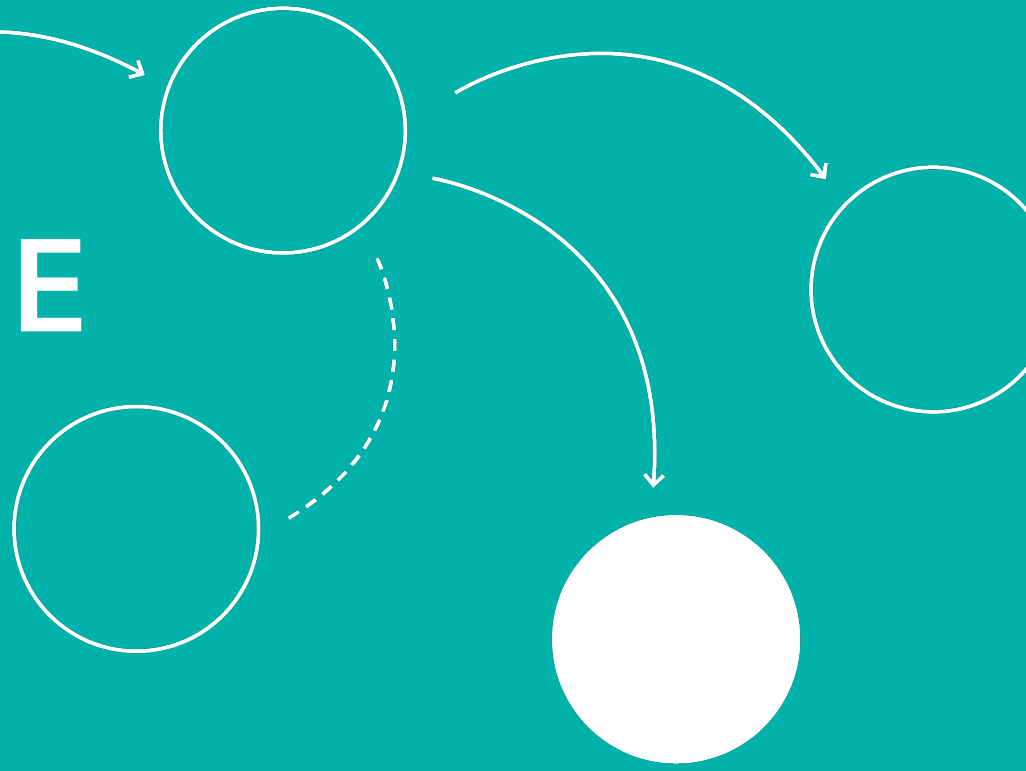
통합 단말 보안 플랫폼

Genian Insights E



Genians

Table of Contents

I. 개요

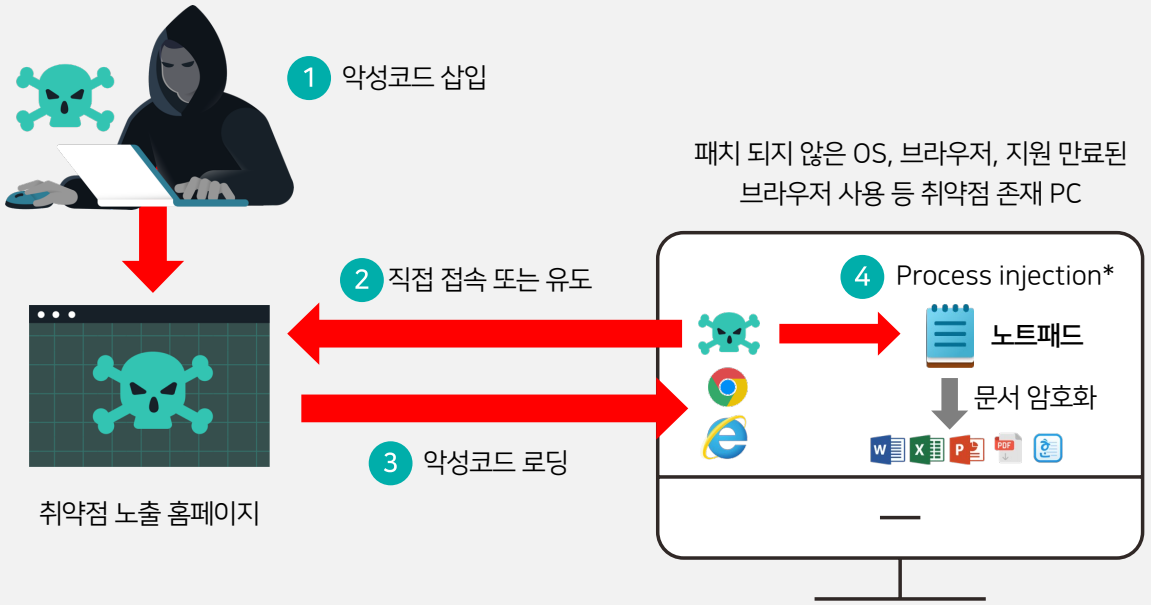
- 기존 보안 체계를 회피하는 고도화된 해킹 기법
- 엔드 포인트의 필수 요소

기존 보안 체계를 회피하는 고도화된 해킹 기법

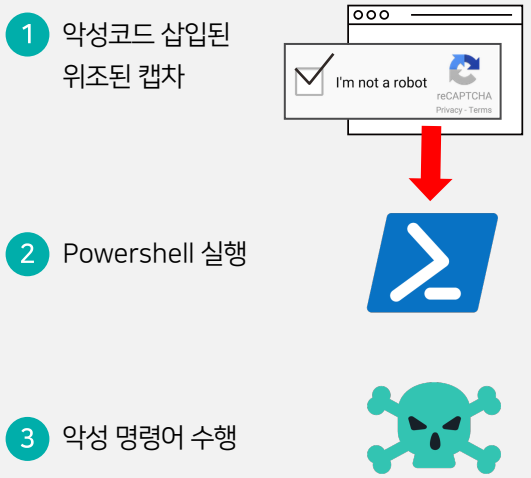
다양한 형태로 발전하는 해킹 기법은 기존의 보안 솔루션을 회피하며 내부에 침투하여 정보 유출 및 파괴를 하고 있습니다.

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



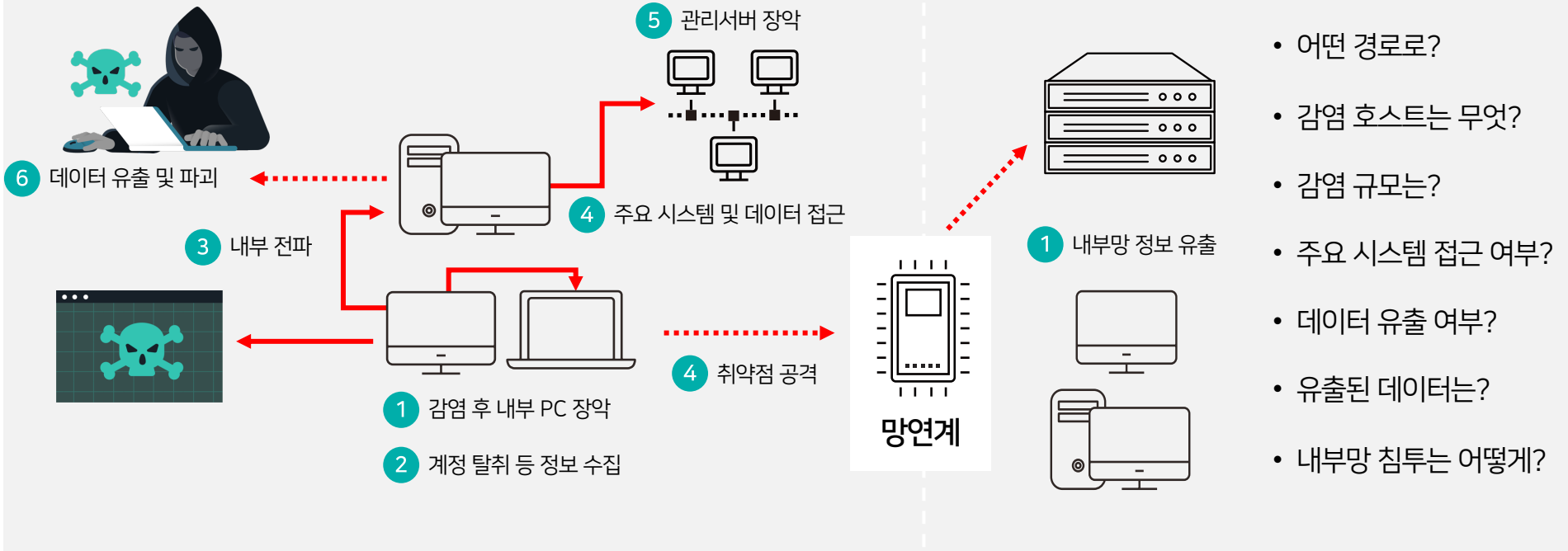
* Process Injection : 정상 프로그램에 악성코드를 삽입하여 이상행위를 수행시키는 기법

