Genians

엔드포인트 위협 대응의 모든 것

# Genian MDR

# INDEX.

Genians

# 01

## 개요

MDR 서비스 필요성
Genian MDR의 차별점

# MDR 서비스 필요성

Genians

## 왜 MDR이 필요한가? (보안 환경 변화)

### 지능화되고 자동화된 사이버 공격

최근 사이버 공격은 더욱 정교해지고 자동화되어 기존
보안 솔루션만으로는 완벽한 방어가 어려워지고 있습니다.
공격자들은 새로운 공격 기법을 지속적으로 개발하며
기업의 취약점을 노리고 있습니다.

### 전문 인력 부족 및 운영 부담 증가

기업 내부 보안팀은 전문 인력 부족과 늘어나는 보안 위협에
대응하기 어려워 운영 부담이 증가하고 있습니다.
또한, 최신 보안 기술을 따라가기 위한 교육 및 훈련의
필요성이 높아지고 있습니다.

**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.**

# Genian MDR의 차별점

Genians

제조사가 직접 운영·관리하는 차별화된 보안 서비스

## 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.

### 통합 보안 기능 제공

Genian MDR은 백신기능을 포함해 랜섬웨어 대응 및 매체제어를 통해 엔드포인트 보안 위협을 사전에 차단합니다. 통합된 보안기능으로 기업의 보안수준을 강화합니다.

### 최적의 탐지 & 대응 환경 제공

Genian Insights E 플랫폼 기반의 실시간 위협 탐지 및 분석, 자동화된 대응, 그리고 효율적인 보안 운영을 지원합니다.

Genians

02

# Genian MDR

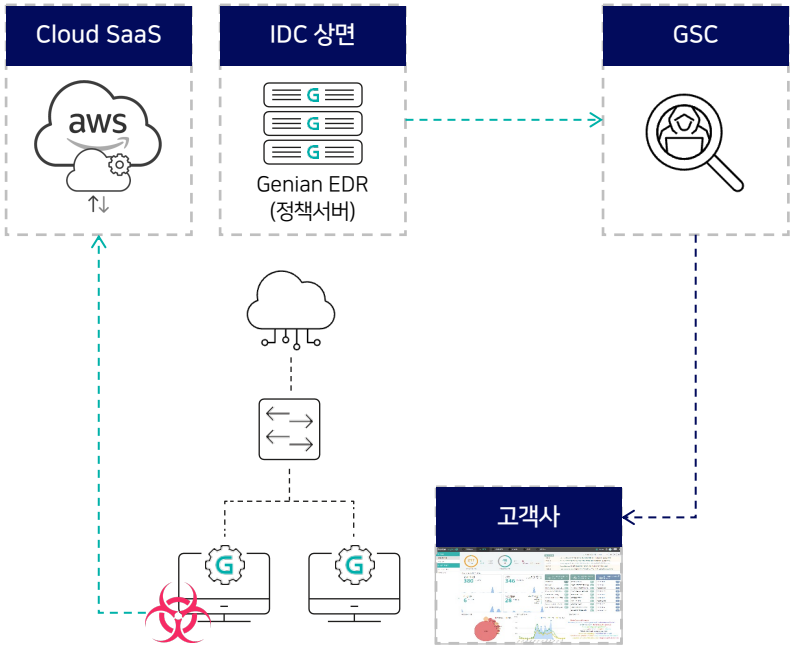
서비스 구성 및 대응 프로세스
서비스 제공 절차
서비스 상세 내용
도입 효과

