통합 단말 보안 플랫폼

Genian Insights E v3.0

Genians

Table of Contents

I. Insights E v3.0

- 신규 기능

Insights E v3.0

✓4개의 신규 기능 + 2개의 신규 서비스

Anti-Virus(백신)

- EDR + AV = One Agent
- AV 단독 운영 가능
- Linux 백신 지원

멀티 OS

- Windows OS/Server
- Linux (Red hat, Debian etc)
- Mac OS

매체제어(Media Control)

- 외장 저장 매체 관리
- 공유 폴더 관리
- 안전 모드 진입 관리

Insights E ver.Cloud

- Cloud 기반 EDR 솔루션
- 고객 환경에 맞춤형 솔루션 제공 가능
- SaaS 방식 서비스 제공(AWS)

MDR

- Managed Service 제공
- 탐지 위협 정기 보고 및 이슈 전달

** 외부 연결 필요

GSC(Genians Security Center)

- 침해사고대응 전문 조직 운영
- 운영컨설팅 서비스 제공
- 침해사고 발생 시 기술 지원

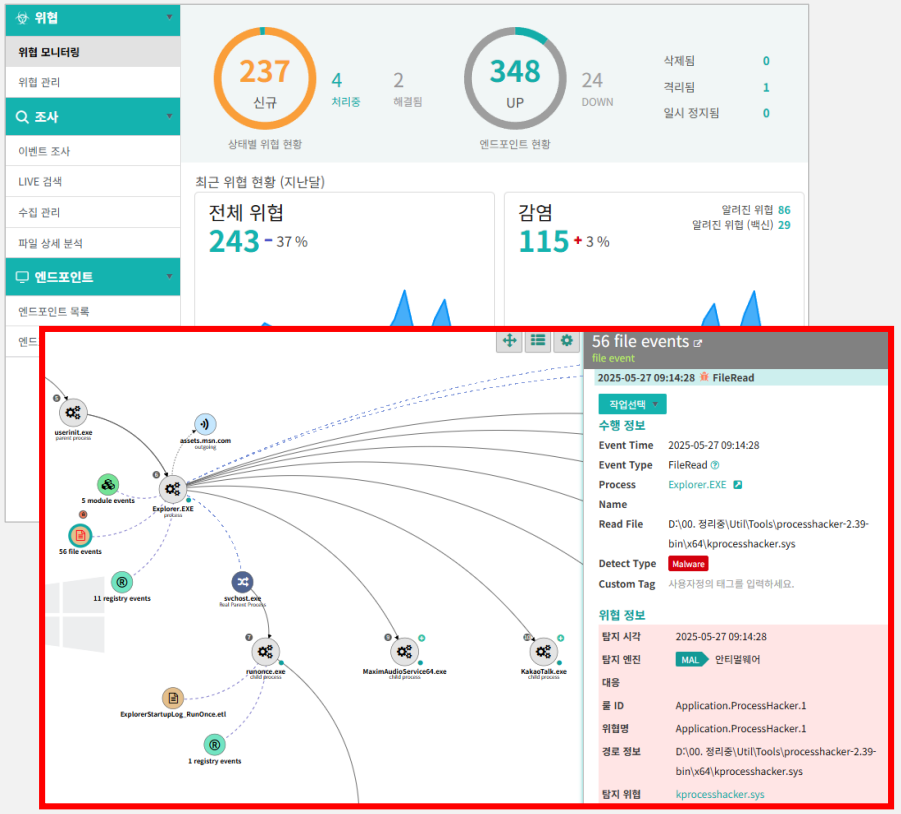
신규 기능 #1 : 백신(Anti-Virus)

✓Anti-Virus

악성파일 탐지 향상을 위해 백신 엔진 추가

Anti-Virus에서 탐지된 위협에 대해 단순 탐지 결과가 아닌 프로세스 간 관계, 행위 트리, 실행 경로 등 EDR 수준의 맥락 정보 제공

관리자 화면 (백신 엔진 탐지 이벤트)



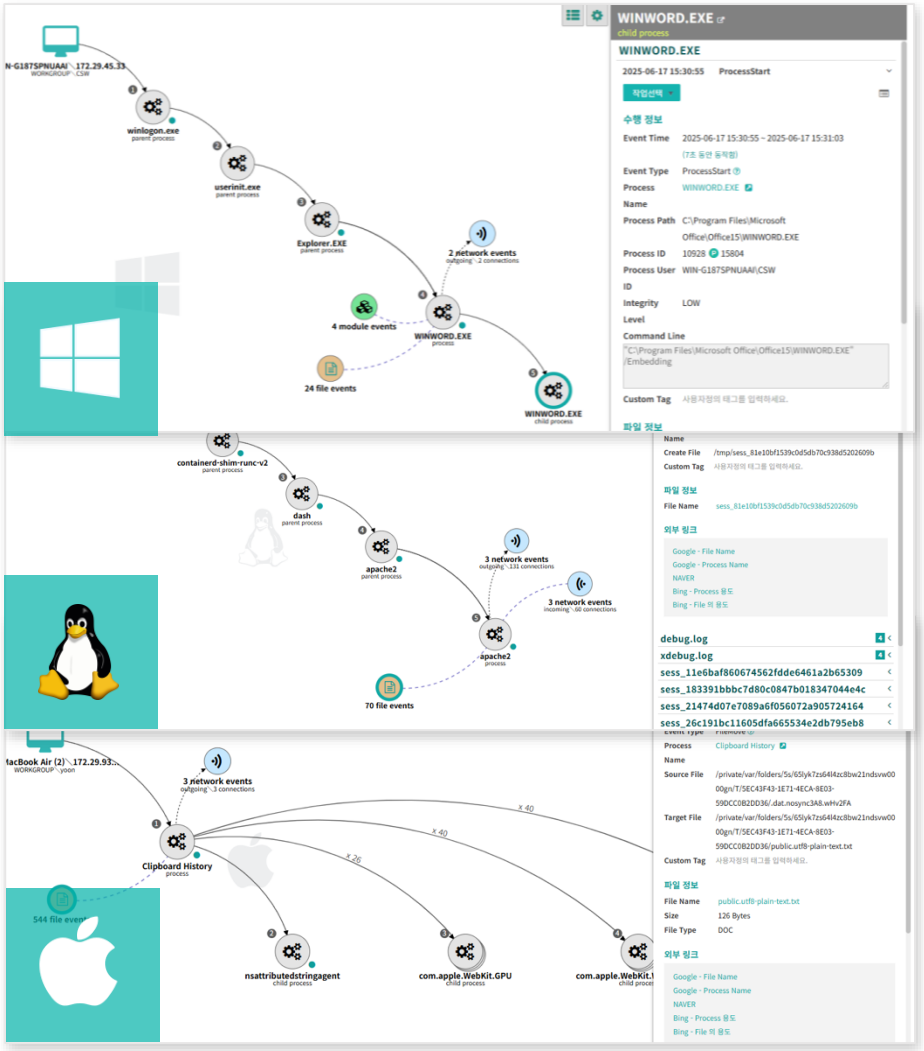
사용자 화면 (사용자 PC 백신 UI)

옵션
(별도 라이선스 필요)

신규 기능 #2 : 멀티 OS 지원

Insights E는 Windows 뿐만 아니라 Linux, macOS 도 지원

Windows	Linux	macOS
Windows 7 (SP1) 이상 ※ hotfix (kb4474419) 적용 필요	**[eBPF 지원 OS]** CentOS 8.4 이상 RHEL 8.4 이상 Rocky 8.4 이상 Ubuntu 20.04.5 이상 Fedora 42 openSUSE 15 ※ 프로세스, 파일, 네트워크 통신 이벤트 수집/대응	11 Big Sur 12 Monterey 13 Ventura 14 Sonoma 15 Sequoia 26 Tahoe (안정화 검증)
ServerServer 2012 이상 (2012 R2, 2016, 2019, 2022, 2025)	**[eBPF 미지원 OS]** CentOS 6.4~8.3 RHEL 6.4~8.3 Ubuntu 18.04, 20.04 Oracle Linux 6.9~8.9 SUSE Linux 11, 12(sp4) openSUSE 11, 12 ※ 프로세스 및 특정 경로의 파일 이벤트 수집/대응 ※ 네트워크 통신 이벤트 수집은 개발 진행 중	



신규 기능 #3 : 매체 제어

✓매체 제어 / 공유 폴더 제어 및 안전모드 진입 방지

- 통제 정책 : 허용/읽기전용/차단
- 공유 폴더 제어 : 허용/everyone 권한 제거/공유 해제
- 안전모드 진입 방지 : 안전모드 진입 패스워드 설정을 통한 화면 차단

Safe mode screen

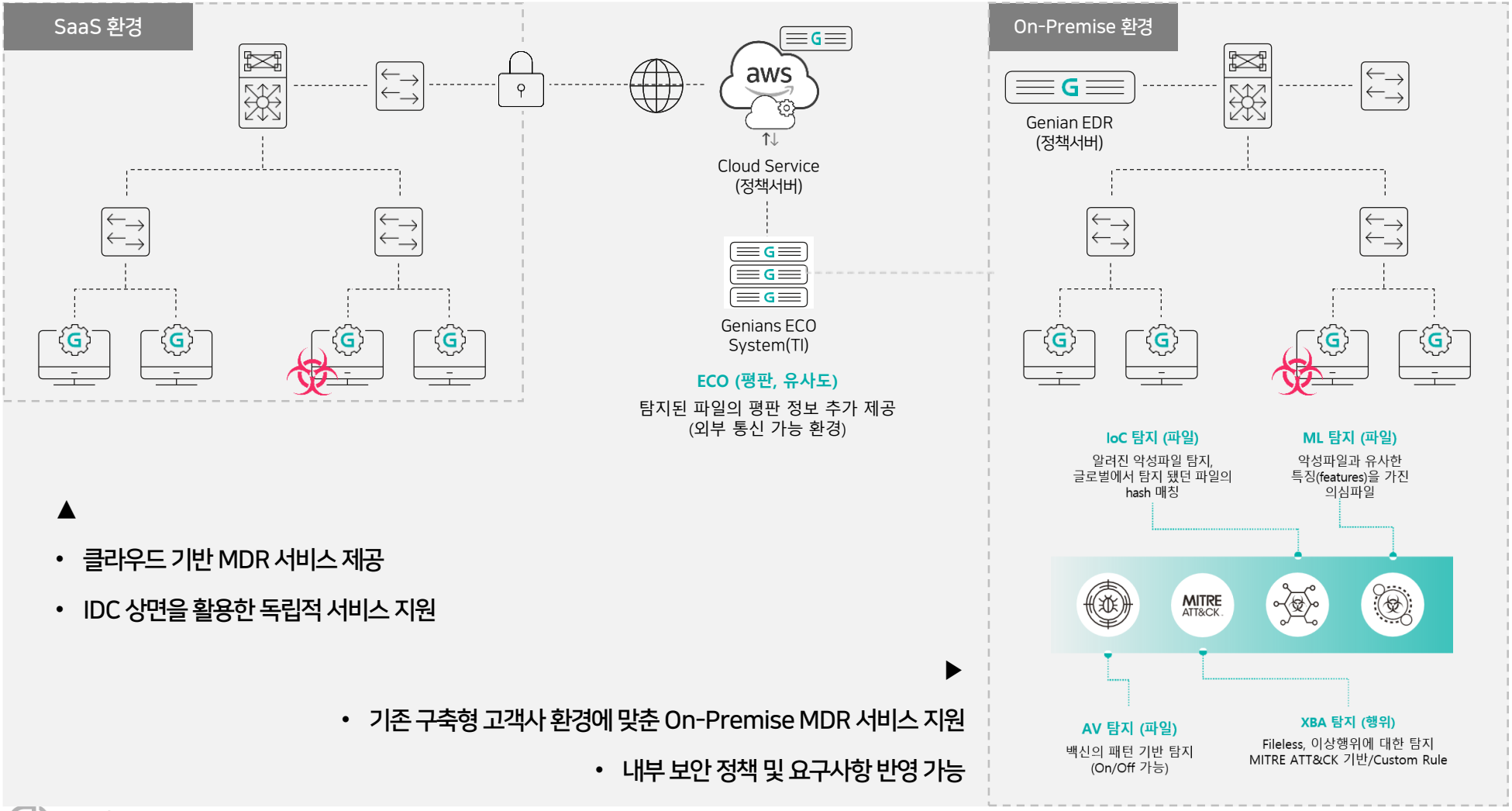
Agent layer

※ 패스워드 입력 시 안전모드 사용 가능

옵션
(별도 라이선스 필요)