엔드포인트의 필수 요소

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



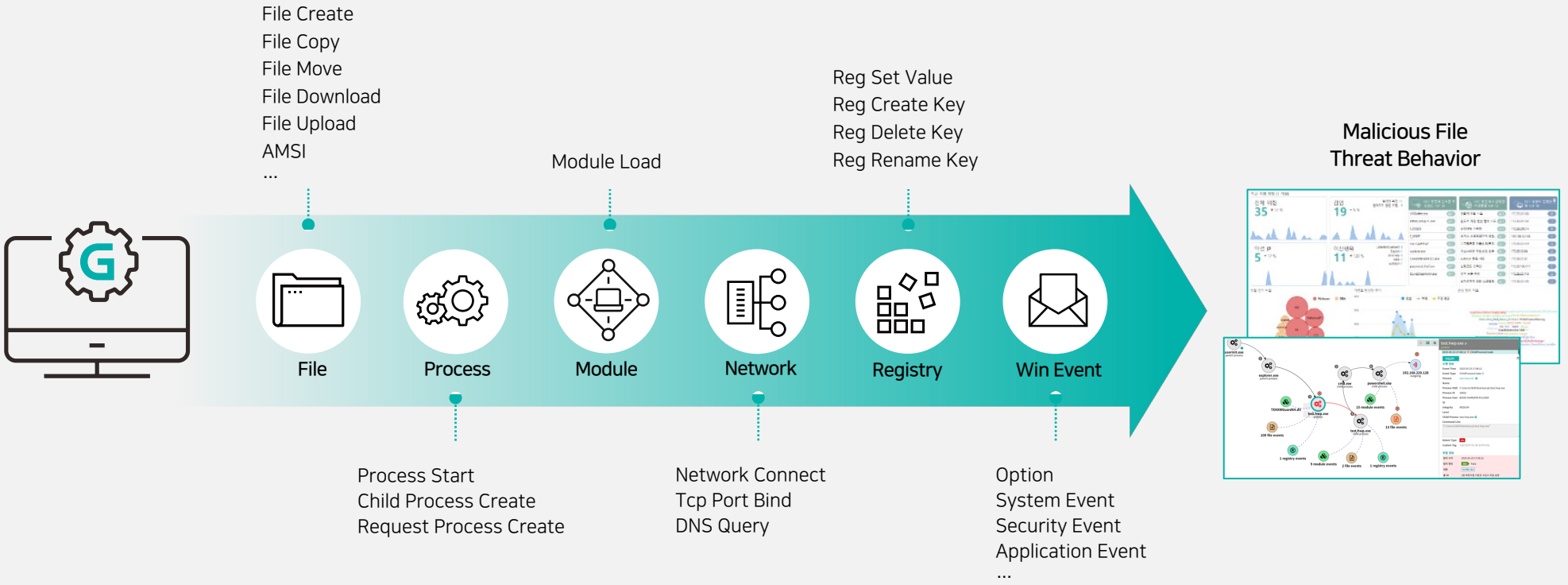
- 어떤 경로로?
- 감염 호스트는 무엇?
- 감염 규모는?
- 주요 시스템 접근 여부?
- 데이터 유출 여부?
- 유출된 데이터는?
- 내부망 침투는 어떻게?

II. Genian Insights E

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

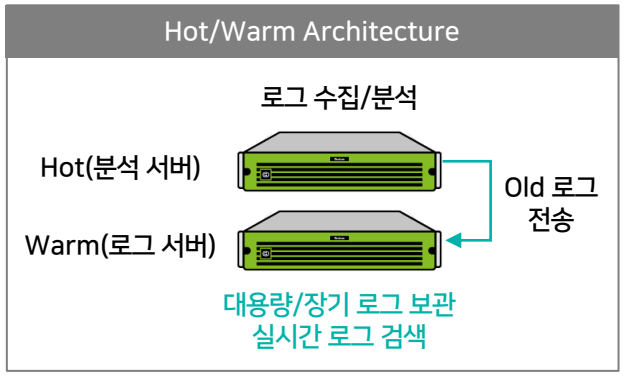
개요

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.



구성

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.

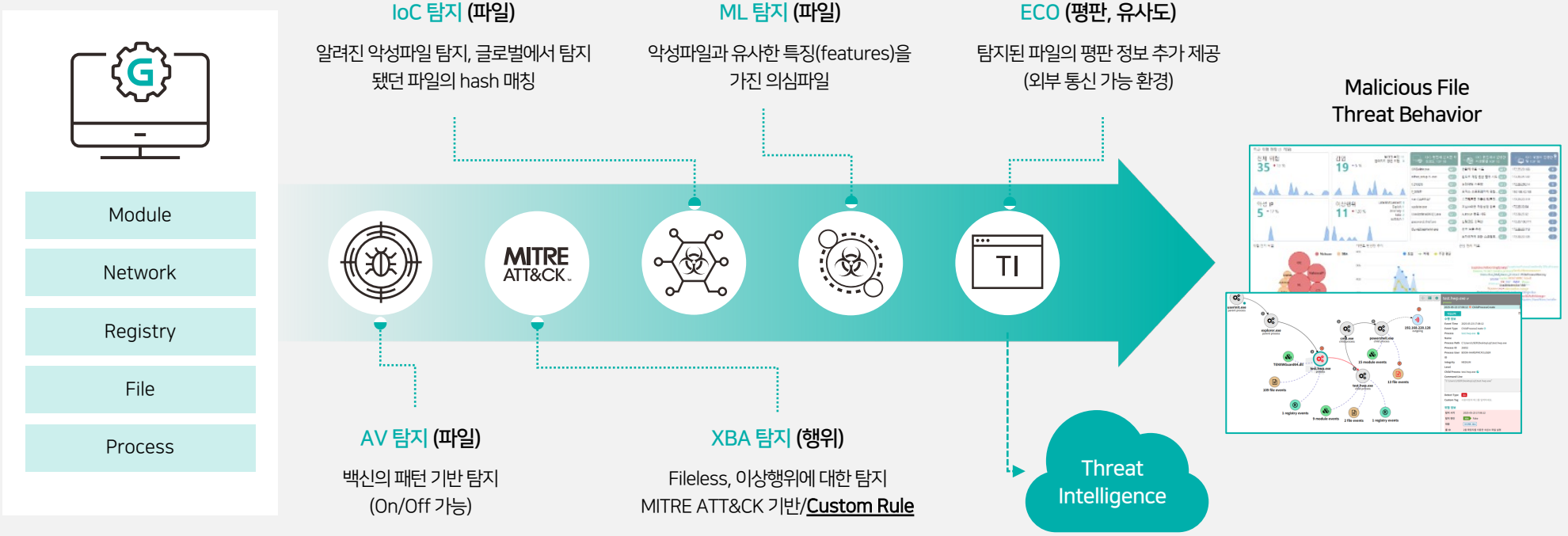


※ Old 로그 : Hot 서버 내 지정한 로그 저장 일을 초과한 과거 로그 (예 - Hot : 3개월, Warm : 9개월)

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

탐지 방식

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.



