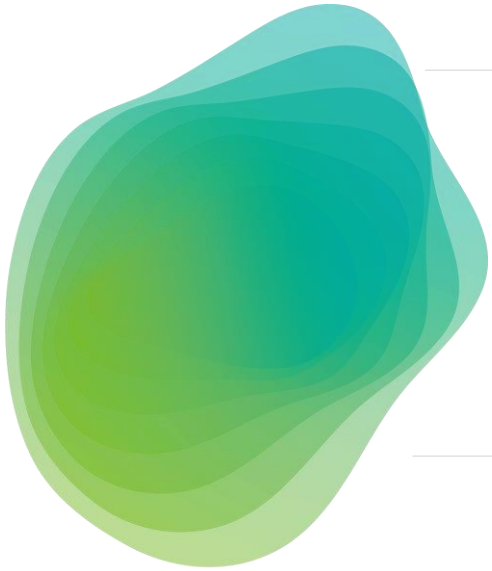
보안 전략의 변화

(지니안 인사이츠 소개)

GeniNet

목 차



변화의 필요성

(방어 전략의 한계)

보안 전략의 변화

시스템, Application의 복잡, 다양성 증가

공격의 지능화, 조직화. 사용자보안의식 개선의 한계

모든 공격 100% 방어는 불가능

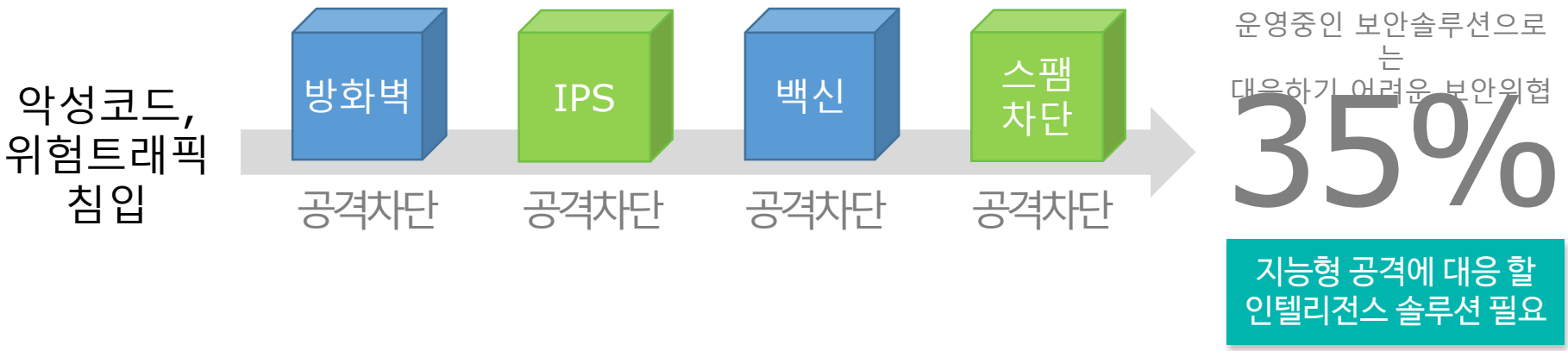
방어 위주의 보안 전략의 한계

방어가 실패했을 경우의 대응 전략이 필요

피해가 확정되기 전에 각 단계별 대응 프로세스 구축 필요

기존 보안솔루션 + a

기 도입한 보안솔루션으로 탐지하지 못하는 지능형 공격 대응방안 도입 필수

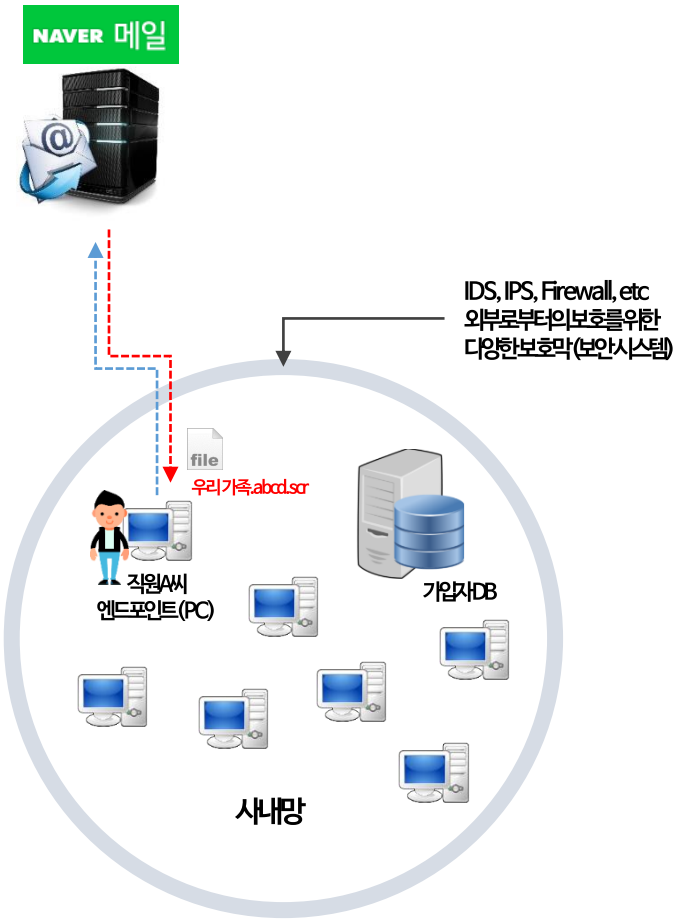


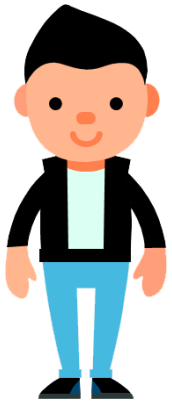
수개월 간 진행 되는 지능형 위협 공격

오늘 보안관리자가 인지한 보안사고는 이미 수개월 전부터 시작된 지능형 공격

인터파크	방송사(MBC, KBS) 은행(신한은행, 농협)	NH NongHyup
최초 공격시작에서 사고 발생까지의 기간		
2개월	8개월	7개월
16년 7월 2,600만건 개인정보유출	13년 3월 3.20대란 전산망 마비	11년 4월 전산망 마비

수개월 간 진행 되는 지능형 위협 공격 (인터파크 사례)





쇼핑몰에서 근무중인 A직원

발신자 동생 이메일주소

첨부파일 file 우리 가족.abcd.scr

수개월 간 진행 되는 지능형 위협 공격 (인터파크 사례)

직원A씨의 엔드포인트 (PC)에서 일어나는 일

file **우리가족.abcd.src**

파일 실행

explorer.exe	1576	24,144 K	43,320 K	0.43	Windows 탐색기	Microsoft
vmtoolsd.exe	1020	6,792 K	18,948 K	3.09	VMware Tools Core S...	VMware, I
SbieCtrl.exe	1332	3,304 K	11,128 K	0.02	Sandboxie Control	tzuk
procexp.exe	2900	12,944 K	23,588 K	2.26	Sysinternals Process E...	Sysinterna
Tcpview.exe	3156	7,456 K	14,528 K	0.17	TCP/UDP endpoint vie...	Sysinterna
FileMonitor.exe	3380	14,304 K	12,432 K	0.69	FileMonitor	Moo0
우리 가족.abcd.scr	3276	1,832 K	15,020 K	14.33		
msoia.exe	2332	872 K	2,972 K	1.80	Internet Low-Mic Utilit...	Microsoft
ielowutil.exe	3296	552 K	2,260 K	0.52	Internet Low-Mic Utilit...	Microsoft
우리 가족.abcd.scr	3312	6,116 K	1,708 K	0.36		

file **msoia.exe**

1. %LOCALAPPDATA%₩microsoft₩office₩15.0₩에생성
2. CreateProcess함수를통해/update 인자와함께실행
3. %LocalAppdata%₩Microsoft₩Internet Explorer₩IECompatData₩ielowutil.exe 에 자기복제
4. ielowutil.exe를 /AUTOSTART 인자를 넣어 실행 후 종료

file **ielowutil.exe**

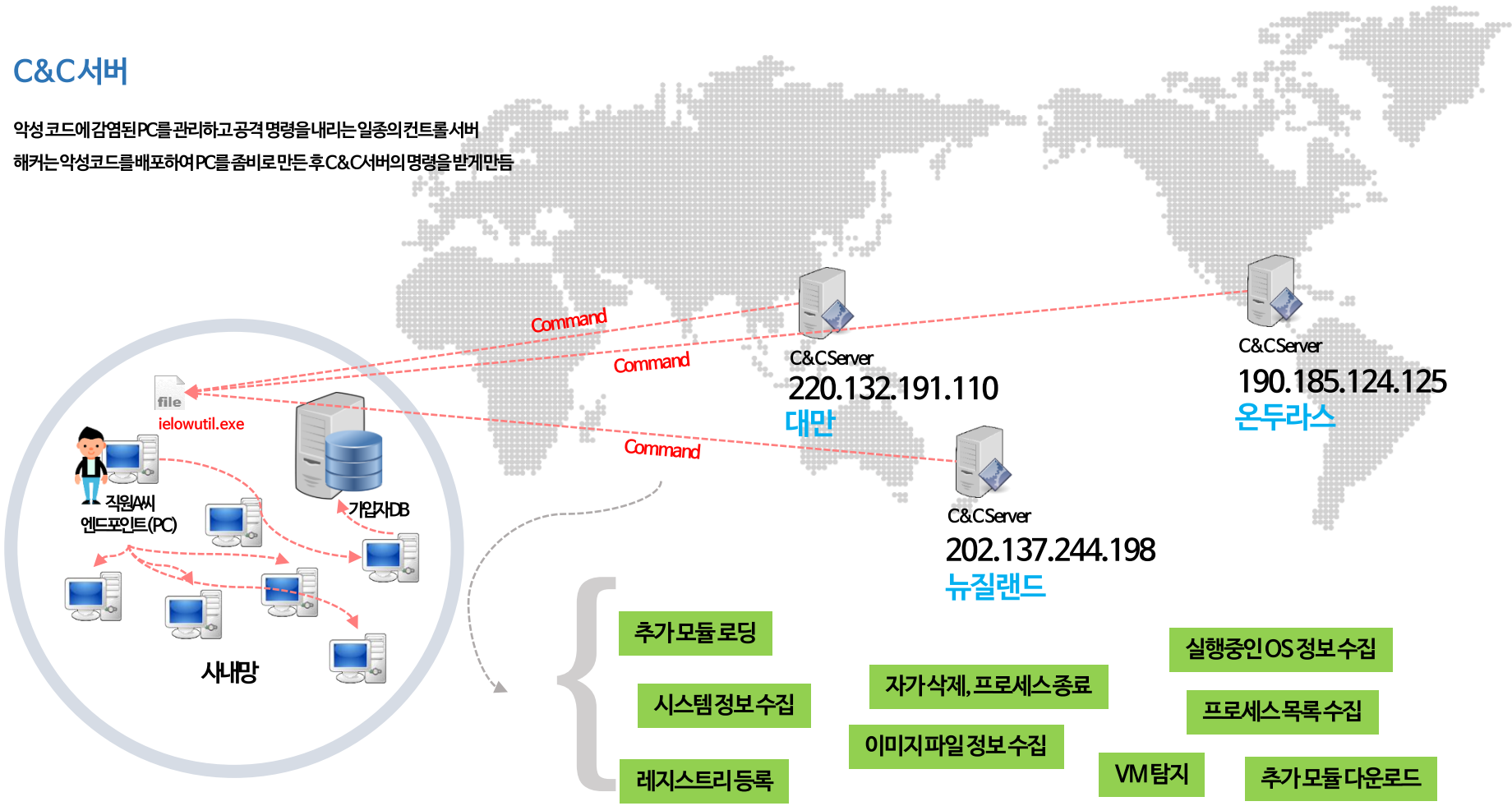
C&C서버와통신시도

file **우리가족.abcd.src (실제로 단말에 설치되는 스크린세이버 파일)**

수개월 간 진행 되는 지능형 위협 공격 (인터파크 사례)

