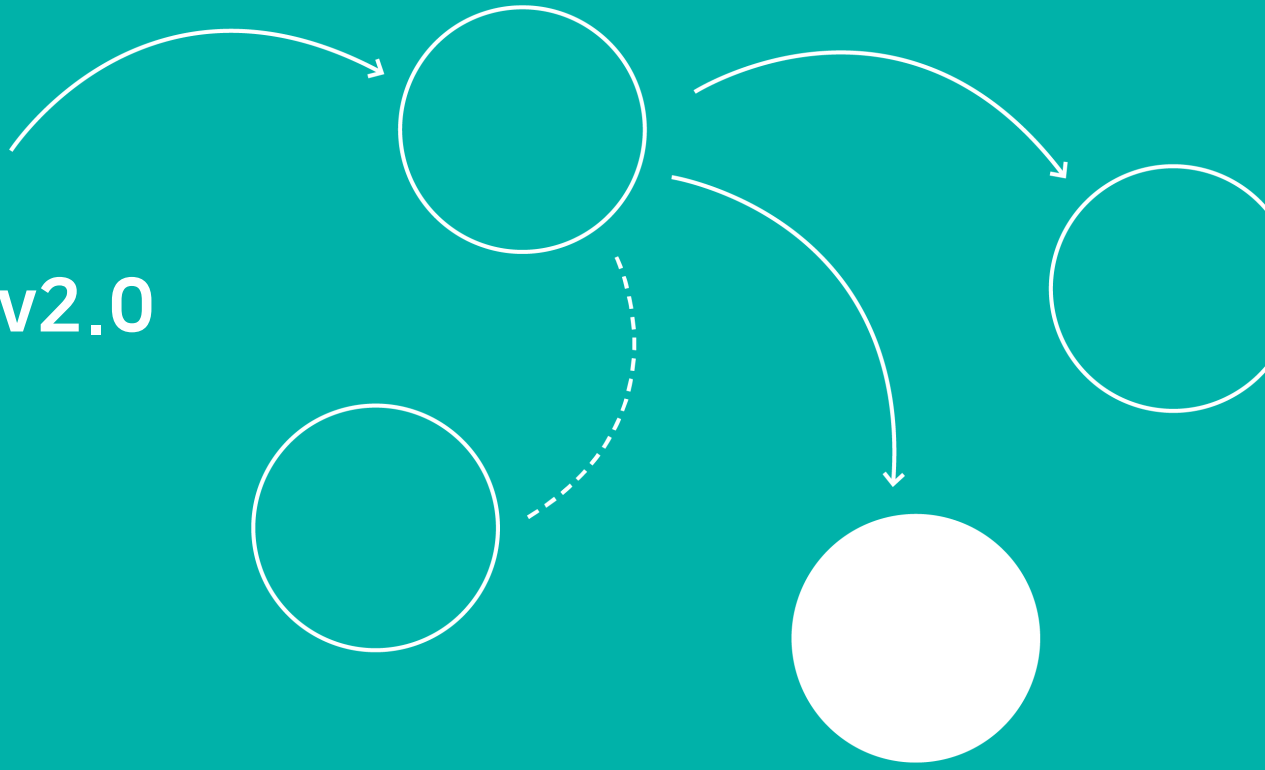
엔드포인트 위협 대응의 모든 것

Genian EDR v2.0



Genians

Table of Contents

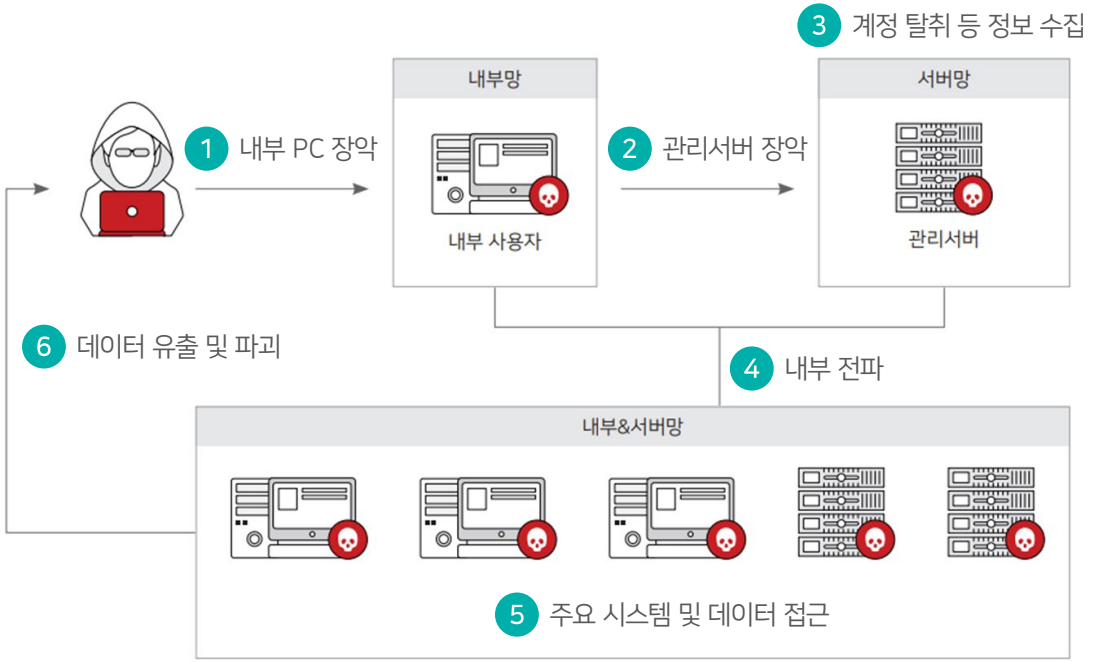
I. 개요

- 사이버 공격의 목표이자 시작점, 엔드포인트
- 지능화/고도화 위협
- 파일 기반 탐지 솔루션의 한계

사이버 공격의 목표이자 시작점, 엔드포인트

엔드포인트는 사이버 공격자가 가장 쉽게 접근할 수 있는 기업·기관과의 접점
엔드포인트 공격은 엔드포인트에서 끝나는 것이 아니라 엔드포인트를 기점으로 전체 시스템에 위협

※ 엔드포인트를 모니터링하고 대응하는 것이 무엇보다 중요



▲ EQST, 보안 위협 전망 보고서

- 어떤 경로로?
- 감염 호스트는 무엇?
- 감염 규모는?
- 주요 시스템 접근 여부?
- 데이터 유출 여부?
- 유출된 데이터는?