# 서비스 구성 및 대응 프로세스

Genians

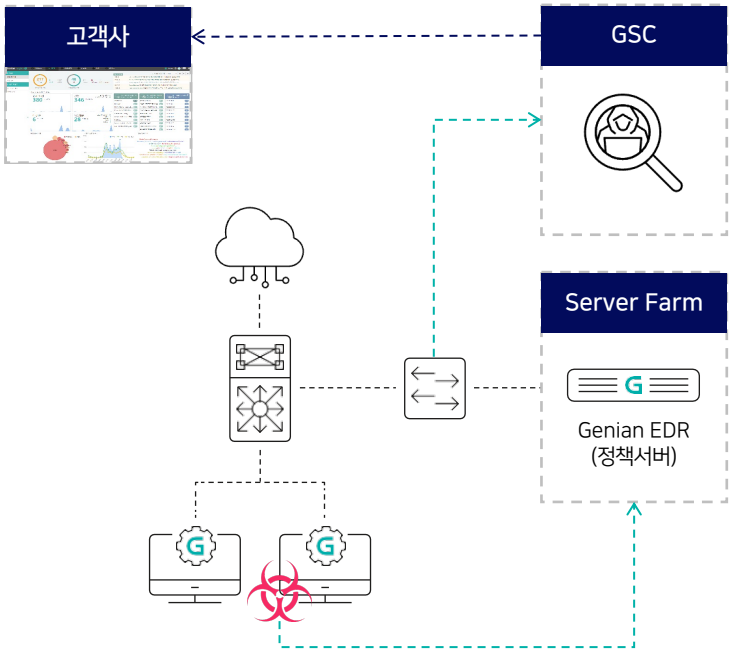
✓ 모든 환경에서 유연한 서비스 제공 (SaaS·IDC·On-Premise)