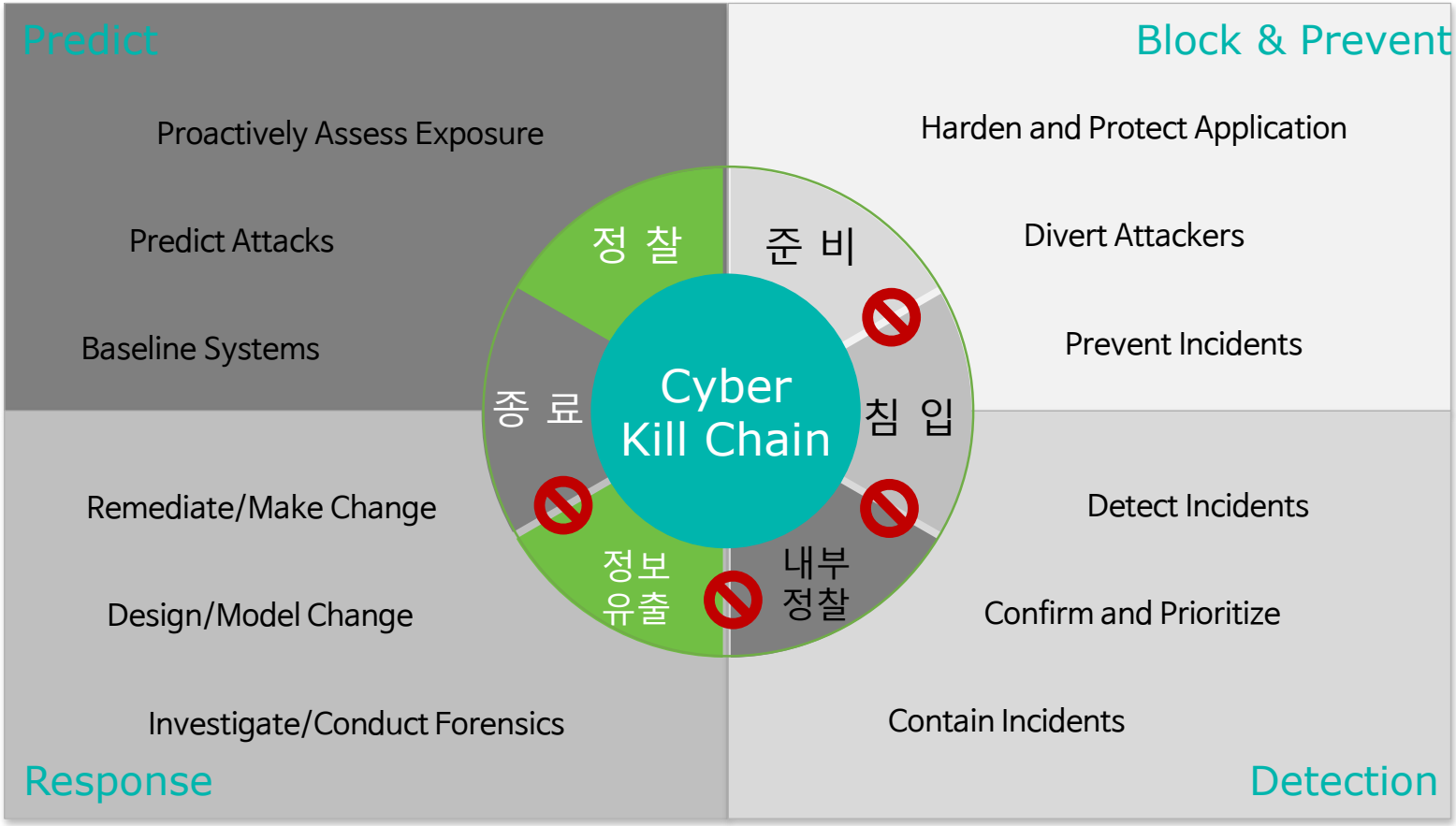
C&C서버

악성코드에감염된PC를관리하고공격명령을내리는일종의컨트롤서버
해커는악성코드를배포하여PC를좀비로만든후C&C서버의명령을받게만듬



침입단계별 대응 프로세스

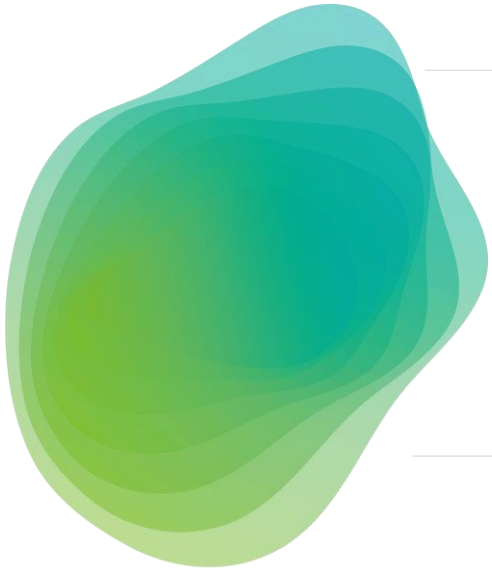
침입을 단계별로 구분하여 단계별 대응 프로세스 구축



미션 : 빠르게 보안공격의 고리를 끊어라

원천적인 보안위협 차단이
불가능한 지능형 공격

신속한 탐지와 대응
(Detection & Response)이
대형 보안사고를 막기하기 위한 **해답**



Genian Insights

제품 소개

확장 – NAC를 활용하자

각각의 정보를 확인할 수 있는 시스템은 많으나,
하나의 시스템에서 통합되어 관리되는 것은 NAC뿐!
그러나, 효과적으로 활용하지 못하고 있다

Genian NAC

Networks Access Control – 내부 보안에 유용한 정보를 가장 많이 보유한 보안시스템

상태정보와 행위정보의 연계

● **행위기반 정보와 상태기반 정보를 연계하여 내부 보안을 더욱 지능화**

상태기반 정보 (NAC 기반 정보)

H/W, S/W 설치 내역 수집/관리/통계

- 마더보드, 메모리, 저장장치, 모니터, 프린터, 소프트웨어 설치 정보 수집
- 파일(유/무, 버전, 해쉬값), 프로세스, 레지스트리 비교를 통한 소프트웨어 설치상태 점검

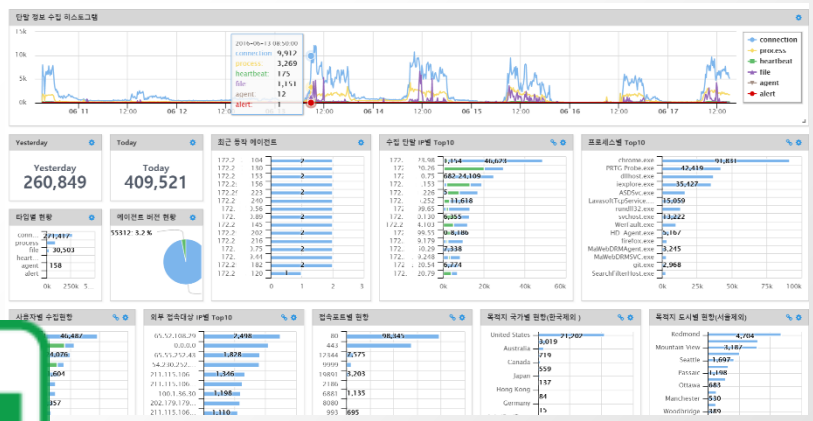
네트워크정보 수집 및 통제

- 단말의 네트워크 인터페이스 탐지 및 제어
- 무선랜 인터페이스에서 탐지된/연결된 AP항목 수집
- 관리자가 지정한 White List 기반의 AP에만 접속 가능한 정책

윈도우 보안설정 점검/관리

- 윈도우 방화벽, 자동업데이트, 바탕화면, 화면보호기 설정 점검
- 사용자 계정, 비밀번호 유효성 점검
- 원격데스크탑, 공유폴더, CD/USB 자동실행 설정 점검

행위기반 정보 + 이상행위 분석

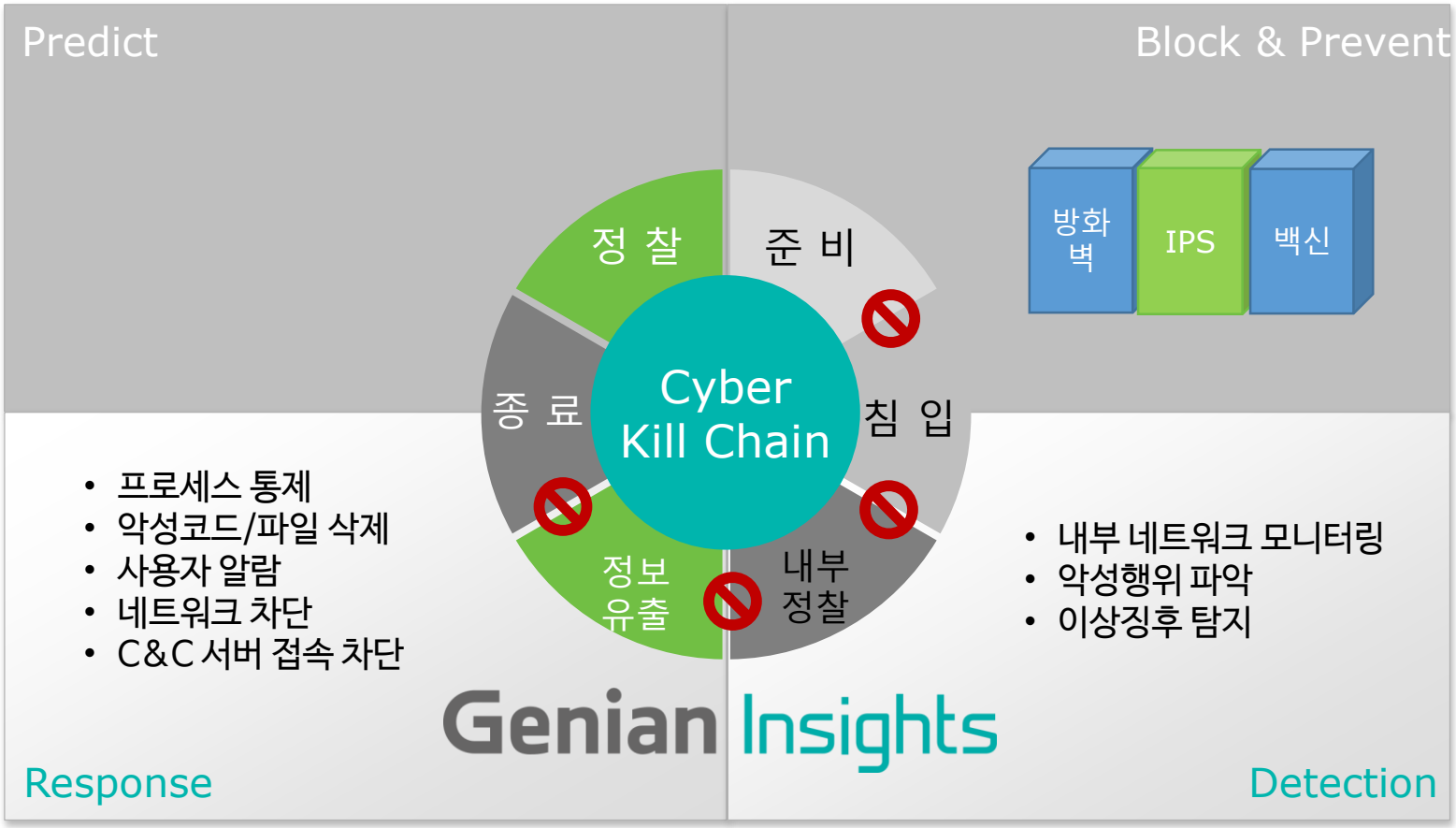


- Process
- Connection
- File
- Heartbeat

E module's func.

