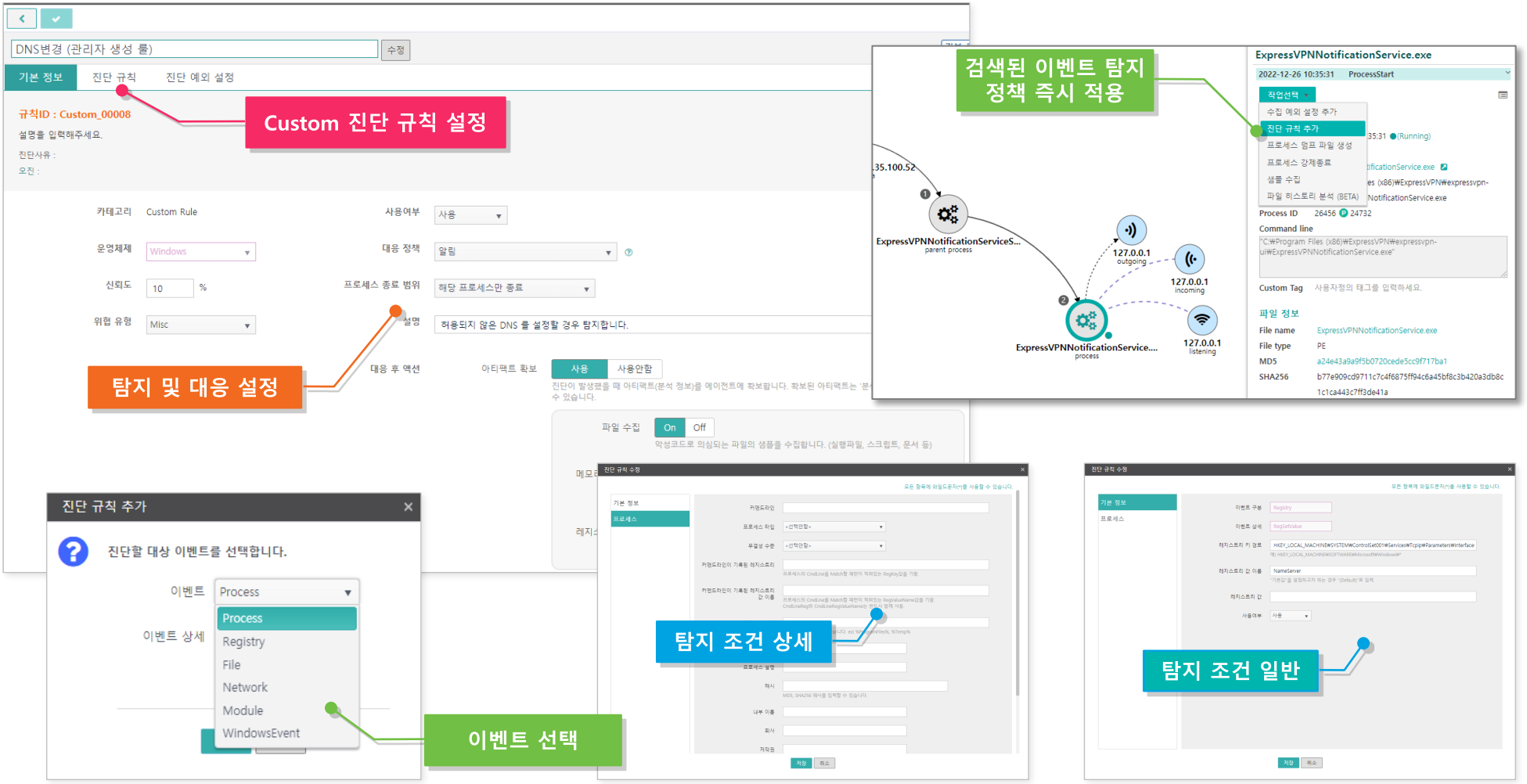


※ 110가지 이상의 이상행위 탐지 규칙 보유
(MITRE ATT&CK 탐지 룰 지속 추가)

4) 탐지 기술

Custom Rule 을 통해 직접 탐지할 수 있는 패턴을 등록할 수 있습니다.

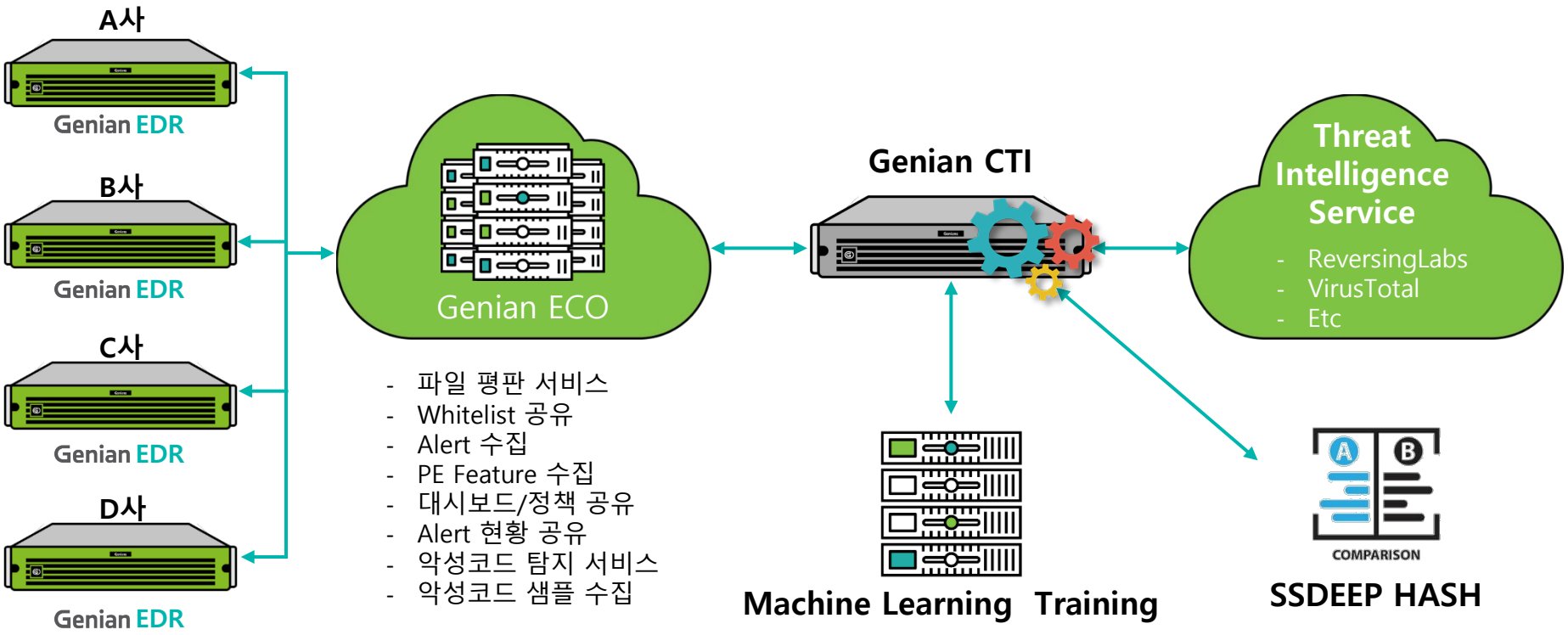
- 기본 제공하지 않는 룰, 필요에 의한 특정 패턴의 룰을 직접 생성 관리



4) 탐지 기술

Ecosystem : Genian 자체의 평판시스템을 제공합니다.

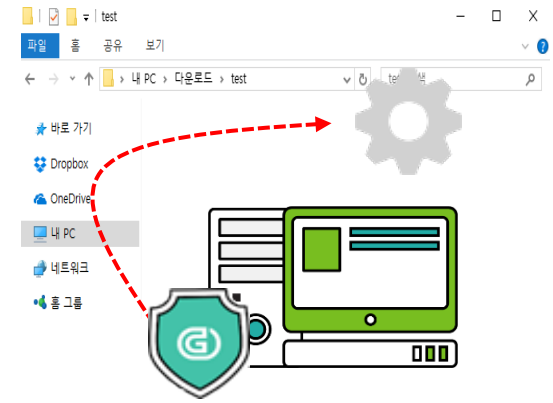
- 오탐 및 최신 악성코드 분석 결과를 고객에게 공유하기 위한 Genian EDR ECO-SYSTEM 구성
- 파일의 근거 (해당 파일이 어떤 역할을 하는 파일인가? 정말 악성인가?) / 오탐 자동 예외 처리
- 지니언스 고객을 통해 수집된 위협과 예외 처리된 데이터를 수집, 가공하여 Genian EDR을 사용하는 모든 고객에게 재배포합니다.
- 이를 통해 Genian EDR을 사용하는 고객들의 오탐을 줄여주며, 위협 혹은 파일 세부 정보 식별이 필요할 때 그 정보를 알려줍니다.



5) 대응

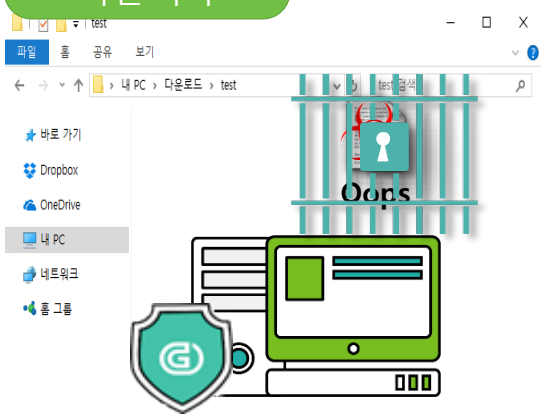
악성 파일에 대한 프로세스 중지, 격리, 사용자/관리자 알람, 네트워크 격리 등의 대응 기능을 제공합니다.