지능화/고도화 위협

지능화/고도화 되고 있는 공격 방법은 기존 보안 솔루션을 우회하거나 무력화
예시) 랜섬웨어의 진화

1. 시스템 화면 잠금

시스템에 접근하지 못하도록 차단하는
시스템 화면 잠금

안전모드 부팅 후 시스템 복원

2. 파일 암호화

악성파일을 활용해 시스템 내부의 문서
파일을 암호화 하는 형태

복원이 어려운 형태로 진화

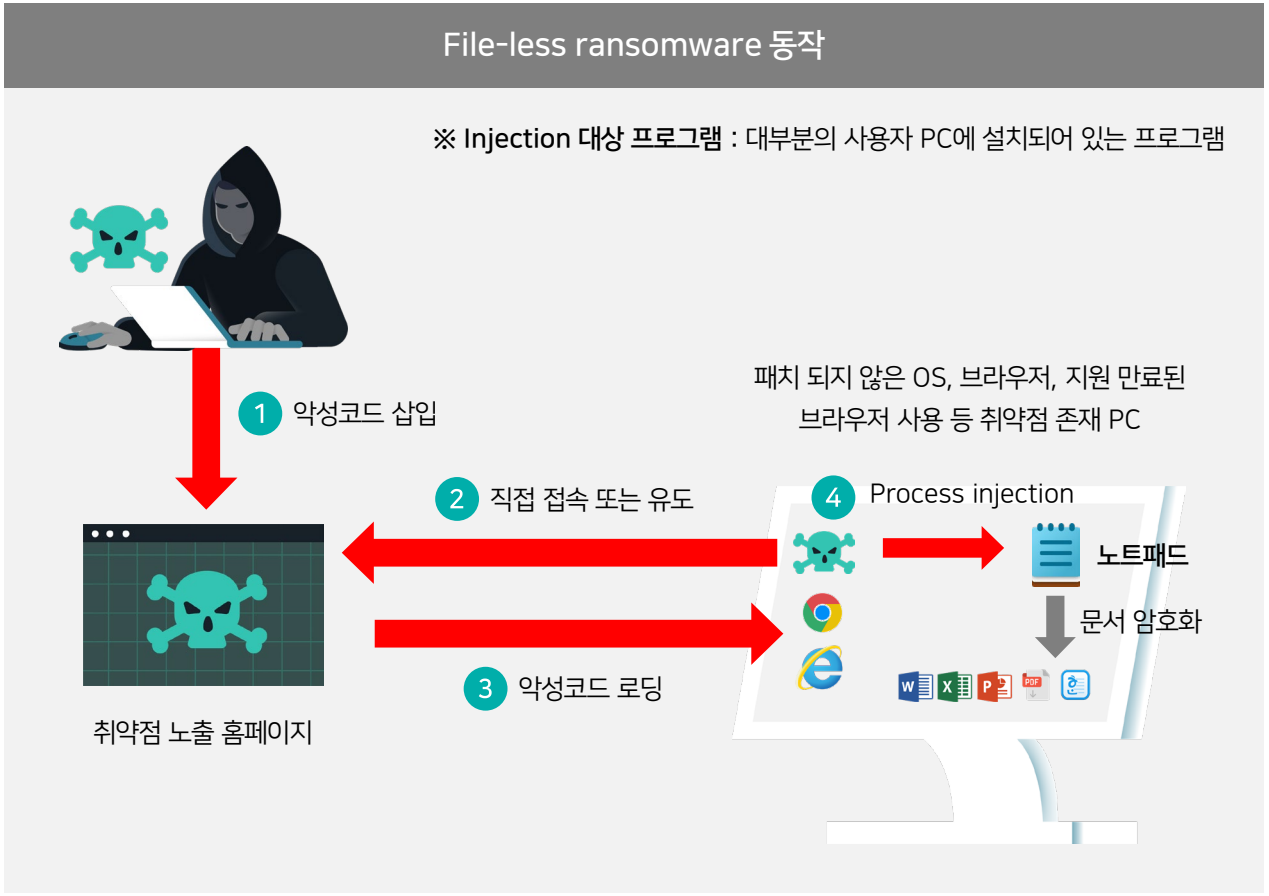
3. 공격 방법의 진화

공격 방법의 지능화/고도화

File-less 형태 제로데이 취약점

파일 기반 탐지 솔루션의 한계

File-less 공격 및 정상 파일(프로세스)을 악용하는 이상행위 탐지 필요



II. Genian EDR

- 개요
- 구성
- 주요 기능
- 특장점

개요

Genian EDR은 단말에 대한 지속적인 모니터링과 상시 정보 수집을 통해 위협을 탐지하고 분석/대응을 제공하는 단말 이상 행위 탐지 및 대응(Endpoint Detection & Response) 솔루션

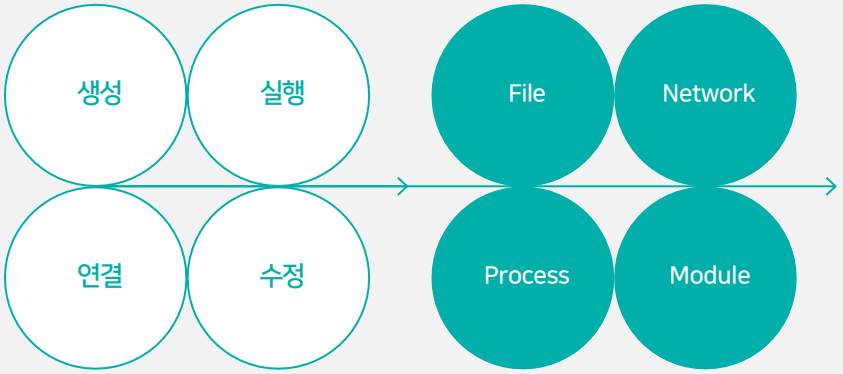
1. 단말 행위 모니터링/수집
- File, Module, Process, Connection, Registry 정보
- 사용자 및 엔드포인트에서 발생하는 이상 행위
- 외부 저장매체 사용 현황
- 윈도우 이벤트 로그 수집
- 다양한 대시보드 제공

2. 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

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

단말 행위 모니터링 단말에서 발생하는 주요 행위를 모니터링하고 상시 저장 후 분석, 이를 통해 지능형 위협 등을 사전에 탐지/예방하고 사후 감사 증적(Audit)이 가능



- 단말 행위 분석 및 이상행위 탐지
- APT, 랜섬웨어 등 지능형 위협의 탐지
- 탐지된 위협 및 이상행위 대응(Response)
- 침해 사고 및 이상행위의 감사 증적(Audit)

개요

Genian EDR은 단말에 대한 지속적인 모니터링과 상시 정보 수집을 통해 위협을 탐지하고 분석/대응을 제공하는 단말 이상 행위 탐지 및 대응(Endpoint Detection & Response) 솔루션

1. 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

2. 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

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

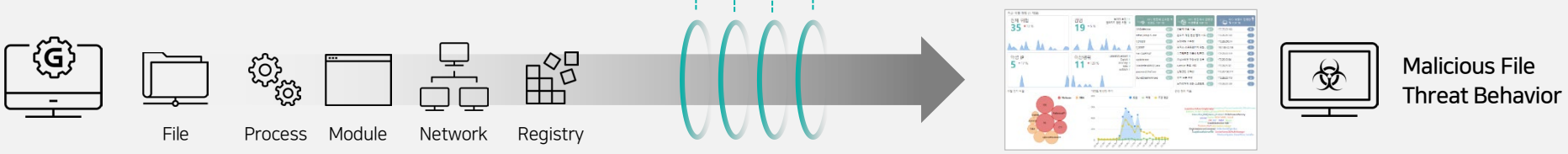
위협 탐지 IOC(침해 지표), 머신 러닝을 이용하여 단계별로 위협을 탐지하고 XBA(행위 기반) 룰을 통해 File-less를 포함한 다양한 형태의 이상행위 탐지

IOC 탐지 (파일)
알려진 악성파일 탐지, 글로벌에서 탐지 됐던 파일의 hash 매칭

ML 탐지 (파일)
악성파일과 유사한 특징(features)을 가진 의심파일

XBA 탐지 (행위)
File-less, 이상행위에 대한 탐지
MITRE ATT&CK 기반/Custom Rule

ECO (평판, 유사도)
탐지된 파일의 평판 정보 추가 제공
(외부 통신 가능 환경)



개요

Genian EDR은 단말에 대한 지속적인 모니터링과 상시 정보 수집을 통해 위협을 탐지하고 분석/대응을 제공하는 단말 이상 행위 탐지 및 대응(Endpoint Detection & Response) 솔루션

1. 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

2. 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

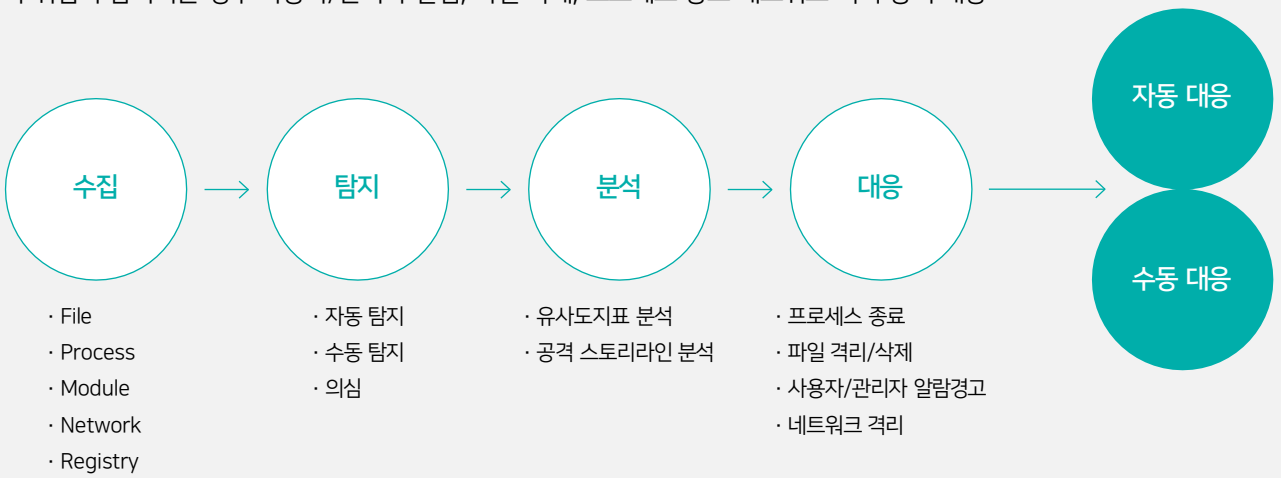
3. 위협의 대응

- 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

위협 대응 엔드포인트에서 위협이 탐지되는 경우 사용자/관리자 알림, 파일 삭제, 프로세스 종료 네트워크 격리 등의 대응



개요

Genian EDR은 단말에 대한 지속적인 모니터링과 상시 정보 수집을 통해 위협을 탐지하고 분석/대응을 제공하는 단말 이상 행위 탐지 및 대응(Endpoint Detection & Response) 솔루션

1. 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

2. 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

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

탐지 위협의 조사

위협의 탐지와 동시에 조치의 대상이 누구인지 알 수 있으며 탐지된 위협의 상세 정보 확인 가능

탐지 기본 정보

일반 정보	탐지 시각 | 위협 분류 | 위협 ID
사용자 정보	부서 | 사용자 이름 | ID
단말 정보	IP | MAC | Hostname | OS | ID
파일 정보	이름 | 경로 | 크기 | 해쉬값

