Data Sheet

Genian EDR v2.x

Genian EDR는 엔드포인트 영역에 대한 지속적인 모니터링을 수행하고 다양한 정보 수집을 통해 위협을 탐지하고 분석, 대응을 제공하는 단말 이상행위 탐지 및 대응 솔루션입니다.

Highlight

이벤트 정보수집 및 연동
- 외부 저장매체 사용 현황 및 파일 정보
- File, Module, Process, Network, Registry 정보
- Syslog, RESTful API, 손쉬운 연동을 위한 서버 플러그인 지원
- 다양한 Sandbox 연동(Trend Micro, Check Point…)

수집정보 검색
- 위협 사냥(Threat Hunting)
- 수집 정보 Full-Text 검색 제공
- 세부정보 탐색이 가능한 타임라인 차트 지원
- 사용자 정의 검색 필터 및 검색 데이터 세부정보 산출

분석정보 가시화
- 위젯 활용 이벤트 분석 정보 제공
- 16종 이상의 기본 분석 위젯 지원
- 관리자 정의 다양한 대시보드 설정 가능
- 위협 목록 및 분석 화면 제공

최신 위협 인텔리전스 활용
- IOC(침해지표), ML(머신러닝)을 통한 최신 위협 및 침해사고 대응
- 탐지된 위협에 대한 위험도, 신뢰도 , 유사도 및 유형 정보 제공
- 커스텀 Malware Hash/IP, Good Hash/IP 추가 및 관리 기능
- 행위 기반의 Fileless 위협 대응
- 관리자 정의(Custom) Rule 지원

엔드포인트 위협 분석
- 탐지된 위협의 상세 정보 제공, 의심 파일 수집
- 감염 및 접속 정보 모니터링 기능
- 파일 및 접속 프로세스 분석
- 이벤트 타임라인 및 연관 분석(Chain of Event)

엔드포인트 추적관리
- 이상 행위 프로세스 발생 시점 및 경로 정보 제공
- 위협에 대한 탐지 히스토리 관리
- 접속 프로세스별 추적 기능(사용자, 출발지 IP, 목적지 IP/포트 등)

안티랜섬웨어
- 랜섬웨어 행위(문서 암호화)에 대한 실시간 모니터링
- 랜섬웨어 탐지 시 실시간 파일 백업/복원 기능 제공
- 탐지된 랜섬웨어 파일 및 랜섬웨어에 의해 생성된 파일 즉시 삭제

보안기능 확인서

Challenges

보안위협의 지능화, 고도화

IT 환경이 급변함에 따라 보안 위협 또한 지능화, 고도화되며 다양한 경로를 통해 유입되고 있습니다. 또한 지속적으로 피해를 야기하고 있지만, 많은 기업과 기관들은 여전히 침해 사고에 무방비한 상태입니다.

기존 보안솔루션의 대응 한계

지능화, 고도화된 위협이 엔드포인트에서 실행 또는 은닉, 확산되고 있습니다. 그럼에도 불구하고 대부분의 기업, 기관에서는 Anti-Virus 제품과 네트워크 기반의 방어 체계로 대응하기 때문에 지능화되고 있는 엔드포인트 공격에 효과적으로 대응하기 어렵습니다.

전방위적인 위협 관리 및 대응 필요성

급변하는 위협 동향에 따라 엔드포인트 레벨에서 가시성을 높이고 다양한 탐지 기법을 활용한 악성코드/이상행위에 대해 조사, 분석하고 빠른 대응 체계를 구축하여 네트워크와 엔드포인트 등 내부 인프라 전반에 대한 체계적인 위협 관리 및 대응이 필요합니다.

key Features

지속 확장 가능한 가시성
- 단말의 모든 행위에 대하여 상시 수집
- 수집된 정보로 악성코드/이상행위에 대한 다양한 분석 기법 제공 (IOC, CTI *, YARA, 머신러닝, 행위 기반)
- 악성코드/이상행위에 대한 체인 이벤트 제공
- 관심 또는 연관성 있는 이벤트 간의 연결 고리 제공

* CTI : 지니언스 평판 시스템

수집된 데이터 기반 관리자 정의 대시보드

수집된 데이터의 분석 및 활용을 극대화하기 위해 관리자가 정의한 위젯을 통해 다양한 대시보드를 제공합니다.