## Cloud SaaS 및 IDC 상면 서비스




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

## 구축형 고객(On-Premise)

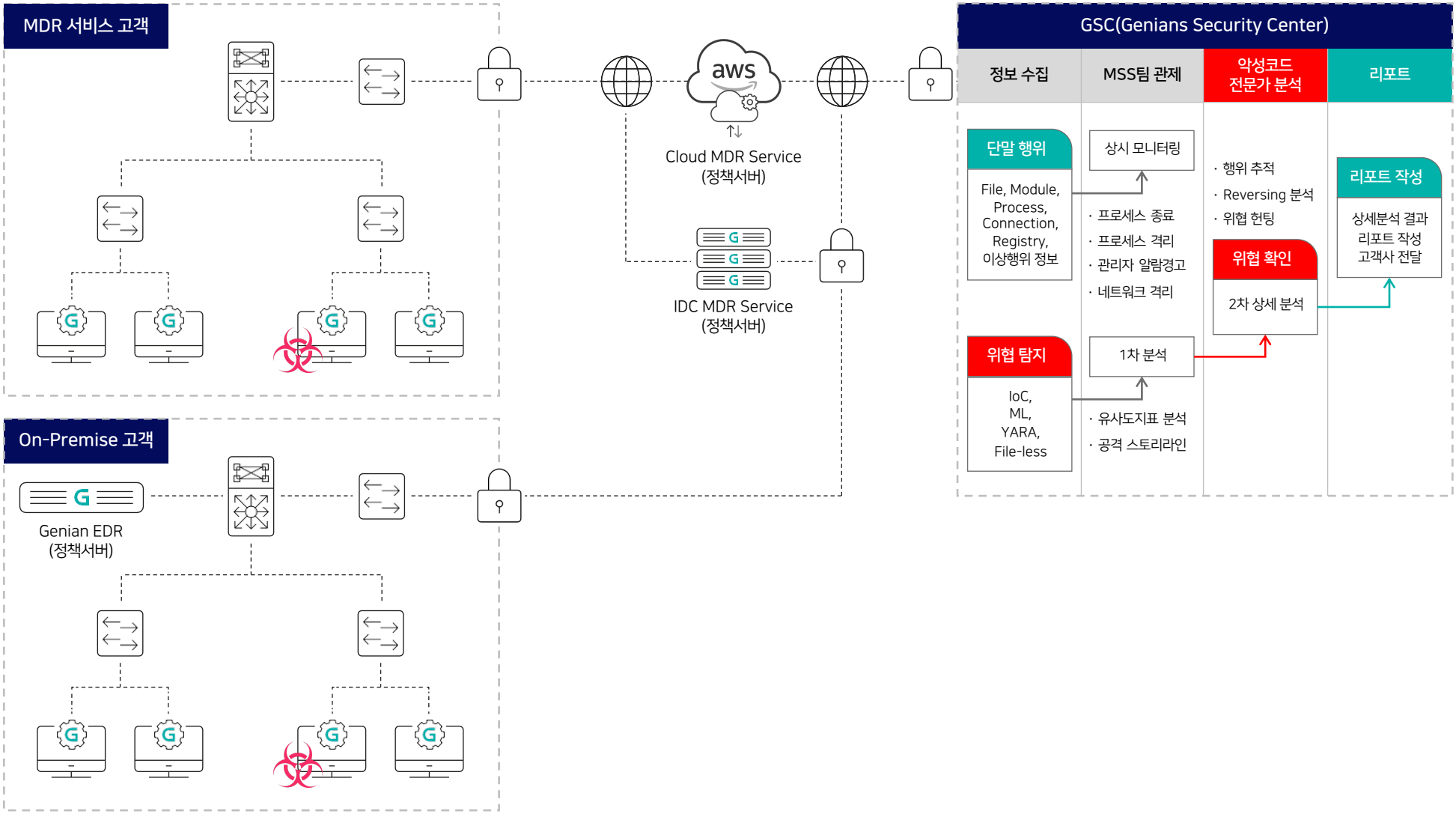



- 기존 구축형 고객사 환경에 맞춘 On-Premise MDR 서비스 지원
- 내부 보안 정책 및 요구사항 반영 가능

# 서비스 구성 및 대응 프로세스

Genians

## 서비스 기반의 보안 위협 탐지 및 대응 프로세스



# 서비스 제공 절차

Genians

## Genian MDR 서비스: 위협 탐지 · 분석 · 대응 · 리포트 제공

### 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 Fileless 위협 탐지
- 야라(YARA)를 이용한 사용자 설정 기반의 심층조사

### 3 위협의 대응

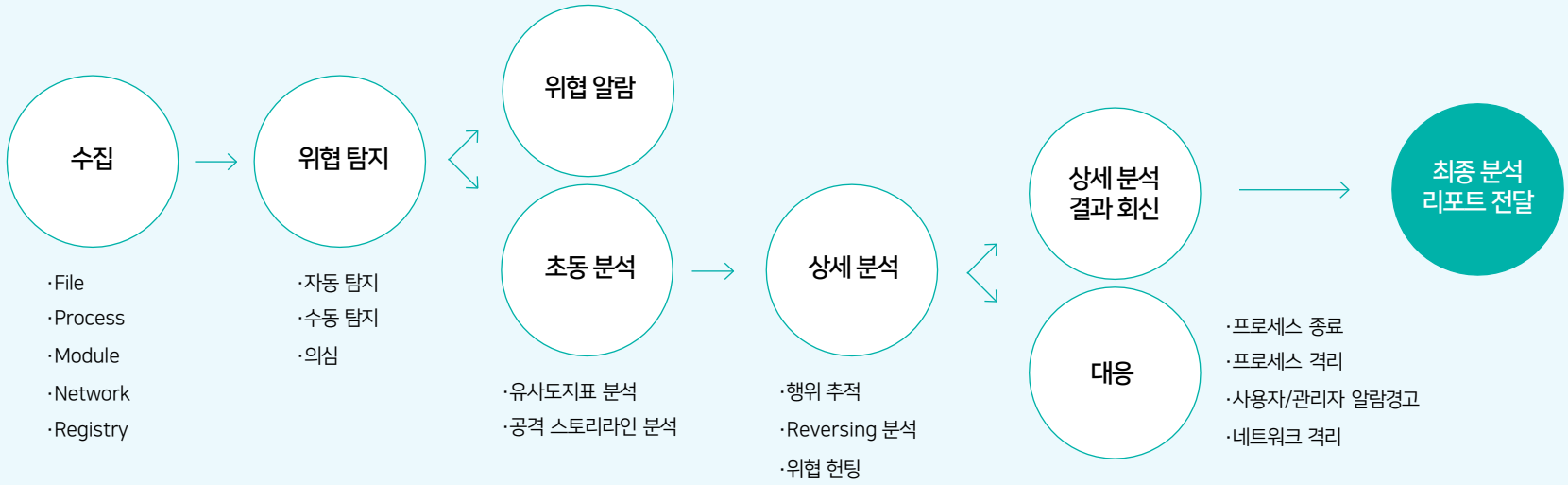
- 탐지된 위협 대상의 고지, 종료, 삭제, 네트워크 격리
- 알려진 위협 사전 대응
- 분석 후 대응(대응 시 동일 이벤트 자동 대응)
- 샌드박스, SIEM 등 기존 보안 솔루션 연동

### 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

### 서비스 제공 절차

MDR 서비스는 수집 → 탐지 → 분석 → 대응 → 리포트 전달의 과정을 통해 신속하고 정밀한 보안 대응을 제공합니다.