정적 분석(Static Analysis) 정보

제품 정보	버전 | 카피라이트 | 이름 등
코드 사인	코드사인(Signature Verification) 정보
PE 정보	섹션 | 타입 | 체크섬 | 엔트리포인트 등
문자열 정보	유형 | 종류 | 문자열 | 위치 등

동적 분석(Dynamic Analysis) 정보

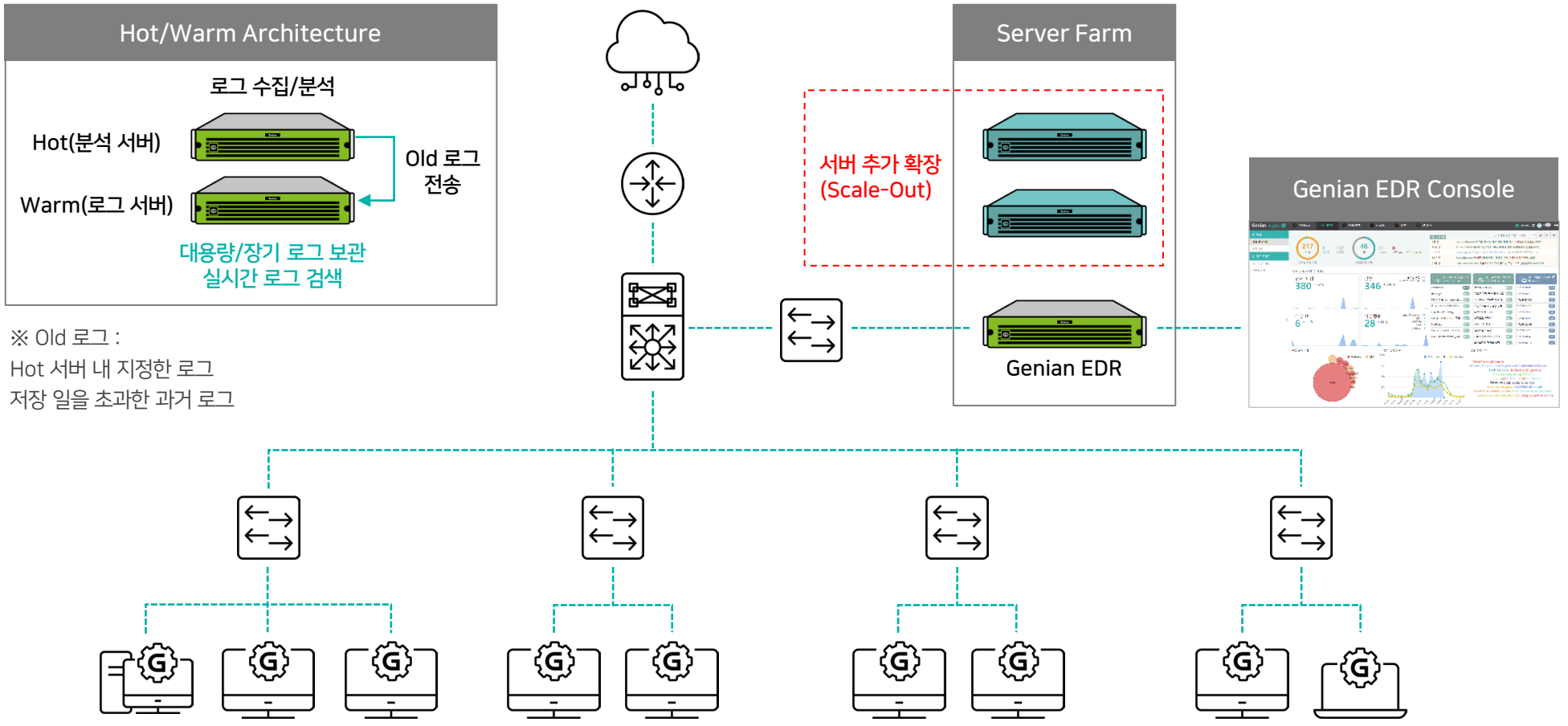
환경 정보	OS | 설치된 프로그램 | 시간 등
행위 요약	프로세스 경로 | 행위 내용 등
시스템 행위	레지스트리, 파일, 동적링크(dll) 등 행위의 발생 시간, 값, 결과 등
네트워크 행위	이름 | 경로 | 크기 | 해쉬값

연관 분석(Chain of Event) 정보

연관 관계	파일 및 프로세스 실행 | 호출 | 연결 등 행위 연관 관계 | 유입 경로
상세 정보	파일 및 프로세스 크기 | Path | IP | Hash | ID 등
수행 명령어	IP | MAC | Hostname | OS | ID

구성

Genian EDR 서버, Agent의 간단한 구성 및 Scale-Out 기능을 제공하여 확장이 용이

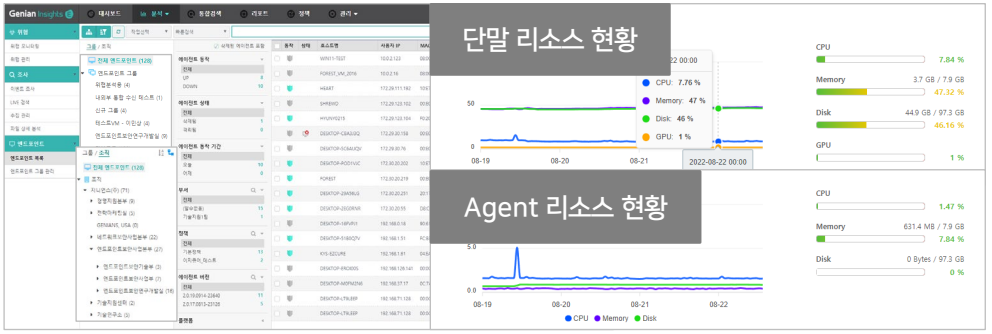


※ Genian NAC 사용 시, NAC Agent에 EDR 플러그인(모듈) 형태의 간단한 배포와 인증 정보 자동 연동 기능 제공

주요 기능

✓ Agent 관리

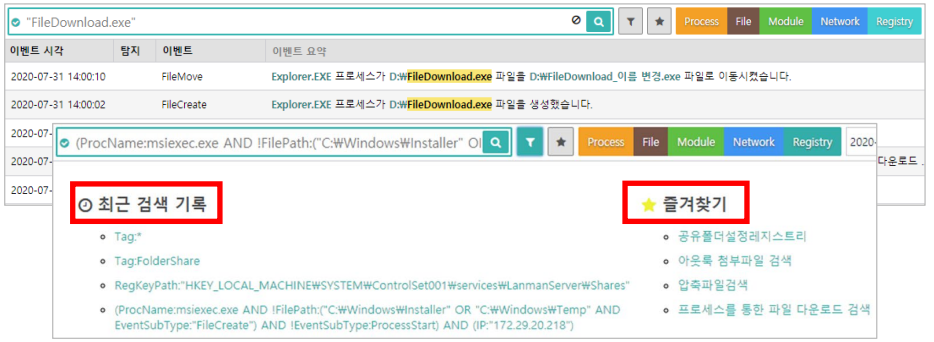
- 설치된 Agent 현황 및 관리
- 단말 리소스 및 Agent 리소스 현황



✓ 이벤트 로그 검색

키워드 및 다양한 조건을 통한 이벤트 로그 검색

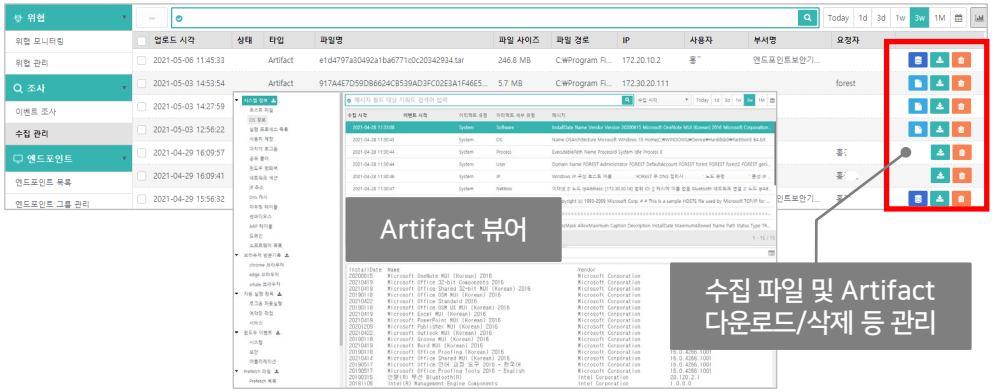
- 최근 검색 기록
- 검색 쿼리 즐겨찾기
- 다중 탭을 통한 검색



✓ 수집 관리

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

Artifact : 시스템 정보, 브라우저 방문 기록, 자동 실행 목록, 윈도우 이벤트, prefatch 파일, 파일시스템, 레지스트리 하이브



주요 기능

✓ Live 검색(파일/레지스트리)