대응

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

위협 대응

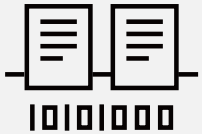
파일 격리/삭제

네트워크 격리

프로세스 종료

사용자 알림

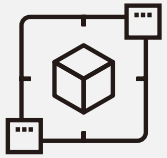
위협 시 아티팩트 자동 수집



파일 수집

레지스트리 수집

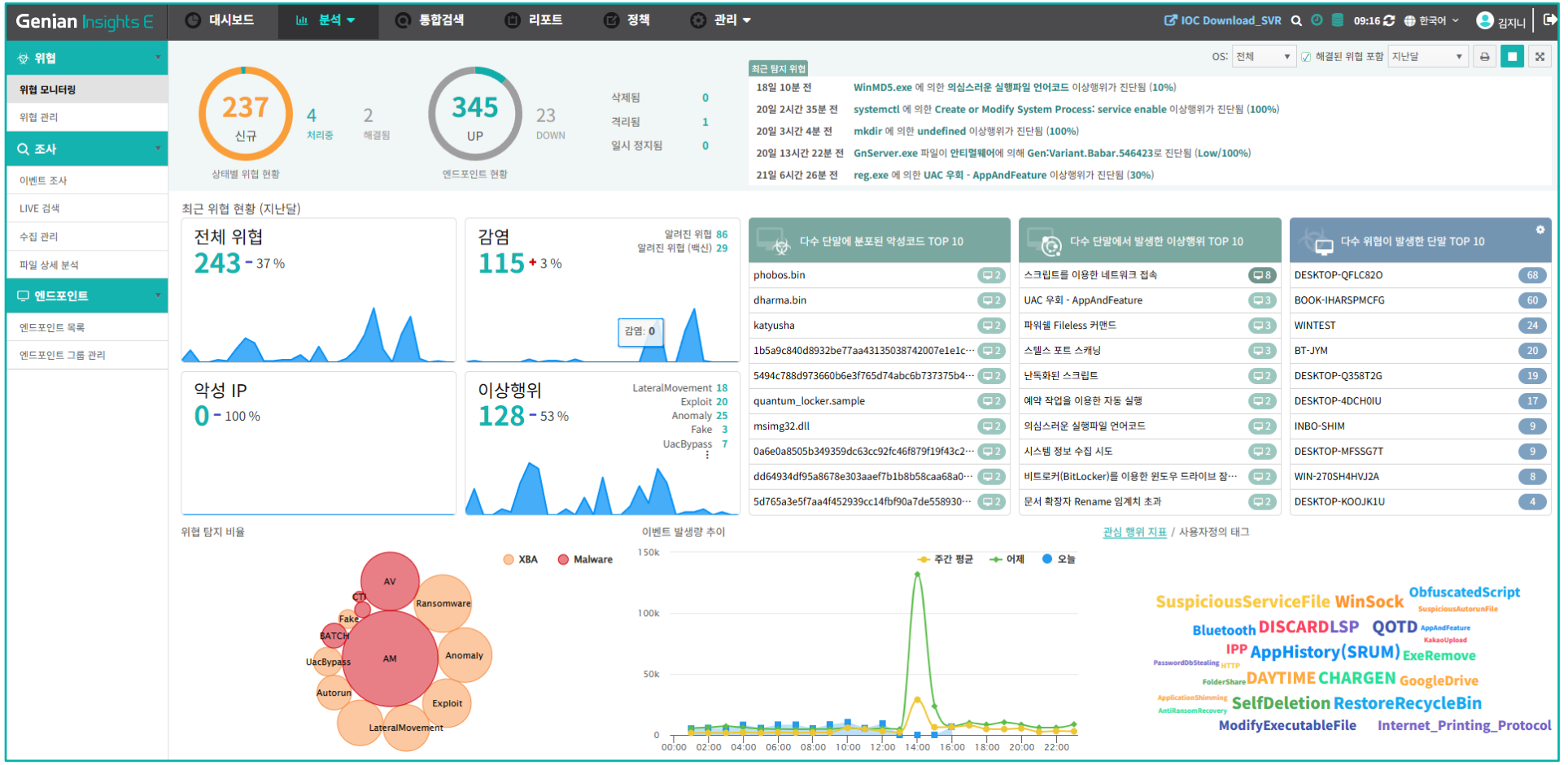
네트워크 패킷 수집



프로세스 덤프

주요 기능

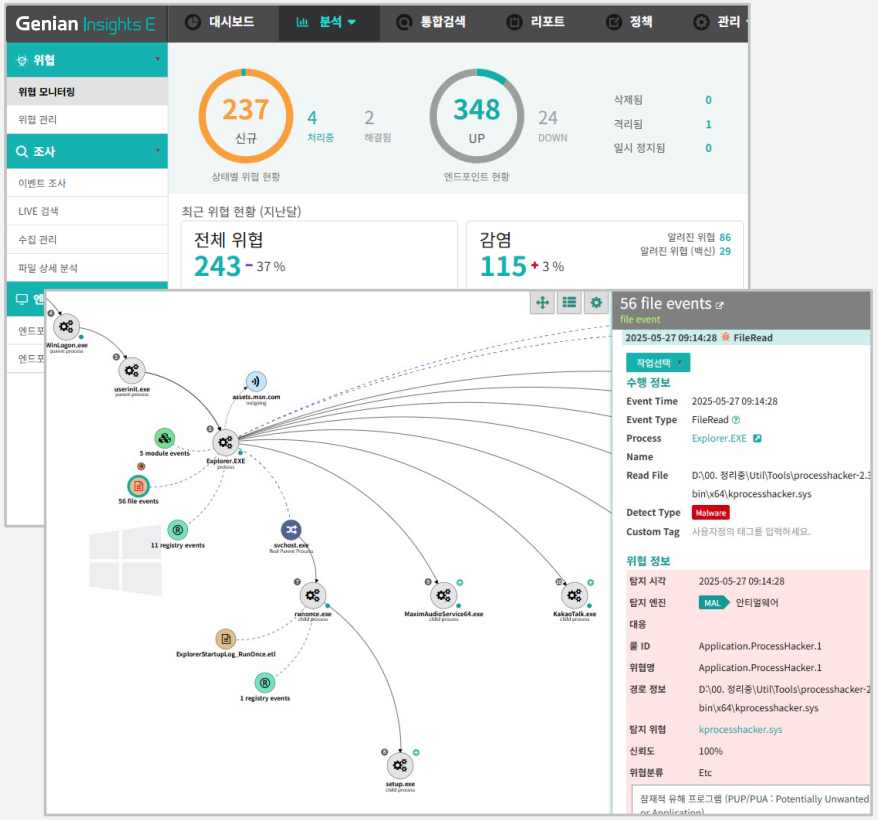
(기본 위협 탐지 현황) 파일, 행위, C2IP 탐지와 전체 탐지 현황을 보여주는 화면으로 각 항목 클릭 시 관련된 상세 정보를 볼 수 있습니다.



주요 기능

(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)

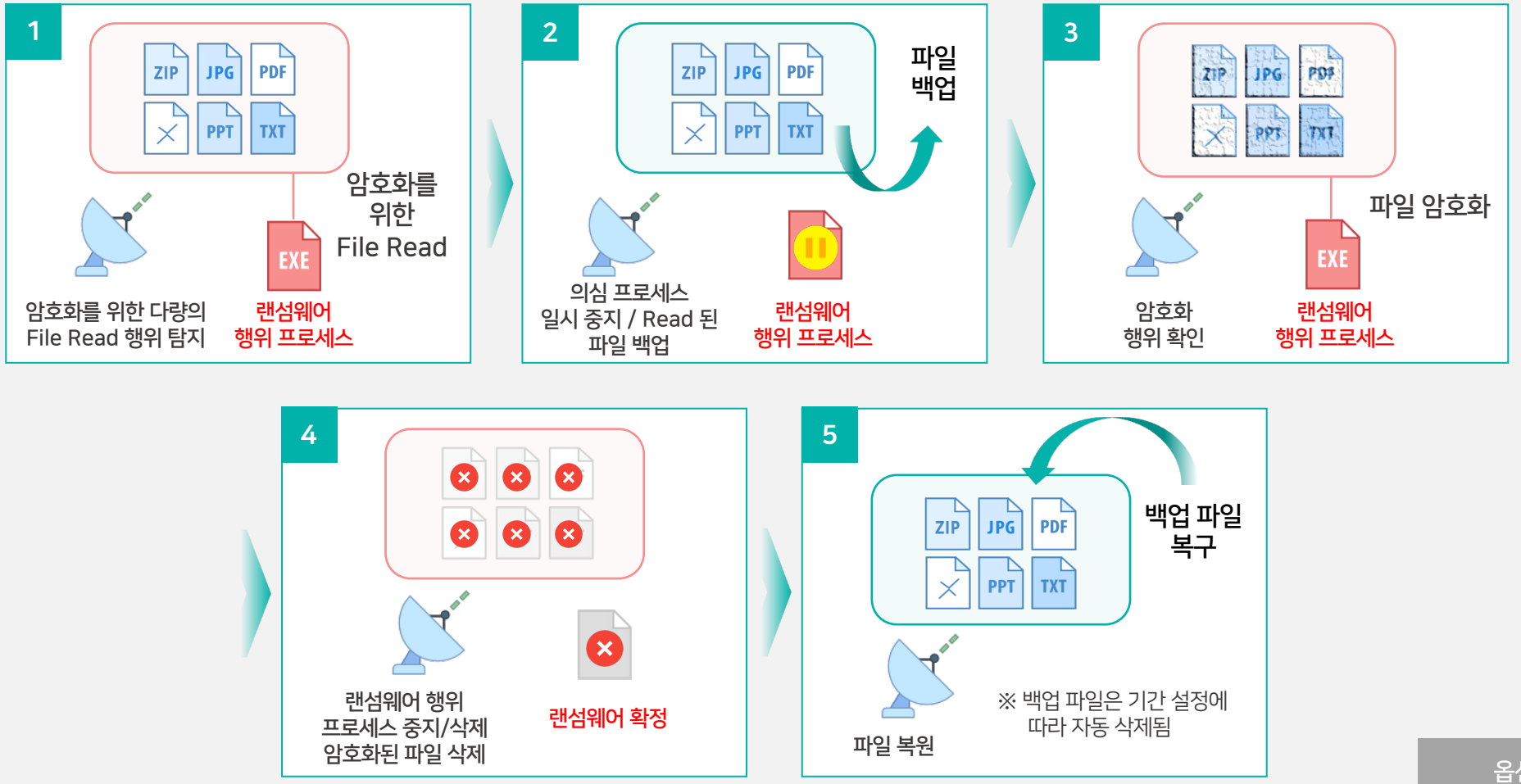


✓ 사용자 PC에서의 백신 화면(UI)

옵션
(별도 라이선스 필요)