프로세스 종료

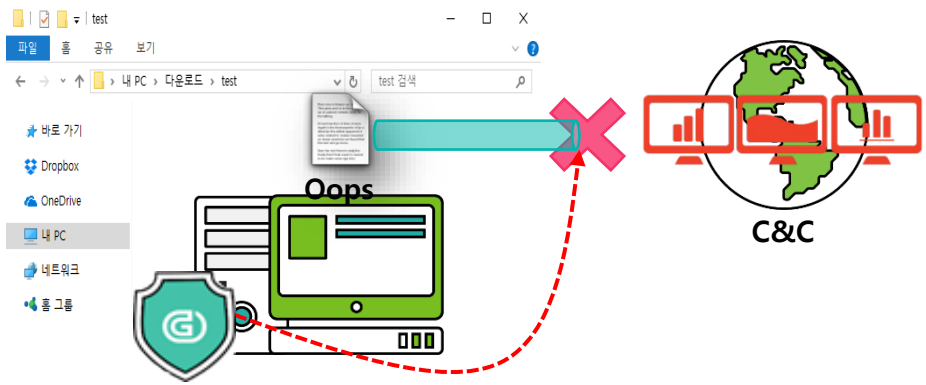


사용자/관리자 알람 경고

파일 격리



네트워크 격리

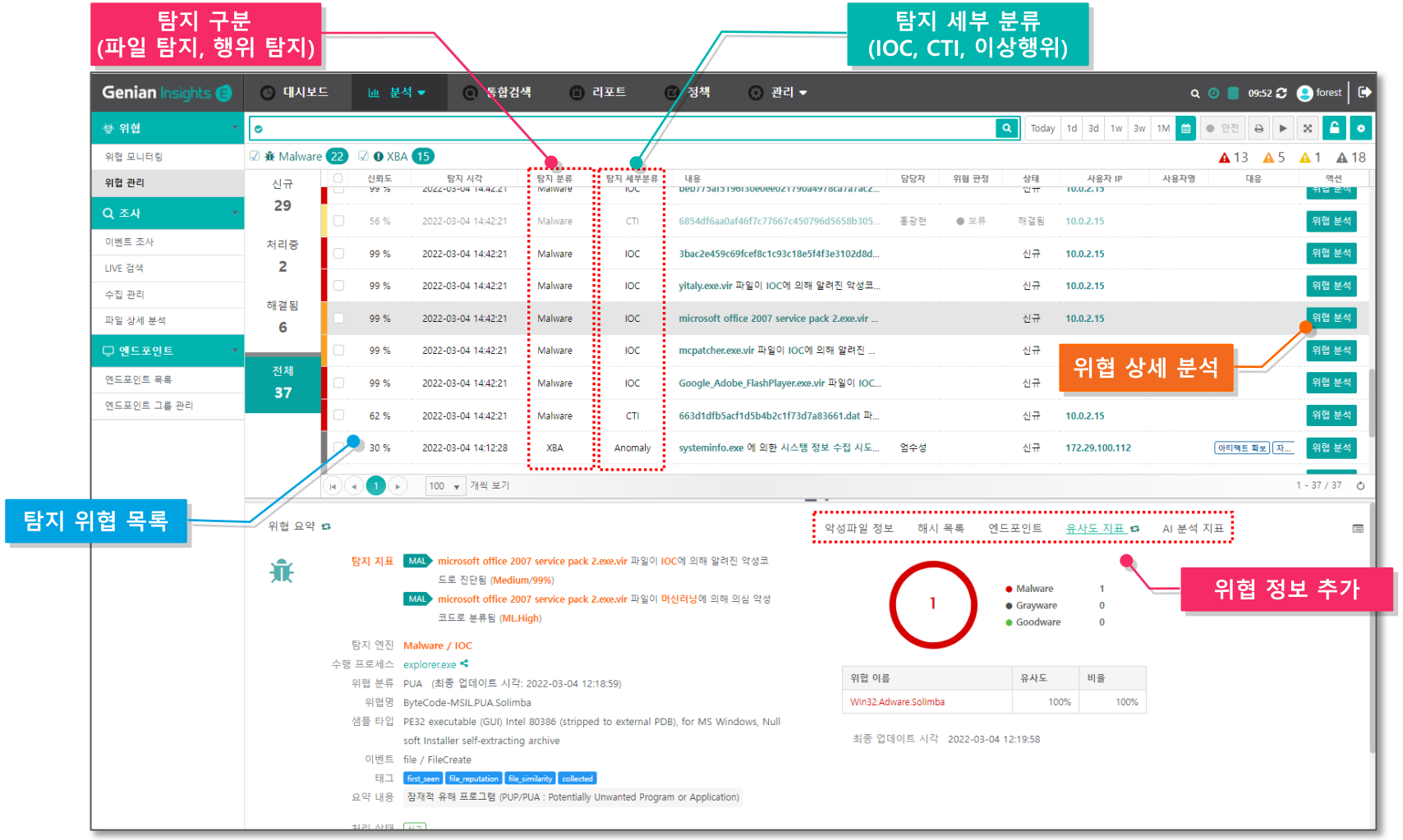


6) 분석

전체 위협에 대한 요약 정보를 보여주는 위협 모니터링화면을 제공합니다.

6) 분석

탐지된 위협 목록에서의 요약 정보와 상세 분석을 할 수 있는 기능을 제공합니다.



6) 분석

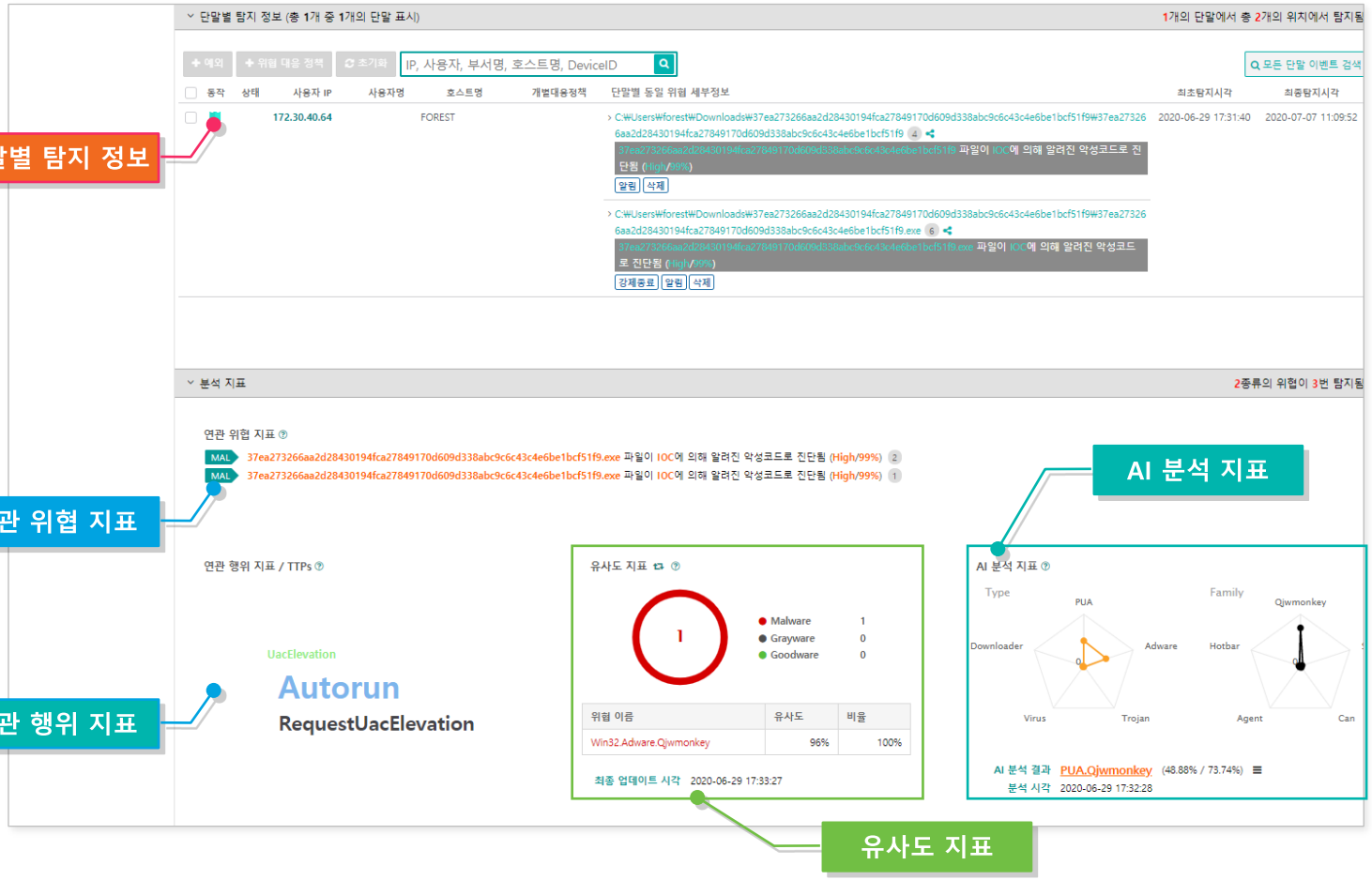
위협 상세 분석에서는 탐지된 파일의 위협 정보와 이상 행위(Fileless) 탐지 시 연관된 MITRE ATT&CK 링크를 제공합니다.