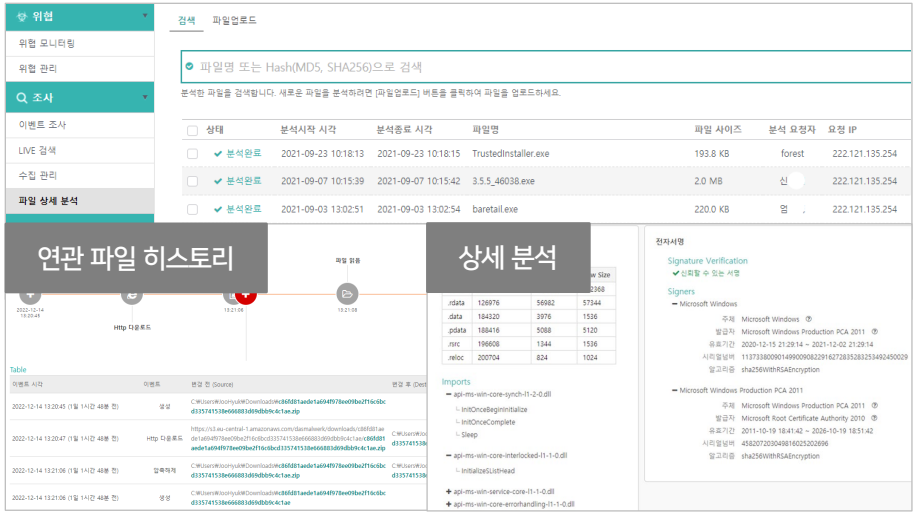
파일 검색을 통해 취약한 버전을 사용하는 프로그램 파일(Potable S/W, 확장프로그램) 존재 여부 및 특정 레지스트리 검색 결과 확인

- 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

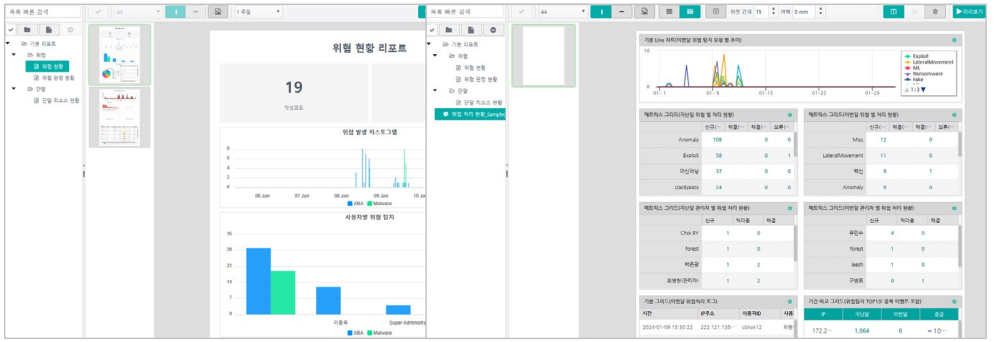
파일의 상세 정보, 문자열, 위협정보, PE정보, 전자서명,
최근 1달간 파일의 히스토리 정보 등



주요 기능

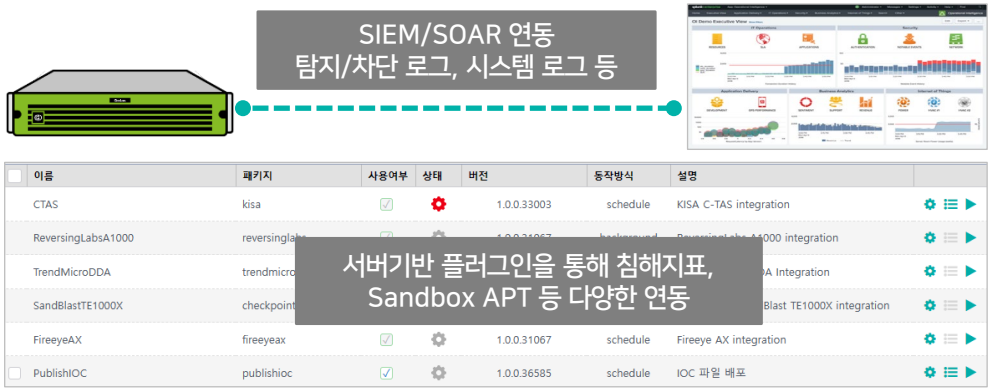
✓ 리포트

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



✓ 연동

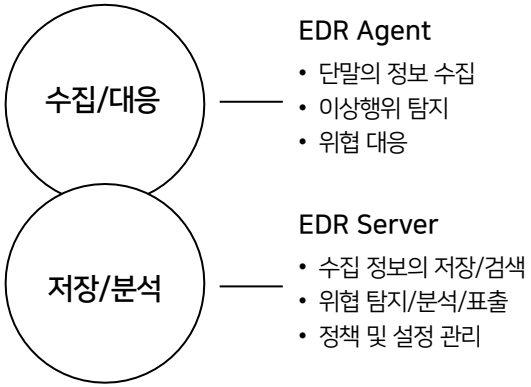
- Syslog, SNMP, Rest API 지원
- 다양한 연동을 위한 플러그인(모듈)을 개발하여 적용
- CTAS(Cyber Threat Analysis & Sharing) 연동 모듈 기본 탑재 (가입 후 연동 키 입력만으로 사용)



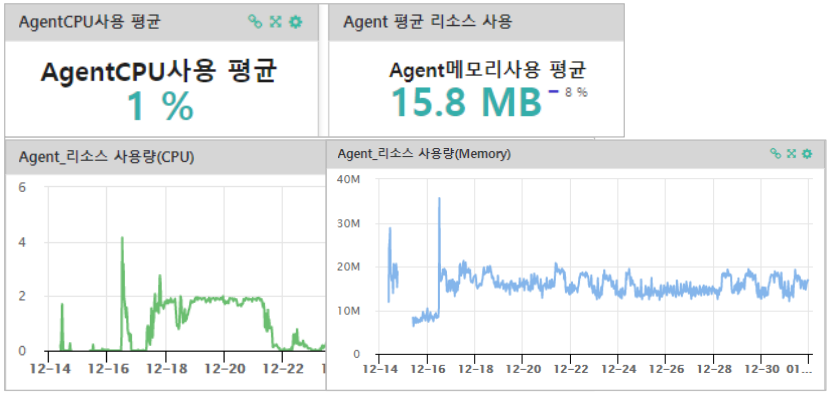
특장점 _ 안정성/호환성

Agent는 단말 영향을 최소화하여 이벤트 수집 및 이상행위를 탐지하고 대응 정책을 수행

✓ Agent는 정보 수집 및 이상행위 탐지/대응 분석은 서버에서 수행하여 단말 부하 최소화



✓ CPU, MEMORY 사용을 최소화하여 동작 /Agent 리소스 사용률 제한 기능 제공

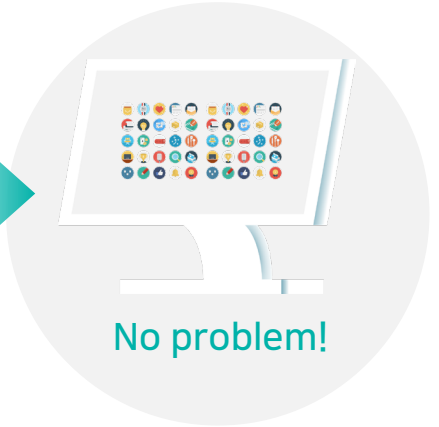


✓ 타 기업/기관 환경에서도 검증된 경량화, 안정적인 시스템(단말 영향 최소화 Agent)을 제공

각종 백신 솔루션

다양한 DRM 솔루션

1. 문서중앙화
2. 매체제어
3. DLP
4. NAC
5. 개인정보보호
6. SSO통합인증
7. PMS
8. 데이터 복원
9. 프린터 보안
10. 메신저
11. 소프트웨어 관리



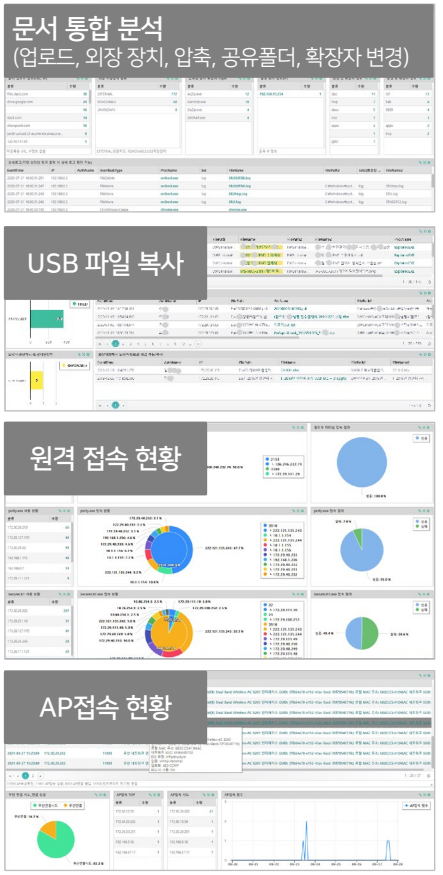
특장점 _ Discovery

CCTV처럼 필요시 녹화된 장면을 확인하듯, EDR을 통해 실시간 수집한 이벤트는 특정 시간에 특정 이벤트를 검색하여 확인

DATA(데이터)