엔드포인트 탐지 및 대응 플랫폼

내부 네트워크와 단말에 대한 악성행위 파악 및 이상징후 탐지 플랫폼
원천적인 방어가 불가능한 지능형 공격(APT) 수행 단계에서 신속한 탐지 및 대응



Genian Insights 특장점

Genian Insights

인텔리전스 위협관리 플랫폼 (Detection & Response)

국내 환경에 적합한 IOC 활용

- IOC 주기적인 업데이트로 최신 위협 및 침해사고 대응
- 탐지된 위협에 대한 위험도, 신뢰도 및 유형 정보 제공
- IOC(Indicators of Compromise) 침해지표 : 악성코드 및 접속 C&C 등 침해사고의 흔적들을 일정한 정형화된 데이터

가벼운 에이전트

- 단말 부하 최소화를 위해 에이전트를 통해 최소 정보만 수집 (약 25MB 리소스 사용)
- 대용량 데이터 Insights 서버에서 수행

유연한 대시보드

- 보안관리자가 필요한 정보 시각화 가능한 유연한 16종 위젯 제공
- 시스템/감염단말/ 위험-이상 단말/프로세스/접속정보/신규생성 파일 모니터링 가능

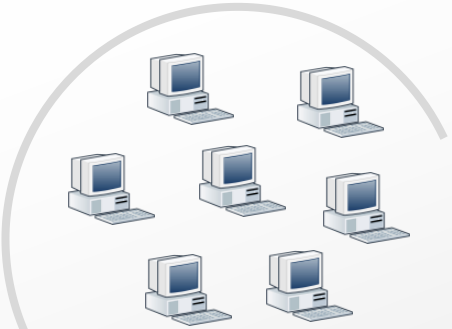
모듈별 손쉬운 적용

- Genian Insights 기본 통합관리 분석 기능 외 엔드포인트(E 모듈), 네트워크 행위 분석(N 모듈)등 선택적 적용 가능
- NAC 플러그인 기반 손쉬운 적용

Genian Insights 동작 개요

- 알람, 프로세스 강제종료, 파일 삭제, 네트워크 차단, 정책 적용 등

- 사용현황, 위협의 시각화를 통한 조직 내 엔드포인트 가시화
- 지속적인 모니터링



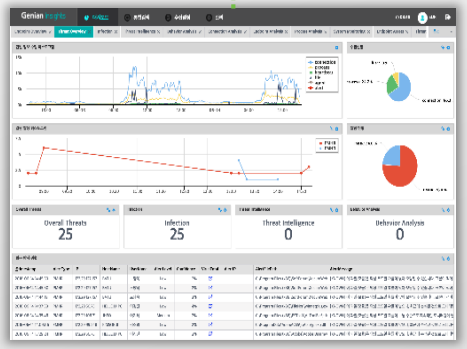
다양한 장치 및 수많은 OS가 존재하는 이질적인 조직 내 엔드포인트 환경

NAC Agent

악성행위 통제

Genian NAC
Control, Enforcer

대응
(Response)



Insights Console

엔드포인트 정보 수집

Genian Insights
IOC Detect Engine

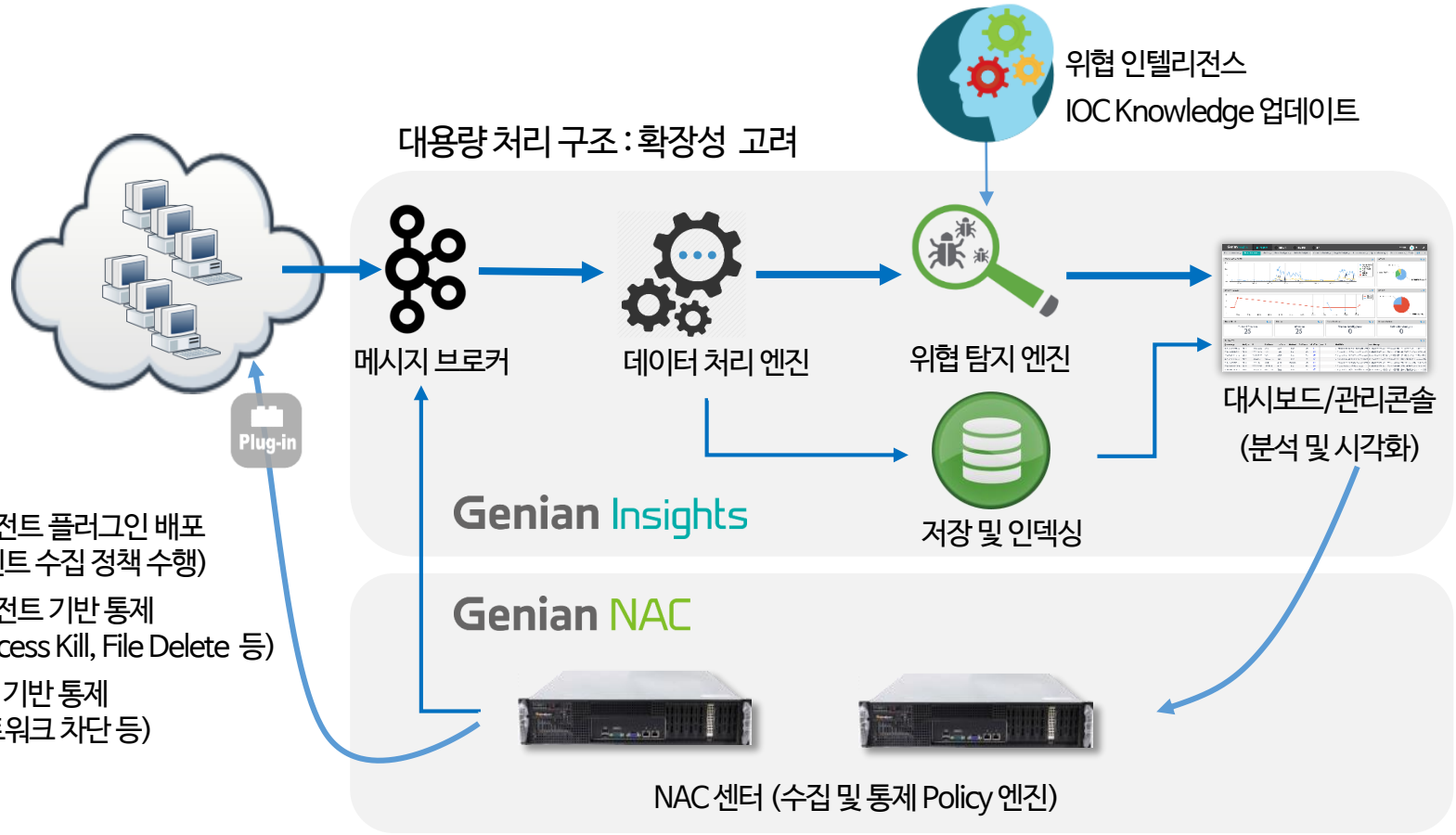
악성 행위 탐지
(Detect)

- 프로세스, 파일, 네트워크 접속정보 등

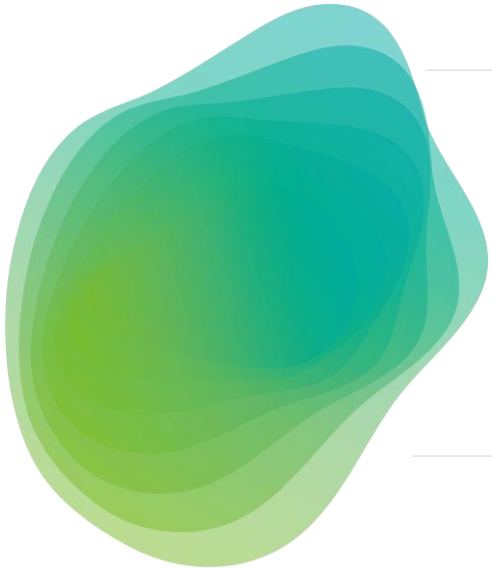
- 보안 관리 및 위협 탐지를 위한 중앙 집중화된 플랫폼
- 엔드포인트가 분산된 환경에서 위협탐지 DB를 최신으로 유지가능

Genian Insights 구성요소 및 역할

Genian NAC에서 수집한 엔드포인트 사용자, 단말 정보 빅데이터 엔진 기반
변화하는 내부 네트워크 정보 저장 및 분석



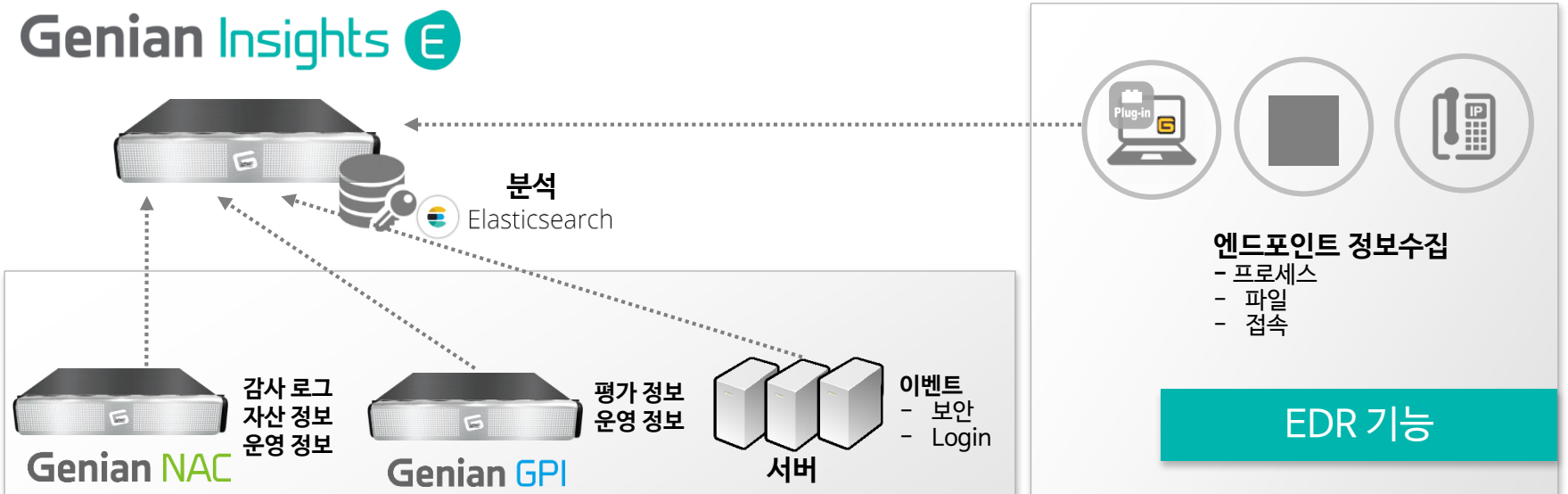
- 에이전트 플러그인 배포
  (이벤트 수집 정책 수행)
- 에이전트 기반 통제
  (Process Kill, File Delete 등)
- NAC 기반 통제
  (네트워크 차단 등)