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

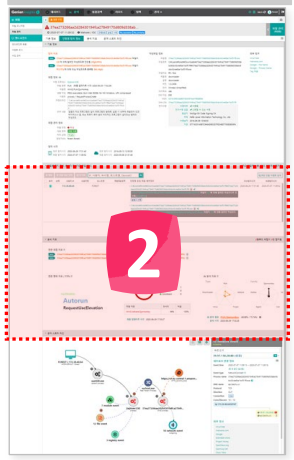
위협 분석 전체 화면

6) 분석

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

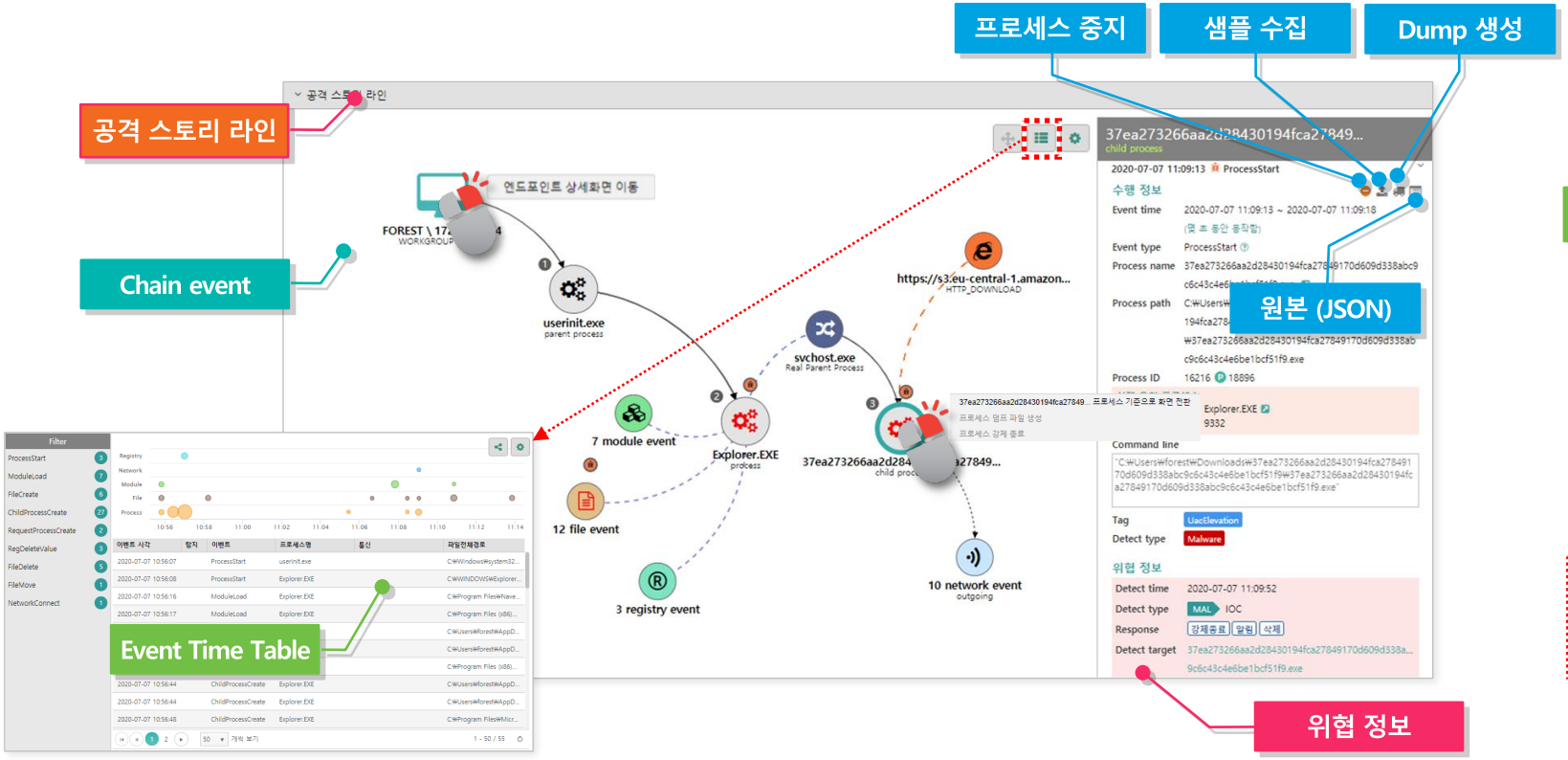


위협 분석 전체 화면



6) 분석

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

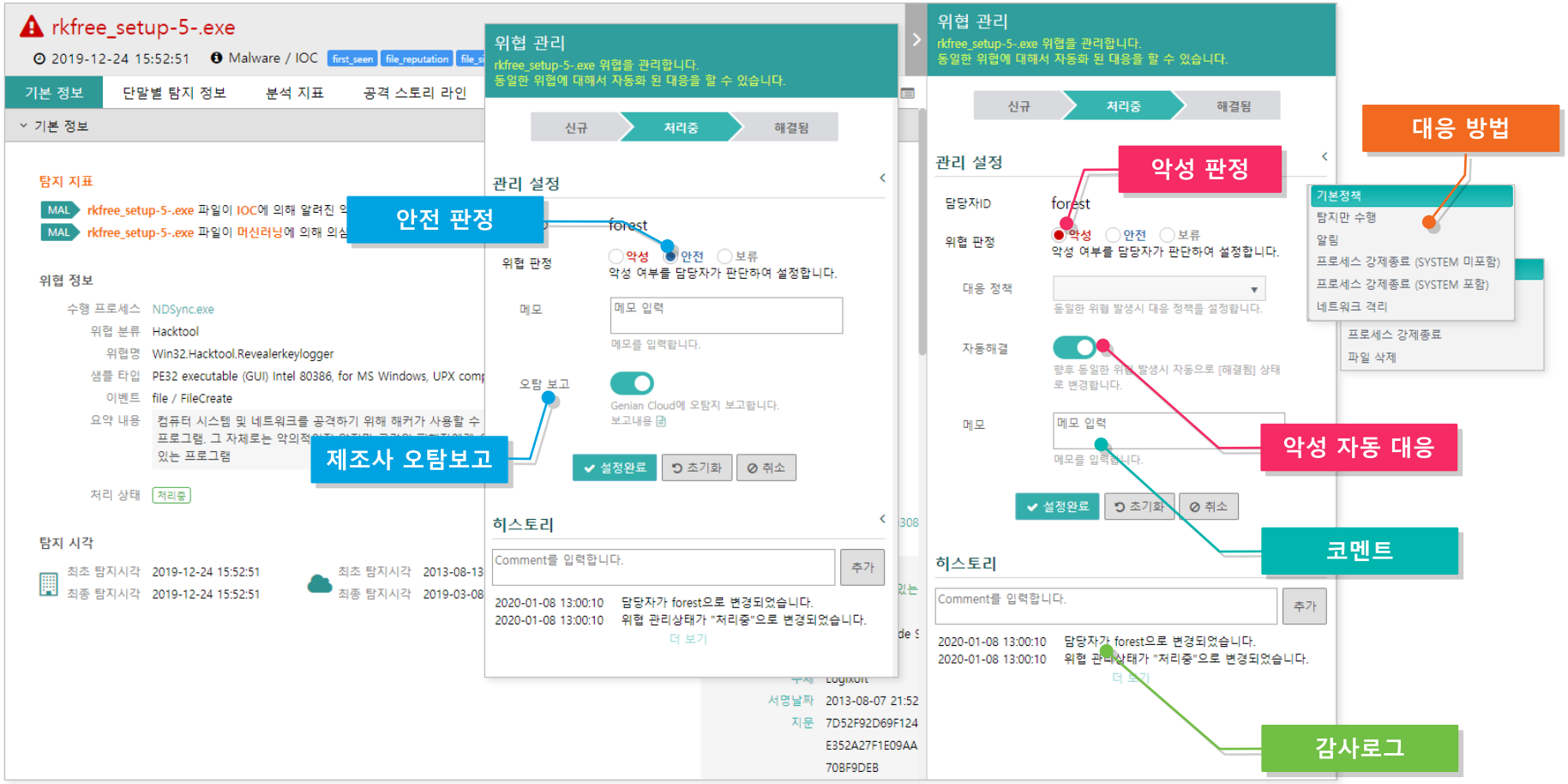


위협 분석 전체 화면

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

6) 분석

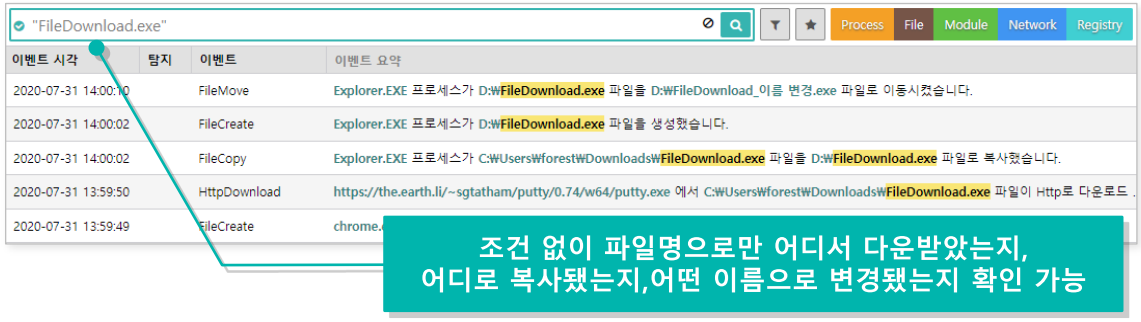
악성 파일에 대한 프로세스 중지, 격리, 사용자/관리자 알람, 네트워크 격리 등의 대응 기능을 제공합니다.



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.

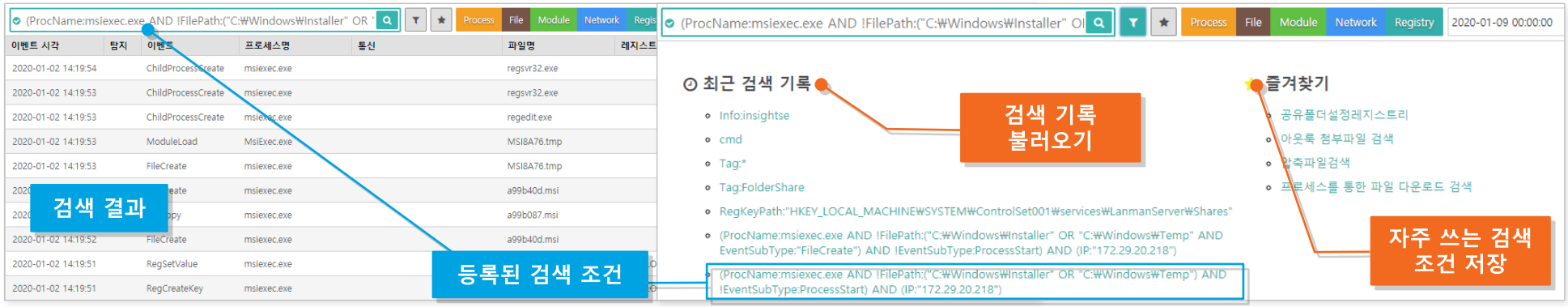
❖ FileDownload.exe 다운로드 ➔ C 에서 D 드라이브로 복사 ➔ D 드라이브에서 이름 변경



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")