# 서비스 상세 내용

Genians

## MDR 서비스 상세 기능 및 보안 대응 프로세스

| 구분 | 서비스 내용 | 비고 |
|---|---|---|
| 실시간 모니터링 | 업무시간 실시간 위협 및 대응 | - |
| 위협 분석 | MDR 초기 대응 | · IoC(알려진 위협/File) 기반 및 XBA(알려지지않은 위협/Fileless) Rule을 통해 위협 탐지된 이벤트 대응 |
| | MDR 대응 상세 분석 | · 탐지 항목에 대한 위험도/신뢰도 등급 존재<br>- 위험도 : 상(High) / 중(Medium) / 하(Low)<br>- 신뢰도 : 0~100%<br><br>· 대응 상세 분석 보고서는 정탐으로 탐지된 위협 대상 中 필요 판단하에 정밀 분석 |
| 위협 대응 방안 | 선 대응 후 보고 | · 대응 안의 경우 고객과 사전 협의 필요<br>- File/Fileless 대응 방안 : 알림, 프로세스 강제종료, 파일 삭제, 네트워크 격리 |
| 상세 위협 대응 | Custom Rule / ComPliance 위반 정보 제공 | · 고객 요청 탐지 정책 적용<br>· 보안 이슈에 대한 탐지 정책 적용<br>· 고객사 컴플라이언스 위배 사항에 대한 고객 요청 탐지 정책 적용 (사규 제공 시) |
| | Threat Hunting | · Custom Rule 생성에 따른 이전 위협 행위 분석 |
| 보고서 | 리포트 보고서 제공 | · 위협 이벤트 기준 통계 현황 (월간 위협 리포트 제공) |
| 전문서비스 | 침해사고 분석 서비스 | · 기술 컨설팅팀 및 Genians Security Center(GSC) 전문 분석 서비스 (침해사고 발생 시) |
| | 악성코드 분석 서비스 | · 기술 컨설팅팀 및 Genians Security Center(GSC) 전문 분석 서비스 (파일 제공 시) |
| | 주요 보안 사고관련 대시보드 제공 | · ECO SYSTEM(자체 평판시스템) 연계 통한 추가 공유 대시보드 제공 |

# 도입효과

Genians

MDR 서비스 도입을 통한 보안 위협 대응 자동화 및 운영 효율성 극대화

## 지능형 위협 탐지 및 자동 대응을 통한 내부 자산 보호 및 보안 운영 강화

### 1. 실시간 위협 탐지

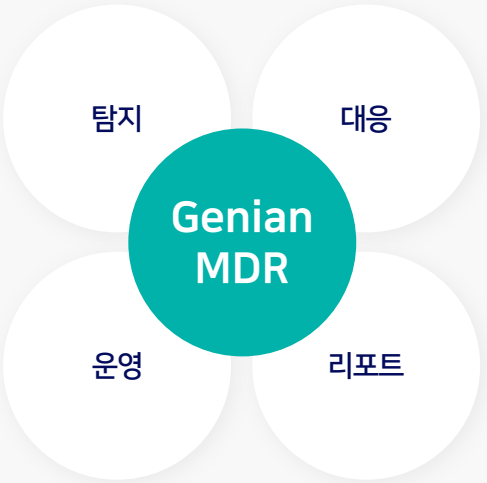
- AI/ML 기반 탐지로 알려지지 않은 위협 대응(Fileless 공격 등)
- IoC, YARA, 이상행위 분석을 활용한 정밀 탐지