신규 기능 #4 : Cloud 지원

✓모든 환경에서 유연한 서비스 제공(SaaS · IDC · On-Premise)



▲

- 클라우드 기반 MDR 서비스 제공
- IDC 상면을 활용한 독립적 서비스 지원

▶

- 기존 구축형 고객사 환경에 맞춘 On-Premise MDR 서비스 지원
- 내부 보안 정책 및 요구사항 반영 가능

신규 서비스 # 1 : MDR

지능화되고 자동화된 사이버 공격이 증가하고, 기업 내부 보안 인력 부족과 복잡한 보안 환경에 따른 대응 한계가 심화됨에 따라, 엔드포인트에 대한 지속적인 모니터링과 전문적인 위협 대응 서비스를 제공하는 MDR(Managed Detection and Response) 체계의 필요성이 더욱 강조되고 있습니다.

지능화되고 자동화된 사이버 공격

최근 사이버 공격은 더욱 정교해지고 자동화되어 기존
보안 솔루션만으로는 완벽한 방어 어려움/ 새로운 공격 기법을 지속적으로
개발하며 기업의 취약점 공격

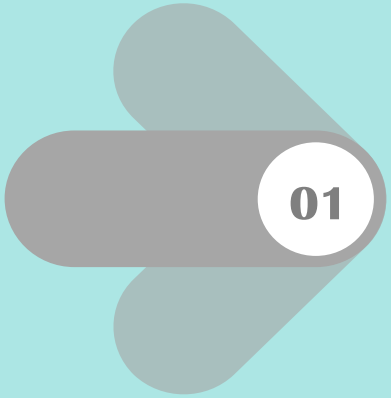
전문 인력 부족 및 운영 부담 증가

내부 보안팀은 전문 인력 부족
늘어나는 보안 위협에 대응하기 어려워 운영 부담이 증가
또한, 최신 보안 기술을 위한 교육 및 훈련의 필요성 증대

Genian MDR은 단말에 대한 지속적인 모니터링과 상시정보 수집을 통해 위협을 탐지하고
분석/대응을 제공하는 단말 이상 행위 탐지 및 대응(Managed Detection & Response) 서비스 입니다.

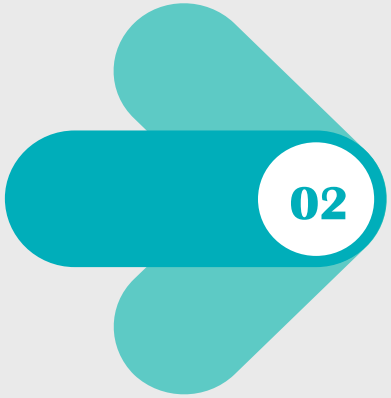
신규 서비스 # 1 : MDR

Insights E MDR 서비스 : 위협 탐지 · 분석 · 대응 · 리포트 제공



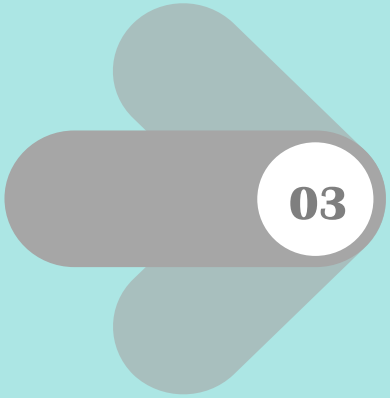
단말 행위 모니터링/수집

- File, Module, Process, Connection, Registry 정보
- 사용자 및 엔드포인트에서 발생하는 이상 행위
- 외부 저장매체 사용 현황
- 윈도우 이벤트 로그 수집
- 다양한 대시보드 제공



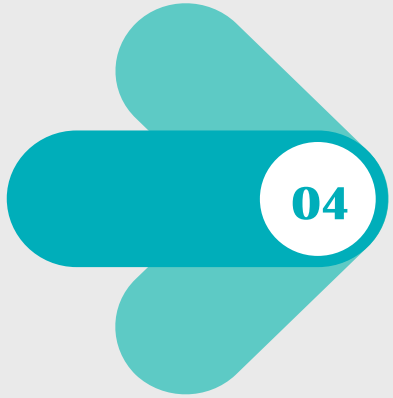
위협의 탐지

- 침해지표(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



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



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(평한서비스) 제공

MDR 보안 관제 위협 대응 보고서

Genian MDR 서비스는 위협 탐지부터 분석, 대응, 예외 처리에 이르는 전 과정을 정량화된 이벤트 분석 및 전문 보고서 형태로 제공하여, 보안 사고에 대한 대응 이력과 조치 결과를 체계적으로 기록하고 고객에게 투명하게 전달합니다.

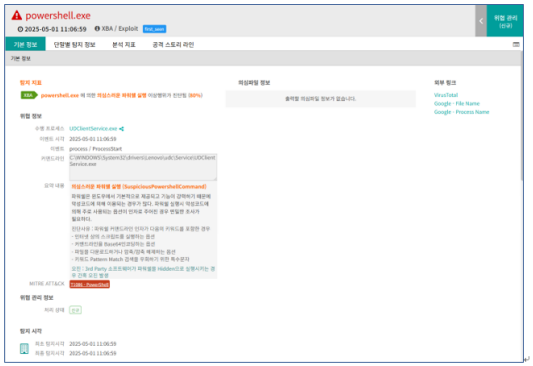
위협 대응 보고서 I

MDR 대응 보고서

개요

1.1 위협 개요

고객사 " Genian EDR 의 XBA(사용자 행위 기반 이상 탐지) 기능을 통해 " " 행위가 탐지되었으며, 이를 통해 악성코드 감염 정황이 확인되었습니다.



[그림 1] EDR 위협 상세 분석 화면 일부

항목	내용
고객사	*
보안 시스템	Genians EDR
탐지 일시	2025 년 *월 *일 *시*분
위협 구분	XBA 탐지
탐지 시나리오	*

위협 대응 보고서 II

대응

2.1 초기 대응

해당 위협 탐지 후, 악성코드 확산을 차단하고 피해를 최소화하기 위한 초동 대응이 이루어졌으며, 관련 조치 내역은 아래 표와 같습니다.

항목	내용
감염 단말 조치	해당 단말의 네트워크를 즉시 격리하여 외부 접속 차단 (네트워크 격리)
악성코드 제거	악성 파일 및 예약 작업 제거 수행
로그 수집	초기 정투 관련 로그 분석 수행
고객사 담당자	탐지된 위협 내용 유선 전달

2.2 피해 범위

Cloud NAC 을 활용하여 특정 악성 파일 및 관련 프로세스의 존재 여부에 대한 점검을 수행하였습니다.

항목	내용
검사 항목	악성 파일 존재 및 '*.exe' 프로세스 동작 여부
검사 방식	Cloud NAC 기반 전사 점검 수행
검사 결과	파일 존재 단말 : 0 대 프로세스 실행 단말 :0 대

신규 서비스 # 2 : 침해사고 대응 센터 운영

Genian Security Center를 통해 최신 위협 인텔리전스 기반의 실시간 탐지와 신속 대응을 제공하여 기업 보안 수준을 강화합니다.

GSC [Genians Security Center]

제조사 직접 운영 지원

Genian MDR은 제조사가 직접 운영·관리하여 최신 위협 인텔리전스와 전문적인 보안 노하우를 바탕으로 기업의 보안을 강화합니다.

최신 위협 인텔리전스 반영

Genian MDR은 최신 위협 인텔리전스를 지속적으로 업데이트하여 새로운 위협에 빠르게 대응하고, 기업의 보안 수준을 향상시킵니다.

기업별 맞춤형 보안 정책 최적화

Genian MDR은 기업의 특성에 맞는 보안 정책을 수립하고, 지속적으로 모니터링하여 최적의 보안 환경을 제공합니다.

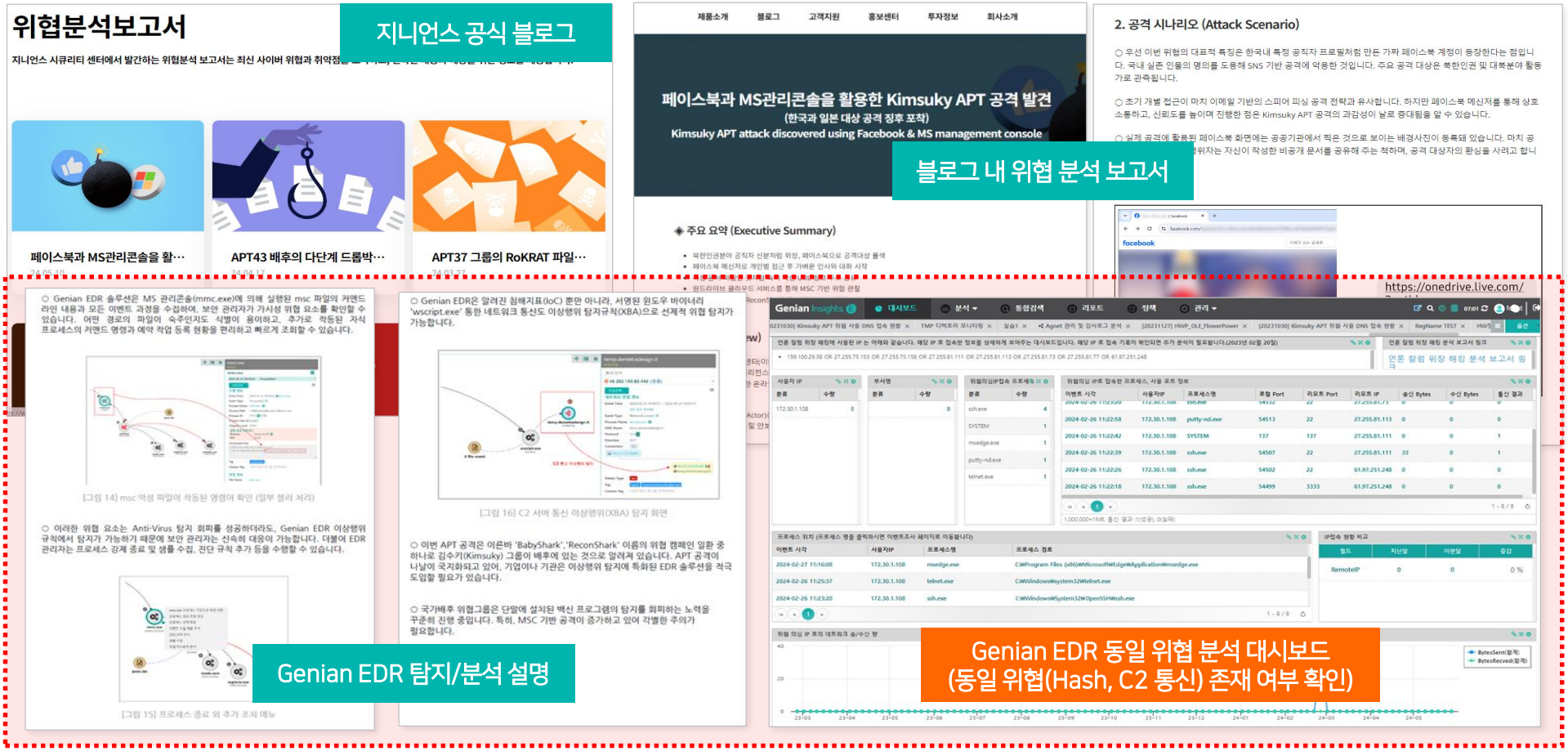
최적의 탐지 & 대응 환경 제공

Genian EDR v2.0 기반의 실시간 위협 탐지 및 분석, 자동화된 대응, 그리고 효율적인 보안 운영을 지원합니다.