주요 기능

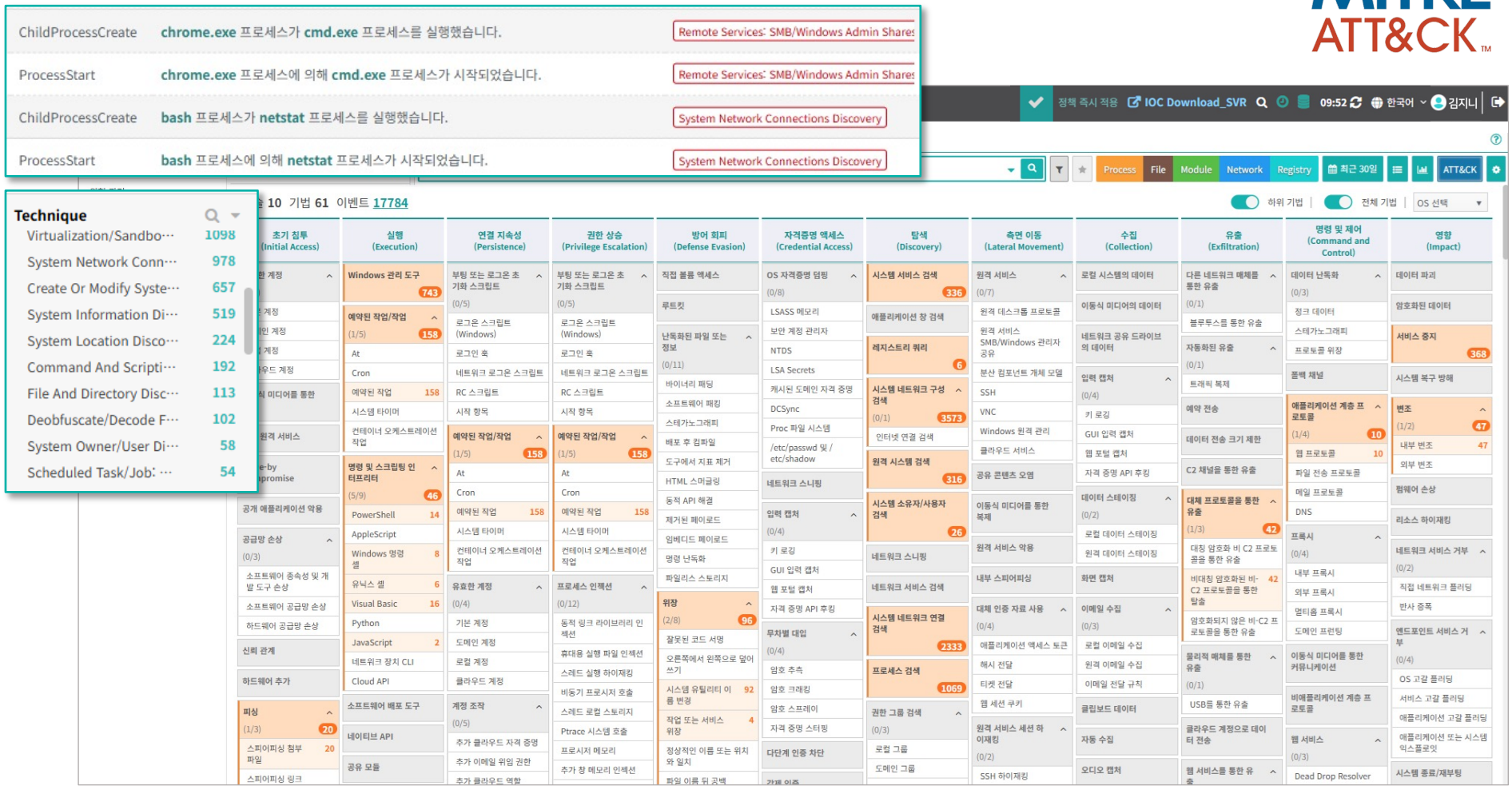
(랜섬웨어 대응) 실시간으로 랜섬웨어 행위를 모니터링하여 탐지 / 백업 / 대응 / 복원을 실시간으로 수행합니다. (옵션)



옵션
(별도 라이선스 필요)

주요 기능

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

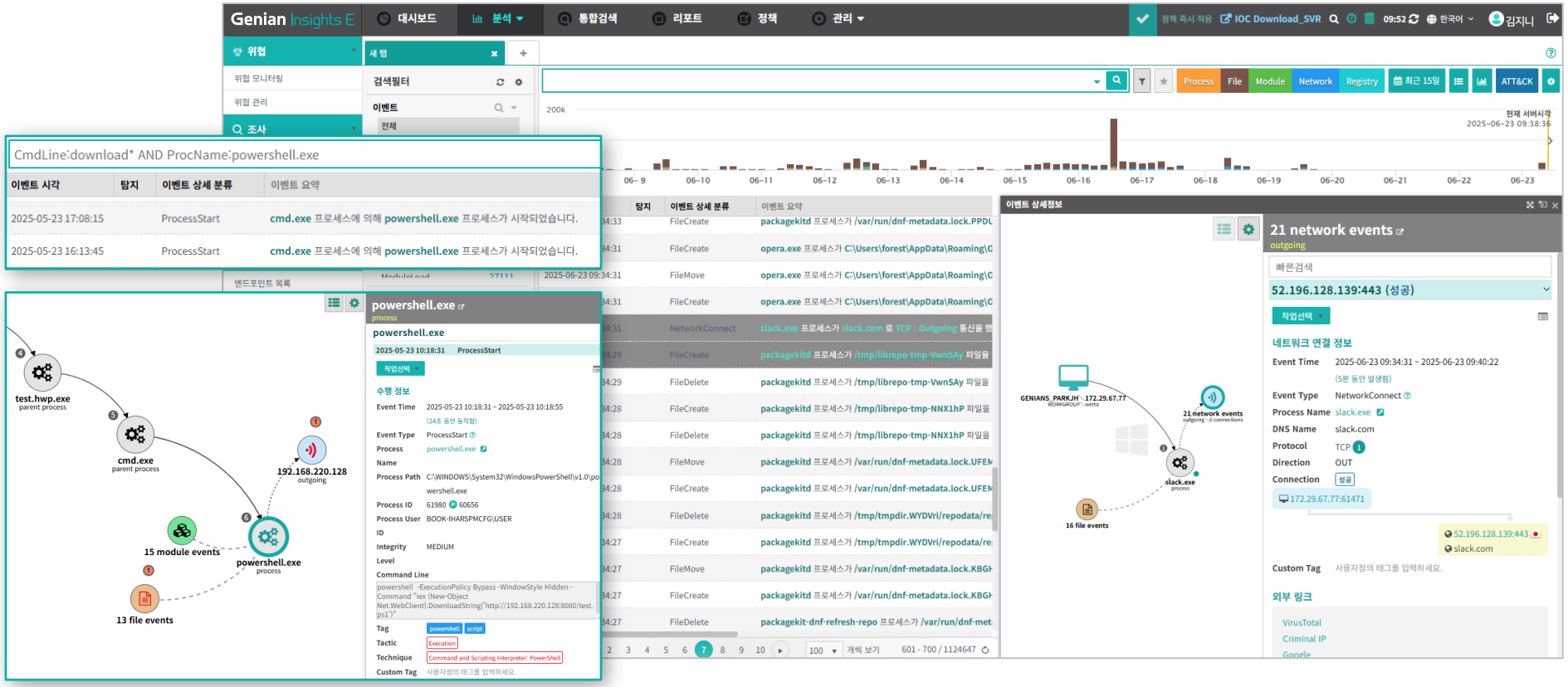


주요 기능

(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)

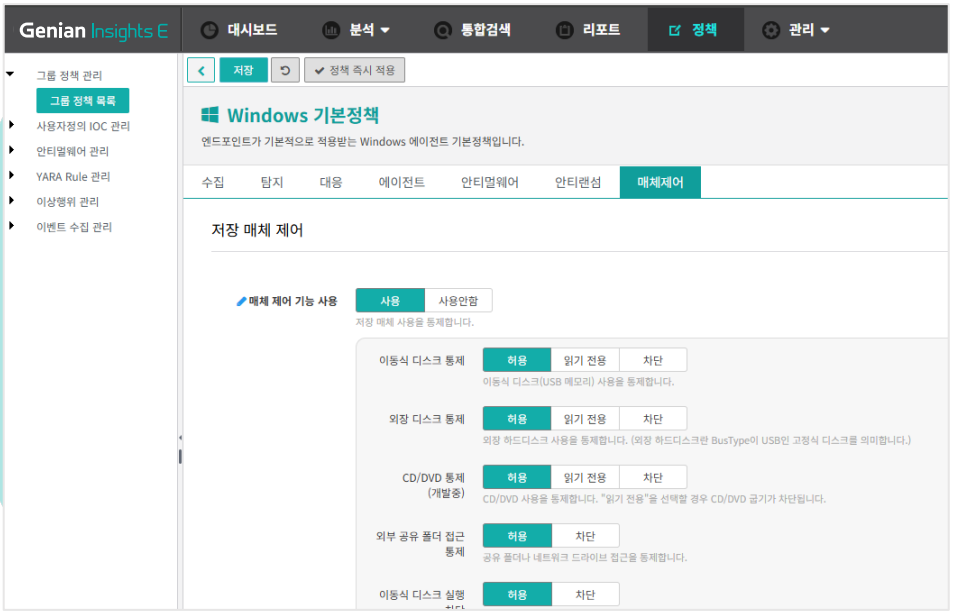
- CmdLine:download* AND ProcName:powershell.exe => powershell 에서 download 명령어 수행 이력 검색
- ReqName:hh.exe AND ProcName:("wscript.exe" OR "mshta.exe" OR "cmd.exe") => hh.exe 에 의해 실행된 wscript.exe, mshta.exe, cmd.exe 이력 확인



주요 기능

(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.