Genian Insights

기능 소개

Genian Insights E 기능 구성



통합 분석관리 기능

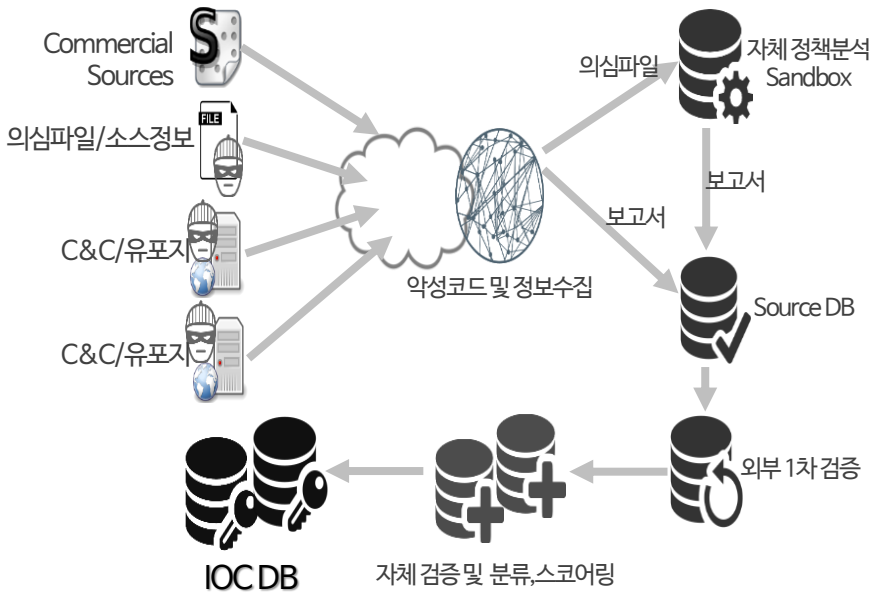
- 이벤트 정보수집 및 연동
- 수집정보 검색 편의
- 분석정보 가시화
- 유연한 대시보드 제공

- 엔드포인트 위협 식별 및 대응
- 침해지표(IOC) 기반 위협탐지
- 탐지위협 상세 분석 정보 제공
- 엔드포인트/위협/공격현황 등에 대한 대시보드 제공

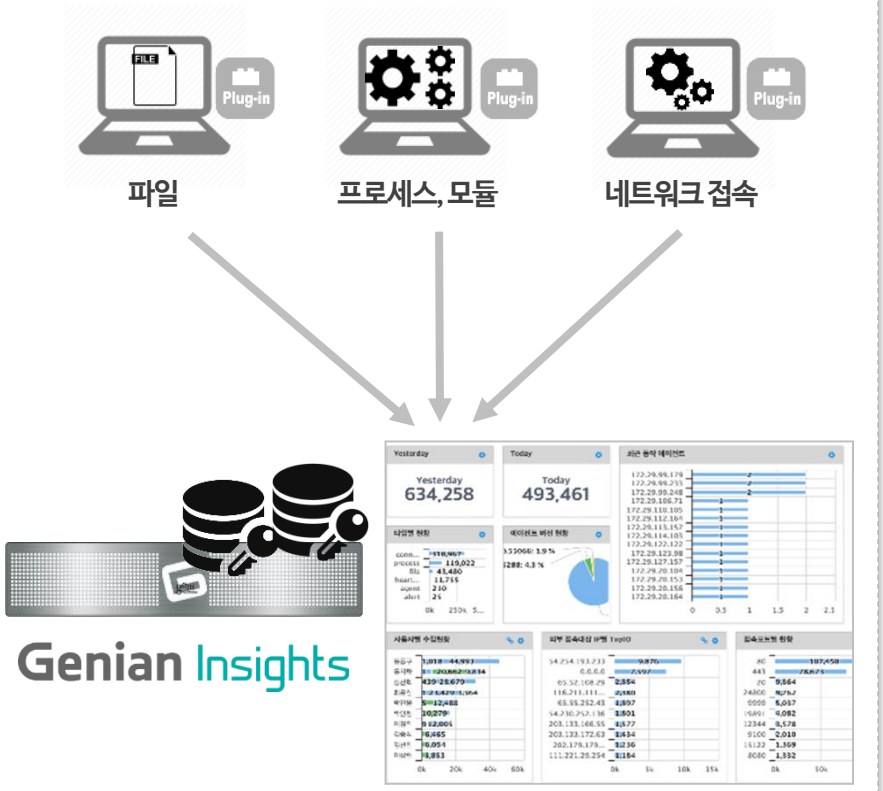
[EDR] 최신 위협 인텔리전스(IOC) 활용

IOC 주기적인 업데이트로 최신 위협 및 침해사고 대응

탐지된 위협에 대한 위험도, 신뢰도 및 유형 정보 제공

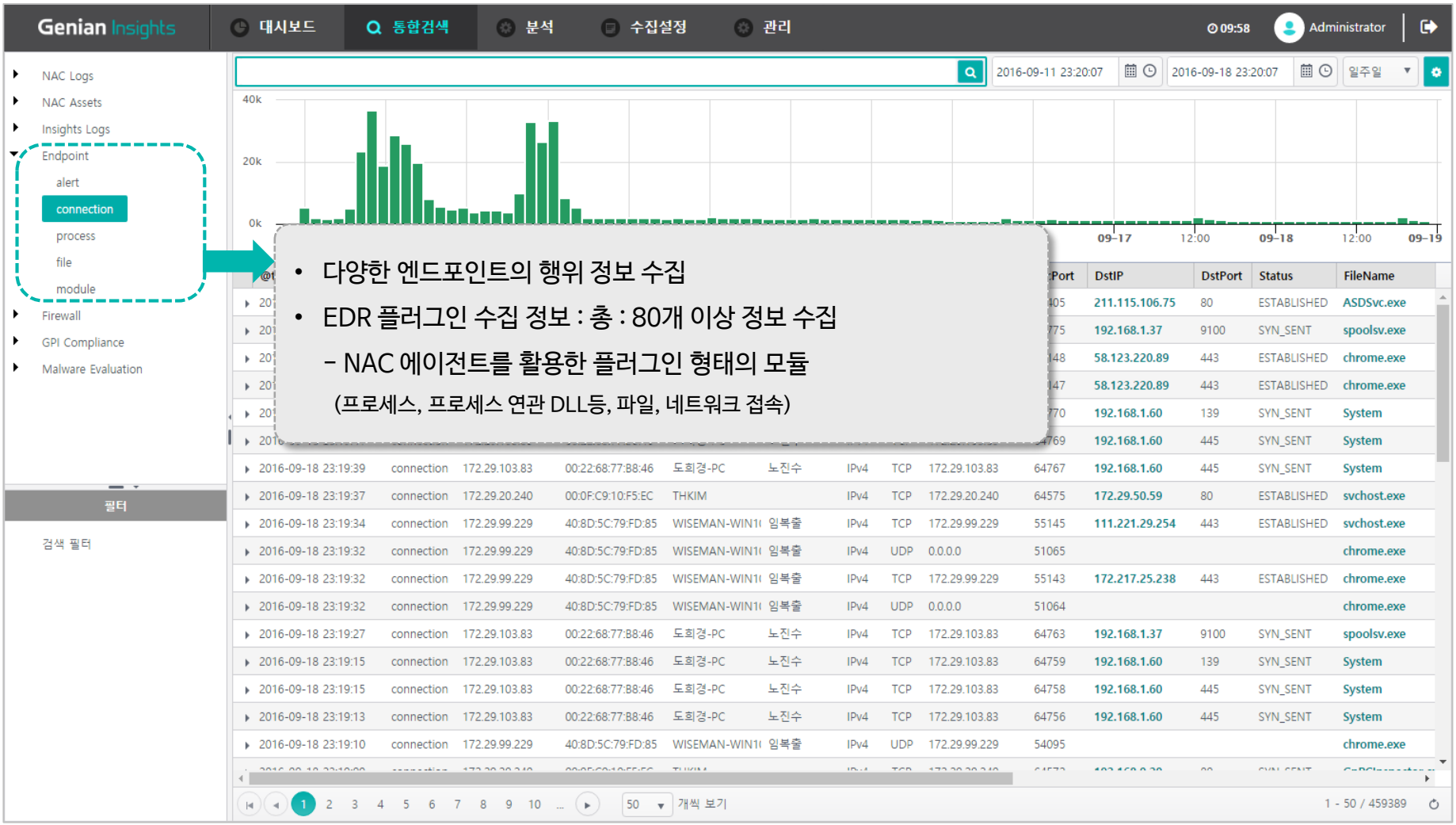


악성코드 유포지 및 C&C정보 (일간 약5,000~10,000개)	Zip, RAR, PE, Office, PDF 문서 기반 악성코드 수집
다양한 오픈 및 상용 소스 소집	최신 위협 인텔리전스 정보 생성