신규 서비스 # 2 : 침해사고 대응 센터 운영

✓지니언스 시큐리티 센터(GSC)

- 선제적 위협 헌팅으로 신·변종 악성파일 수집 및 공격 기법 분석
- 최신 공격 기술을 종합 분석해 탐지 대응력 고도화 연구
- 국내외 주요 정보 기관 보안 자문 역할 다수 수행 중
- 정부기관에서 내사중인 위협 첩보 우선 접수

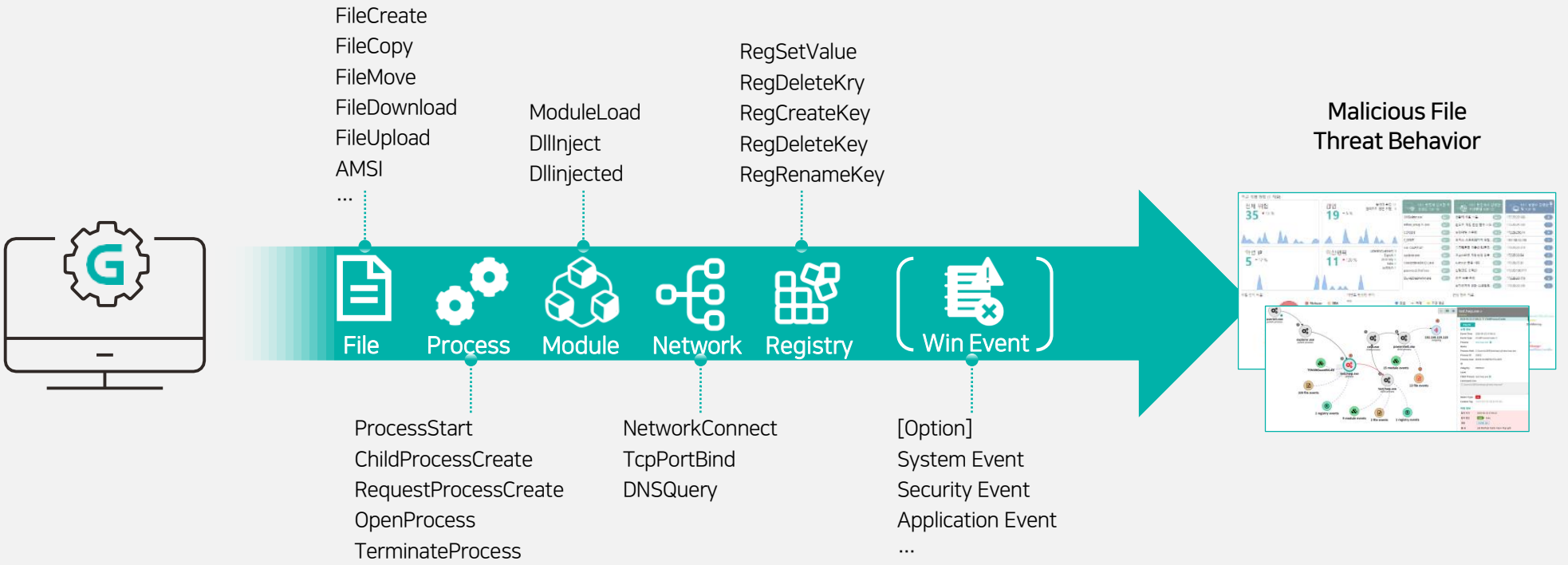


I. Insights E v3.0

- 주요 기능 및 특장점

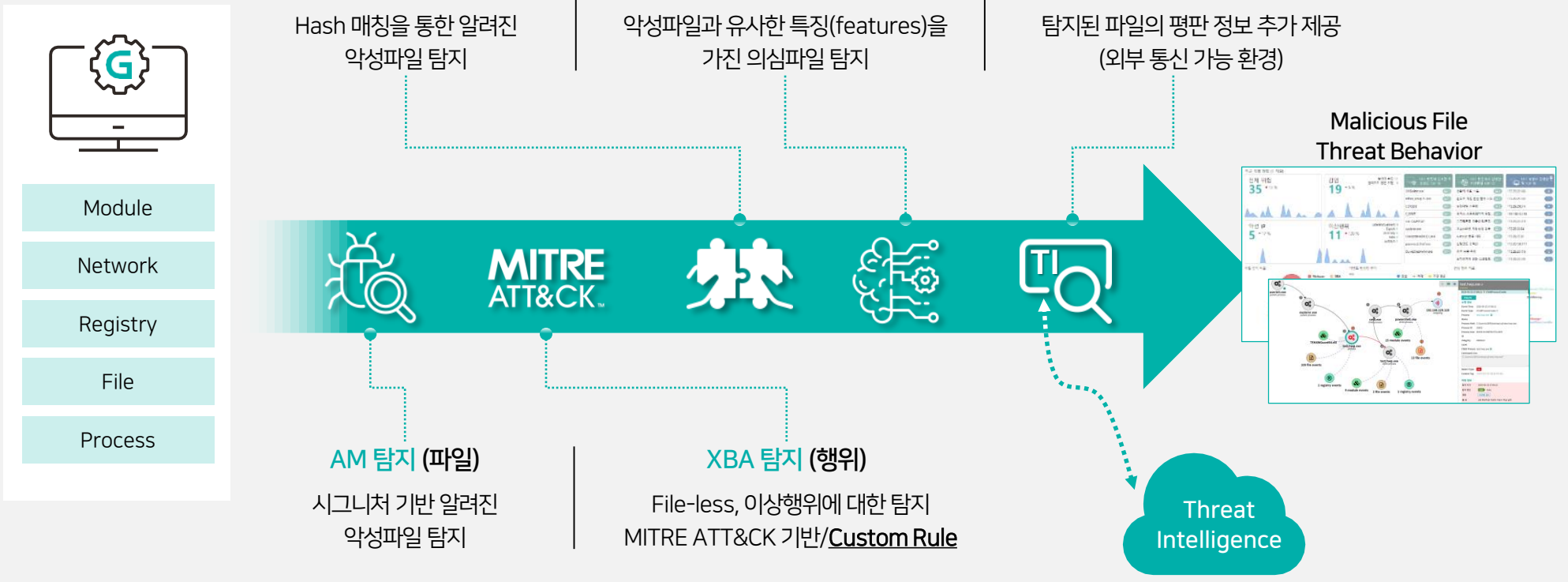
수집(Windows)

Genian Insights E는 Endpoint(PC 등)에 Agent를 설치하여 발생하는 모든 이벤트를 상시 수집하여 위협을 탐지하고 분석/대응을 제공하는 단말 이상 행위 탐지 및 대응(Endpoint Detection & Response) 솔루션



탐지

위협 파일은 백신과 IoC, ML 엔진에서 탐지를 하고 이상행위는 MITRE ATT&CK 기반의 XBA 엔진에서 탐지
외부 통신이 가능하다면 제조사에서 제공하는 TI(Threat Intelligence)에 조회



대응

위협 파일에 대한 격리와 복원 그리고 삭제, 프로세스 강제 종료, 위협 의심 단말기에 대한 네트워크 격리, 사용자에 알림 창 기능과 더불어 심층분석을 위한 자동/수동 프로세스 메모리 덤프 기능도 제공