### 2. 신속한 위협 대응 및 차단

- 탐지된 위협에 대해 자동 또는 전문가 분석 기반 조치 수행
- 악성코드 실행 차단, 프로세스 강제 종료, 네트워크 격리 등 선제적 대응

### 3. 침해 사고 대응 프로세스 강화

- 보안 사고 발생 시 행위 기반 공격 스토리라인 분석 제공
- 1차 탐지 후 전문가의 2차 상세 분석 및 대응 전략 제시




### 4. 운영 비용 절감 및 인력 부담 완화

- MDR 서비스를 통한 SOC 운영 부담 감소
- 모니터링 및 자동화된 탐지·대응 기능으로 보안 인력 최소화 가능

### 5. 최신 보안 위협 대응 역량 강화

- 랜섬웨어, APT 공격, 공급망 공격 등 지능형 위협에 대한 대응 강화
- 위협 헌팅 및 리버싱 분석을 통해 공격의 근본 원인 파악

### 6. 보안 리포트 제공 및 규제 대응 지원

- 탐지된 위협에 대한 상세 분석 리포트 제공
- 고객사 보안 정책 수립 및 내부 감사 지원

Genians

# 03

## 취약점 탐지 사례

S/W 취약점 이용 및 랜섬웨어 탐지
이력서로 위장한 랜섬웨어 탐지

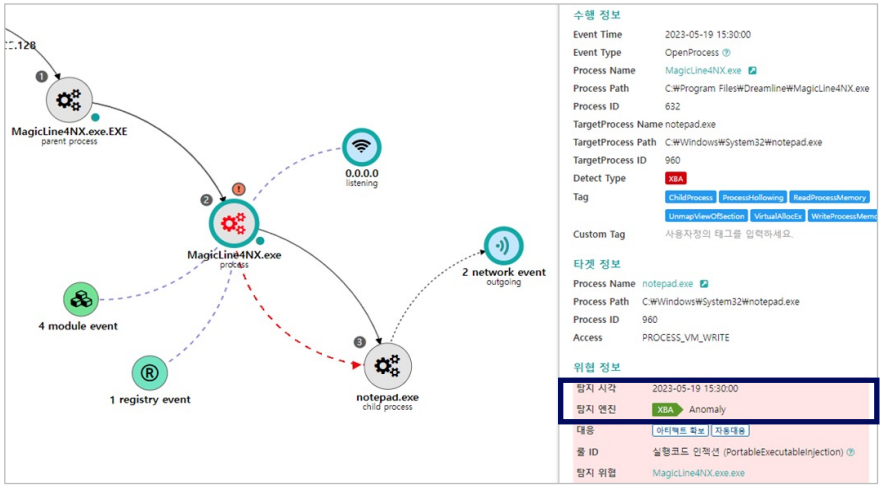
# S/W 취약점을 이용한 위협 탐지

Genians

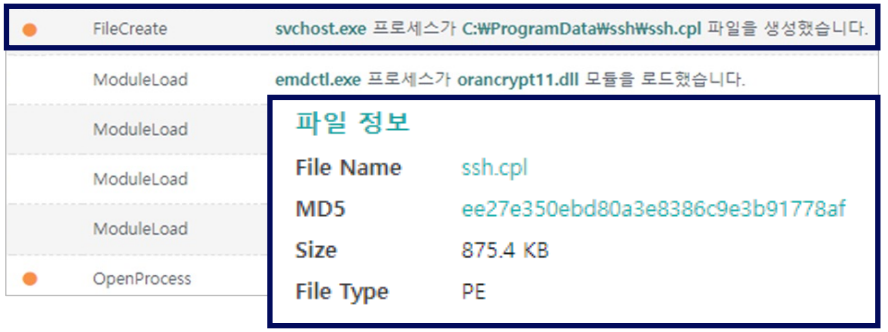
## 최초 감염

### 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

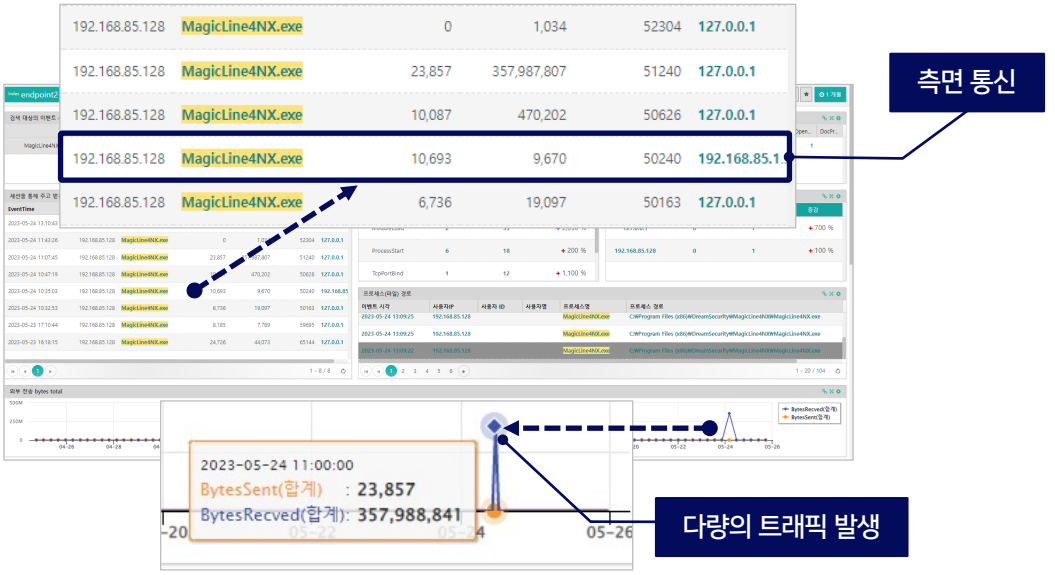


# S/W 취약점을 이용한 위협 탐지

Genians

## 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 유입 시키고, 해당 악성코드를 통해 다시 외부망으로 자료 유출 시도 확인
- 악성코드의 실행 명령어를 통한 침투 확인
- 외부 유출을 금지한 내부망 문서의 외부망 유입 경로 확인

