

# Genian MDR

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.

## MDR 필요성

### 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 MDR 특징점

### 1. 제조사 직접 운영 지원

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

### 2. 최신 위협 인텔리전스 반영

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

### 3. 기업별 맞춤형 보안 정책 제공

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

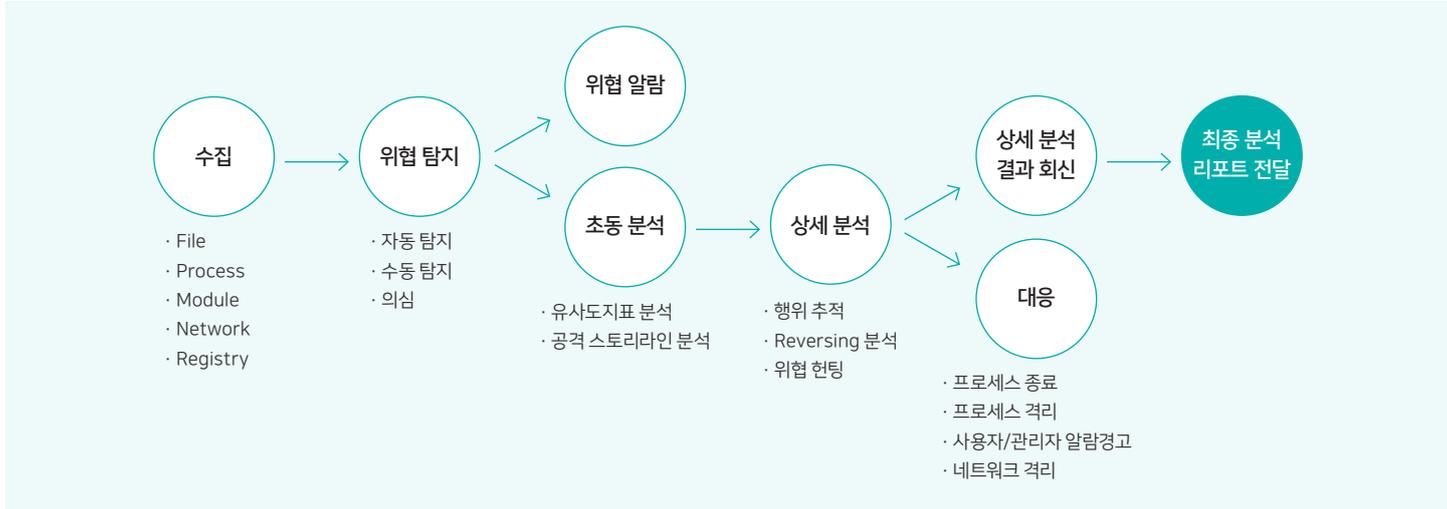
### 4. 최적의 탐지 & 대응 환경 제공

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

# 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 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

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



## 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 - 위험도: 상(High) / 중(Medium) - 신뢰도: 0~100% · 대응 상세 분석 보고서는 정탐으로 탐지된 위협 대상 중 필요 판단하에 정밀 분석
위협 대응 방안	선 대응 후 보고	· 대응 안의 경우 고객과 사전 협의 필요 - 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 · 보안 이슈에 대한 탐지 정책 적용 · 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 기존 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