※ 패스워드 입력 시 안전모드 사용 가능



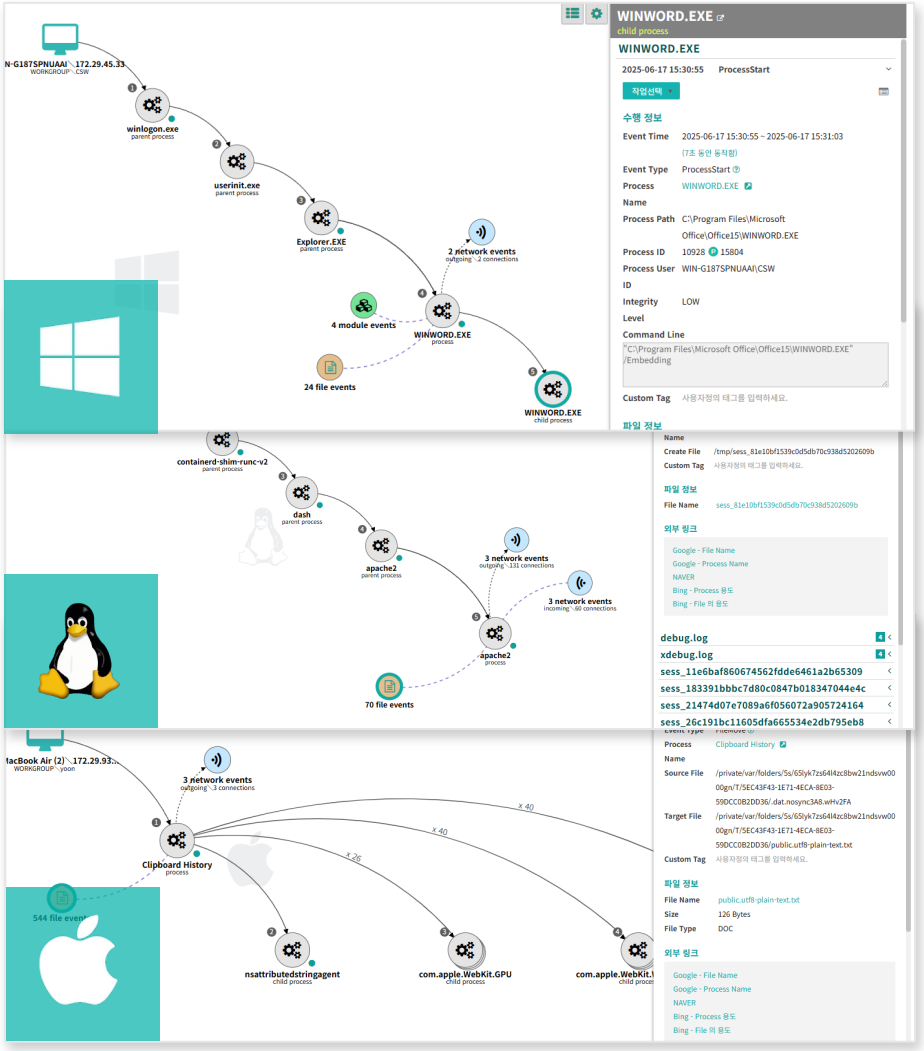
옵션
(별도 라이선스 필요)

주요 기능

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

Windows	Linux	macOS
Windows 7 SP2 이상	Unbuntu : 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)

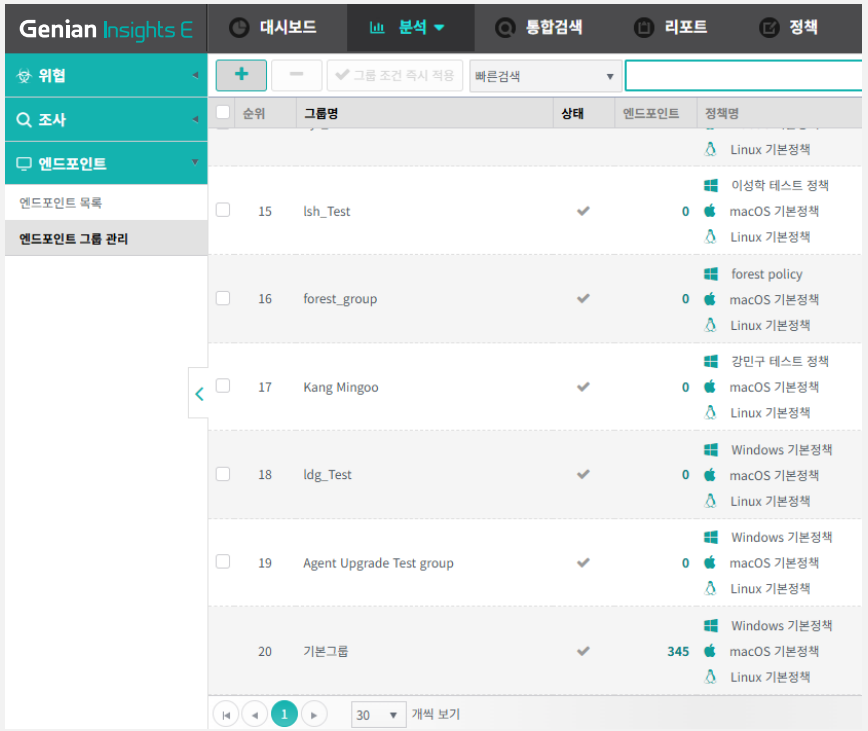
OS	플랫폼
Red Hat Enterprise Linux, x86_64	macOS Sequoia
Red Hat Enterprise Linux 9.1 (Plo	Ubuntu 20.04.6 LTS, x86_64
CentOS Linux 7 (Core), x86_64	Microsoft Windows 11 Professional x64
Ubuntu 22.04.4 LTS, x86_64	macOS Sonoma
Red Hat Enterprise Linux, x86_64	Microsoft Windows 11 Home x64
Rocky Linux 8.7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



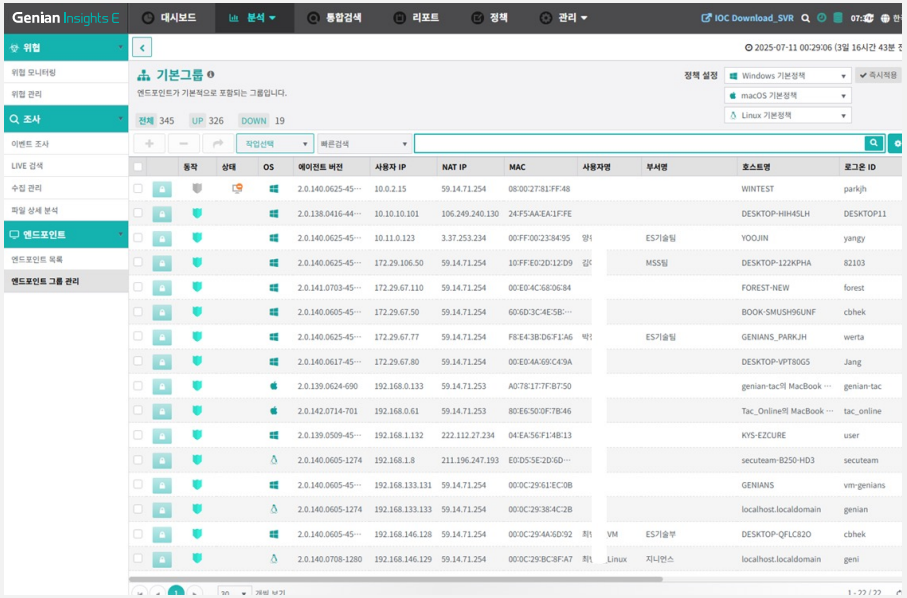
주요 기능

(그룹관리) Agent 별 그룹을 만들어 별도의 정책으로 관리할 수 있습니다.