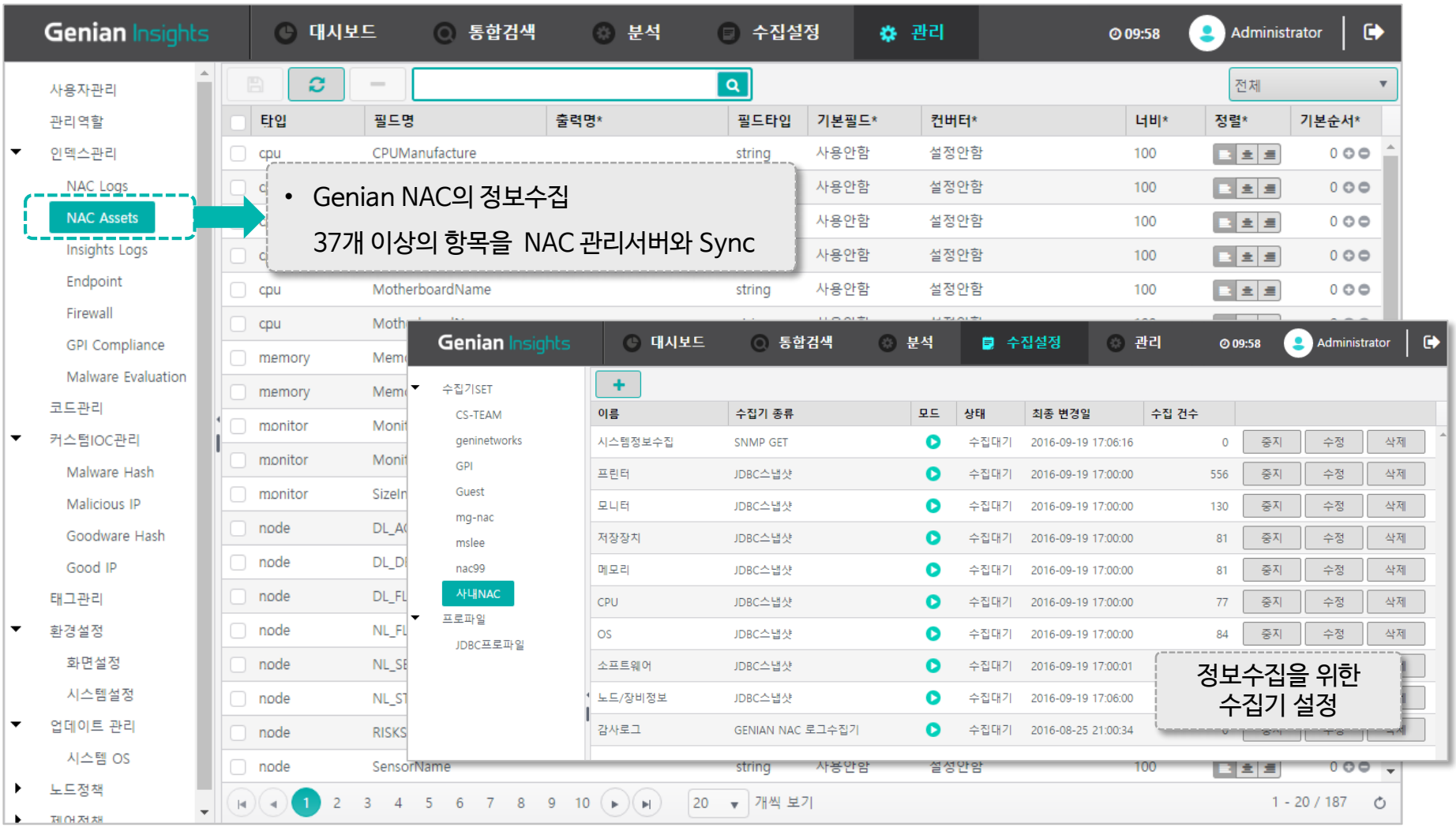
[EDR] 이벤트 정보수집

80개 이상의 엔드포인트 정보 수집



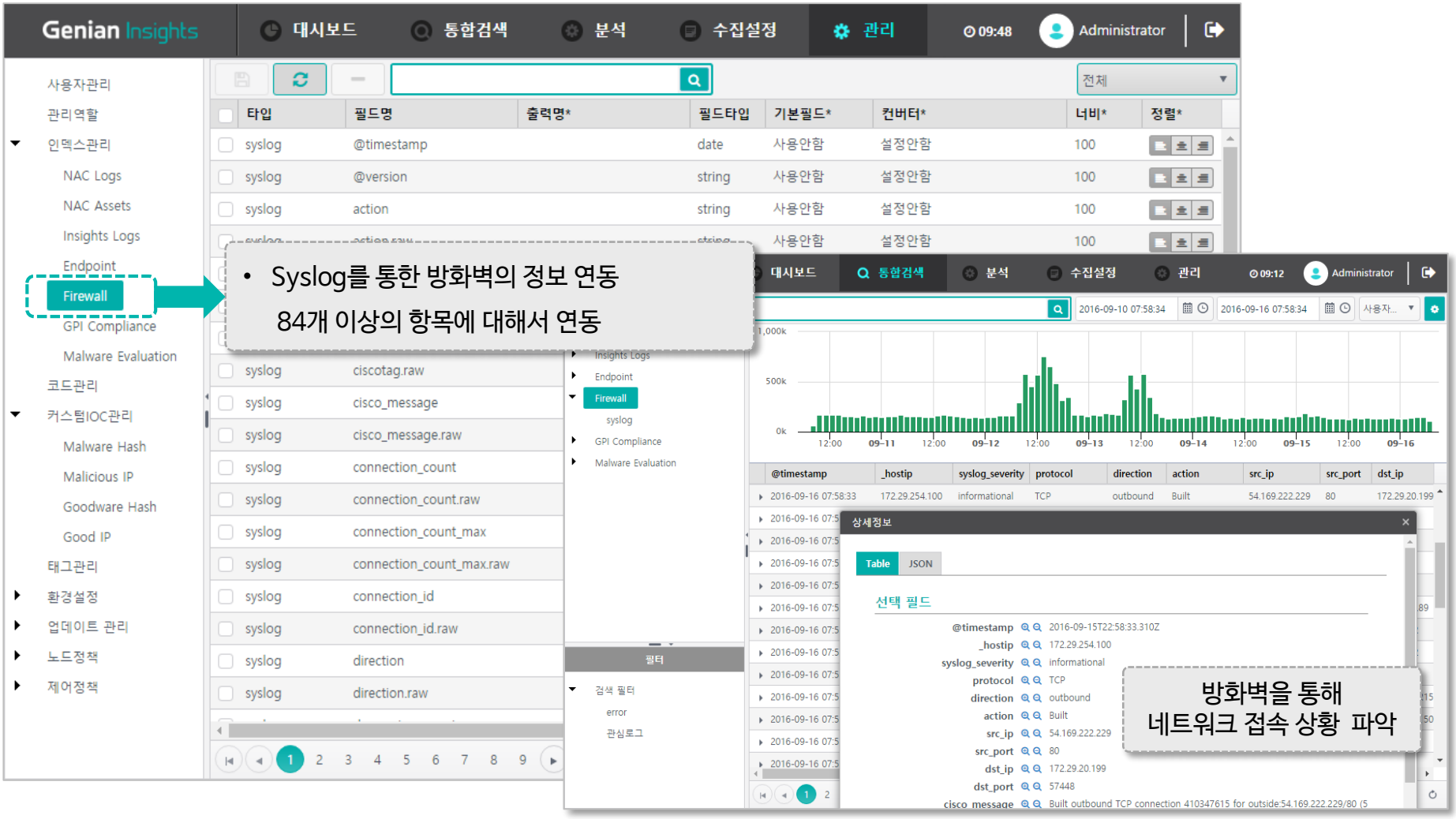
[통합 분석관리] 이벤트 정보수집

NAC 정보수집



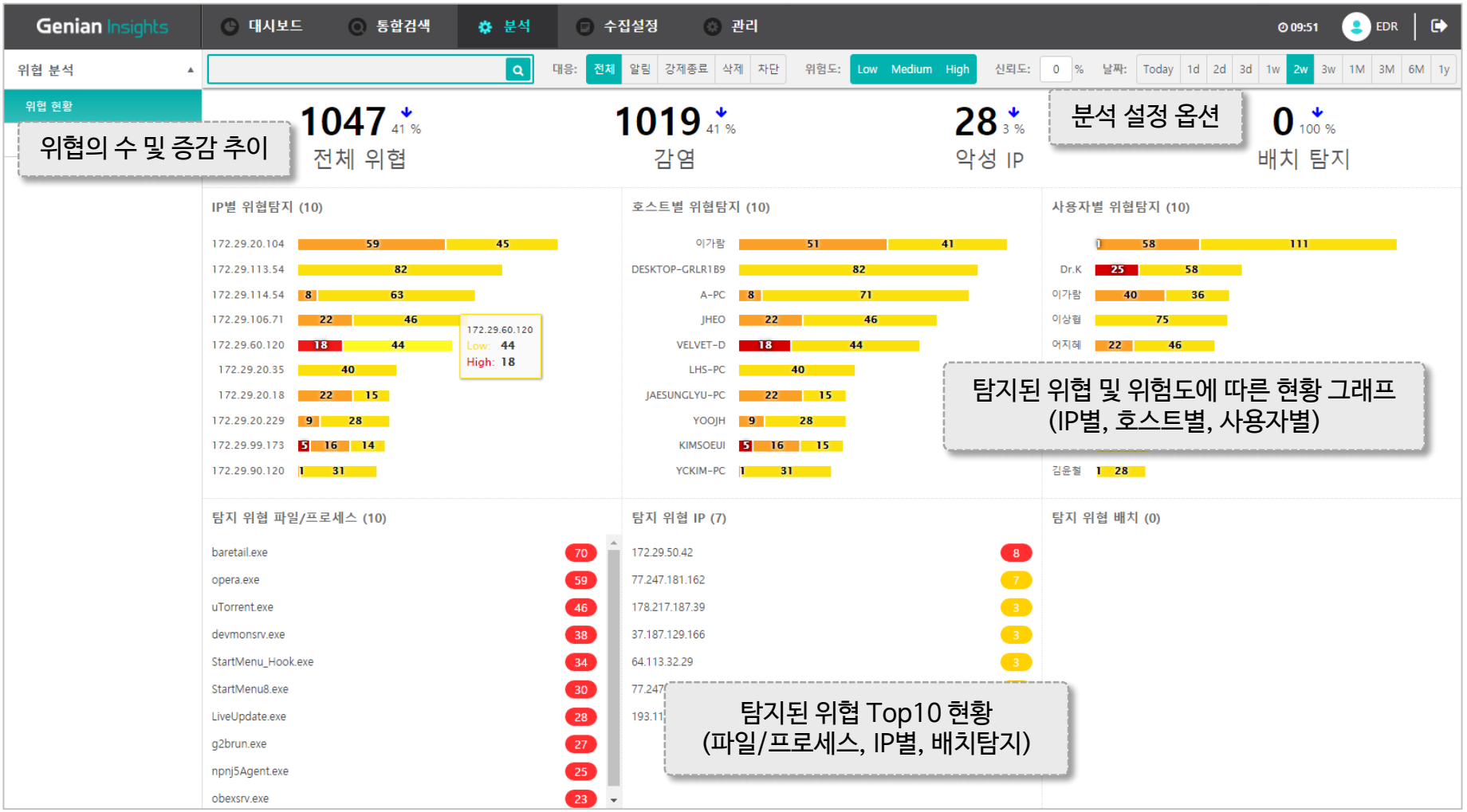
[통합 분석관리] 이벤트 정보수집

외부시스템 방화벽 정보수집



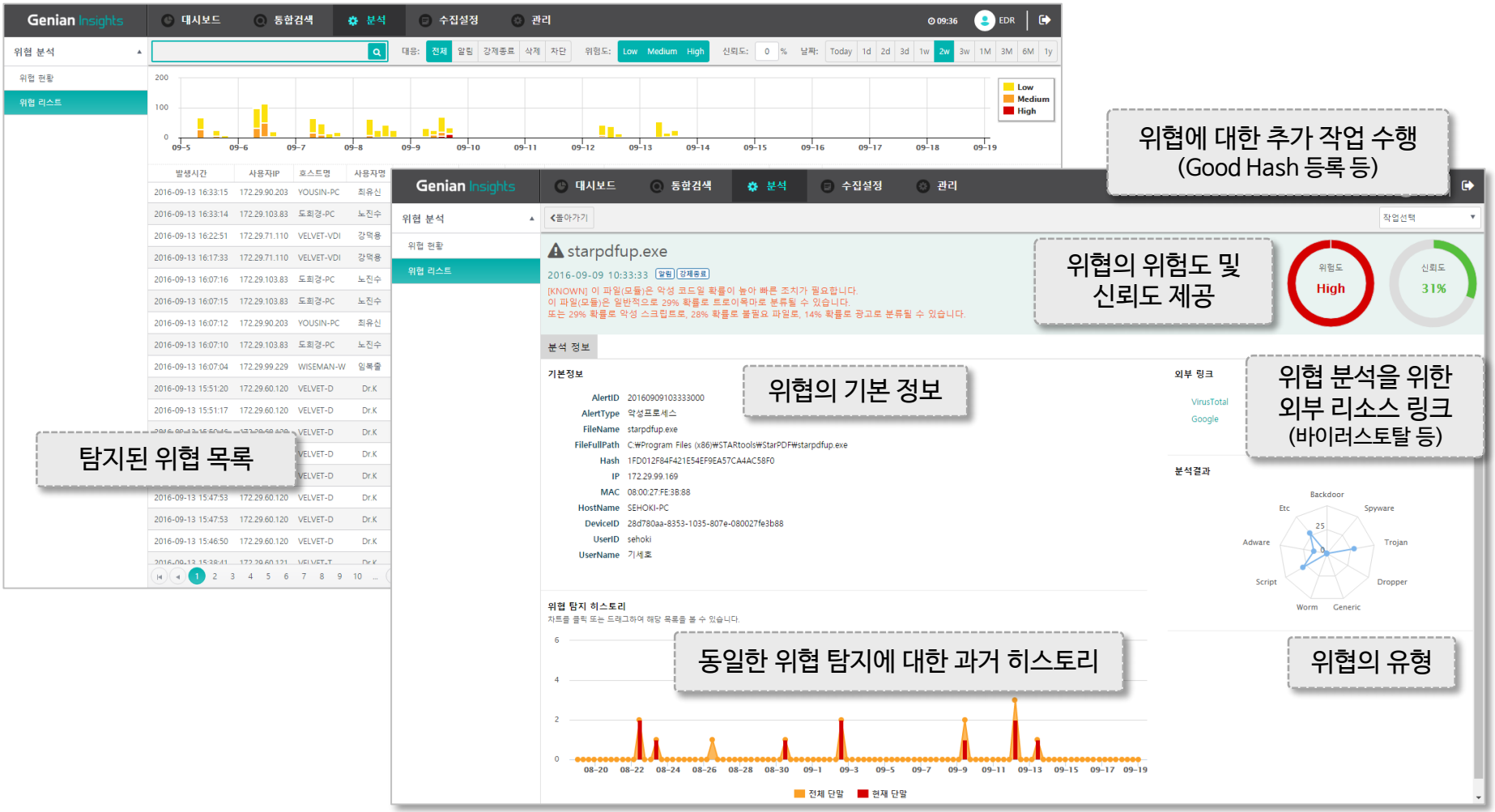
[EDR] 위협분석 – 현황

감염, 악성IP 등 위협 현황을 한눈에 파악 할 수 있는 위협분석 현황 제공



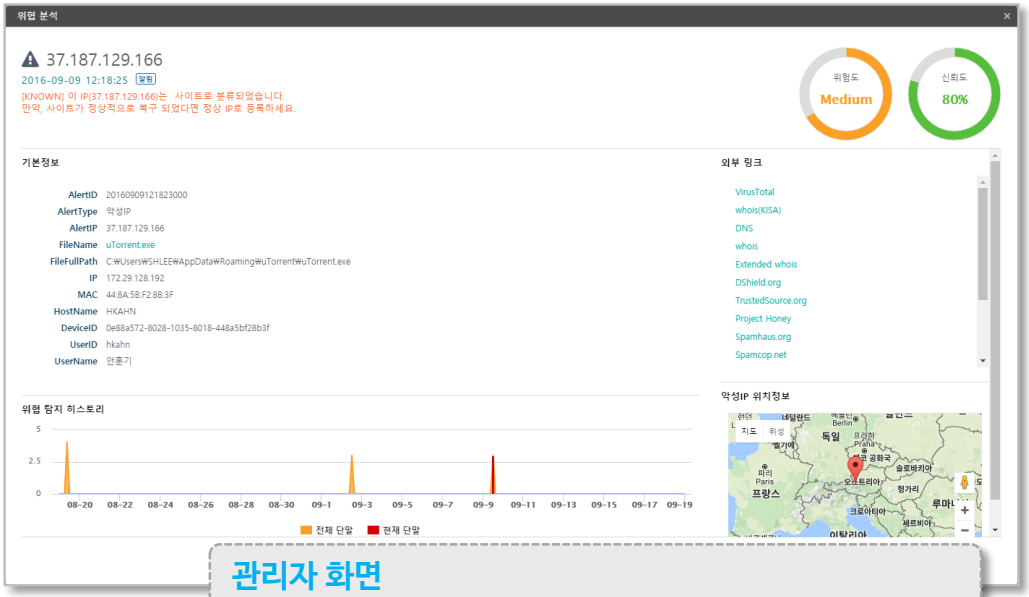
[EDR] 위협분석 - 목록 및 상세

탐지된 위협의 목록과 개별 위협에 대한 상세 분석 정보 제공



[EDR] 엔드포인트 위협 식별 및 대응