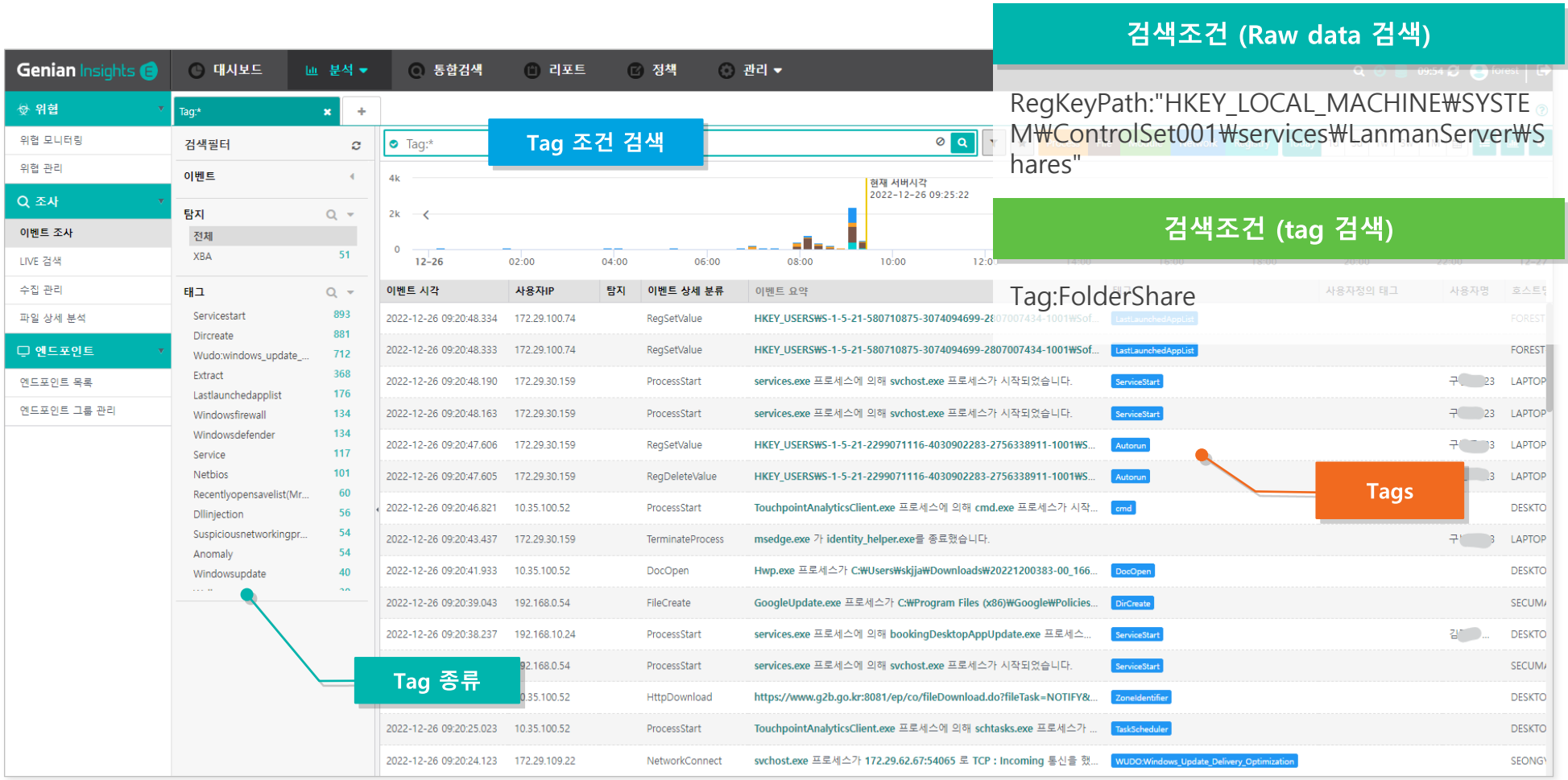


❖ 3개월 로그 39억 8천만 건 상황에서의 2가지 조건 검색 속도 : 약 3초

6) 분석

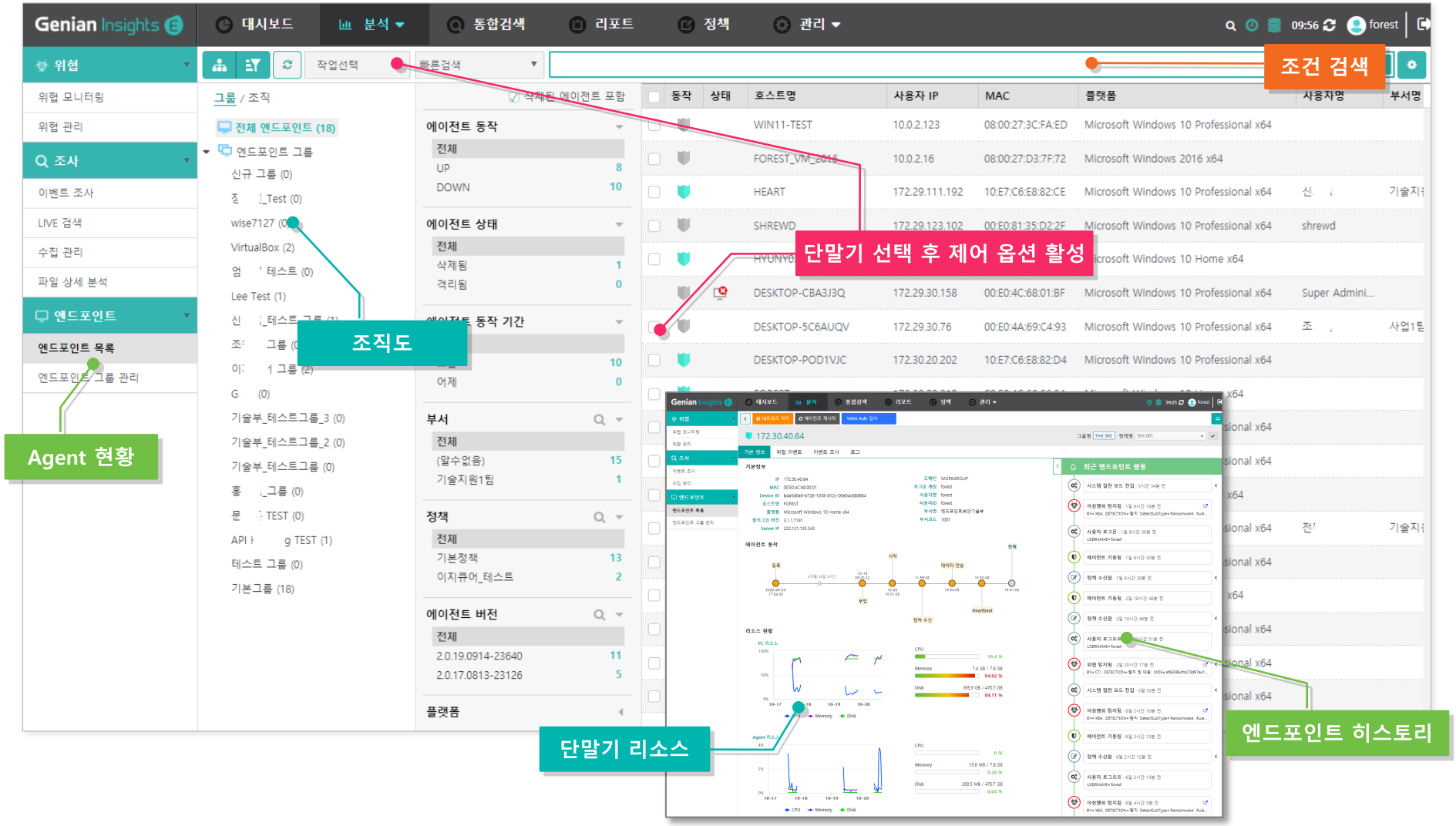
Into the unknown : TAGs

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



7) Agent 관리

설치된 Agent 현황 파악

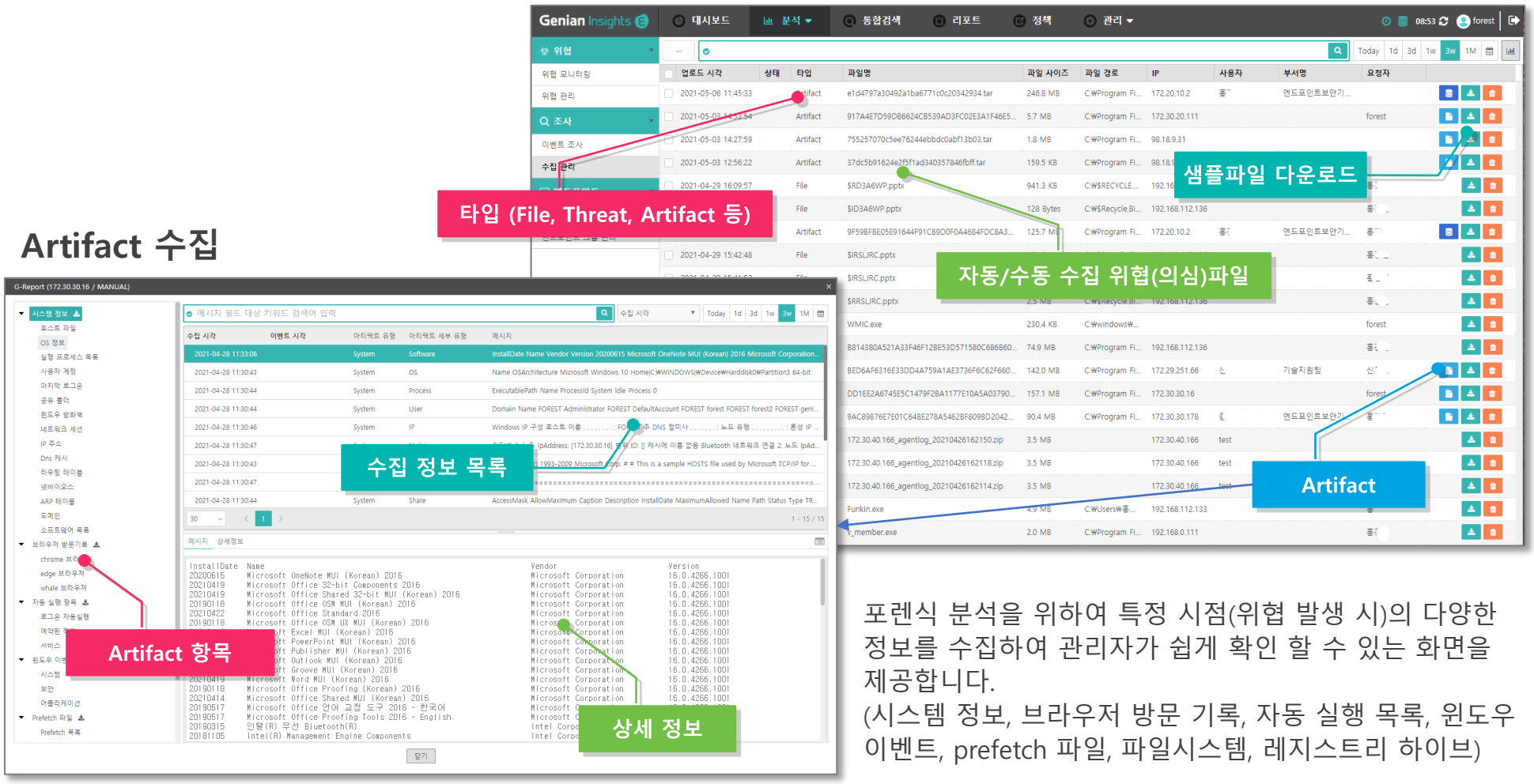


8) 수집관리

위협/의심파일(PE)은 선택에 따라 자동/수동 수집하고 필요시 artifact 를 수집하는 기능을 제공합니다.