엔드포인트 그룹 관리

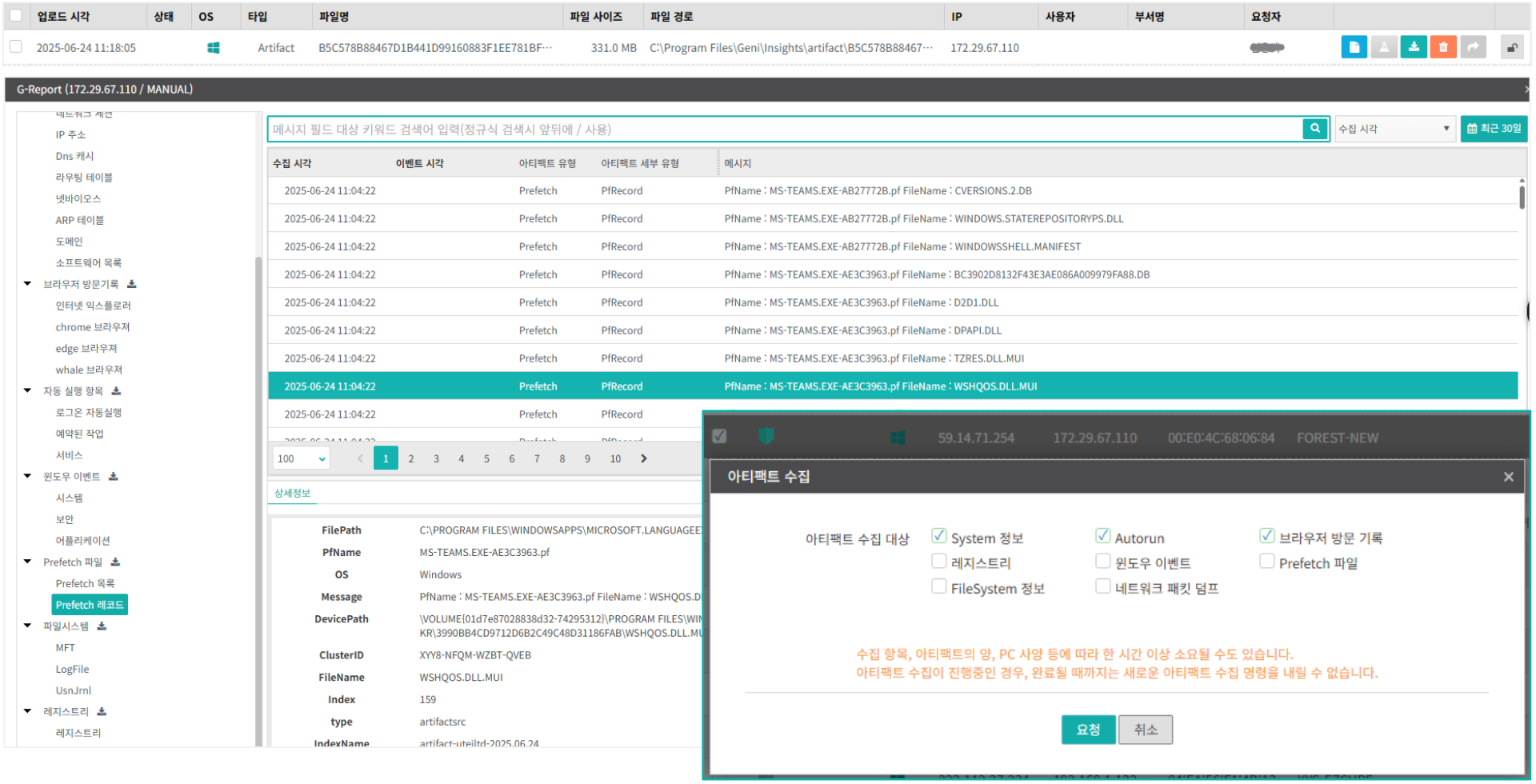


각 그룹 별 정책 설정



주요 기능

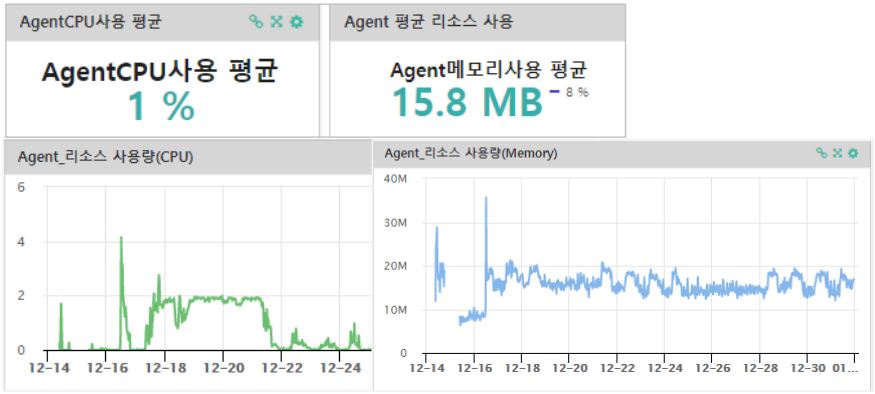
(아티팩트 수집) 시스템 정보, Prefetch 파일, 레지스트리, 브라우저 방문 기록 등의 포렌식을 위한 아티팩트를 수집합니다.

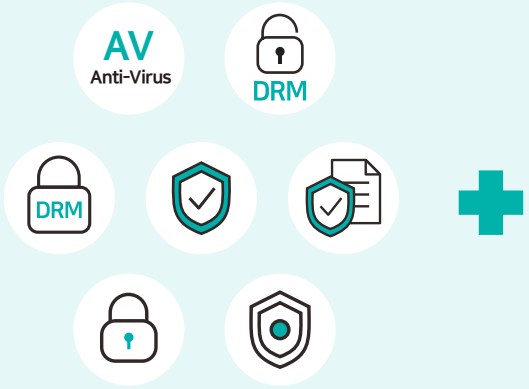


주요 기능

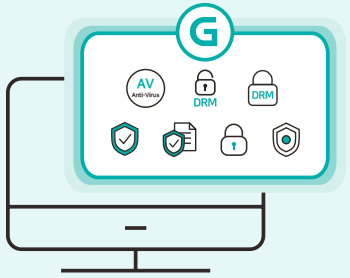
(가벼운 에이전트) 에이전트는 사용자가 불편함을 느끼지 못하도록 가볍게 동작하며 다양한 환경에서도 안정적으로 동작하도록 구현되어 있습니다.

Windows





- 문서중앙화
- PMS
- 매체제어
- 데이터 복원
- DLP
- 프린터 보안
- NAC
- 메신저
- 개인정보보호
- 소프트웨어 관리
- SSO통합인증

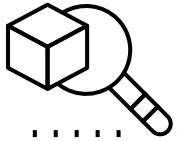


No problem!

특장점

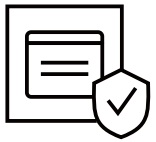
(이벤트 활용) 수집된 방대한 이벤트 데이터를 다양한 방식으로 활용할 수 있습니다. 특정 프로세스나 IP를 기준으로 전체 행위를 빠르게 조회하여, 내부 위협이나 의심스러운 활동을 쉽게 식별하고 검증할 수 있습니다.