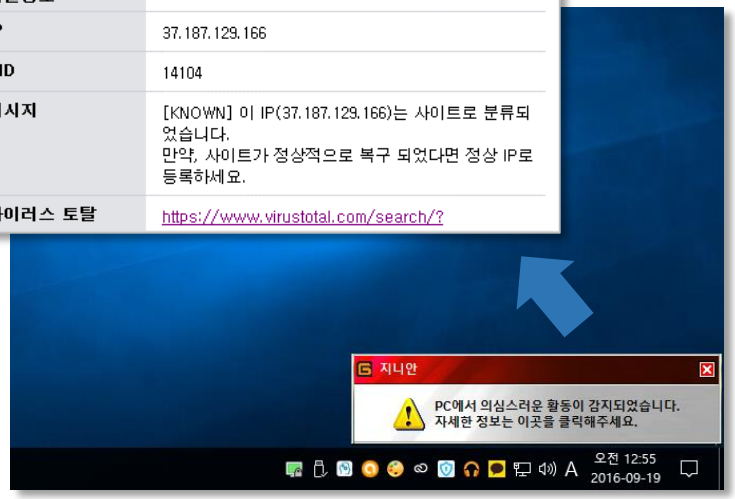
이상 행위 악성 IP 접속 프로세스



관리자 화면
특정 프로세스가 C&C서버로 의심되는 IP주소로 연결되는 이상 행위 발생

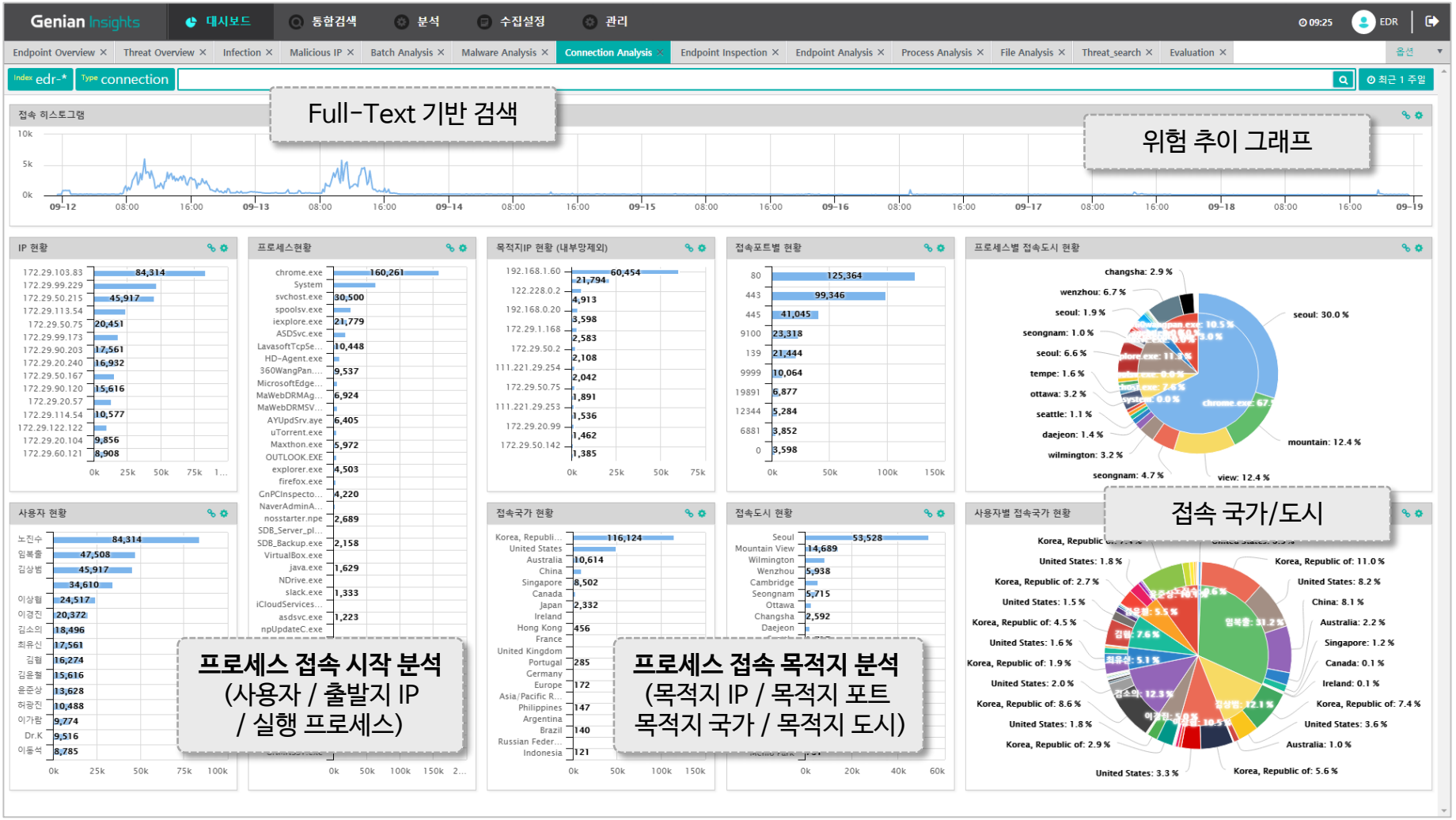
사용자 화면
해당 행위가 발생된 단말에서 Process Kill 이후 경고창을 발생하도록 설정

알람ID	
발생시각	2016-08-19 오전 9:19:22.826
신뢰도	80%
위험도	Medium
종류	악성IP - IPR
파일경로	
IP	37.187.129.166
PID	14104
메시지	[KNOWN] 이 IP(37.187.129.166)는 사이트로 분류되었습니다. 만약, 사이트가 정상적으로 복구 되었다면 정상 IP로 등록하세요.
바이러스 토탈	https://www.virustotal.com/search/?