위협 대응

파일 격리/삭제

네트워크 격리

프로세스 종료

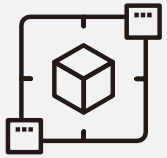
사용자 알림

위협 시 아티팩트 자동 수집

파일 수집

레지스트리 수집

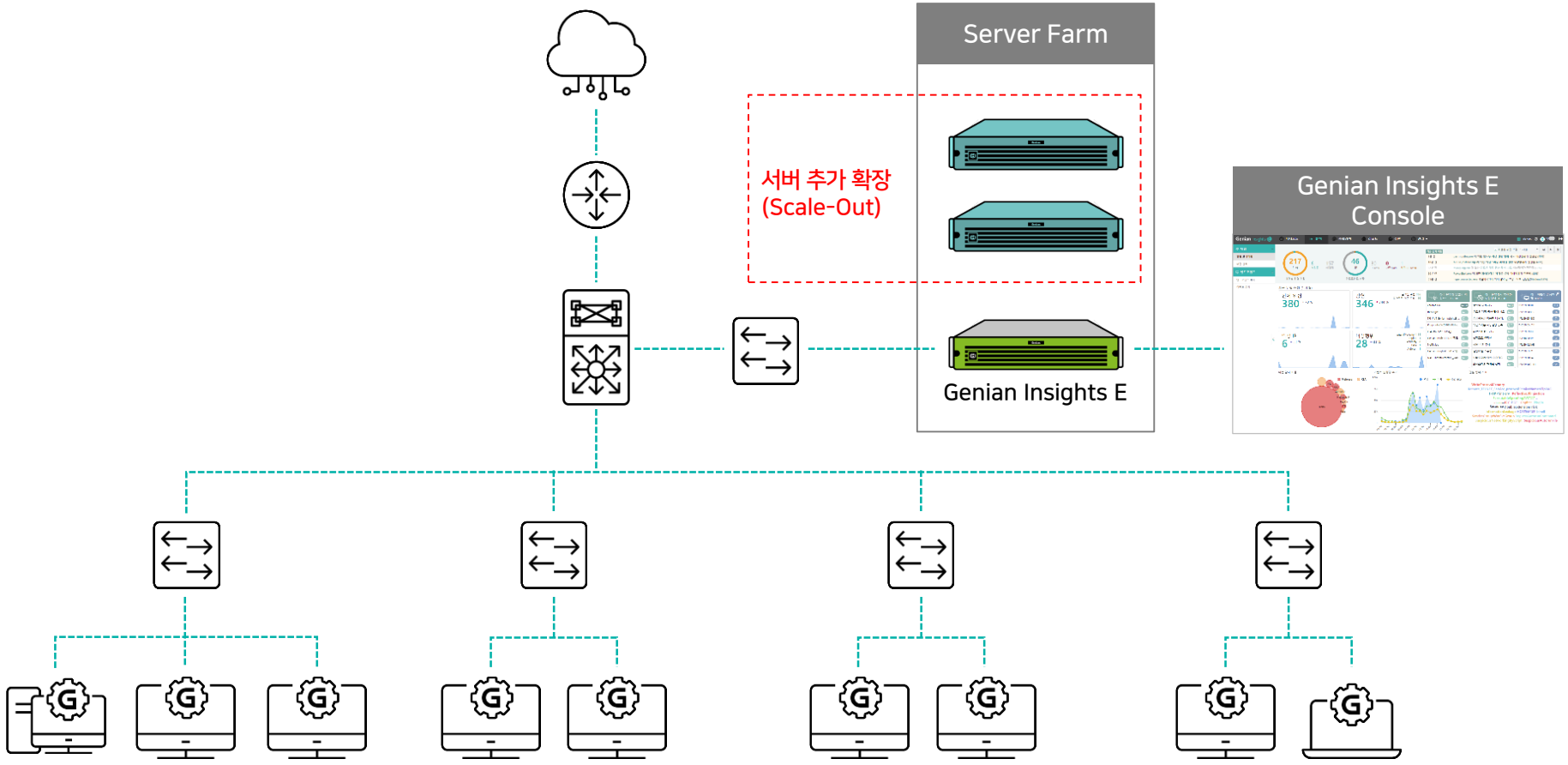
네트워크 패킷 수집



프로세스 덤프

구성

Genian Insights E 서버와 Agent로 구성되며 Scale-Out 기능을 제공하여 확장이 용이
필요시 별도의 로그 서버(warm server) 구성으로 장기간 로그(이벤트)를 저장하여 실시간으로 검색



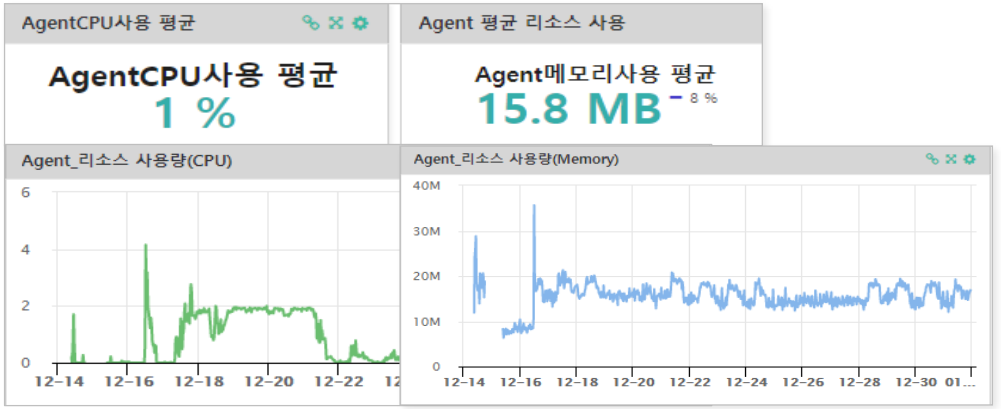
※ Genian NAC 사용 시, NAC Agent에 Genian Insights E 플러그인(모듈) 형태의 간단한 배포와 인증 정보 자동 연동 기능 제공

주요 기능

✓ Lightweight Agent

Agent는 사용자가 불편함을 느끼지 못하도록 가볍게 동작하며 다양한 환경에서도 안정적으로 동작하도록 구현

Windows



문서중앙화	PMS
매체제어	데이터 복원
DLP	프린터 보안
NAC	메신저
개인정보보호	소프트웨어 관리
SSO통합인증	

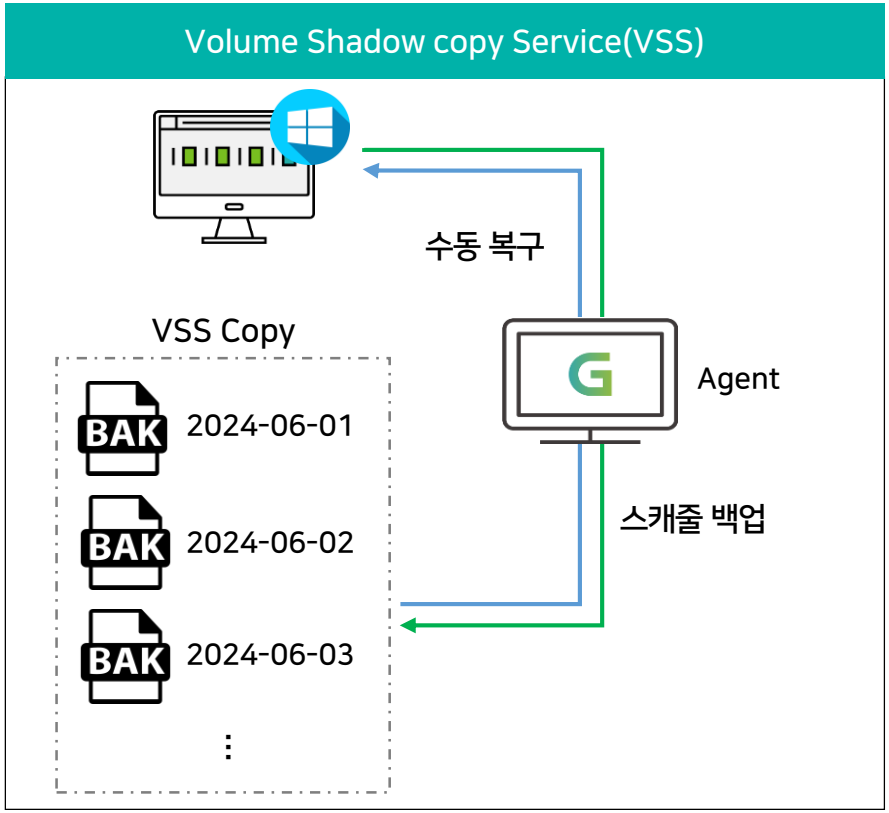
No problem!

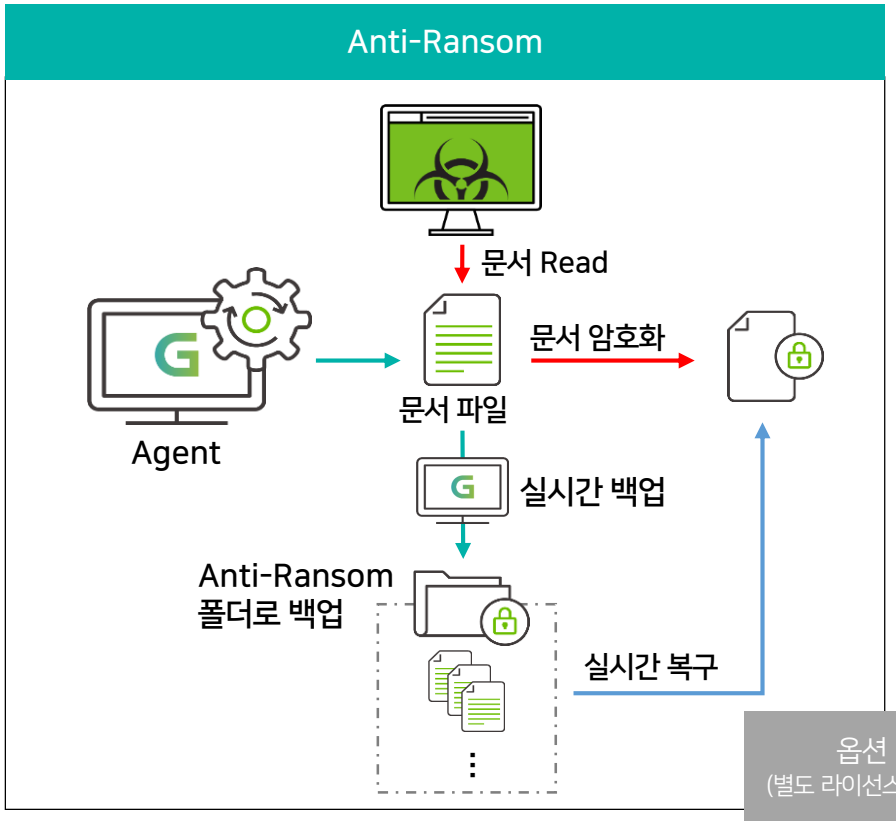
주요 기능

✓ Anti-Ransom

랜섬웨어에 특화된 전문 안티랜섬 탐지 엔진을 탑재하여 보다 정확하게 랜섬웨어를 탐지 및 차단

- 랜섬웨어의 악성 행위를 분석하여 행위 기반으로 탐지
- 랜섬웨어 탐지 시 프로세스 강제종료, 실행파일 삭제 또는 재실행 차단
- 랜섬웨어가 파일을 암호화하기 전 실시간 백업 및 자동 복원
- 행위 기반으로 탐지하기 때문에 File-less 및 신·변종 랜섬웨어에도 대응 가능

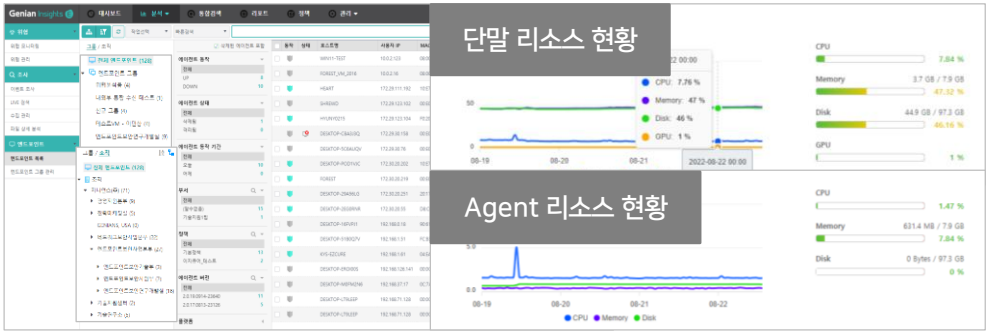




주요 기능

✓ Agent 관리

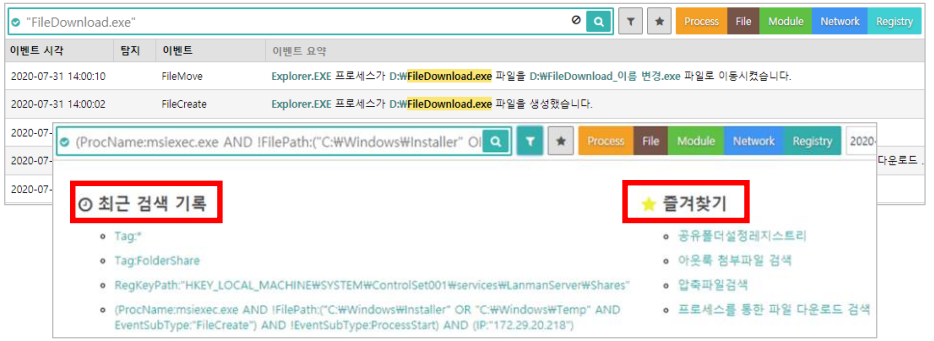
- 설치된 Agent 현황 및 관리
- 단말 리소스 및 Agent 리소스 현황