일반적인 EDR's



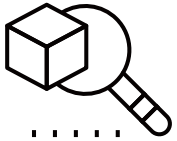
Detection

Trace/Analysis



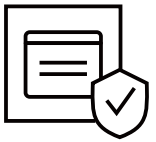
Response

Genian Insights E



Detection

Trace/Analysis



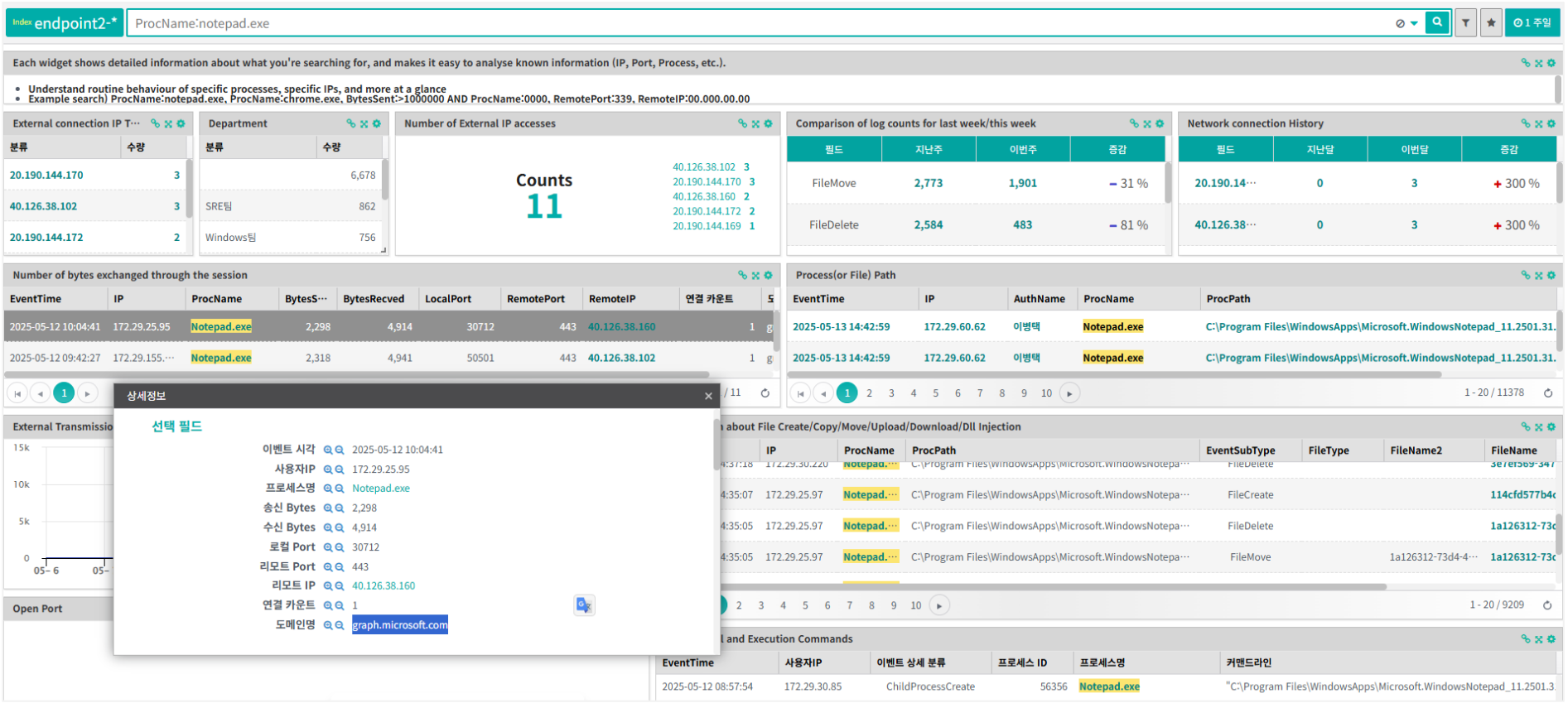
Response

다양한 활용

특장점

(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.