탐지된 위협 파일은 사용자 PC 에서 자동/수동 업로드 (위협이 아닌 지정한 PE 파일 수동 수집 기능 제공)
필요시 특정 사용자 PC 의 artifact 수집

Artifact 수집



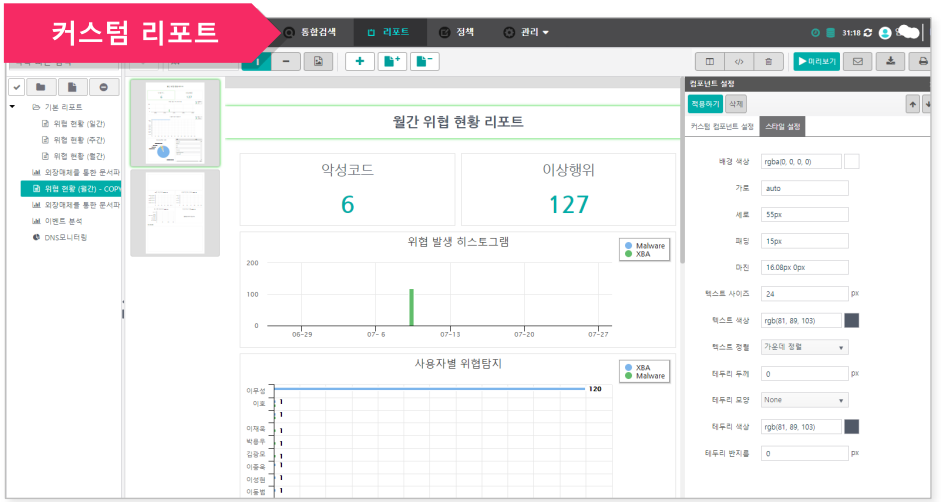
포렌식 분석을 위하여 특정 시점(위협 발생 시)의 다양한 정보를 수집하여 관리자가 쉽게 확인 할 수 있는 화면을 제공합니다.
(시스템 정보, 브라우저 방문 기록, 자동 실행 목록, 윈도우 이벤트, prefetch 파일, 파일시스템, 레지스트리 하이브)

9) 리포트

기본 제공 리포트와 대시보드를 리포트로 변환할 수 있습니다.
리포트는 관리자가 직접 생성/수정할 수 있도록 다양한 옵션을 제공합니다.

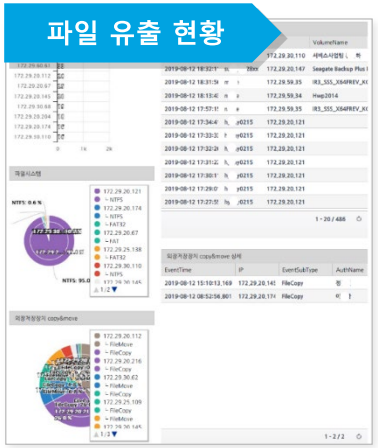
악성코드 탐지 현황

커스텀 리포트

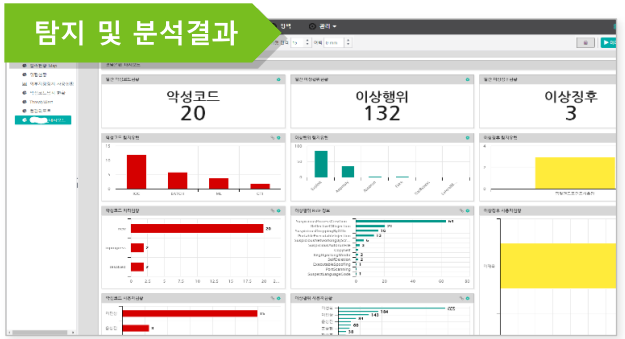


HTML 수정 가능

파일 유출 현황



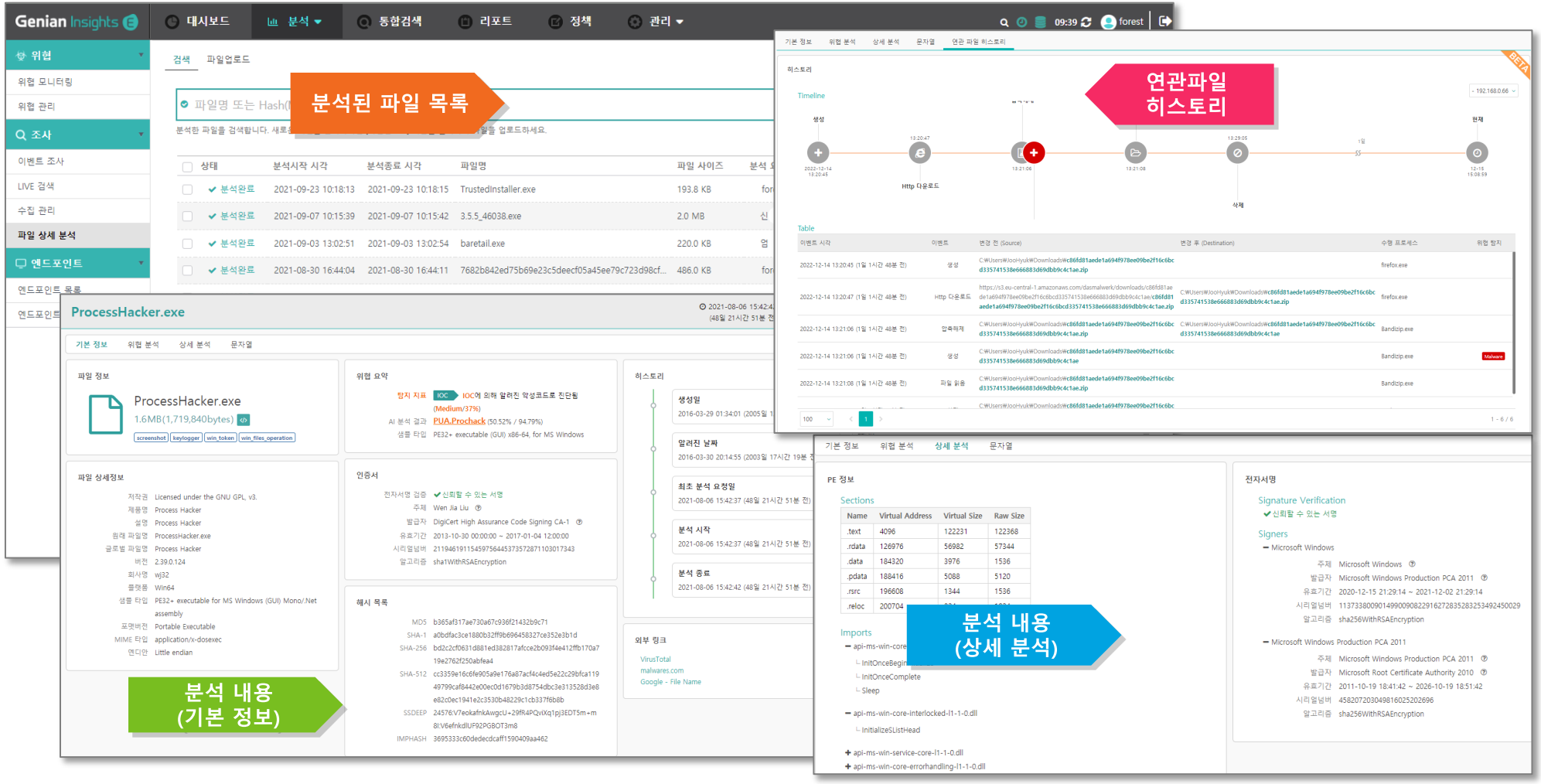
탐지 및 분석결과



10) 파일 상세 분석

추가 분석이 필요한 파일을 서버로 업로드하여 정적 분석 결과를 제공합니다.