✓ 이벤트 로그 검색

키워드 및 다양한 조건을 통한 이벤트 로그 검색

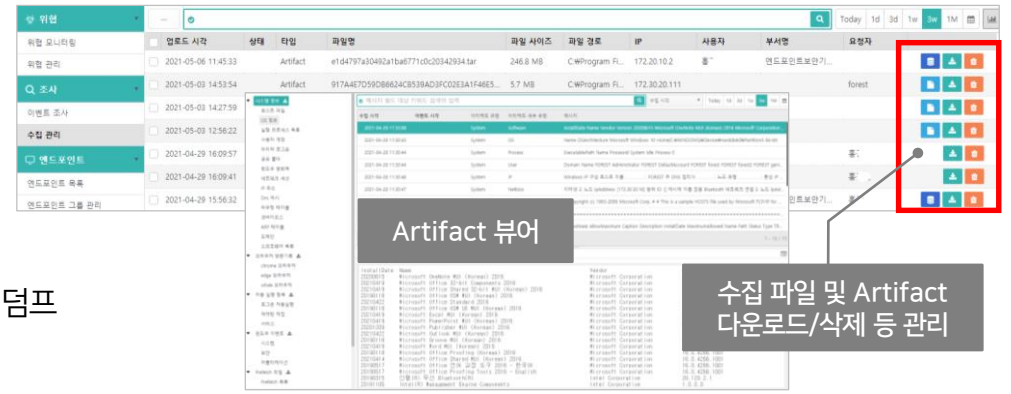
- 최근 검색 기록
- 검색 쿼리 즐겨찾기
- 다중 탭을 통한 검색



✓ 수집 관리

위협 파일, 의심 파일(PE)은 선택에 따라 자동/수동 수집 필요 시 Artifact를 수집하는 기능 제공

Artifact : 시스템 정보, 브라우저 방문 기록, 자동 실행 목록,
윈도우 이벤트, Prefatch 파일, 파일시스템, 레지스트리, 네트워크 패킷 덤프



주요 기능

✓ Live 검색(파일/레지스트리)

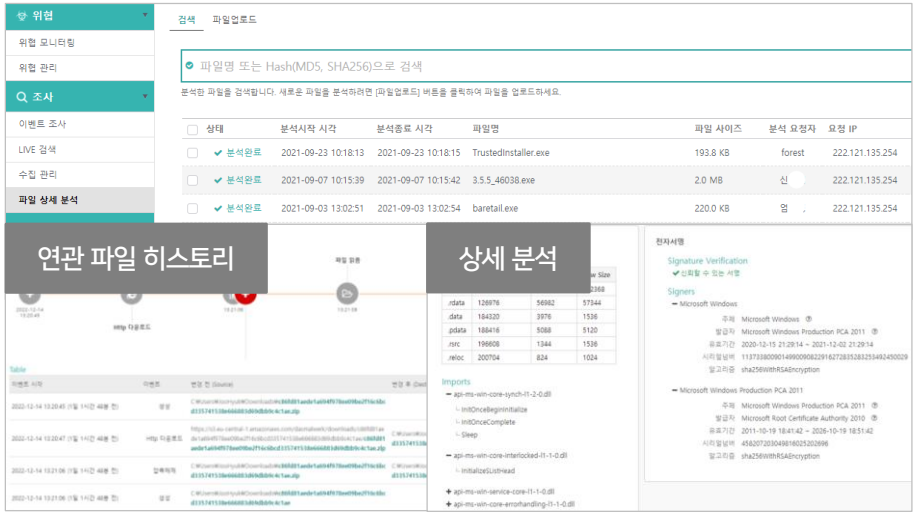
파일 검색을 통해 취약한 버전을 사용하는 프로그램 파일(Potable S/W, 확장 프로그램) 존재 여부 및 특정 레지스트리 검색 결과 확인

- 다양한 검색 조건
- 파일명, 경로, 버전, 해시(MD5, SHA256), 코드사인 여부/주체 등
- 레지스트리 경로, Keys, Values, Data 등

✓ 파일 상세 분석

특정 파일을 EDR 서버로 업로드하여 정적 분석 결과를 제공

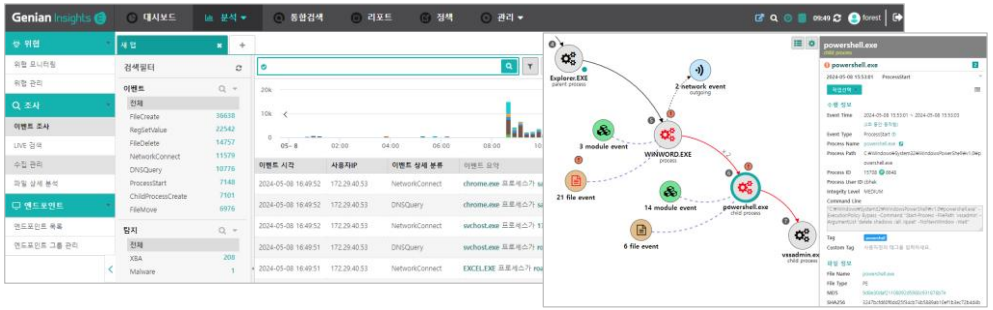
파일의 상세 정보, 문자열, 위협정보, PE정보, 전자서명,
최근 1달간 파일의 히스토리 정보 등



주요 기능

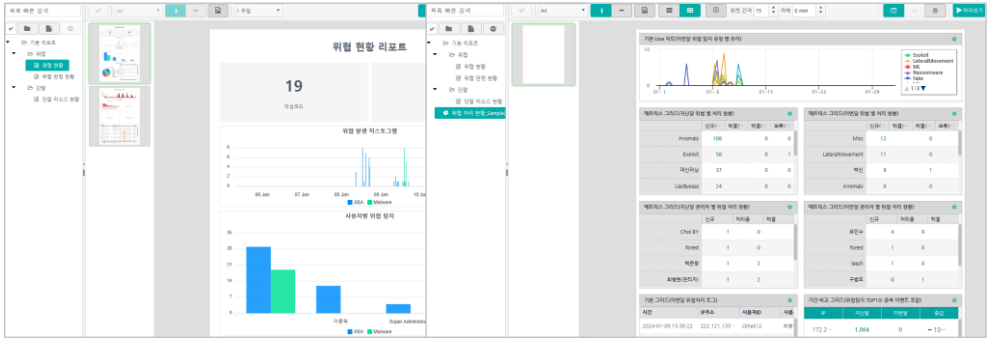
✓ Forensic

항상 엔드포인트 이벤트를 수집하여 사용자 PC 가 포맷이 되어도
수집된 이벤트를 분석하여 추적/검사



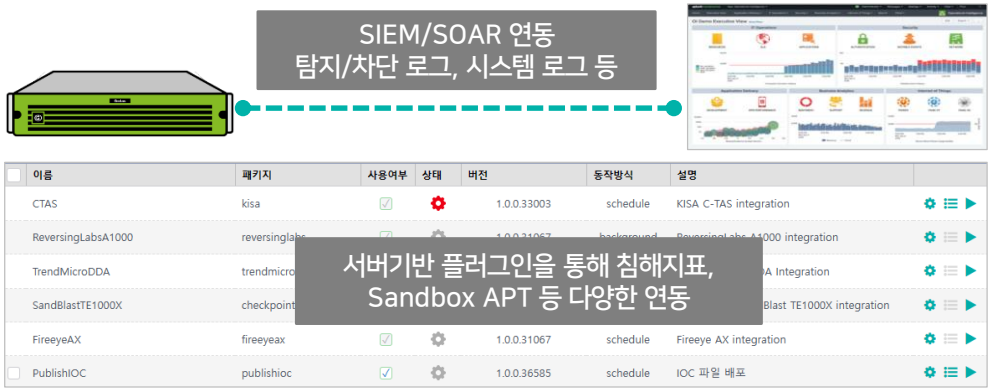
✓ 리포트

기본 제공 리포트와 대시보드를 리포트로 변환 리포트는 관리자가
직접 생성/수정할 수 있도록 다양한 옵션 제공



✓ 연동

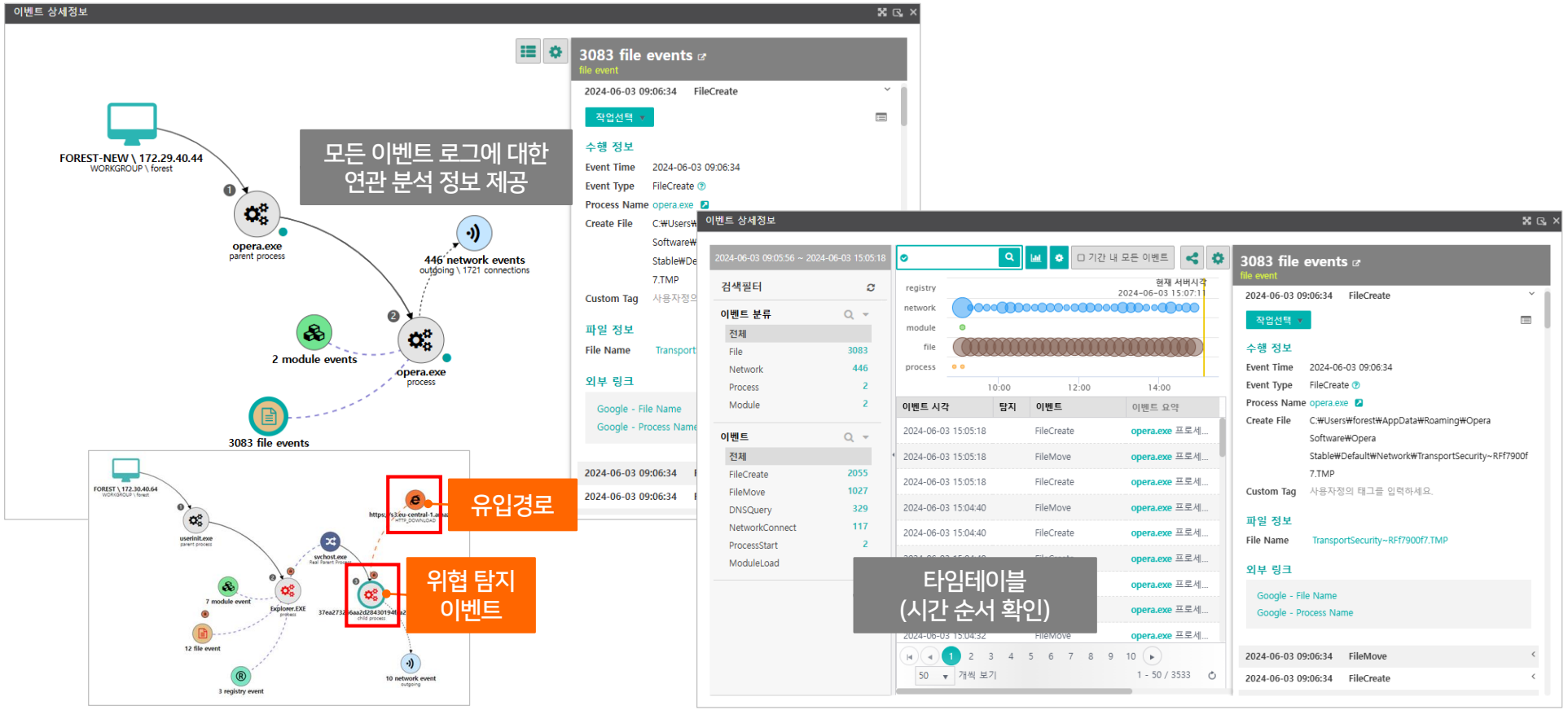
- Syslog, SNMP, Rest API 지원
- 다양한 연동을 위한 플러그인(모듈)을 개발하여 적용
- CTAS(Cyber Threat Analysis & Sharing) 연동 모듈 기본 탑재(가입 후 연동 키 입력만으로 사용)