Create File
Upload File
Copy File
Ping
Messenger
Share Folder
File Copy to USB
Connect Server
Compress

INFORMATION(유용한 정보)

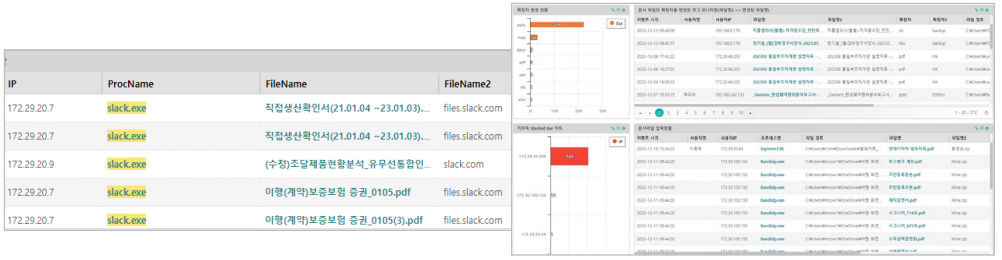


특장점 _ Discovery

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

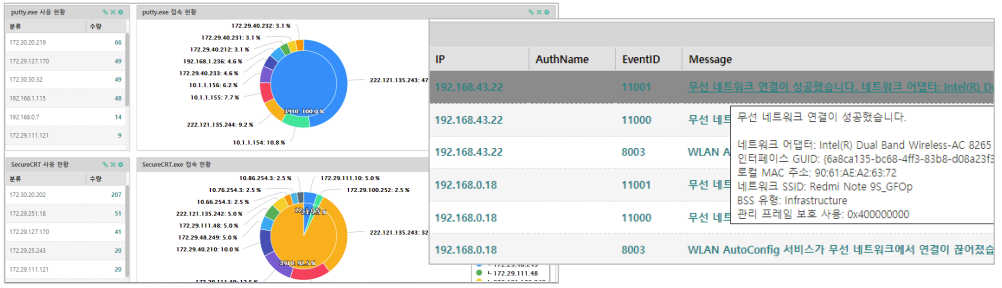
✓ 문서 현황 모니터링

- 문서/압축 파일 업로드 및 복사/이동
(Web, 메신저, 공유폴더, 외장 저장장치 등)
- 문서 확장자 변경
- 문서 압축 등



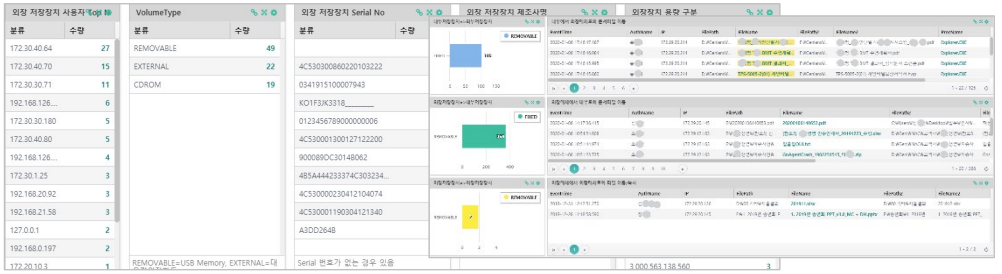
✓ 네트워크 접속 현황

- 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 _ Anti-Ransomware

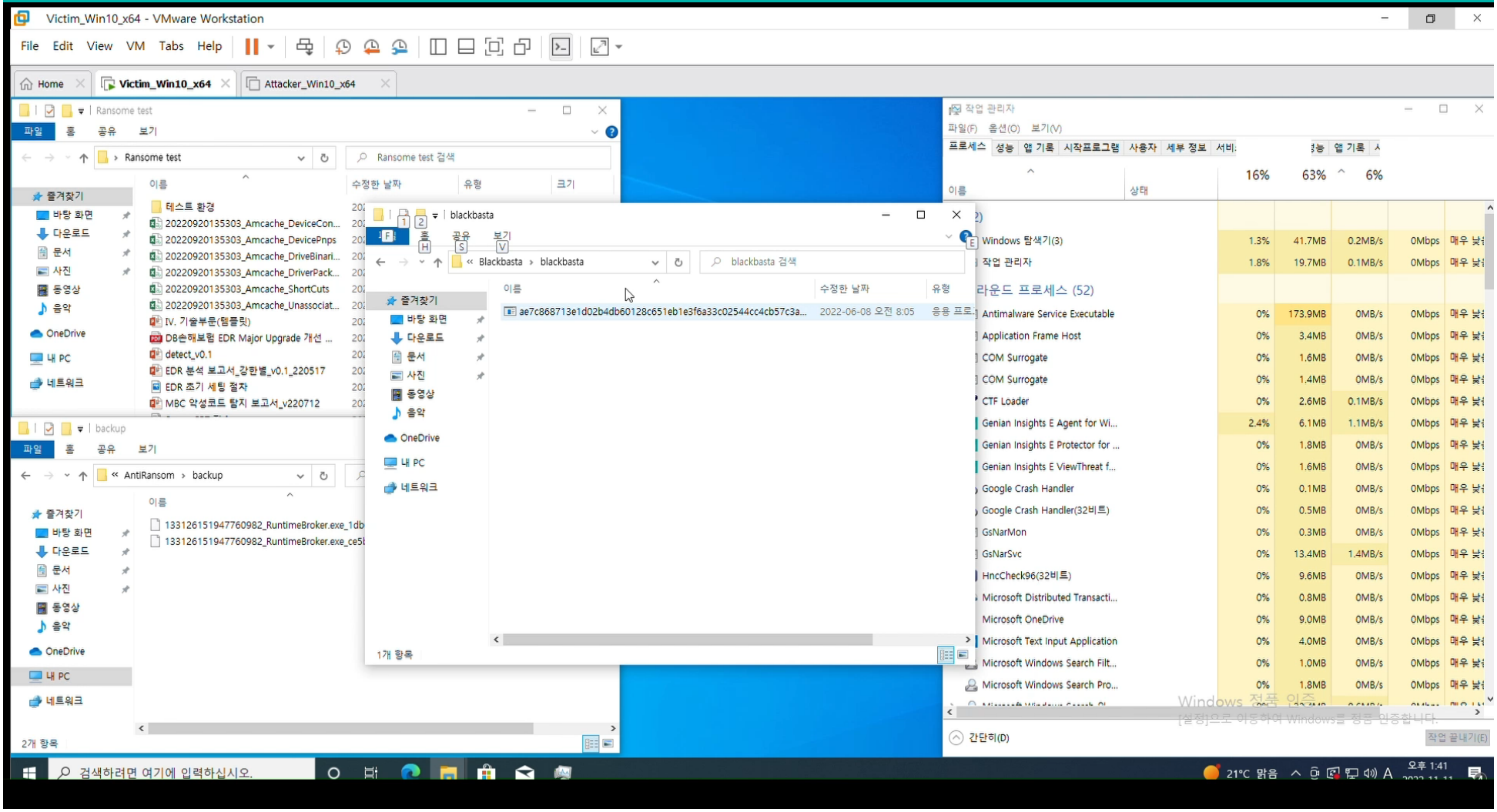
랜섬웨어에 특화된 전문 안티랜섬 탐지 엔진을 탑재하여 보다 정확하게 랜섬웨어를 탐지 및 차단

- 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

구분	기본 기능 : Window shadow copy 백업/복원(VSS)	고도화된 기능 : Anti-Ransomware
백업 대상 파일	시스템 파일을 제외한 전체 파일	랜섬웨어 감염 대상 파일(문서, 압축파일, 이미지 등)
백업 파일 확장자 지정	불가	지원
백업 공간	최소 5GB 이상 항상 사용	**사용자 디스크 여유 공간(Free space)의 10% 이내 사용 (권장 5GB 이상)**
백업 주기	스케줄링 백업 (일 1회)	**주기 없음 (암호화 작업 직전 대상 실시간 파일 백업)**
백업 방식	최초 전체 백업 후 증분 백업	**랜섬웨어 행위 발생 시 대상 파일 즉시 백업**
백업 위치	사용자 PC (Local Disk)	사용자 PC (Local Disk)
백업 데이터 보호	자체 보호 못함	**자체 보호 기능**
복구 방식	수동 복구	**랜섬웨어 감염 시 자동 복구**