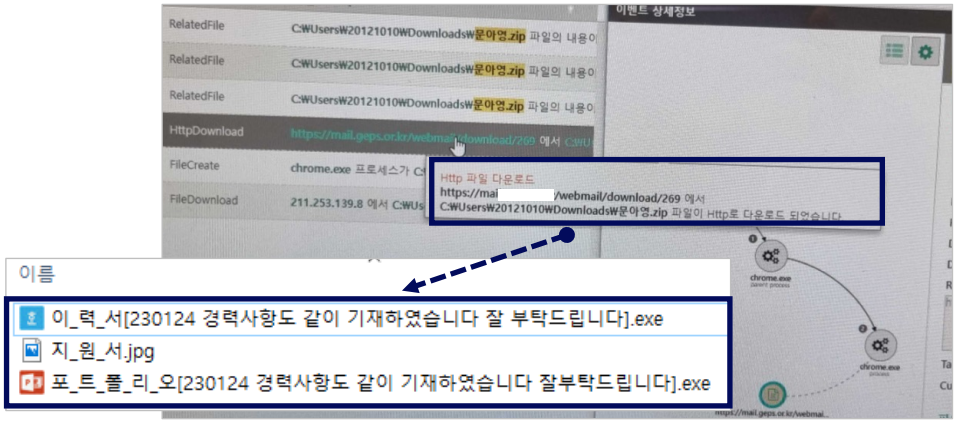
# 이력서로 위장한 랜섬웨어 탐지

Genians

## 유입 경로

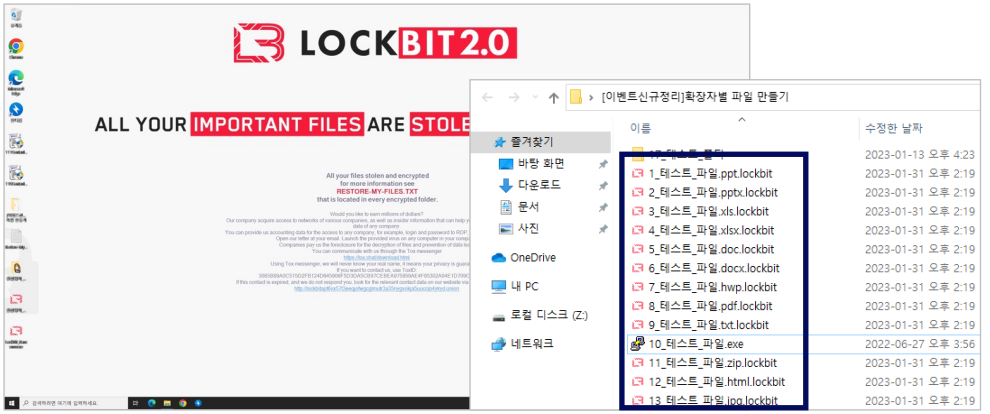
웹메일(https://mail.*****.or.kr/webmail/download/26)
통한 이력서 파일 다운로드

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

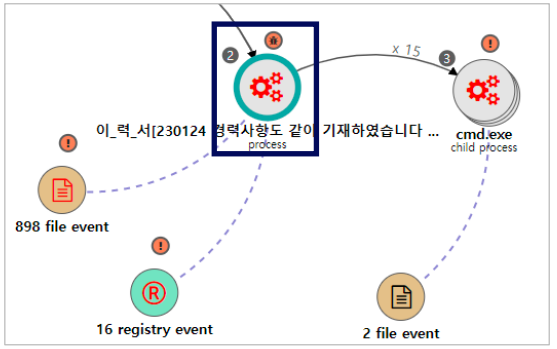
Genians

## 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) 명령 프롬프트를 수행 후 특정 명령어를 실행 (vssadmin.exe, WMIC.exe 등)
4) 부팅 시 재 실행되도록 AutoRun 등록