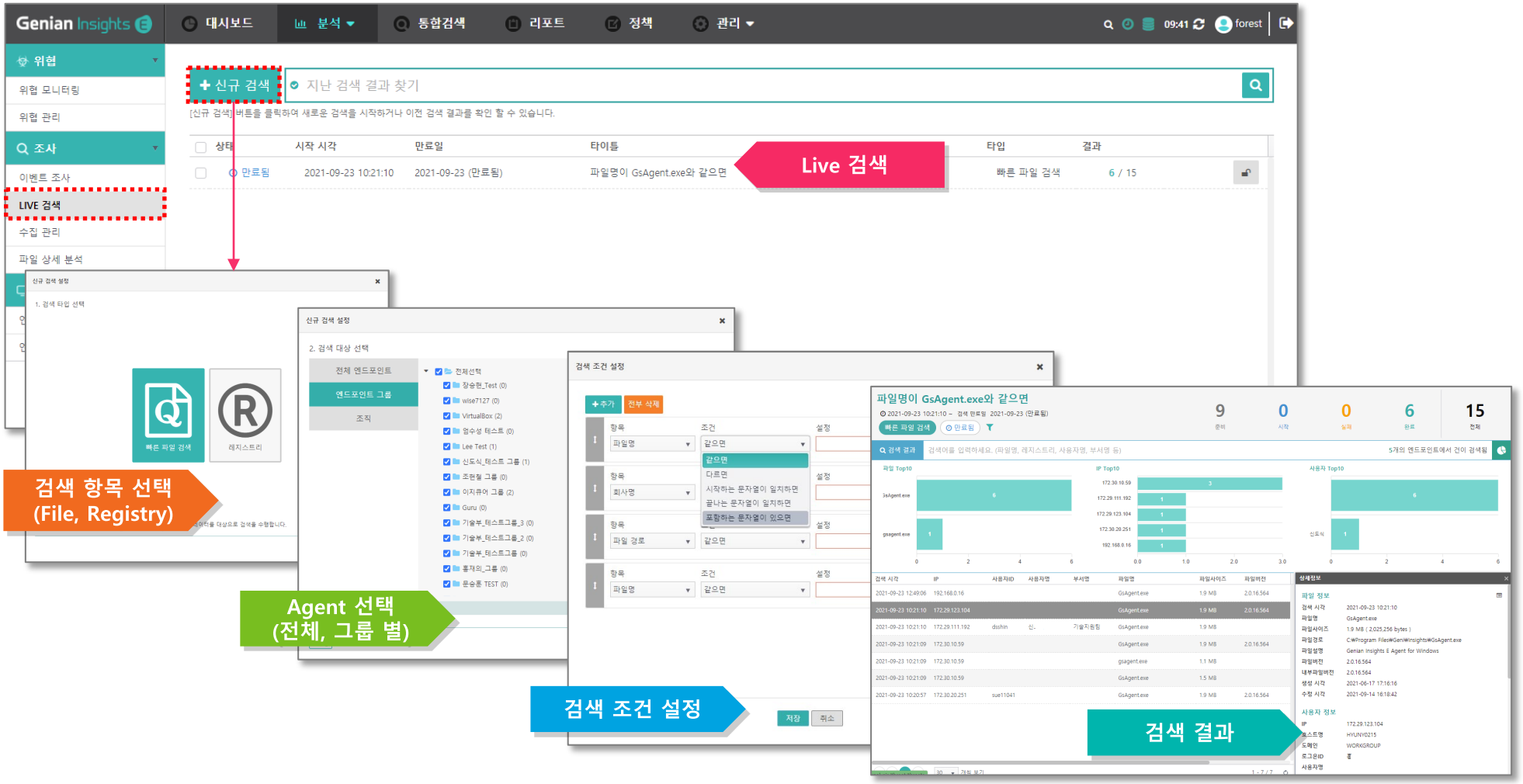
파일의 상세 정보, 문자열, 위협정보, PE정보, 전자서명, 최근 1달간 파일의 히스토리 정보 등



11) Live 검색

현재 PC 내에 존재하는 파일, 레지스트리를 검색하여 결과를 보여줍니다.

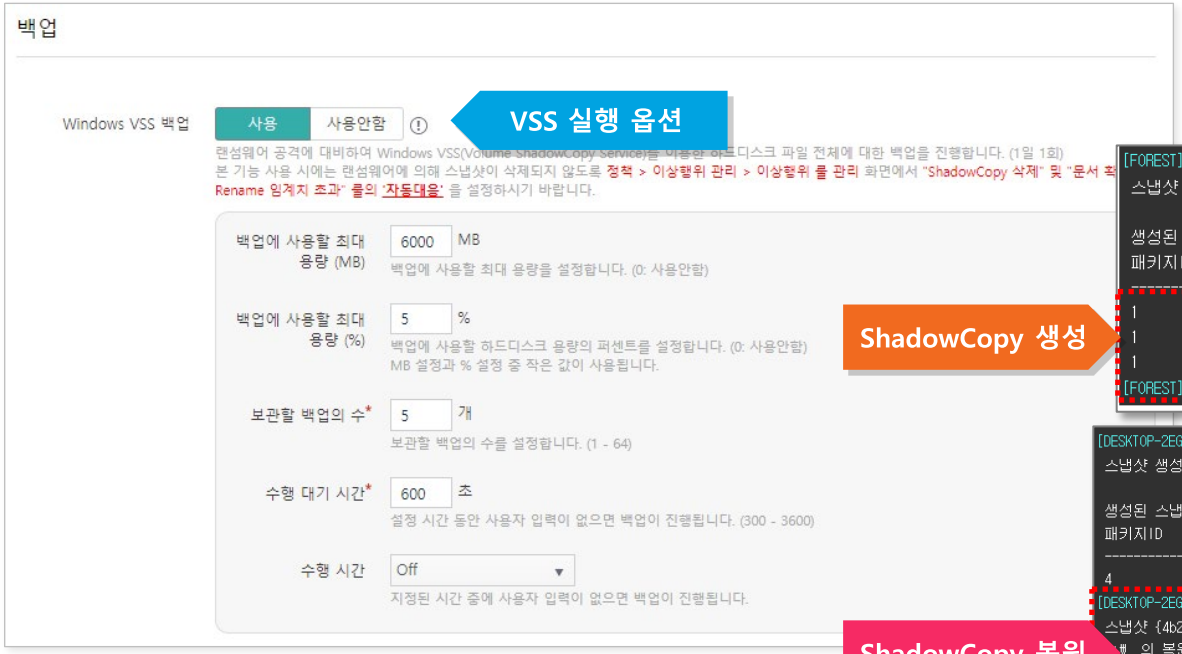
사용자 PC 내의 파일, 레지스트리를 다양한 조건 검색



12) VSS 관리

윈도우의 Window shadow copy 백업/복원 (Volume Shadow Copy Services) 서비스를 관리합니다.

사용자 PC 의 데이터를 디스크 내의 특정 용량 이내, 몇일, 백업 수행 시간 설정으로 snapshot 저장



ShadowCopy 생성

```
[FOREST] C:₩Program Files₩Genian₩Insights> shadowcopy /create
스냅샷 생성에 성공하였습니다. (패키지ID : 1)

생성된 스냅샷 정보 :
패키지ID    볼륨    스냅샷ID                                    생성일                상태
1           C:₩     {e1fc0cfe-c647-4741-a5a3-bbd9114328b9}      2021-01-21 17:28:32   SUCCESS
1           D:₩     {53bd8491-df53-46e2-80fb-95d930e6bbb1}      2021-01-21 17:28:38   SUCCESS
1           E:₩     {fee06af8-bf17-4e9f-9505-762c869fefcd}      2021-01-21 17:28:45   SUCCESS
[FOREST] C:₩Program Files₩Genian₩Insights>
```

ShadowCopy 복원

```
[DESKTOP-2EGDRNR] C:₩Program Files₩Genian₩Insights> shadowcopy /create C:
스냅샷 생성에 성공하였습니다. (패키지ID : 4)

생성된 스냅샷 정보 :
패키지ID    볼륨    스냅샷ID                                    생성일                상태
-------------------------------------------------------------------------------------------
4           C:₩     {4b2db4a0-0c09-4135-8d52-eb07ac4a89aa}      2021-01-21 18:25:51   SUCCESS
[DESKTOP-2EGDRNR] C:₩Program Files₩Genian₩Insights> shadowcopy /restore /all 4
스냅샷 {4b2db4a0-0c09-4135-8d52-eb07ac4a89aa} 이 "C:₩vss₩{4b2db4a0-0c09-4135-8d52-eb07ac4a89aa}" 에 마운트되었습니다.
₩ 의 복원 작업이 시작되었습니다.
복원 작업은 백그라운드로 진행되며, 복원 완료 시 결과가 감사 로그에 기록됩니다.
[DESKTOP-2EGDRNR] C:₩Program Files₩Genian₩Insights>
```

File 복원 결과

2021-02-15 17:17:18		192.168.0.19	CC:3D:82:34:D1:E0	ShadowCopy 복원 완료 (총 35 파일 복원됨). VOLUME='D:₩'
2021-02-15 17:17:18		192.168.0.19	CC:3D:82:34:D1:E0	ShadowCopy 복원 시작. VOLUME='D:₩'
2021-02-15 17:17:17	에이전...	192.168.0.19	CC:3D:82:34:D1:E0	명령 전송됨. COMMAND='shadowcopy /restore /all 3', SESSIONID='forest_20210215171620808', ID='fore...
2021-02-15 17:16:33	에이전트	192.168.0.19	CC:3D:82:34:D1:E0	ShadowCopy 스냅샷 생성 성공 (D:₩).
2021-02-15 17:16:32	에이전...	192.168.0.19	CC:3D:82:34:D1:E0	명령 전송됨. COMMAND='shadowcopy /create D:', SESSIONID='forest_20210215171620808', ID='forest', I...

13) 안티랜섬웨어 기능

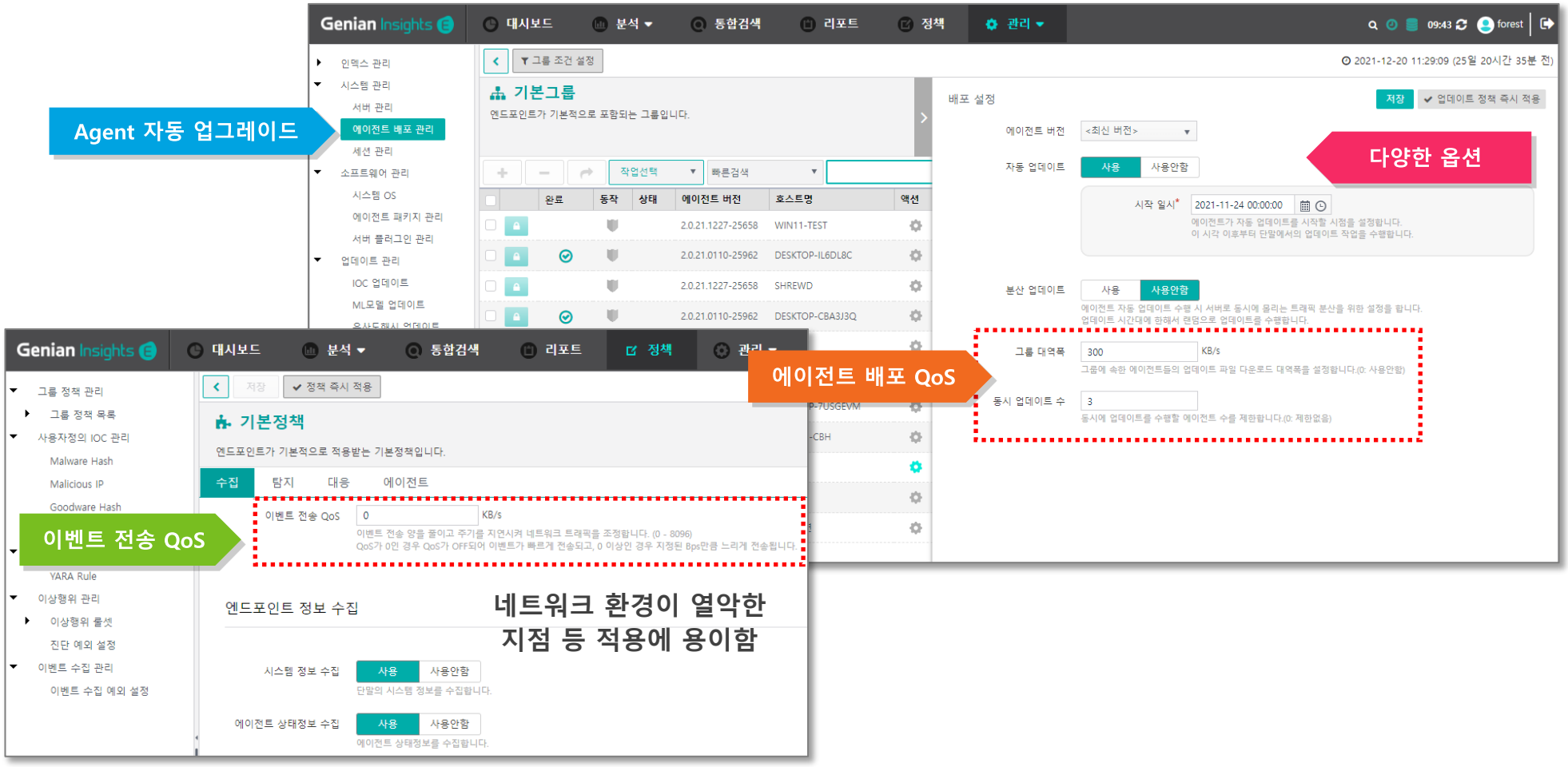
윈도우 볼륨 새도우 카피보다 효율적이고 고도화된 안티랜섬웨어 기능을 제공합니다.