특장점 : Discovery

수집된 모든 이벤트 상세 정보 제공

- APT 공격 등을 대응하기 위해서 위협이 아닌 일반 이벤트에 대한 상세 분석 필요
- 위협으로 탐지된 이벤트 로그 뿐만 아니라 상시 수집되는 정상 이벤트 로그에 대해서도 연관 분석 정보 제공

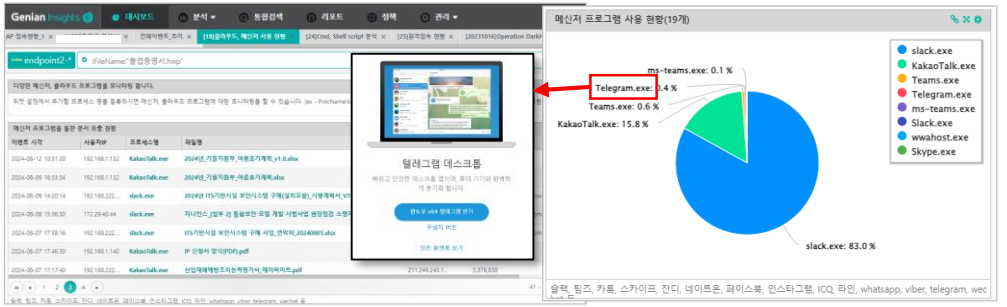


특장점 : Discovery

위협 탐지를 위해 상시 수집된 로그를 활용하여 사용자 PC 내에서 발생하는 다양한 행위 모니터링
문서/압축파일 업로드, 내부 시스템 접속, AP 접속, 외장 저장장치 사용 등 다양한 현황 정보 확인

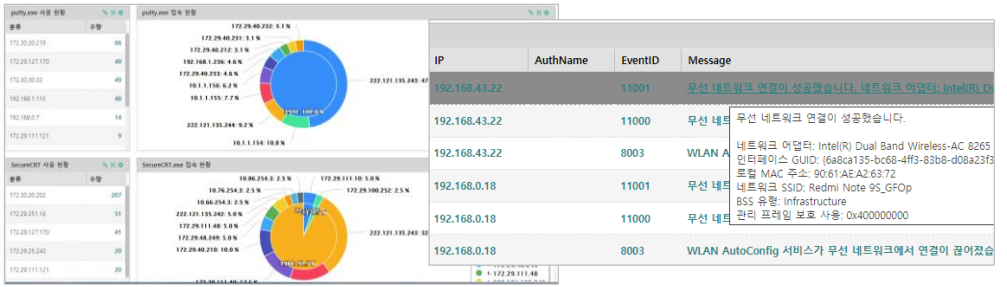
✓ 메신저, 클라우드 사용 현황

- 메신저, 클라우드 프로그램 사용 현황 모니터링
- 특정 프로그램을 통한 문서 유출 모니터링
- 비설치형 프로그램 사용 및 정보유출 확인



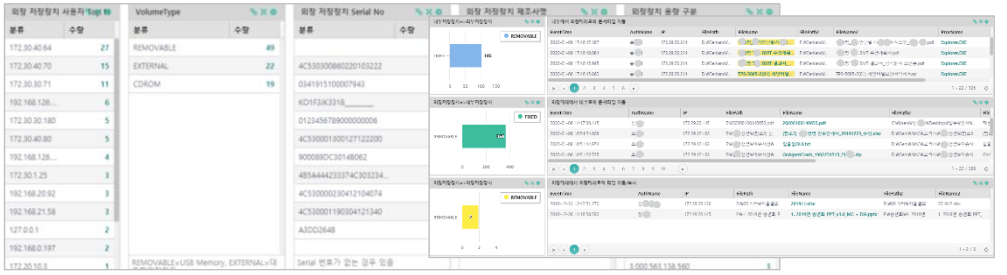
✓ 네트워크 접속 현황

- AP 접속 현황
- 원격 접속 현황 (원격 데스크탑, 원격 터미널, Putty, SecureCRT 등)
- 오픈 포트 및 프로세스
- 외부 IP 접속 프로세스 등



✓ 외장 저장장치 사용 현황

- 외장 저장장치 사용 정보 및 복사/이동 현황
- PC -> 외장 저장장치
- 외장 저장장치 -> PC
- 외장 저장장치 -> 외장 저장장치

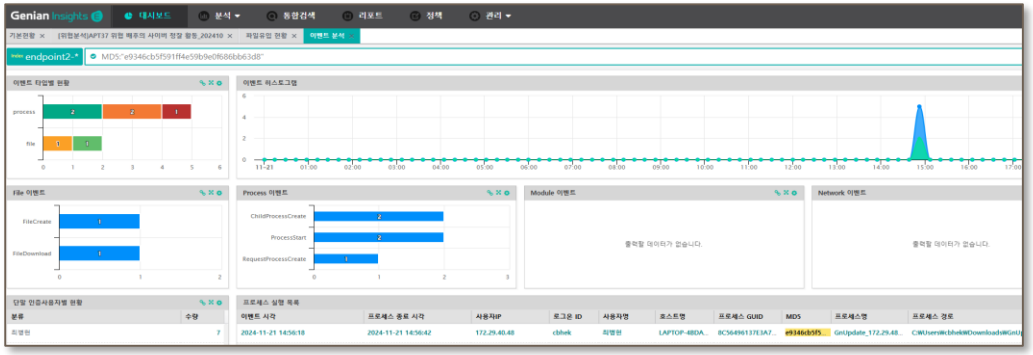


특장점 : Discovery

위협 탐지를 위해 상시 수집된 로그를 활용하여 사용자 PC 내에서 발생하는 다양한 행위 모니터링
악성 HASH, 포트, 네트워크 사용 등 다양한 현황 정보 확인

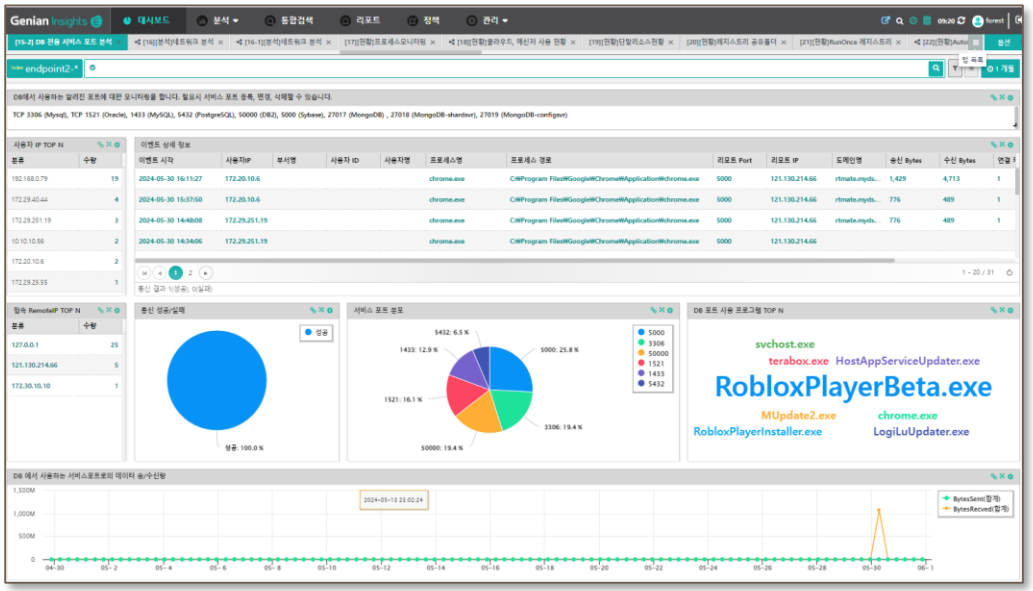
✓ 빠른 HASH 검색

- 악성 hash 검색 기능
- 과거 악성 파일 존재 여부 및 유입 경로 확인



✓ 특정 포트 사용 모니터링

- 내부에서 사용중인 포트 목록 확인
- 알지 못하는 포트 사용에 대한 모니터링
- 공격 표면 관리(Attack Surface Management)등을 통한 외부에 OPEN 된 서비스 포트를 사용하는 프로세스 및 추가 행위 확인



I. Insights E v3.0

- 탐지 및 운영 사례

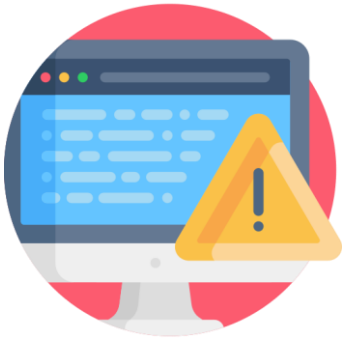
S/W 취약점을 이용한 위협 탐지

✓ 최초 감염

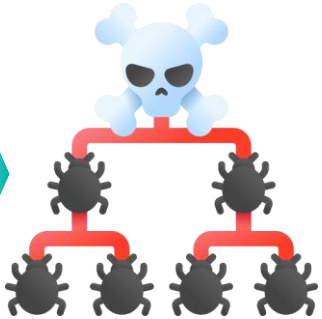
- **특정 금융보안프로그램 취약점을 이용한 악성코드 감염**
  - 금융보안프로그램은 최초 설치 자동 실행
  - 금융 사이트를 접속하지 않으면 자동 업데이트 되지 않음

금융 보안 프로그램 설치 상태

언론사 페이지 접속
(기사 링크)