Ecosystem

기업, 기관에서 수집된 위협을 Ecosystem으로 보내 위협에 대한 분석 결과(평판 서비스)를 제공하며 고객사에서 수집된 위협과 예외 처리된 데이터를 확인 및 가공하여 Genian EDR를 사용하는 기업, 기관에 재배포합니다.

Genians

Components&Deployment

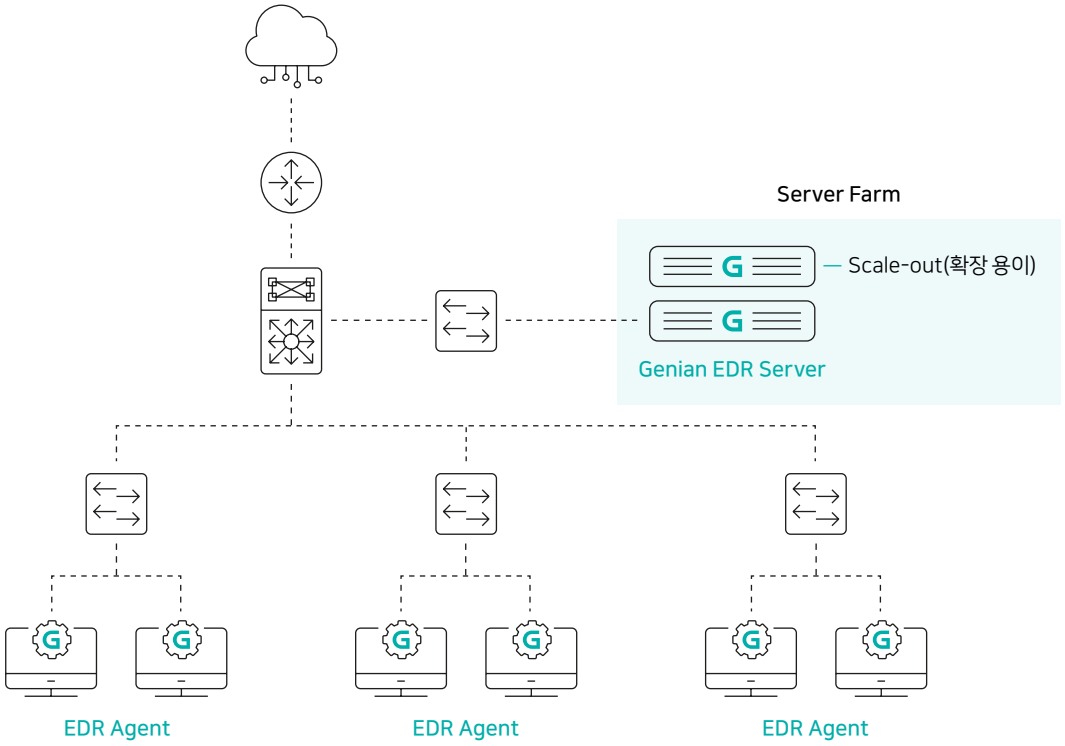
Genian EDR는 EDR Server/Agent로 구성됩니다. 각 구성요소의 역할과 동작은 기존 인프라에 미치는 영향을 최소화하도록 설계되었습니다. 그리고 Out-of-Band 동작 방식은 네트워크 성능에 영향을 주지 않으며 장애 발생 시 네트워크 영향을 최소화합니다.