- EDR에서 각 행위 시 사용된 세부 명령 확인




1

이_력_서[230124 경력사항도 같이 기재하였습니다 잘 부탁드립니다].exe 프로세스가 Z:₩$RECYCLE.BIN 파일의 속성을 변경했습니다.
이_력_서[230124 경력사항도 같이 기재하였습니다 잘 부탁드립니다].exe 프로세스가 Z:₩$RECYCLE.BIN 파일을 생성했습니다.
이_력_서[230124 경력사항도 같이 기재하였습니다 잘 부탁드립니다].exe 프로세스가 Y:₩$RECYCLE.BIN 파일의 속성을 변경했습니다.
이_력_서[230124 경력사항도 같이 기재하였습니다 잘 부탁드립니다].exe 프로세스가 Y:₩$RECYCLE.BIN 파일을 생성했습니다.

2

경력사항도 같이 기재하였습니다 잘 부탁드립니다].exe 프로세스가 C:₩Users₩Test₩Desktop₩[이벤트신규정리]확장자별 파일 만들기₩16_테스트_파일.png

파일 이동
이_력_서[230124 경력사항도 같이 기재하였습니다 잘 부탁드립니다].exe 프로세스가
C:₩Users₩Test₩Desktop₩[이벤트신규정리]확장자별 파일 만들기₩16_테스트_파일.png 파일을
C:₩documents and settings₩test₩desktop₩[이벤트신규정리]확장자별 파일 만들기₩16_테스트_파일.png.lockbit 파일로 이동시켰습니다.

3

ChildProcessCreate cmd.exe 프로세스가 bcdedit.exe 프로세스를 실행
ChildProcessCreate cmd.exe 프로세스가 bcdedit.exe 프로세스를 실행
ChildProcessCreate cmd.exe 프로세스가 WMIC.exe 프로세스를 실행
ChildProcessCreate cmd.exe 프로세스가 vssadmin.exe 프로세스를 실

4

| | |
|---|---|
| Event type | RegSetValue |
| Process name | 이_력_서[230124 경력사항도 같이 기재하였습니다 잘 부탁드립니다].exe |
| RegKeyPath | HKEY_USERS₩S-1-5-21-2241927125-3729333954-3270684726-1001₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Run |
| RegValueName | {B86730D8-2222-CFA4-089E-08ED1790086A} |
| RegValue | "C:₩Users₩Jang₩Desktop₩랜섬웨어 5개 파일₩이력서23₩이_력_서[230124 경력사항도 같이 기재하였습니다 잘 부탁드립니다].exe" |
| RegDataSize | 170 |