감염

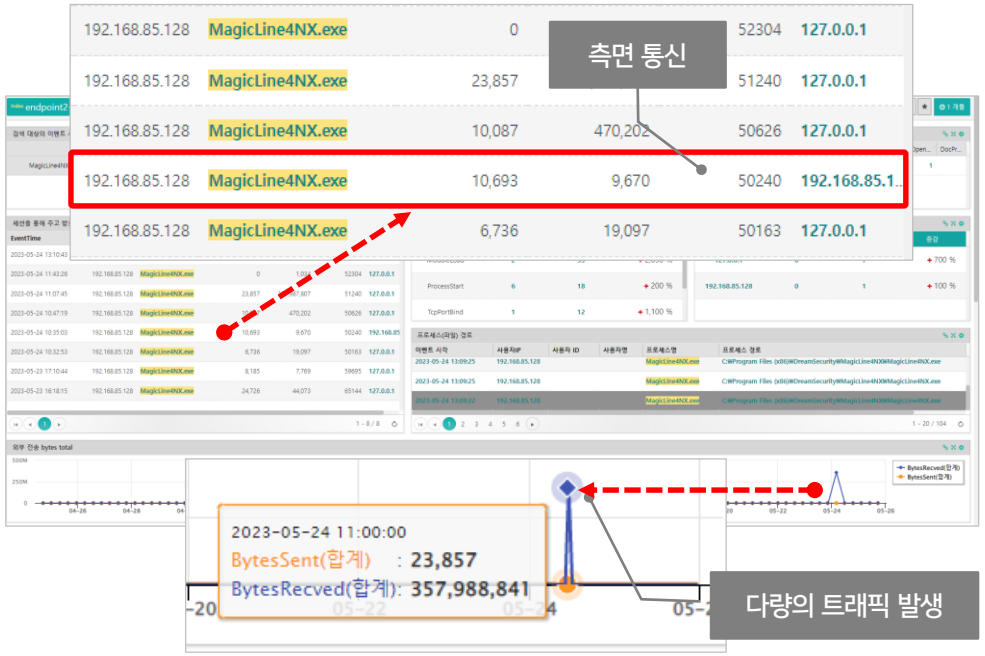


Lateral Movement

S/W 취약점을 이용한 위협 탐지

✓ 확산 시도

동일 금융보안프로그램 취약점을 이용한 측면 이동 (Lateral Movement) 시도



✓ 내부망 침투

망간자료전송시스템 취약점을 이용한 내부망 악성코드 유입 및 자료유출 시도

- 망간자료전송시스템 취약점을 이용하여 내부망으로 악성코드를 유입시키고, 해당 악성코드를 통해 다시 외부망으로 자료 유출 시도 확인
- 악성코드의 실행 명령어를 통한 침투 확인
- 외부 유출을 금지한 내부망 문서의 외부망 유입 경로 확인

워터링홀 공격을 이용한 정보 유출 탐지

✓ 최초 감염

- **필수 사이트의 어플리케이션 관리 소프트웨어 감염**

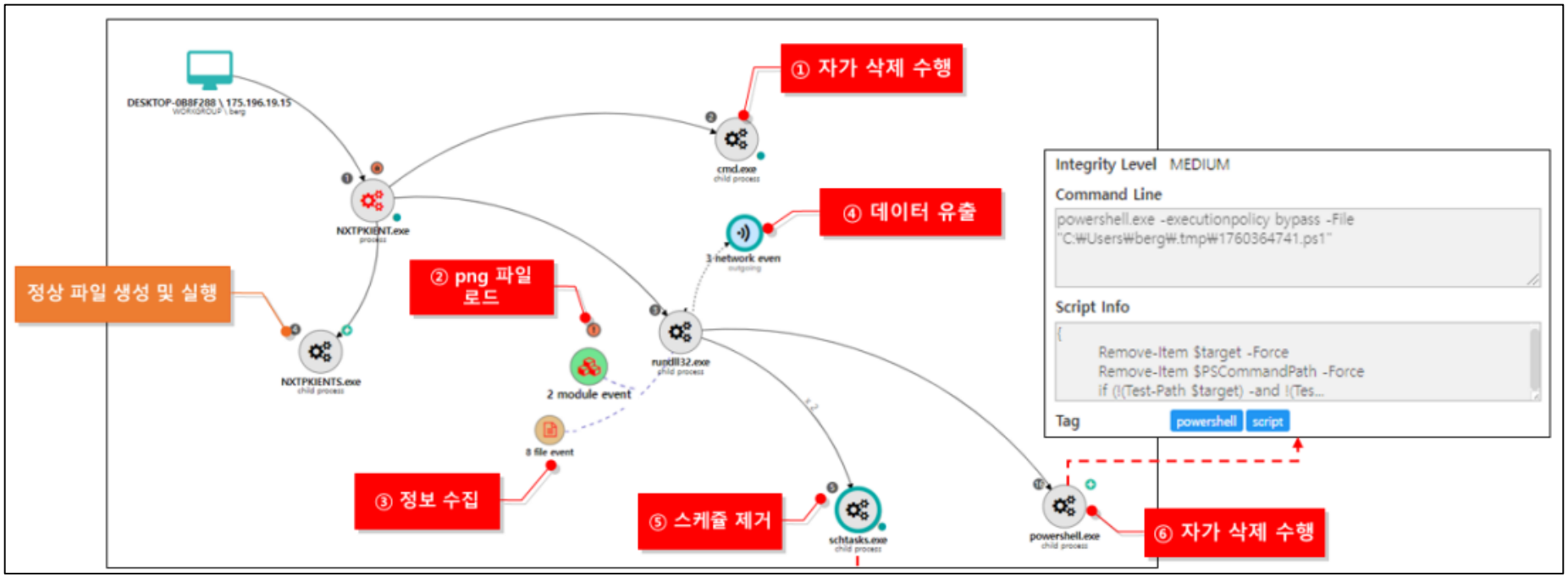
  - 업무 특성상 접속이 필요한 사이트를 감염시켜 악성코드가 로드 될 수 밖에 없는 환경 구성
  - 통합설치프로그램을 통해 특정 보안프로그램을 정상적인 프로그램으로 위장하여 공격 수행

워터링홀 공격을 이용한 정보 유출 탐지

✓ 사고 분석

- **정보 유출 후 자가 삭제 수행**

1. 특정 사이트의 필수 보안 프로그램 감염
2. 해당 프로그램 유효한 서명이 확인되었으나, 탈취된 서명
3. 정상적인 프로그램이 실행되고, 추가로 png 파일 생성
4. png 파일은 dll 파일이며, rundll32 를 통해 실행
5. **시스템 정보 수집 후 유포 서버로 정보 유출**
6. 유출 완료 후 **자가 삭제**



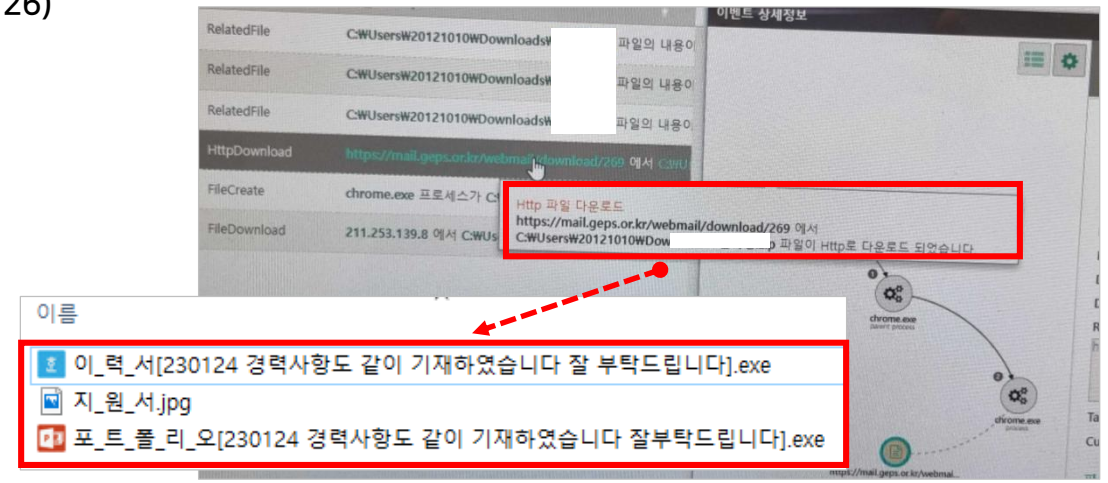
이력서로 위장한 랜섬웨어 탐지

랜섬웨어 대응

✓ 유입 경로

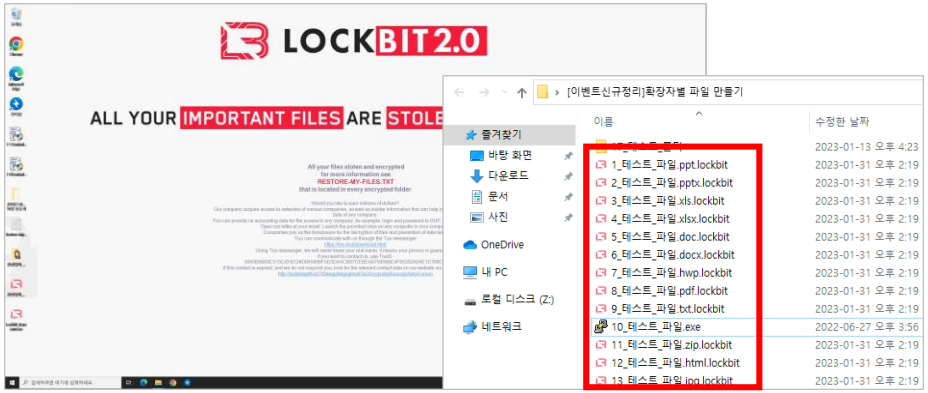
- 웹메일(https://mail.*****.kr/webmail/download/26) 통한 이력서 파일 다운로드

- 압축 해제 시 위 화면과 같이 3개의 파일 생성 (문서 파일로 위장한 실행파일)



✓ 문서 암호화

- 이력서 실행 시 문서파일 암호화 및 바탕화면 변경



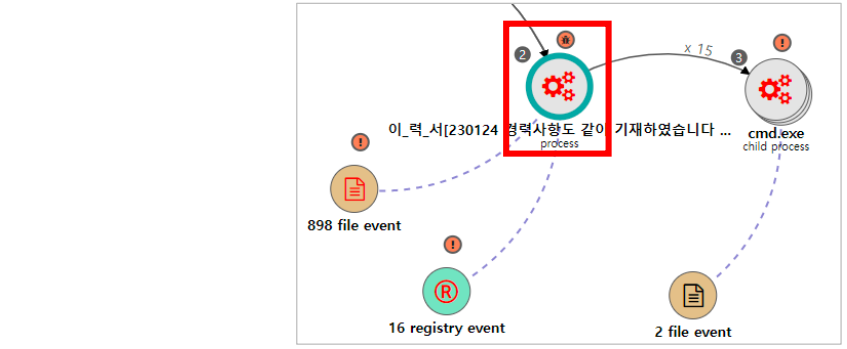
이력서로 위장한 랜섬웨어 탐지

랜섬웨어 대응

✓ EDR 분석 내역(이_력_서**.exe)

- 악성 행위는 아래와 같은 순서로 진행

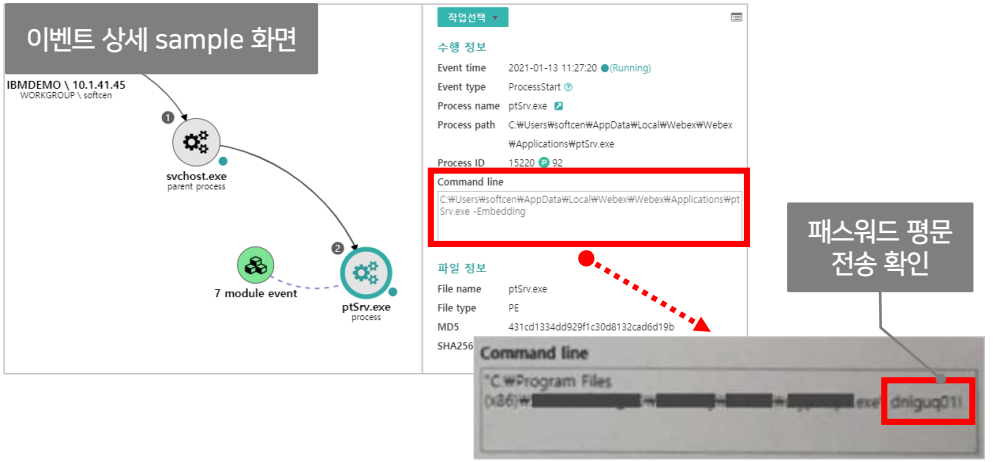
1) 파일 실행과 동시에 특정 드라이브에 파일 생성을 진행해 사용하지 않는 드라이브를 활성화
2) 문서 및 js파일 등을 암호화 수행 (파일명.lockbit)
3) 명령프롬프트를 수행 후 특정명령어를 실행 (vssadmin.exe, WMIC.exe 등)
4) 부팅 시 재 실행되도록 AutoRun 등록