EDR Server

- Data 분석을 통한 위협 및 이상 징후의 탐지
- 탐지된 위협의 상세 내용 분석
- 로그 저장 및 검색 기능 제공
- 이벤트 통합 분석 및 연관 분석, 시계열 분석, 근원 분석 등
- 관리자 단계별 권한 위임을 통한 효율적 관리
- 분석 내용의 보고서, 위젯, 대시보드 등 시각화 및 표출

EDR Agent

- 단말 주요 행위(파일, 프로세스, 접속, 레지스트리 등)의 모니터링 및 수집
- 추가 분석 필요한 PE 파일 Server 전송(샘플 수집)
- 위협 탐지 시 고지, 차단, 종료 등 단말 수준의 대응
- 위협 대상(파일 등)의 격리 및 사용자 알람, 네트워크 차단
- Off-Line 로그 수집



* Genian NAC 사용 시, NAC Agent에 EDR 플러그인(모듈) 형태의 간단한 배포와 인증정보 자동 연동 기능 제공

Specifications

EDR Server

- 자체 OS(이중화 및 DB 분리 구성 지원)
- 전용 어플라이언스 외 상용 서버 지원
- 표준 브라우저 지원(익스플로러, 크롬, 파이어폭스 등)

EDR Agent

- Windows 7/10/11 지원
- 단독 에이전트 설치
- Genian NAC 사용 시 에이전트 모듈로 추가
- 메모리 점유 9~12M
- 일 평균 10M 수준의 정보 수집*