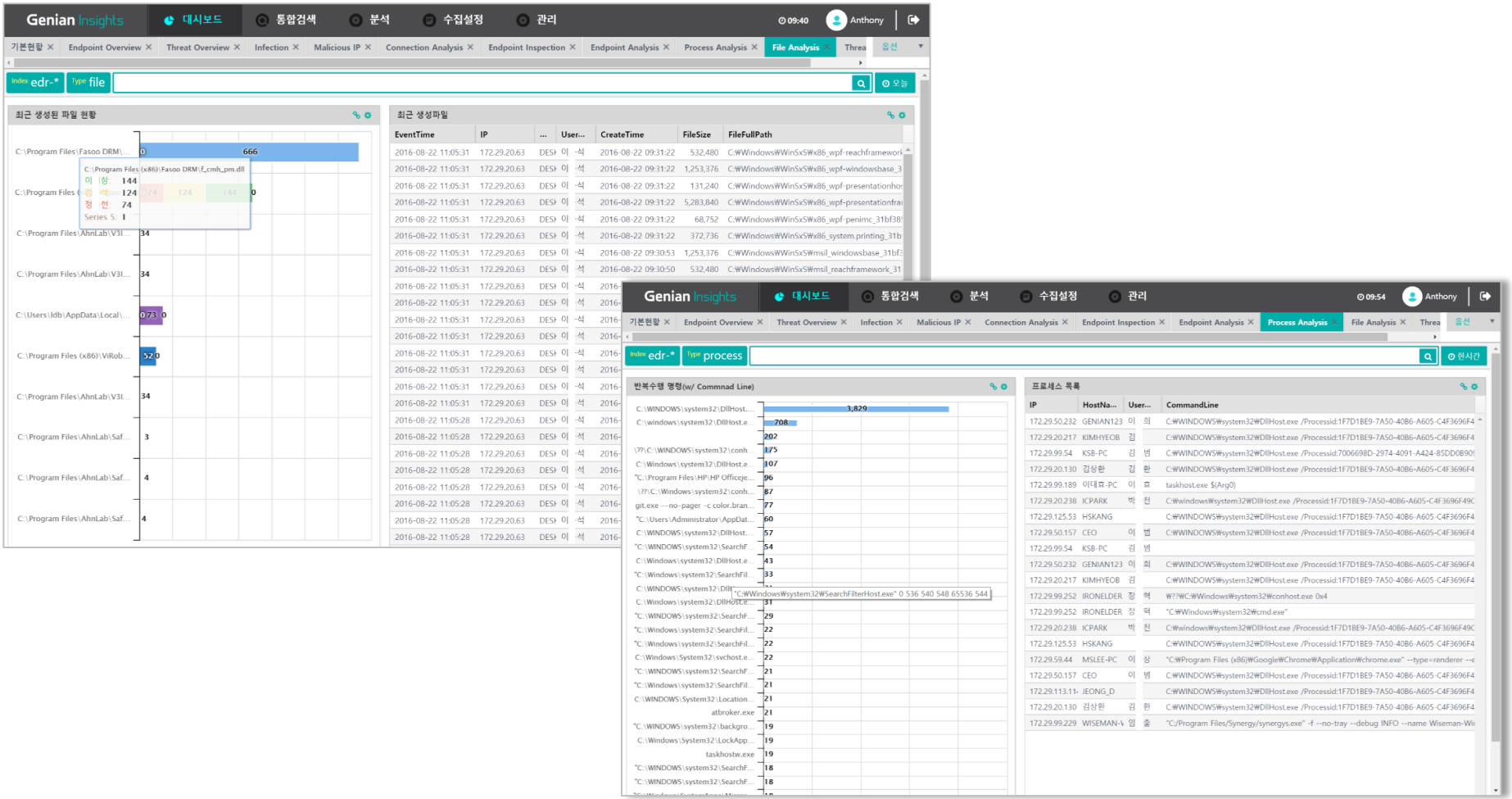
[EDR] 대시보드

사용자(단말) connection 정보 분석 화면



[EDR] 대시보드

파일 및 프로세스 분석

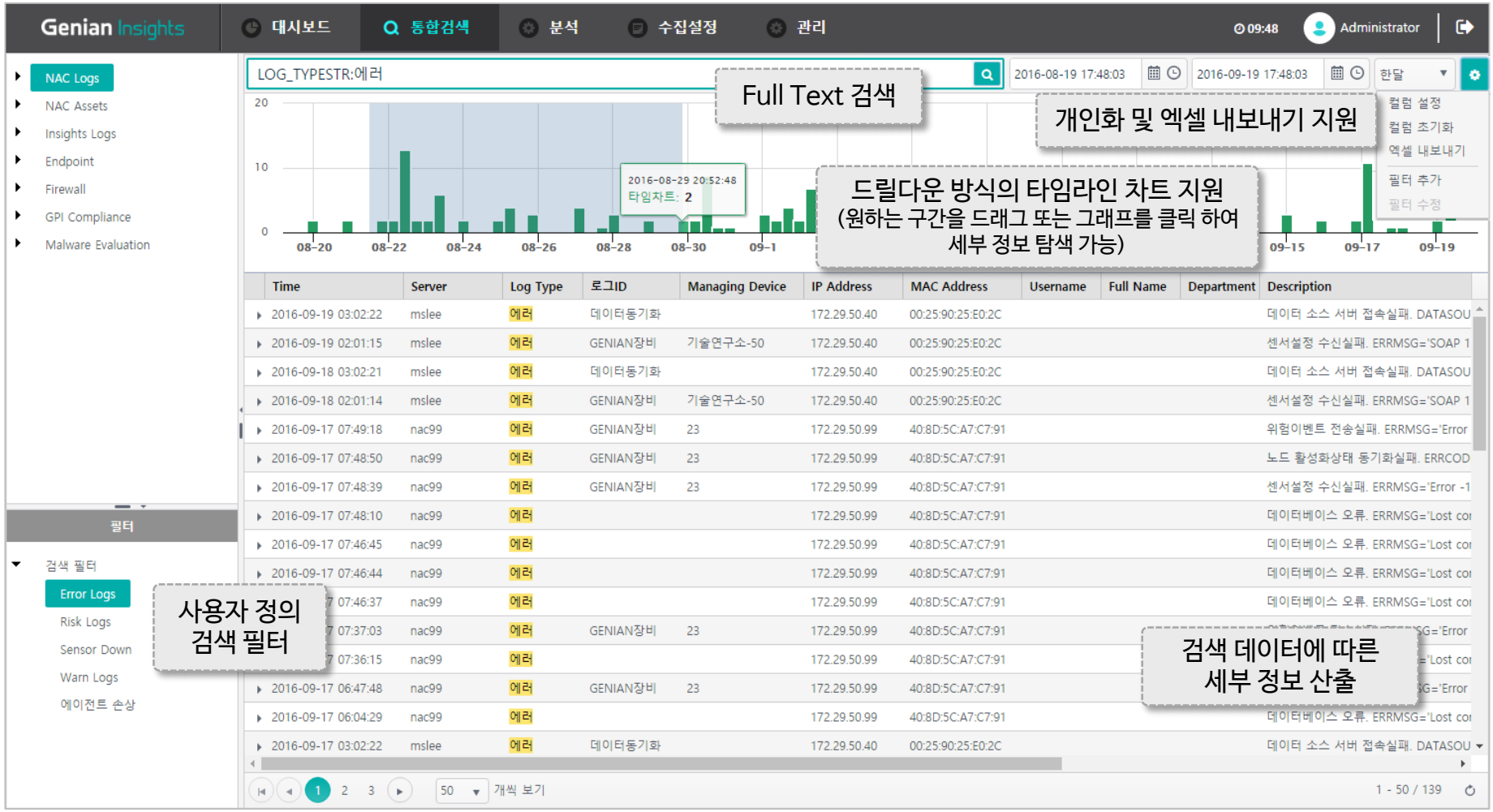


[EDR] 관리기능

커스텀 멀웨어 Hash/IP, Good Hash/IP 추가 및 관리 기능

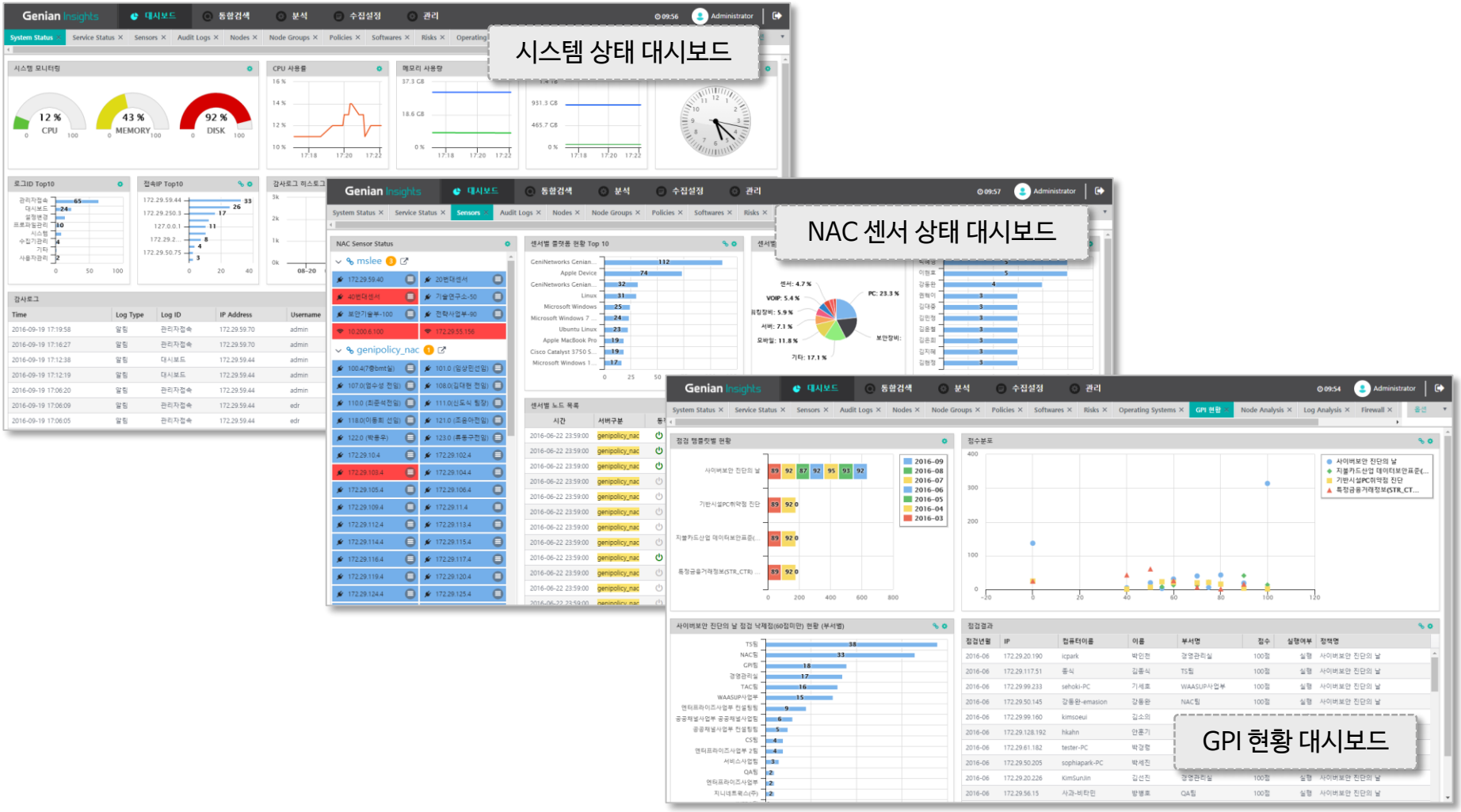
[통합 분석관리] 정보검색

수집된 정보에 대한 통합검색



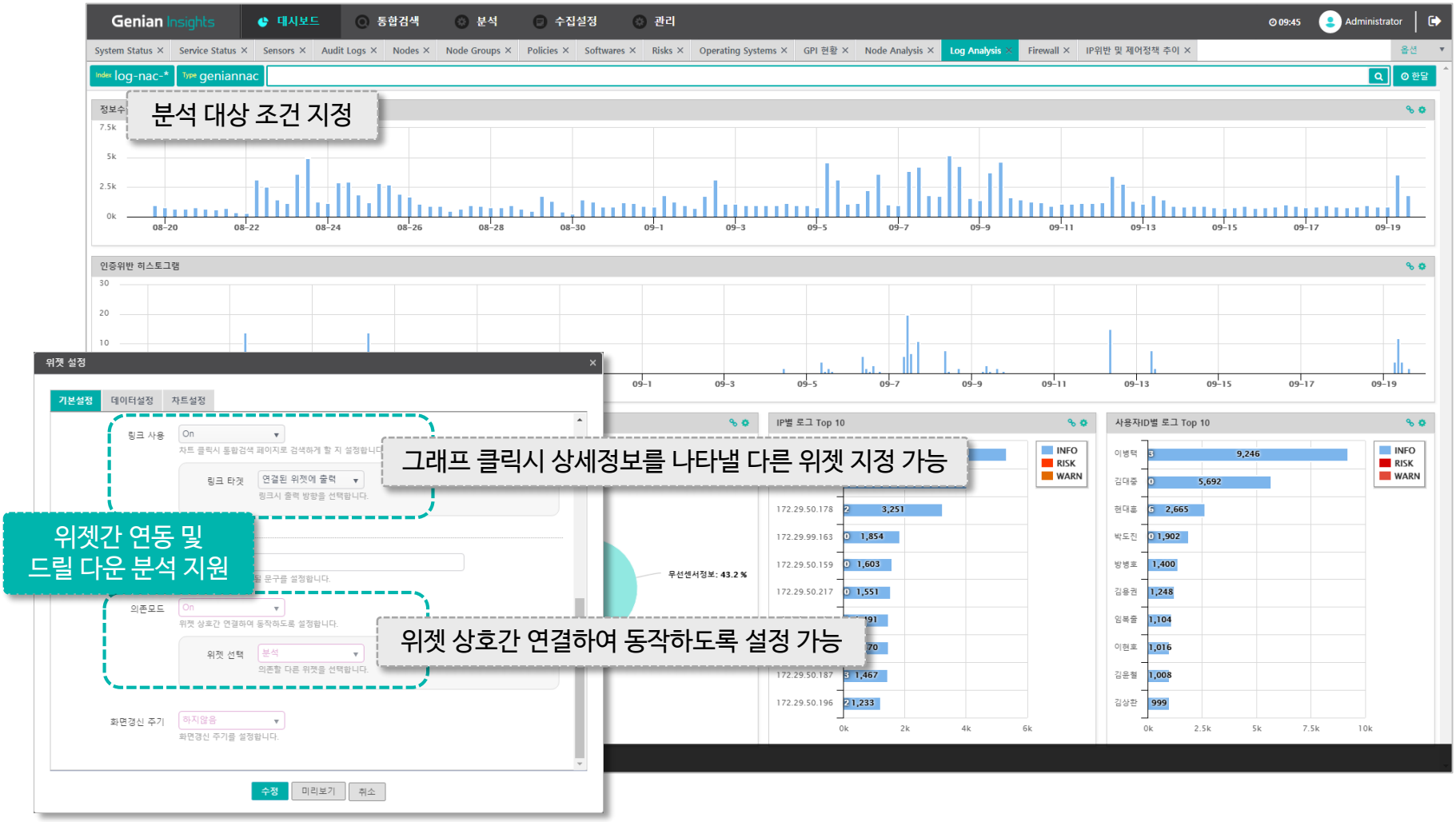
[통합 분석관리] 대시보드

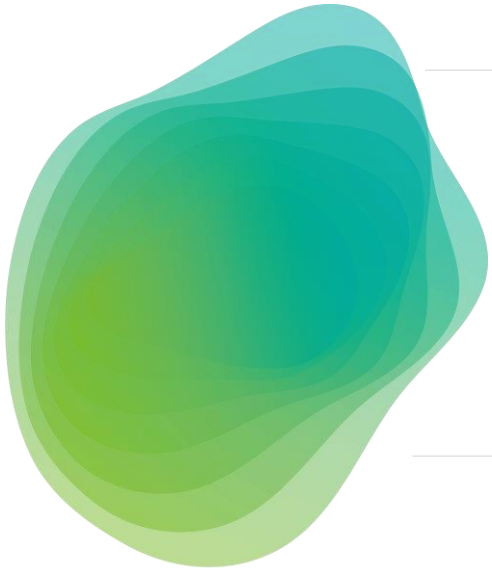