수집 정보 활용

✓ 평문 패스워드 전송

고객사는 내부적으로 자체 응용 관리 프로그램을 개발하여 사용 중 Genian EDR 도입 후 모니터링 중 관리 프로그램에 접속 시 패스워드가 암호화 되지 않고 평문으로 전송되는 것을 확인



트래픽 모니터링을 통한 패스워드 탈취 및 공격이 가능,
해당 고객사는 문제 발견 후 수정/보완 조치 진행

✓ 매체 제어 우회

외부 저장장치 사용 현황을 통해 매체 제어 솔루션이 정상 동작하는지에 대한 검증

- 사용자의 우회 사용
- 매체 제어 솔루션 오동작으로 인한 사용

수집 정보 활용

✓ 내부 시스템 무력화 프로그램 사용

사용자가 직접 제작한 내부 보안솔루션 무력화 프로그램 실행

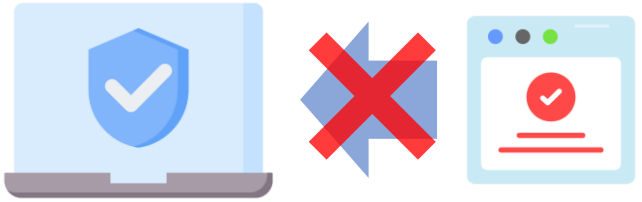
내부 보안 프로그램 종료

: 근태 관리, PC-OFF, 개인정보 지킴이, 문서보안

,스크린 워터마크, 안전 모드 제어 솔루션

자체 프로그램 제작

보안 프로그램 무력화



임직원이 제작한 프로그램으로 백신 등에 등록 되지 않음

불법 프로그램 사용

Insights E v3.0 도입 사례

✓국내 금융권 주요 레퍼런스

Your Best Credit Partner SGI서울보증

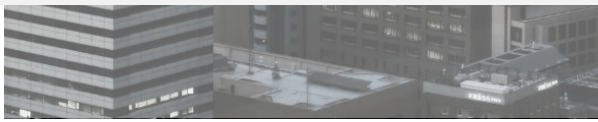
KB 국민은행

KB 증권

meritz 메리츠화재

meritz 메리츠증권

그 외 다수의 금융권에서 도입을 목표로 PoC 진행 중

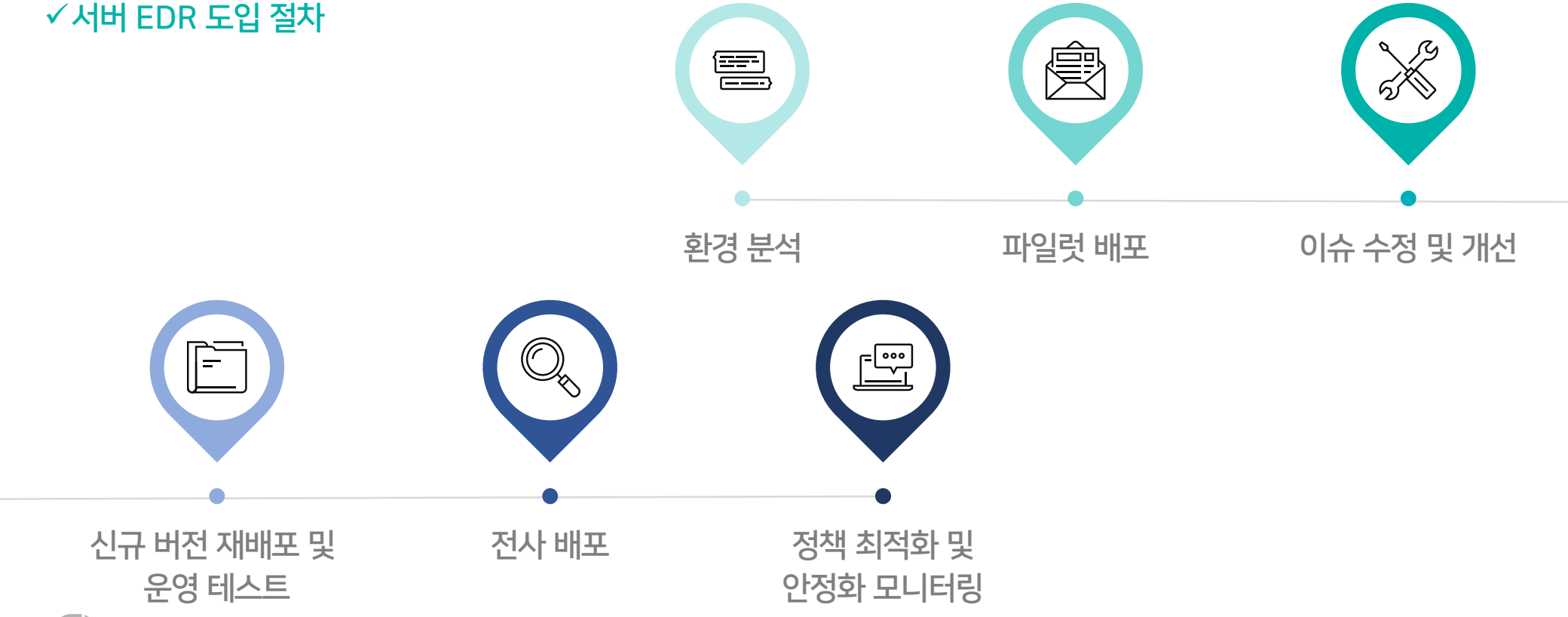


Insights E v3.0 도입 사례

✓S사 사례

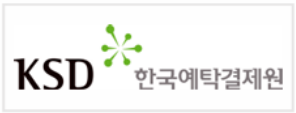
- 랜섬웨어 대응 강화를 위한 **안티랜섬** 모듈 도입
- EDR과 **매체제어**의 통합으로 엔드포인트 보안 가시성 극대화
- 서버 가시성 확보를 위한 **리눅스 에이전트** 배포

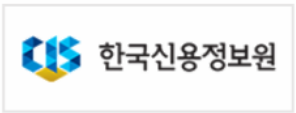
✓서버 EDR 도입 절차



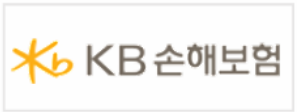
금융권 주요 고객사

1금융 및 공금융





2금융 외



Summary

안정성

낮은 리소스 사용
충돌 회피 기술 적용

시장점유 1위

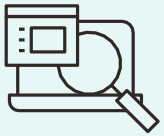
23/24년 조달 점유율 1위
240여 곳 고객사 구축

안티바이러스

백신 모듈이 추가되어
더욱 강력한 탐지 기능 제공

빠른 성능

고성능의 SSD 탑재
1억 건 5초 이내 조회
(빅데이터 필수 사항)



강력한 분석

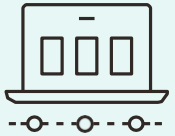
수집된 정보를 활용
입체적인 분석 가능

안티랜섬웨어

특화된 안티랜섬웨어 기능
실시간 백업/탐지/대응/복원

장기간 로그 저장

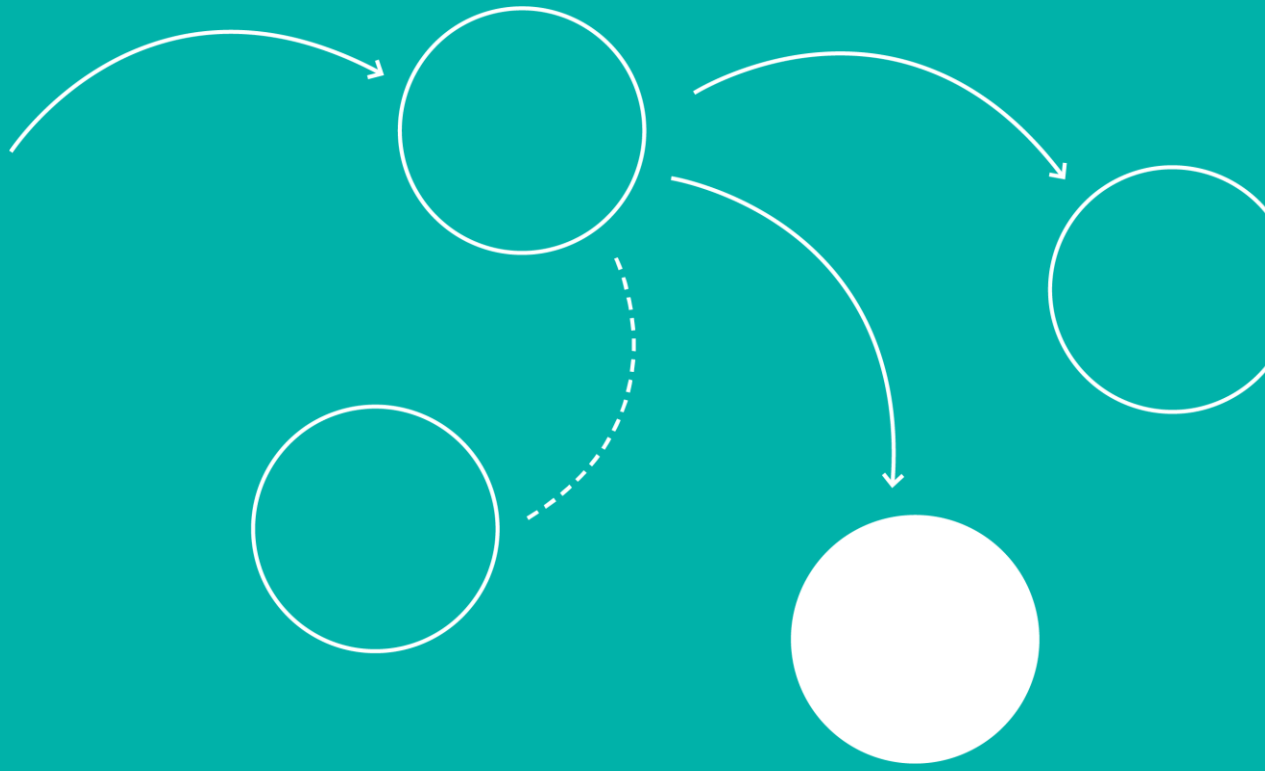
로그 서버 추가 시
12개월 이상의 로그 보관
(+Scale Out)



탐지/대응 기본

EDR에서 제공하는
기본 이상의 다양한
기능+정보 제공

Thank you



Genians