실시간 탐지 및 백업과 복원 기능 제공 (추가 라이선스 필요함)

14) QoS 기능

Agent 업그레이드, 이벤트 전송 시 QoS 기능으로 네트워크 부담 없이 배포, 전송할 수 있습니다.

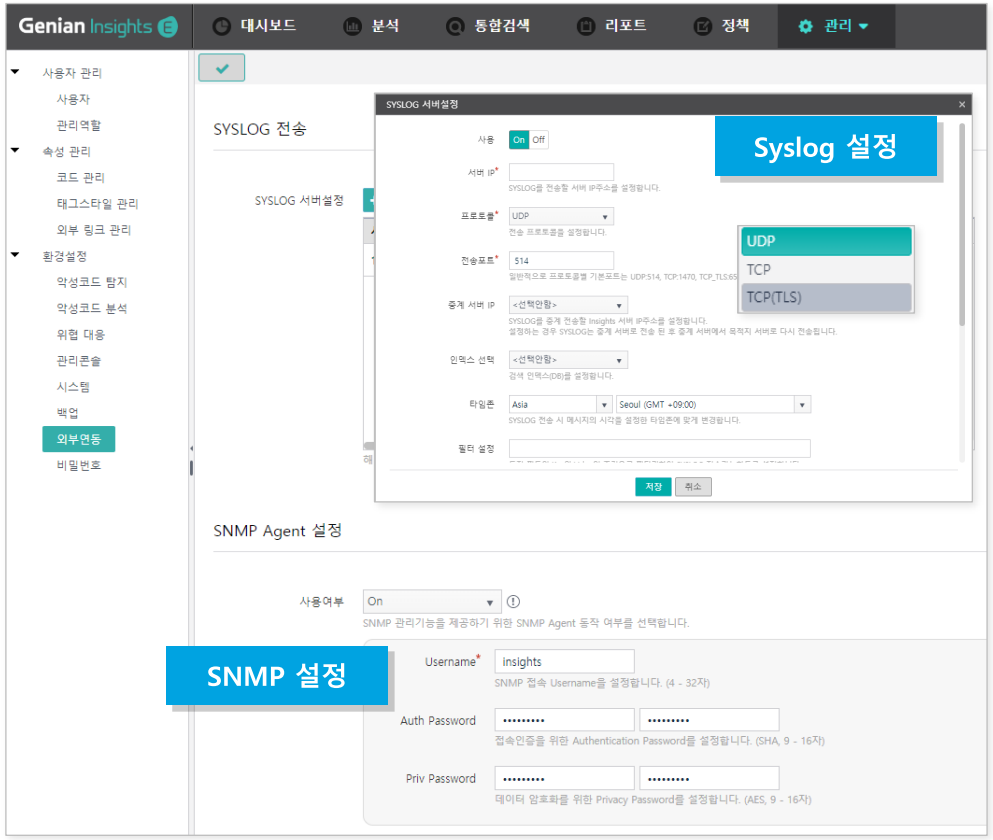
다양한 옵션 및 그룹 관리를 통해 agent 업그레이드 및 이벤트 전송 시 네트워크에 부담을 주지 않는 옵션



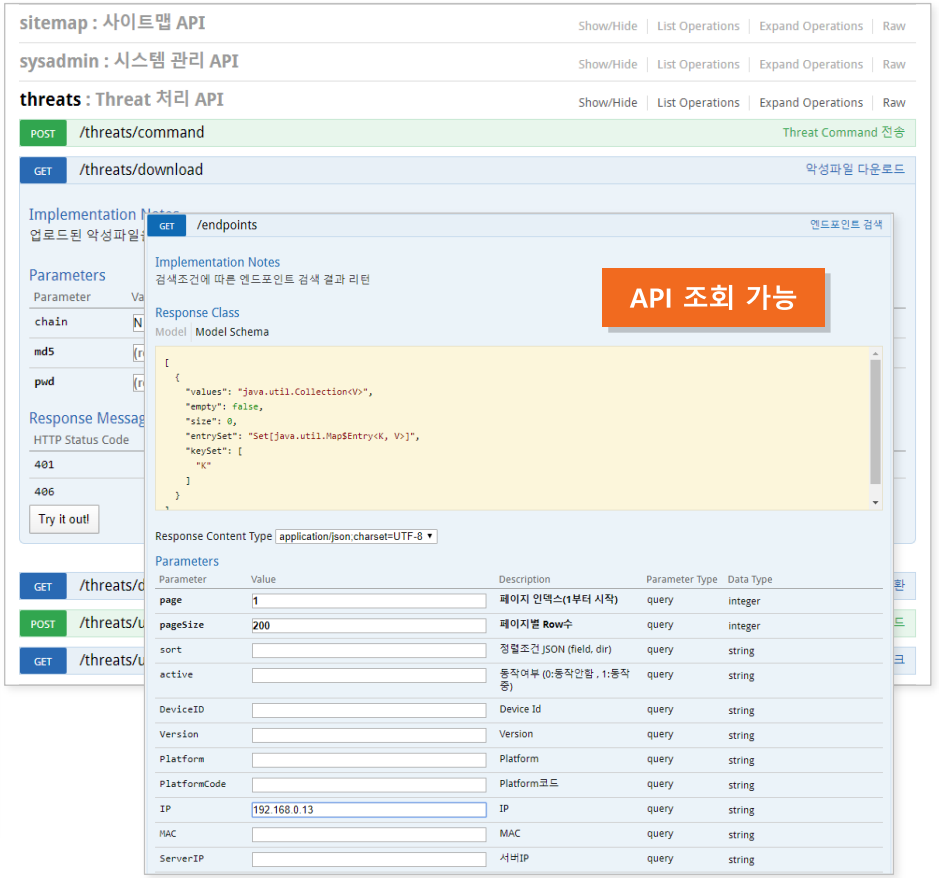
15) 연동

Syslog, SNMP, Rest API 를 지원, 타 시스템과 다양한 연동을 지원합니다.

※ Syslog, SNMP 설정



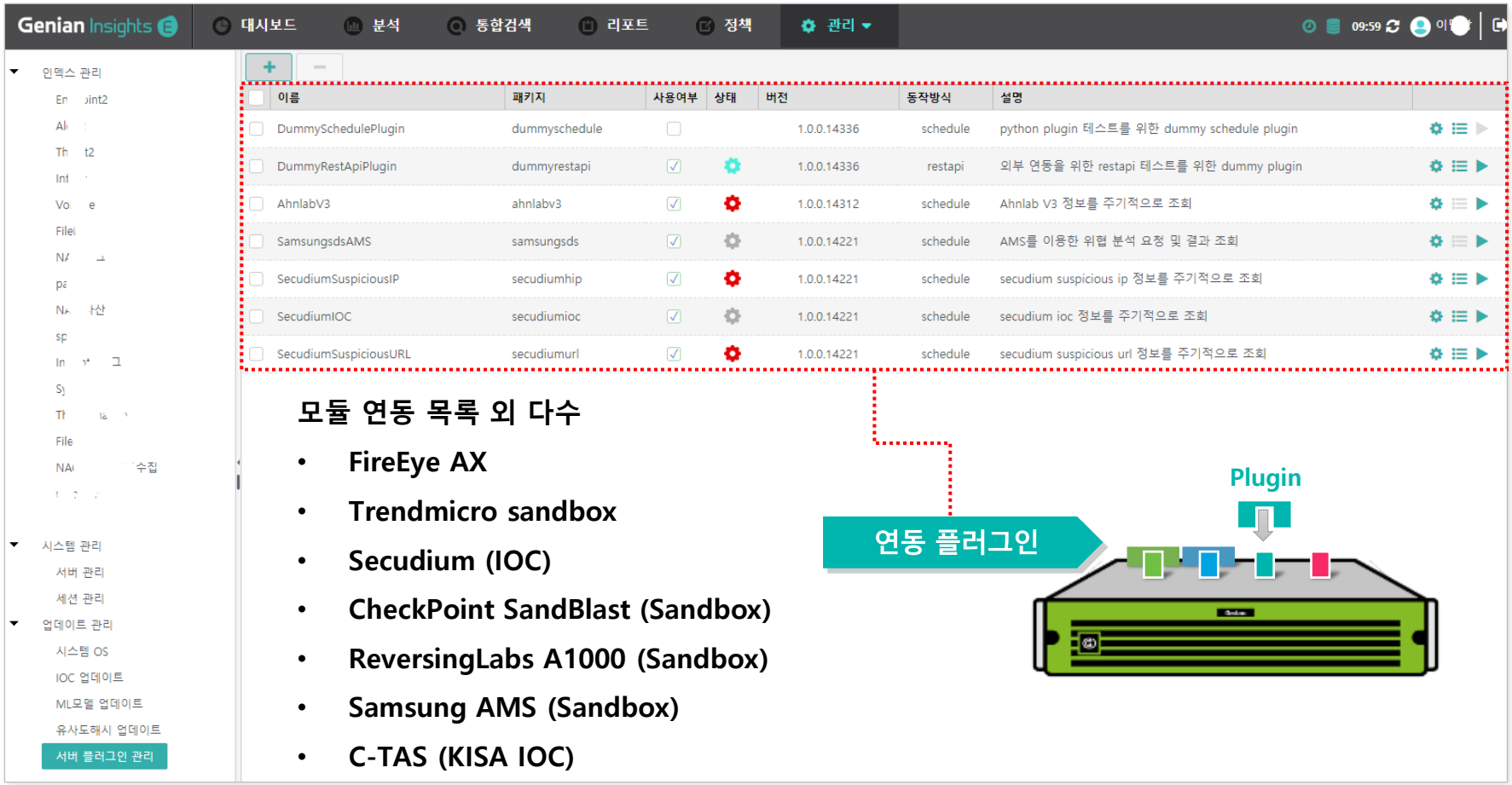
※ REST API



15) 연동

Syslog, SNMP, Rest API 외의 다양한 연동이 될 수 있도록 연동 플러그인(모듈)을 개발하여 적용할 수 있습니다.