특장점 _ Anti-Ransomware

[시연 영상] 랜섬웨어 감염 시 실시간 탐지 및 대응, 자동 복원 과정



III. 탐지 및 활용 사례

- S/W 취약점 이용 및 랜섬웨어 탐지
- 수집 정보 활용
- SOAR 연동

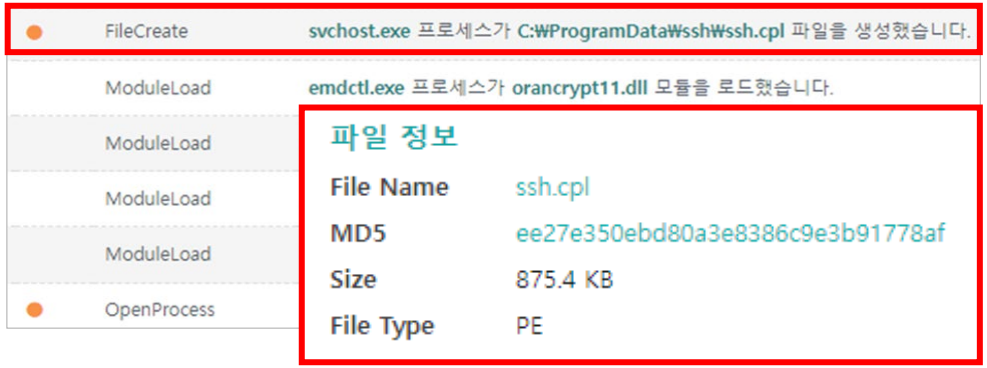
S/W 취약점을 이용한 위협 탐지

✓ 최초 감염

- **특정 금융보안프로그램 취약점을 이용한 악성코드 감염**

통신에 사용된 프로세스는 모두 일반적으로 네트워크 통신을 발생시키는 프로세스가 아닌, 악성코드에 의해 인젝션된 프로세스 혹은 정상 파일로 위장한 악성코드 파일에서 발생

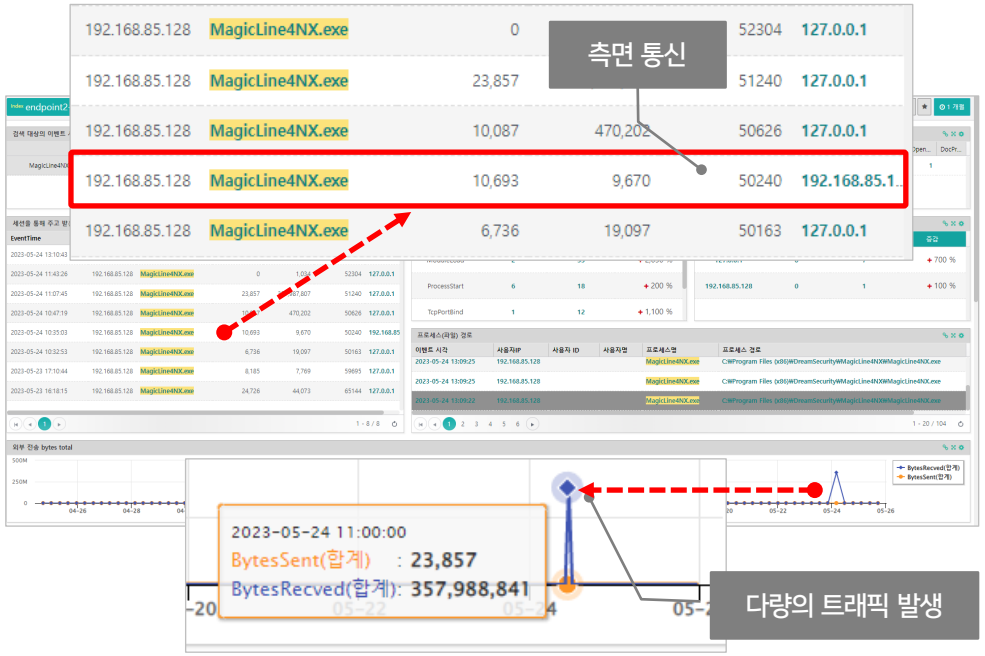
- **동 시간대에 시스템 프로세스(svchost.exe)에 의한 의심 파일 생성 행위도 확인**



S/W 취약점을 이용한 위협 탐지

✓ 확산 시도

동일 금융보안프로그램 취약점을 이용한 측면 이동 (Lateral Movement) 시도



✓ 내부망 침투

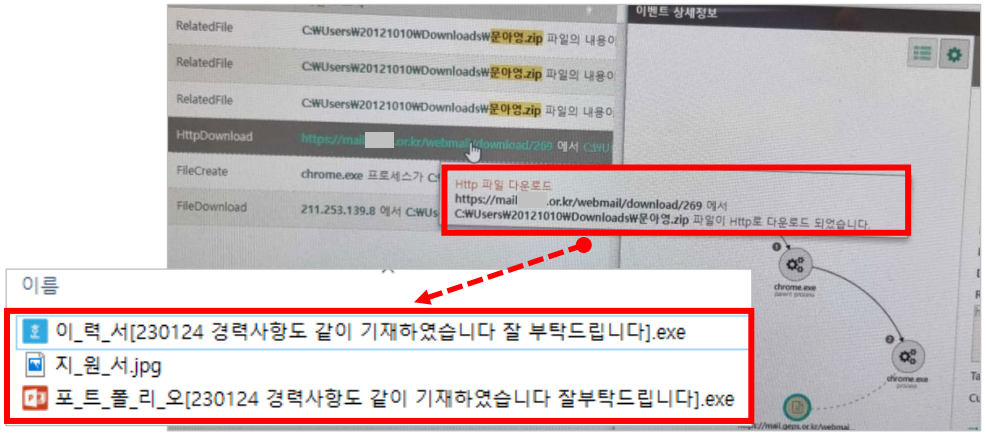
망간자료전송시스템 취약점을 이용한 내부망 악성코드 유입 및 자료유출 시도

- 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

이력서로 위장한 랜섬웨어 탐지

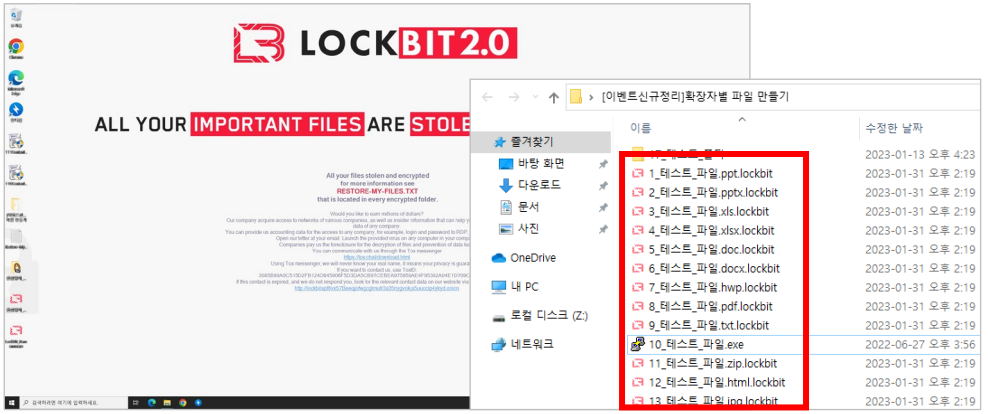
✓ 유입 경로

- 웹메일(https://mail.****.or.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



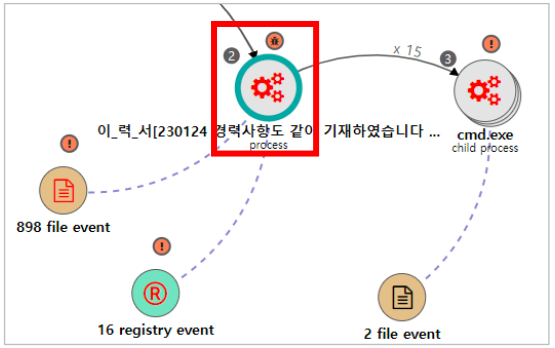
이력서로 위장한 랜섬웨어 탐지

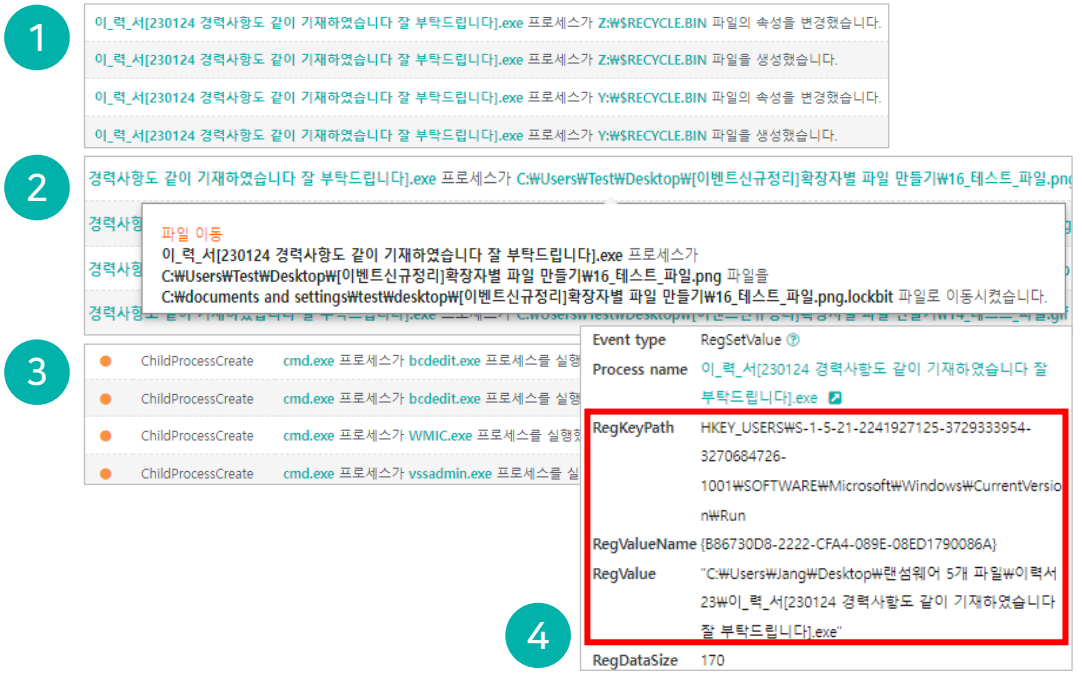
✓ EDR 분석 내역(이_력_서**.exe)