Genians

# 04

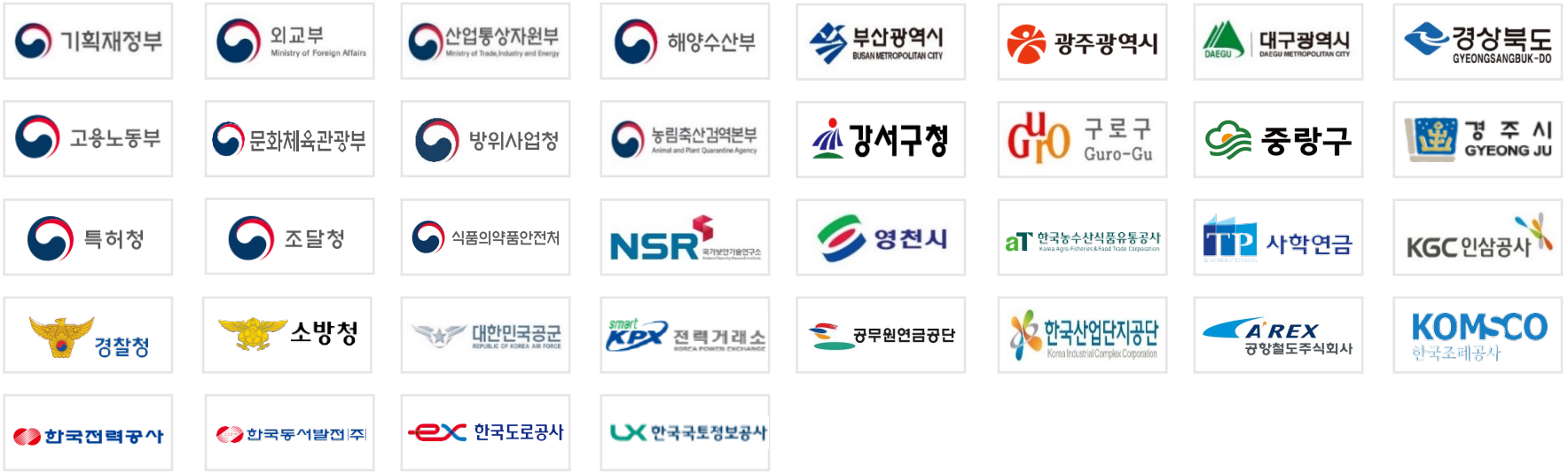
# 별첨

Genian EDR 레퍼런스
Summary

# 주요 레퍼런스

Genians

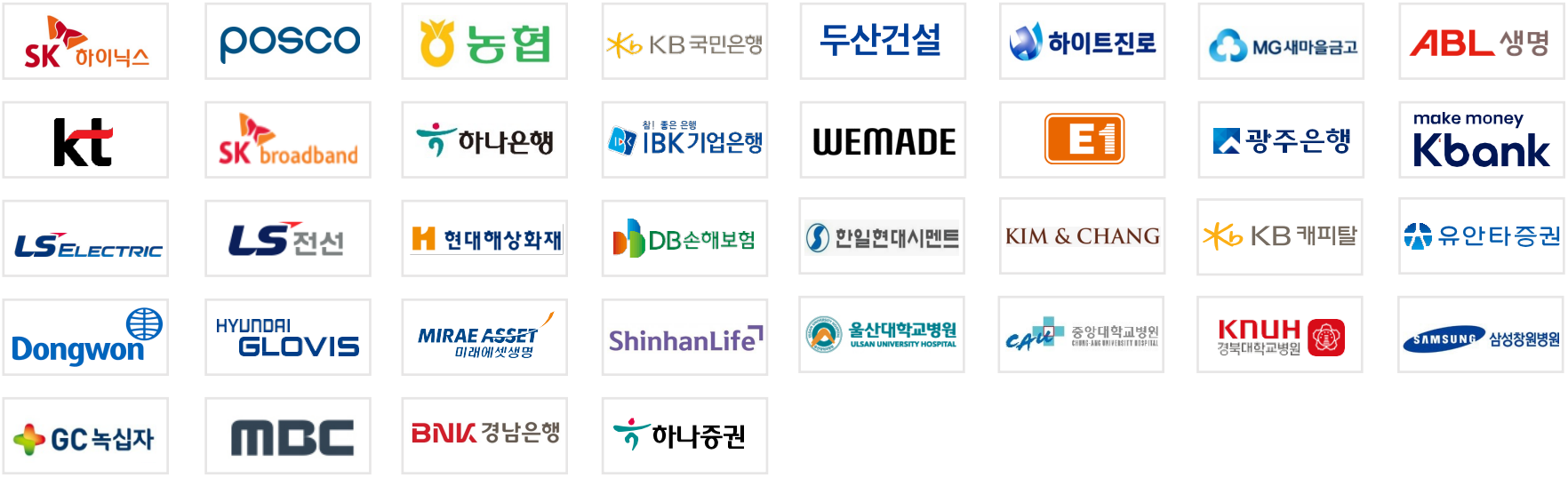
## 공공



# 주요 레퍼런스

Genians

## 금융/기업



# Summary

Genians

## 안정성

낮은 리소스 사용
충돌 회피 기술 적용

## 시장점유 1위


23/24년 조달 점유율 1위
240여 곳 고객사 구축
(Agent 약75만대-25.05)

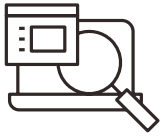
## 안티바이러스

백신 모듈이 추가되어
더욱 강력한 탐지 기능 제공
(필요에 따라 On/Off)

## 빠른 성능

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

## 강력한 분석



수집된 정보를 활용
입체적인 분석 가능

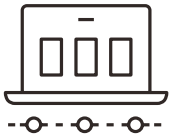
## 안티랜섬웨어

특화된 안티랜섬웨어 기능
실시간 백업/탐지/대응/복원

## 장기간 로그 저장

로그 서버 추가 시
6개월 이상의 로그 보관
(+Scale Out)

## 탐지/대응 기본



Genian Insights E 에서
제공하는 기본 이상의
다양한 기능+정보 제공

Genians

# Thank you!