연동 플러그인 적용으로 서버 업그레이드 불필요



03.

Genian EDR 도입 효과

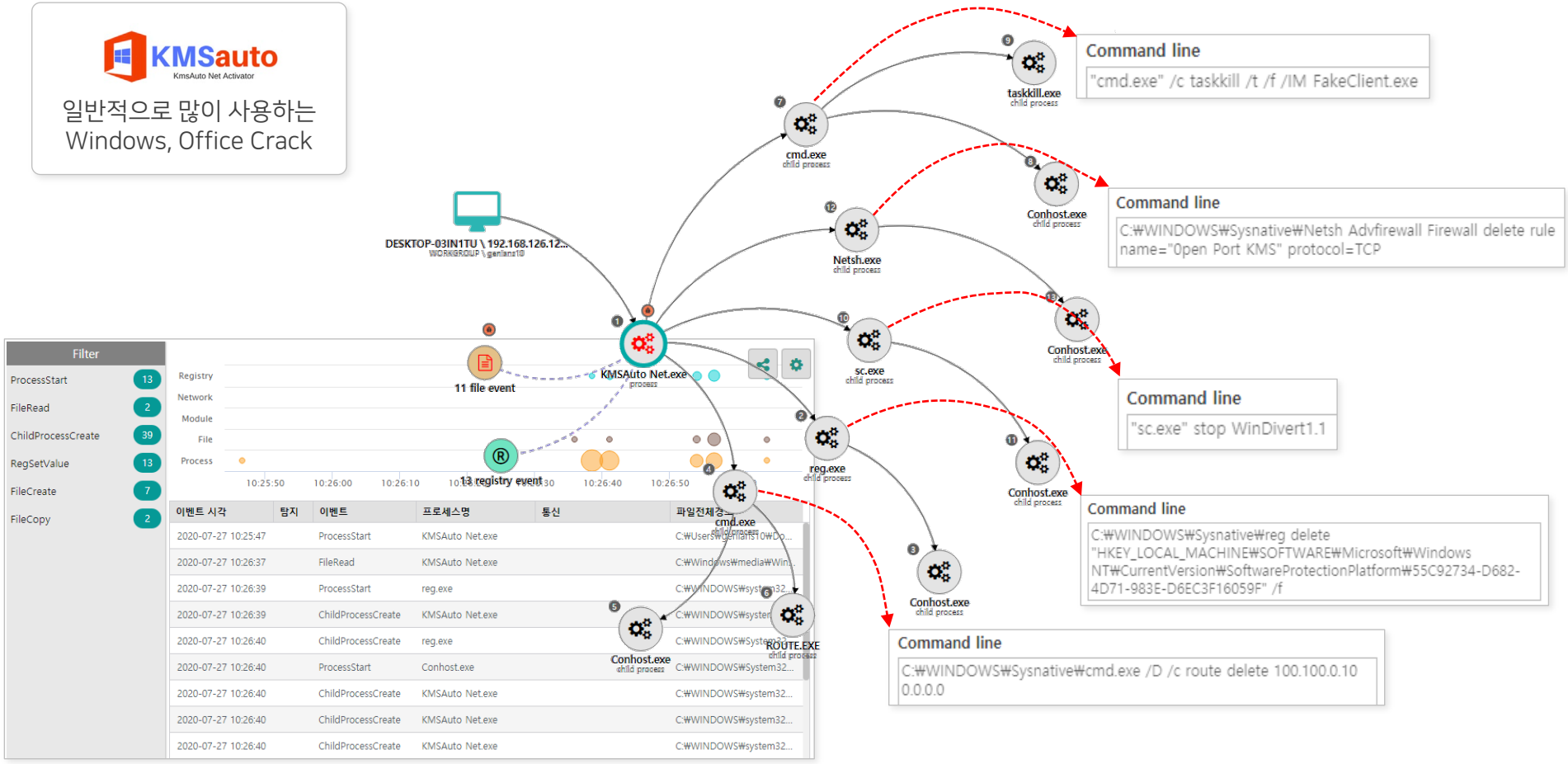
침투 경로와 행위에 대한 파악

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

KMSauto
KmsAuto Net Activator

일반적으로 많이 사용하는
Windows, Office Crack



엔드포인트의 다양한 정보 제공

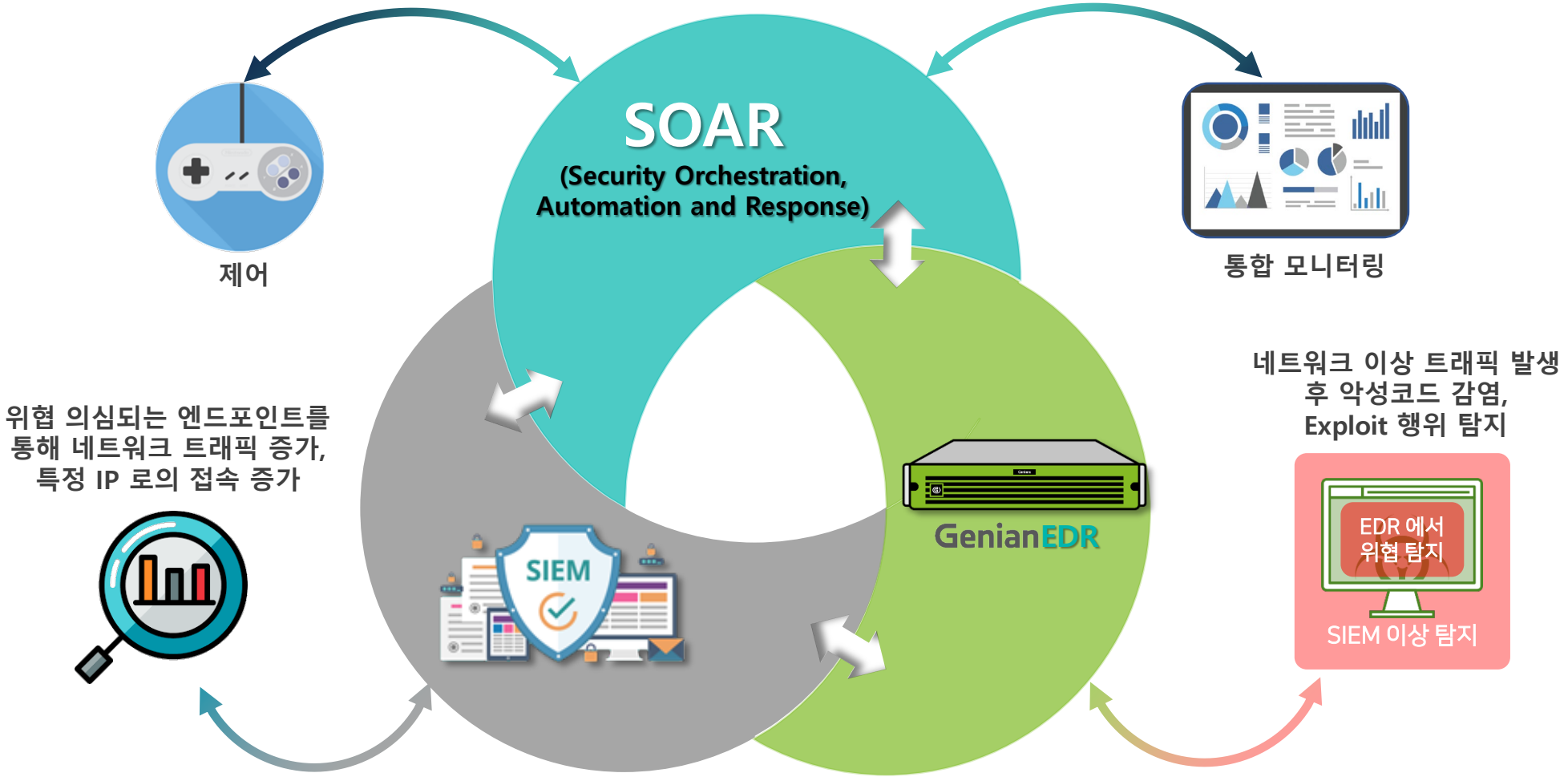
대시보드는 다양한 커스터마이징을 통해 엔드포인드의 가시성을 극대화 합니다. (Endpoint Discovery)

위협 탐지를 위해 수집한 로그는 원하는 다양한 형태의 대시보드로 구성하여 사용자 PC 내에서 발생하는 행위를 쉽게 모니터링
내부 정책 위반, USB 등의 저장 장치를 통한 문서 이동, 내부 시스템 접속, AP 접속 현황 등 기존 확인할 수 없던 정보 제공

DATA(데이터) → **INFORMATION(유용한 정보)**

네트워크와 엔드포인트의 연관성, 그리고 SOAR

SIEM, SOAR 연동하여, 네트워크 상의 이상 행위가 엔드포인트에서의 악성 행위나 악성파일 탐지와 연관이 있는 지에 대한 분석과 자동 대응 및 모니터링을 할 수 있습니다.



통합 보안 플랫폼 기업, 지니언스

PC 가시성의 모든 것

Genian EDR v2.0

THANK YOU :)

Genians