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

- EDR에서 각 행위 시 사용된 세부 명령 확인



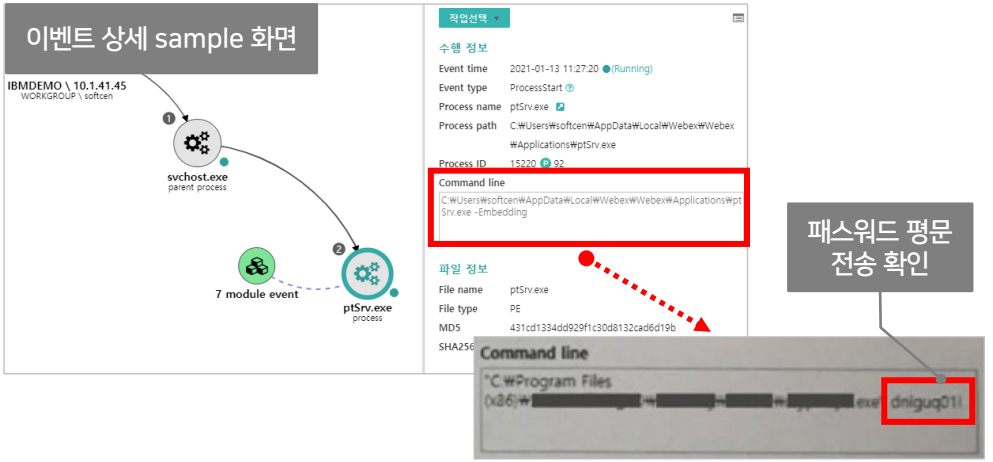


수집 정보 활용

✓ 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

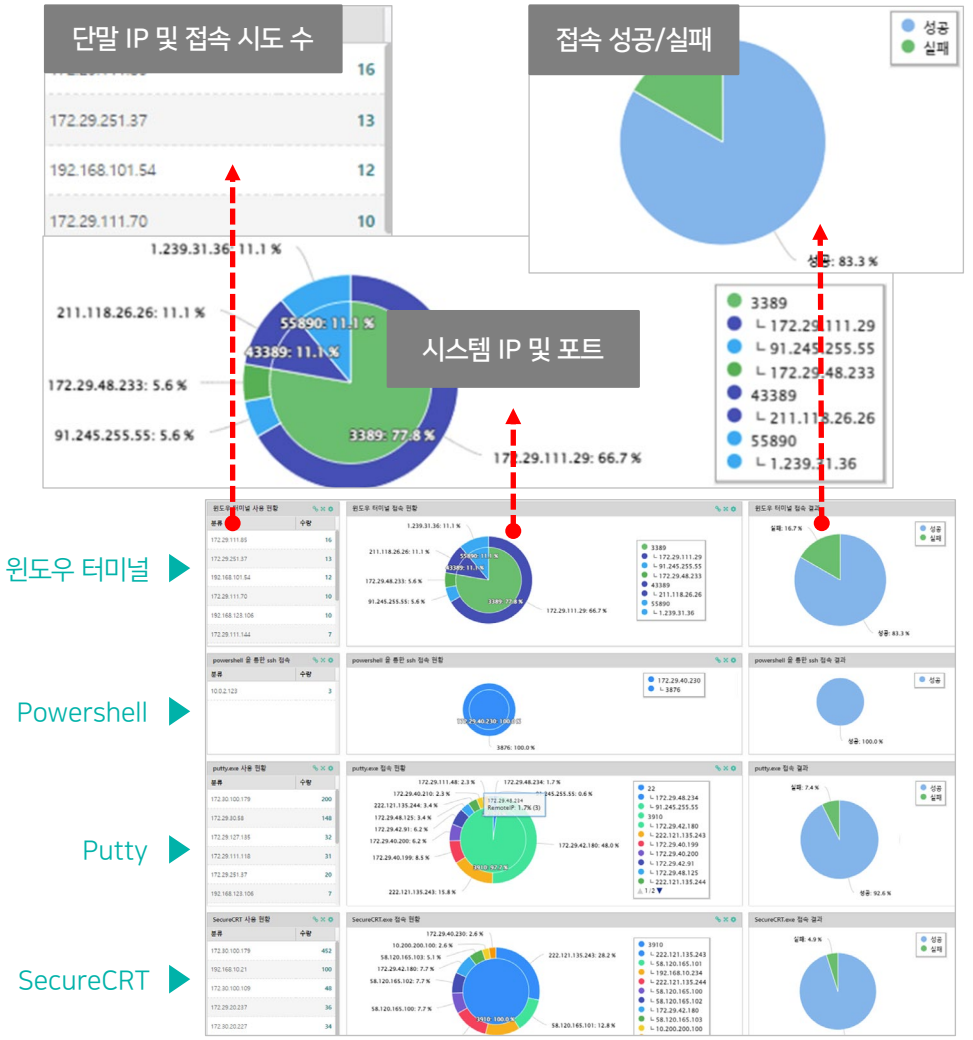
- 사용자의 우회 사용
- 매체 제어 솔루션 오동작으로 인한 사용

수집 정보 활용

✓ 시스템 접근 모니터링

서버 접속 시 시스템 접근 제어를 통하지 않고 직접 접속하는 사례 및 비인가 단말에서의 접근을 확인하여 조치

- 단말에서 원격 관리 툴을 통한 접속 이력 확인
- 시스템 접속 시도, 성공/실패, 사용 포트 등

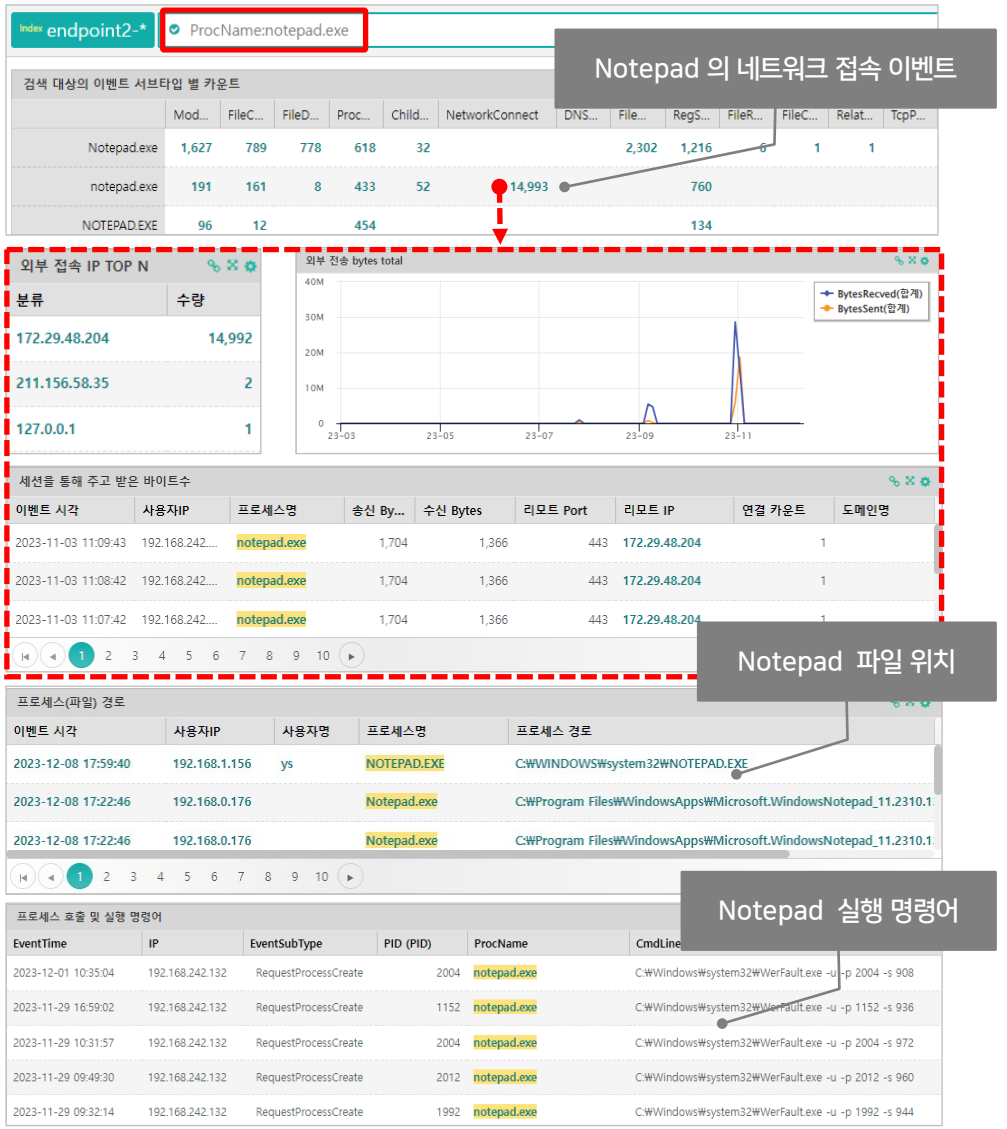


수집 정보 활용

✓ 위협 분석 및 검증

수집된 모든 정보는 다양한 형태의 대시보드로 재 구성하여 일반적이지 않은 행위와 위협 행위를 쉽게 구분하여 내부 위협 존재 여부를 파악하여 조치

- 취약점 프로그램의 전체 행위 중 위협 의심 행위 구분
- 특정 프로세스의 전체 행위를 확인하여 일반적이지 않은 행위 구분 및 분석
- 위협 IP 접속한 모든 프로세스 정보 확인



SOAR 연동

Genian EDR

단말 이상행위 탐지 및 대응 솔루션

- 위협 탐지 정보 전송

- IP, Hash 위협 정보 등록
- IP, Hash 위협 정보 차단 (Process Kill, Isolate)
- IP, Hash 위협 정보 차단 해제

syslog

API