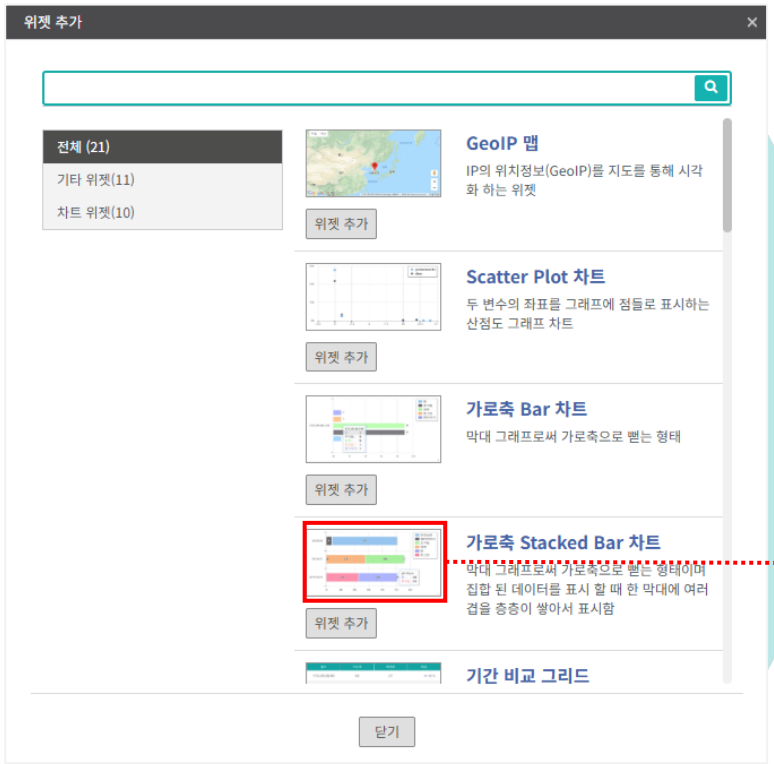


※ 실제 notepad.exe 에 의한 이상행위 사례 다수 확인 됨

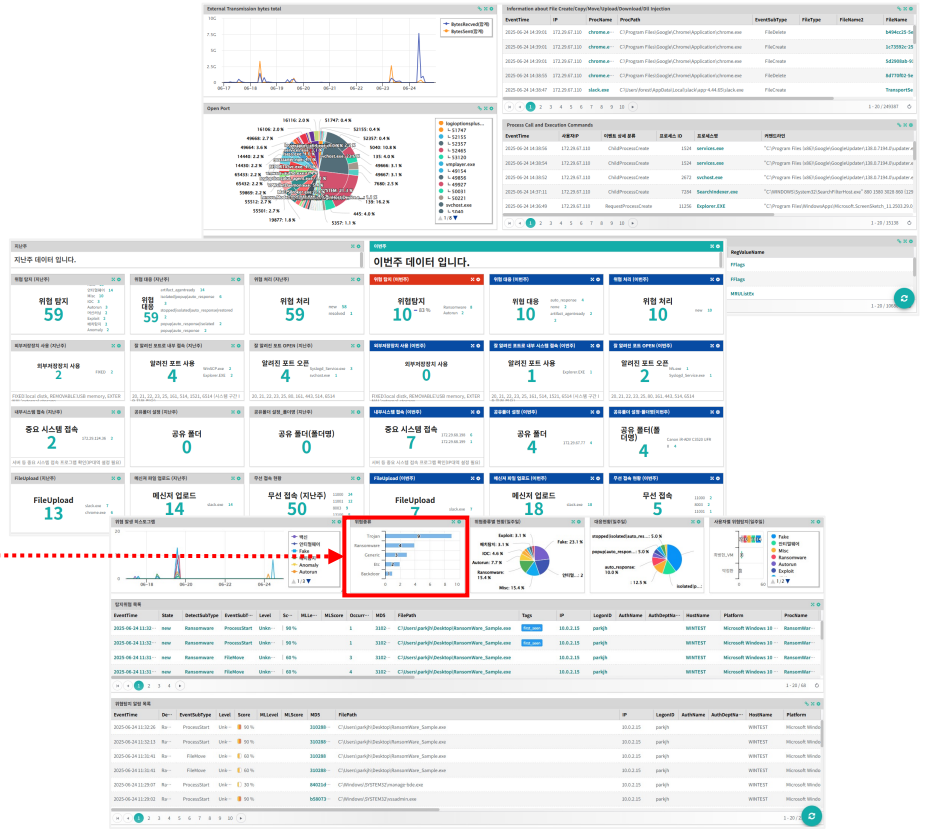
특장점

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

위젯 선택



다양한 위젯으로 구성된 대시보드

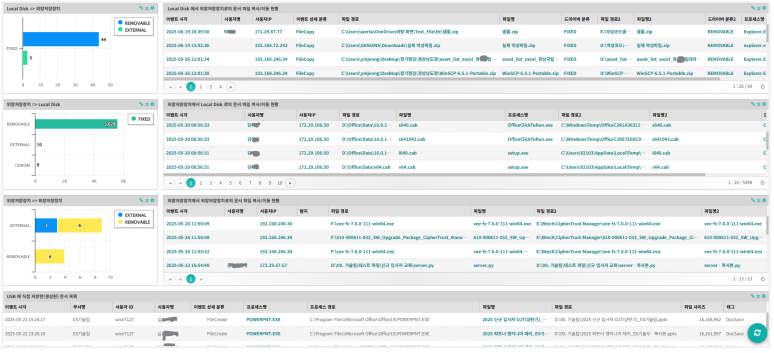


특장점

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

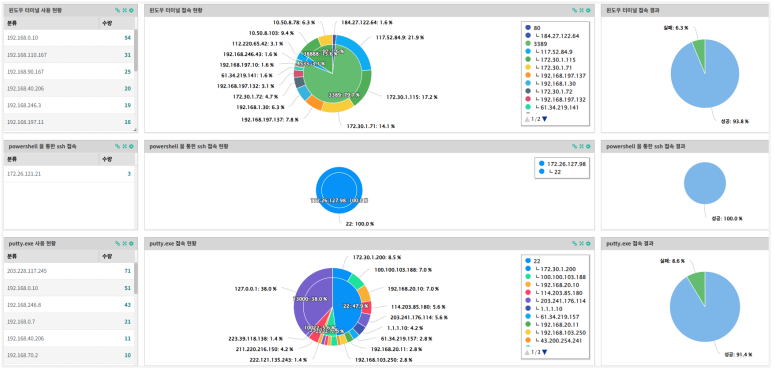
✓ 외장 저장장치 사용 현황

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



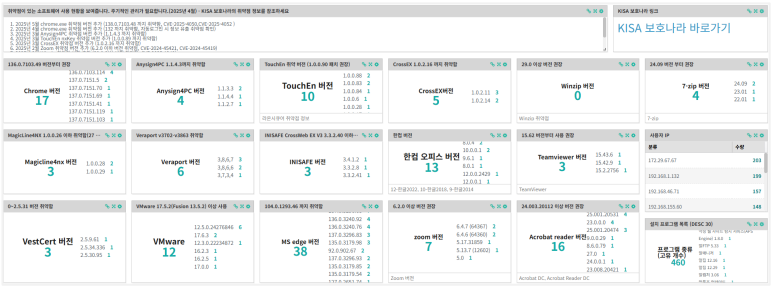
✓ 원격 접속 현황

- 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

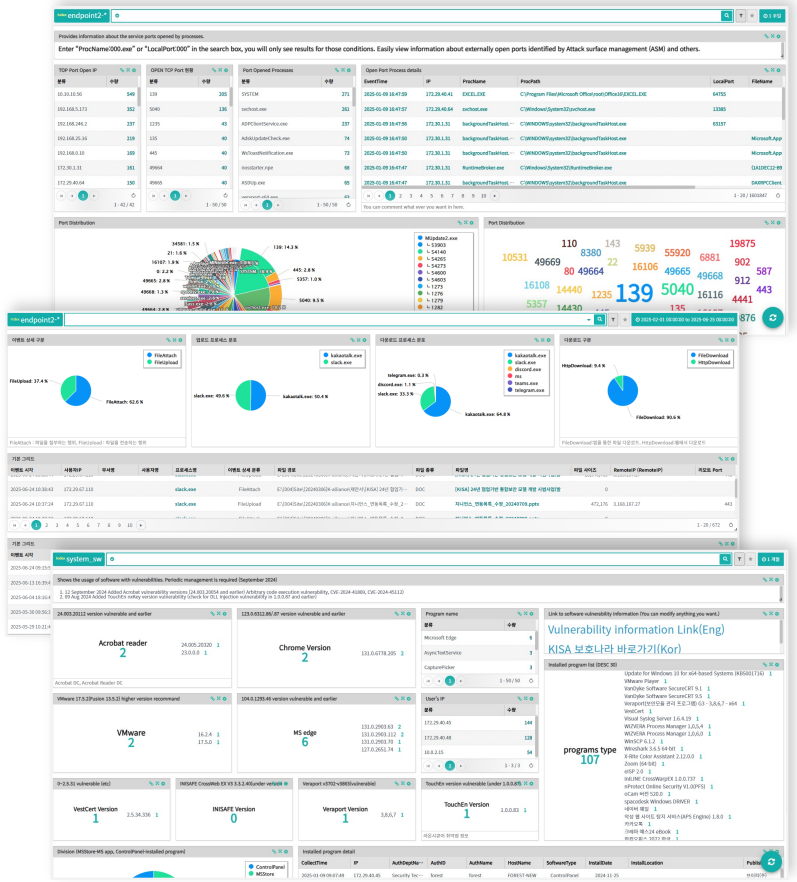


※ 그 외 다수의 엔드포인트 디스커버리 정보 제공

특장점

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

제조가 제공 공유 대시보드-cloud

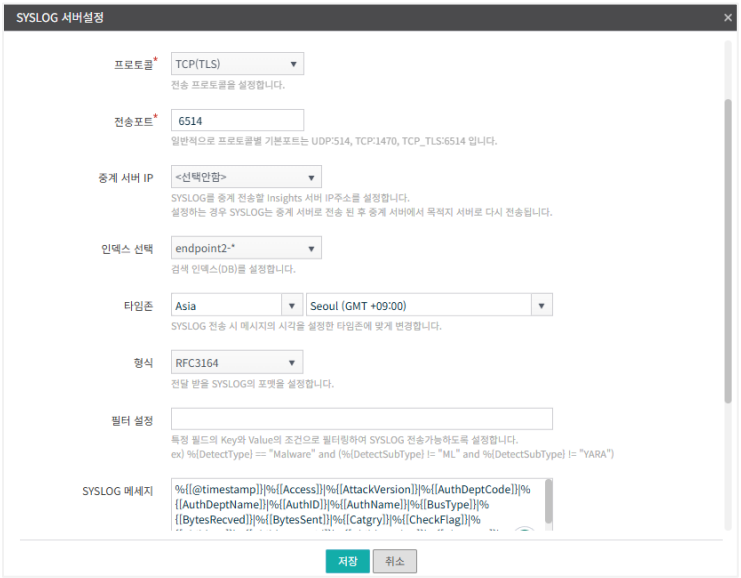


연동

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

도입 효과

기존 보안체계에서 개선이 어려웠던 이슈 → 해결

AS-IS	TO-BE
✓ **Anti-virus 의 한계** 백신에서 탐지할 수 없는 신종 악성코드 및 Fileless 형태의 공격 증가	✓ **행위 탐지** 백신에서 탐지할 수 없는 신종 악성코드및 Fileless 형태의 공격 탐지
✓ **가시성 부족** 엔드포인트 내에서 어떤 활동이 일어나는지 실시간으로 파악 불가	✓ **가시성 확보** 엔드포인트 내에 CCTV 가 설치 된 것처럼 실시간 확인 및 조회
✓ **정확한 원인 분석 어려움** 침해사고 발생 후 포렌식에 시간/인력 낭비	✓ **원인 분석 가능** 빠른 추적과 분석으로 원인을 찾아 대응
✓ **취약한 버전 확인 어려움** 설치된 SW 확인 및 취약점이 있는 프로그램 사용 여부 확인 어려움	✓ **취약한 버전 확인** 취약점이 있는 프로그램을 통해 위협 의심 행위 확인
✓ **대응 속도 느림** 이상 징후 발생 후 대응까지 수일 또는 그 이상 소요됨	✓ **대응 속도 빠름** 이상 징후 발생 후 분석 및 대응까지 몇 시간 내에 가능함

Summary

안정성

낮은 리소스 사용
충돌 회피 기술 적용

시장점유 1위

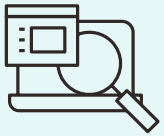
23/24년 조달 점유율 1위
240여 곳 고객사 구축
(Agent 약75만대-25.05)

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

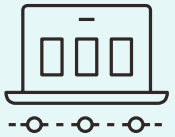
수집된 정보를 활용
입체적인 분석 가능

안티랜섬웨어

특화된 안티랜섬웨어 기능
실시간 백업/탐지/대응/복원

장기간 로그 저장

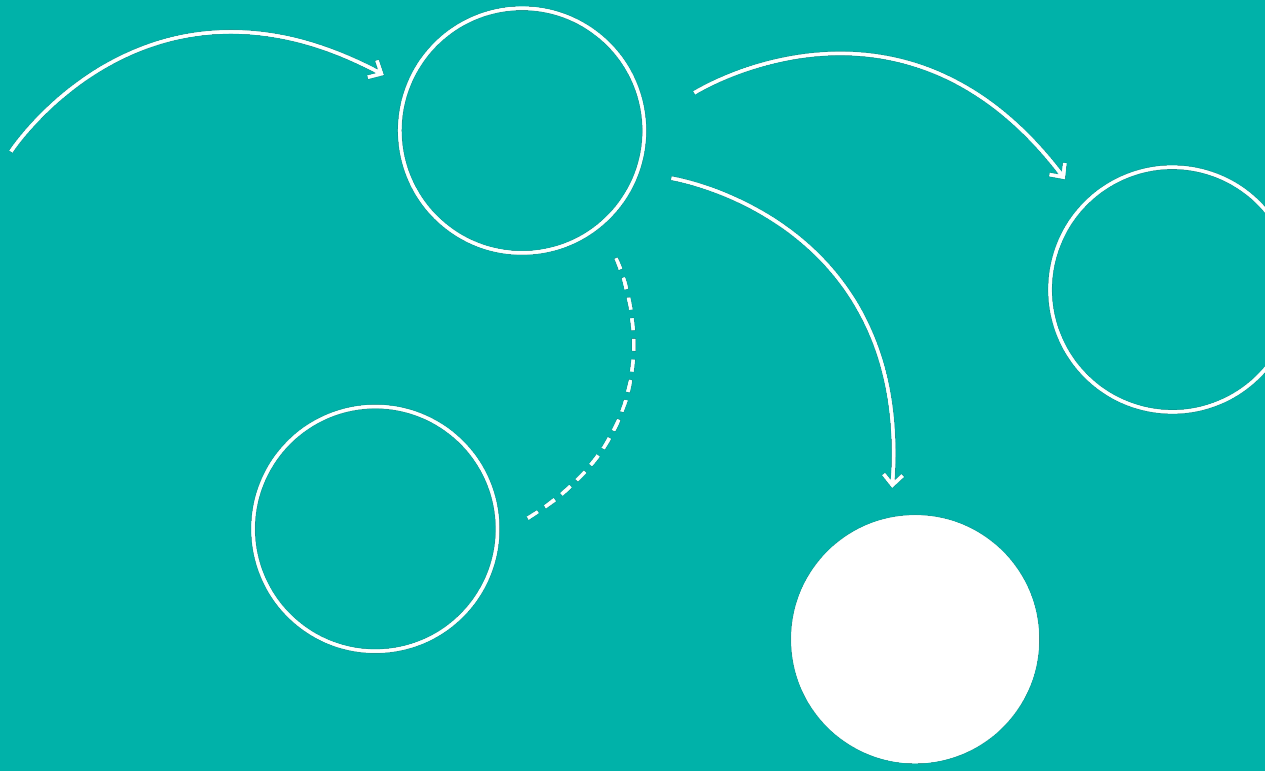
로그 서버 추가 시
6개월 이상의 로그 보관
(+Scale Out)



탐지/대응 기본

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

Thank you



Genians