Product Funtion

Category	Features
정보 수집	실행 파일 Features 및 전자 서명 정보 수집, 파일 생성, 수정, 삭제, 이동(파일 다운로드, 업로드 이벤트, 문서 open) 등 실시간 정보 수집
	프로세스 실행, 자식 프로세스 생성에 대한 실시간 정보 수집
	모듈 정보(DllLoad, DllInject, DllInjected) 관련 실시간 정보 수집
	Network Connect 및 TcpPortBind ,TCP/UDP 이벤트 관련 실시간 정보 수집
	레지스트리 생성, 삭제, 변경 관련 이벤트 정보 수집
	엔드포인트의 IP, MAC, 인증정보, 부서, 플랫폼, 플러그인 등 동작 및 운영 상태 정보 수집
	엔드포인트에서 발생하는 모든 이벤트를 Local DB에 저장, 서버와 통신이 되지 않는 환경에서 발생하는 이벤트에 대한 확인 가능
탐지 및 분석	탐지된 악성파일에 대한 샌드박스 연동을 통한 상세 행위정보 분석(TRENDMICRO Deep Discovery Analyzer, Checkpoint sandbox 등)
	엔드포인트에서 탐지된 악성코드 + 이상행위에 대한 종합적인 분석 화면 제공
	엔드포인트에 위협으로 탐지되는 파일을 수집하는 기능 제공
	탐지 위협/인시던트에 대한 관리 워크플로우 제공을 통한 상태 및 자동 해결 지원
	엔드포인트에 위협으로 탐지되는 파일 및 프로세스 관련 정보 제공
	탐지된 위협에 대한 다양한 시각화 정보 제공(Root Cause / Chain Analysis 등)
	HTTP 접속을 통해 다운로드받거나 IP를 직접 입력하여 파일을 다운로드할 경우 유입 경로에 대한 정보 제공
	엔드포인트에서 Domain Name으로 접속 시 IP와 함께 Domain Name 정보 제공
	머신러닝을 이용하여 악성으로 의심되는 파일을 탐지하는 기능
	YARA 규칙에 해당되는 악성 파일을 탐지하는 기능(엔드포인트 수동 검사 명령)
	정책/권한 우회: 시스템 설정 파일 및 계정의 임의 조작 행위 탐지
	의심스러운 프로세스 행위: 일반적이지 않은 파일, 프로세스 이름 또는 경로를 통한 프로세스의 실행 탐지
	시스템 명령어 오용: powershell, WMI 등 관리 목적 시스템 명령어의 일반적이지 않은 사용 탐지
	알려진 위협 탐지: RAT(백도어) 등 특정 공격 및 위협에 사용한다고 알려진 파일, 프로세스, 레지스트리 값, 접속 등의 행위 탐지
	권한탈취 또는 오용: 사용자 권한 (UAC : User Account Control) 정책 우회(Bypass)를 통한 불법 권한 획득 탐지
	자기삭제: 이상 행위 주체(파일, 프로세스 등) 및 로그(Log)등의 변경 또는 삭제 행위 탐지
	자동 재 실행: 윈도우 시작 폴더 또는 레지스트리 이상 값 등록 행위 탐지
	횡적 확산(Lateral Movement): 포트스캐닝 등을 통한 타 시스템으로의 감염 확산 시도 행위 탐지
	의심스러운 Office 행위 탐지: Word 등 Office 애플리케이션에 의한 매크로, 스크립트 등 동반 실행 행위 탐지
	Compliance 관점에서의 이동식 매체 사용, 복사, 파일 실행 탐지 기능
	문서에 관한 외부 유출(인터넷 업로드, 메신저, 공유 폴더, 외장 저장장치, 블루투스 등)에 대한 모니터링
	악성코드 유사도 SSDEEP HASH(%), AI 분석 지표 제공
	관리자 커스텀 룰 설정을 통한 탐지 기능 제공
	위협 의심 단말기에 원격(Remote Shell) 접속하여 분석할 수 있는 기능 제공
	탐지된 위협을 Ecosystem을 통해 추가 검증하고, 정보가 등록된 파일의 경우 파일 정보를 표시하는 기능 지원
	랜섬웨어 탐지 시 실시간 파일 백업/복원 기능 제공
대응	탐지된 악성 파일 격리 및 삭제
	파일 원격 수집(Fetch)
	사전 프로세스 차단(Block)
	실행중인 프로세스의 강제 종료(Kill) 및 덤프(Dump)
	위협 탐지 단말의 네트워크 격리(추가 조치 및 분석 가능)
	탐지된 위협의 사용자 및 관리자 알람(팝업, 이메일)
	단일 및 복수 단말 대상 일괄 대응 조치(Global Ban)
	동일한 위협의 재발견 또는 탐지 시 자동 대응
관리	대시보드 위젯 자유 배치, 다양한 위젯 및 레이아웃을 통한 데이터 분석/시각화 지원, 다중 탭 지원
	위젯 및 대시보드 내보내기/가져오기 기능 지원
	Agent 그룹 관리 기능
	권한에 따른 관리 역할 설정, 관리자 별 대시보드 화면 구성/데이터 출력 항목/배치에 대한 개인화 지원
	사용자 정의 IOC 및 YARA Rule 관리 기능
	진단 규칙 별 예외 처리 설정 화면 제공
	탐지된 위협 예외 처리 공유를 위한 오탐지 보고 제공(Genian Ecosystem)
	제품에 포함된 버전 이외에 최신 머신러닝 모델 업데이트 기능 제공
	폐쇄망에서의 IOC, 유사도, AI 분석 지표 수동 업데이트 기능 제공
	Agent가 설치된 PC의 리소스(CPU, MEMORY, DISK) 사용률과 Agent가 사용하는 리소스(CPU, Memory, Disk) 사용률 제공
	지정 조건의 이벤트/로그 검색 필터 저장 및 조회 기능 제공
구성	서버 성능 최적화 및 확장을 위한 Scale Out 구성 지원
	신규 데이터 Hot Node에 저장, 오래된 데이터는 Warm Node에 분리 저장하여 장기간 데이터 보관 구조 제공

Appliance Line Up

EDR Server

모델명	ES30	ES50
모델 이미지		
CPU	Intel 2.1G (8C16T) * 1	Intel 2.1G (8C16T) * 2
Memory	64GB	128GB
HDD/SSD	10TB/1.92TB	10TB/3.84TB
Port	1G/10G * 2	1G/10G * 2

14058 경기도 안양시 동안구 벌말로 66 평촌역 하이필드 지식산업센터 A동 12층
기술지원: 1600-9750(평일 오전 9시~오후 7시) / 도입문의: sales@genians.com