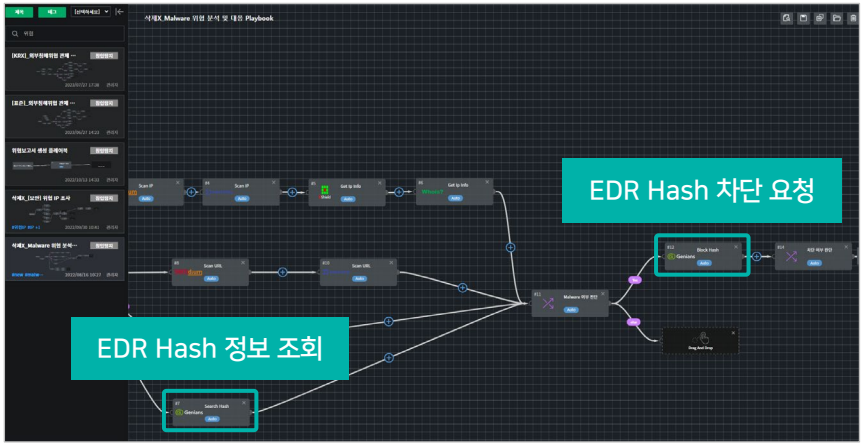
SOAR/XDR

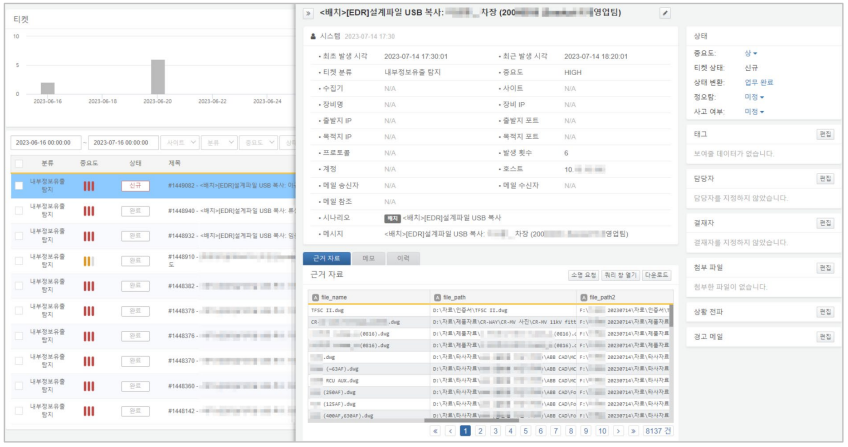
자동화 기반 통합보안관제솔루션

- 위협 탐지 정보 전송 수집
- 위협 탐지 이벤트
- 위협 탐지 상관분석

- IP, Hash 위협 정보 조회
- IP, Hash 위협 정보 차단 요청
- IP, Hash 위협 정보 차단 해제 요청

- SOAR는 Genian EDR 연동을 통해 단말 행위에서 발행하는 위협을 수집, 분석하여 관제를 수행
- SOAR는 타 보안장비에서 발생한 위협의 위협정보를 추출하여 EDR에 위협정보를 등록
- EDR에 IP, Hash(파일) 차단 요청을 수행하며, 자동분석 기능의 플레이북 구성을 통해 자동화된 보안관제 환경 구현





주요 고객사

공공 레퍼런스

금융/기업 레퍼런스

Summary

안정성
낮은 리소스 사용
충돌 회피 기술 적용

시장점유 1위
23년 조달 80%이상 점유
200여 곳 고객사 구축
(Agent 약60만대-24.01)

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

탐지/대응 기본
EDR 에서 제공하는
기본 이상의 다양한
기능+정보 제공

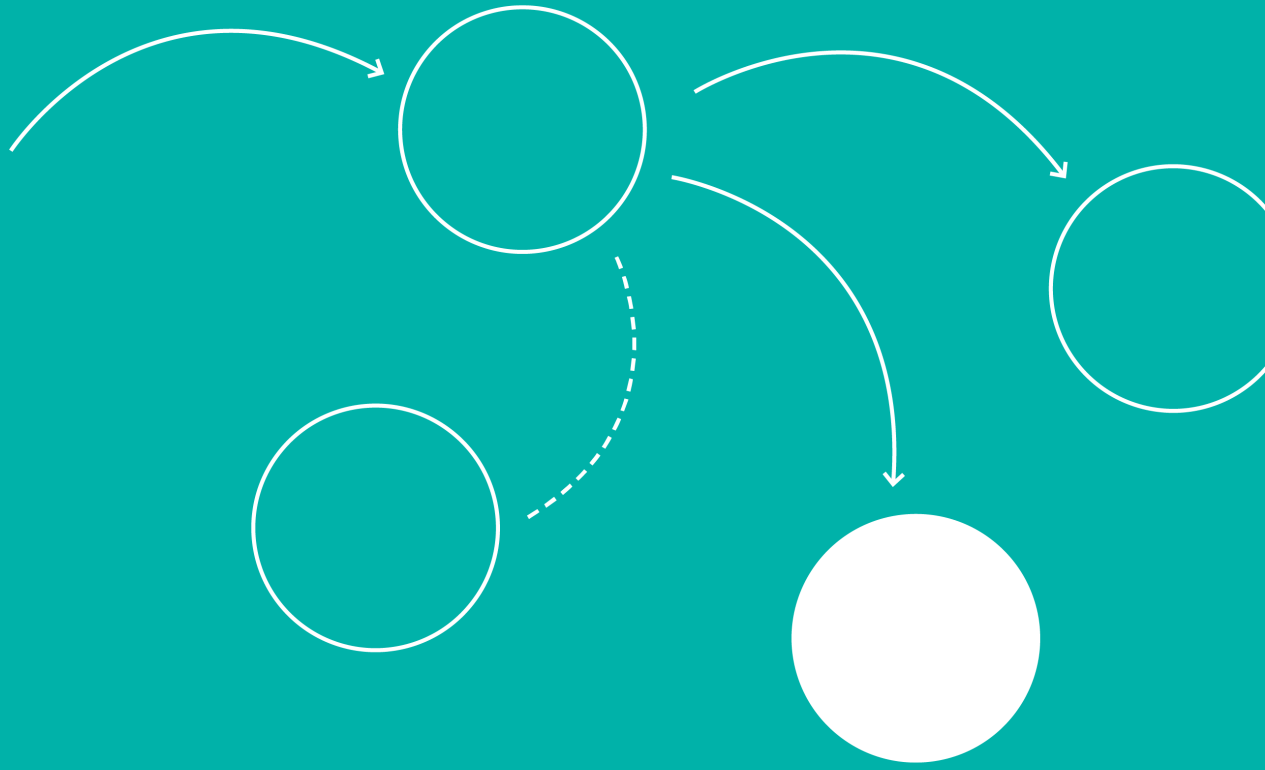
강력한 분석
수집된 정보를 활용
입체적인 분석 가능

안티랜섬웨어
특화된 안티랜섬웨어 기능
실시간 백업/탐지/대응/복원

장기간 로그 저장
로그 서버 추가 시
6개월 이상의 로그 보관
(+Scale Out)

다양한 지원
주기적 위협 정보 제공
위협 정보 확인 가능한 대시보드,
검색 조건 등의 제공

Thank you



Genians