용도에 따른 다양한 분석 대시보드 설정 가능



[통합 분석관리] 위젯 기능 소개

분석대상 조건지정, 클릭시 링크 타겟 설정, 위젯간 연동 지원(의존모드)



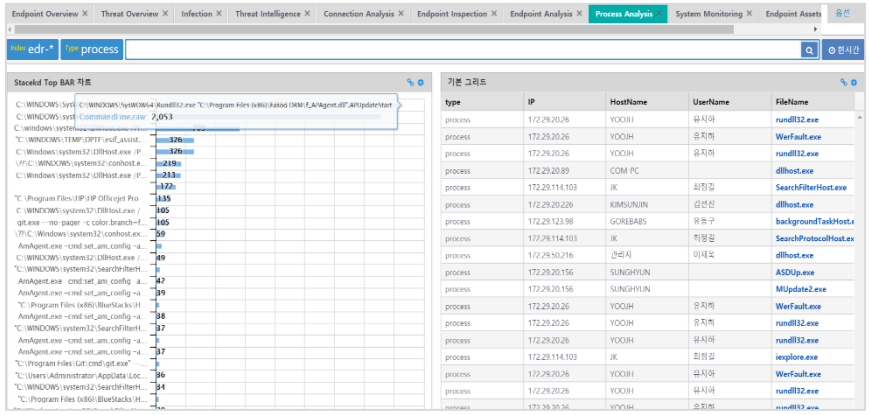


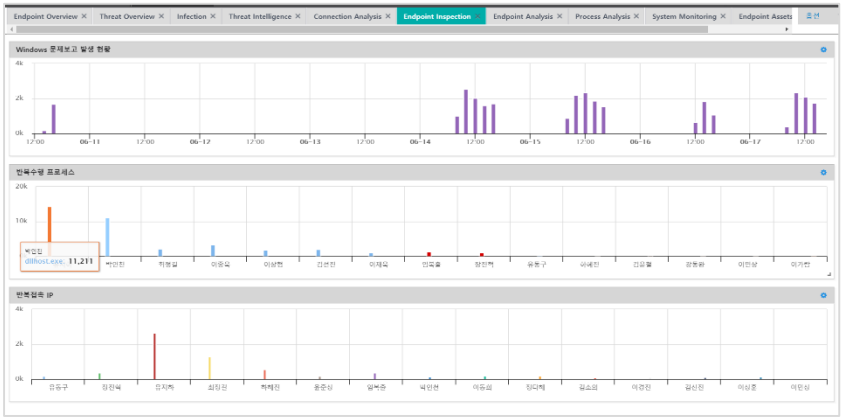
Genian Insights

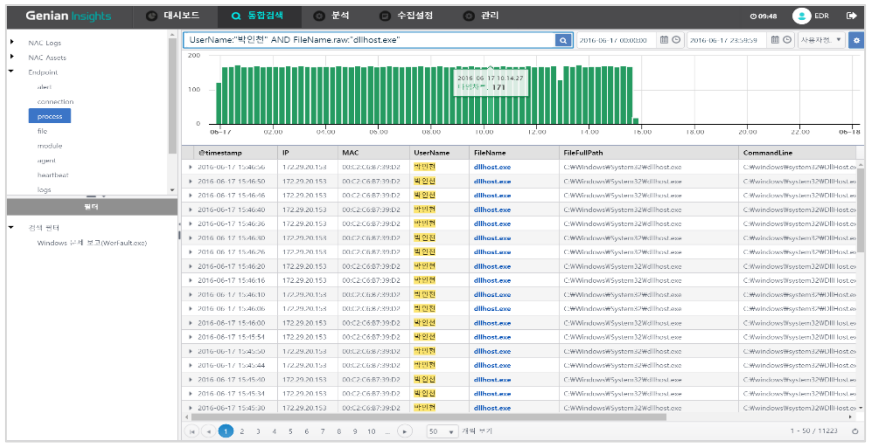
활용 예

활용 – 단말 이상유무 사전 파악

사용자 단말의 동작 이상 유무 사전 파악

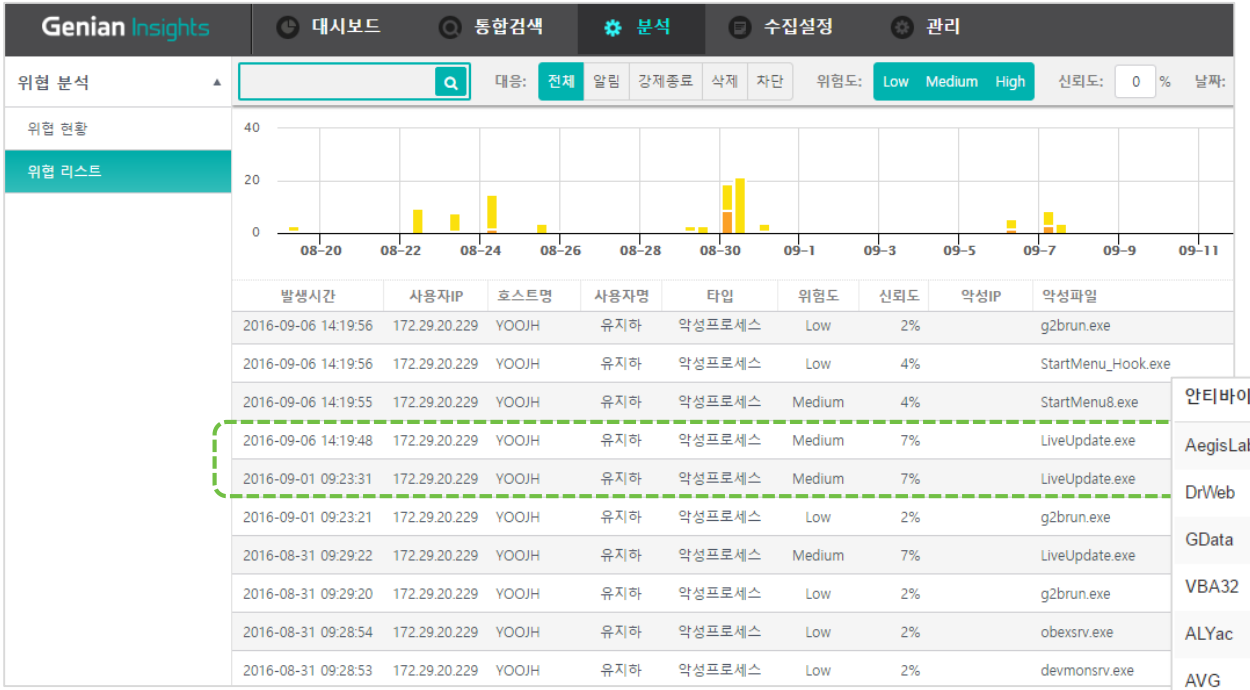






활용 – 기존 보안솔루션 미탐지 공격 대응

안티바이러스 솔루션 미탐지 프로세스 탐지 및 대응 가능



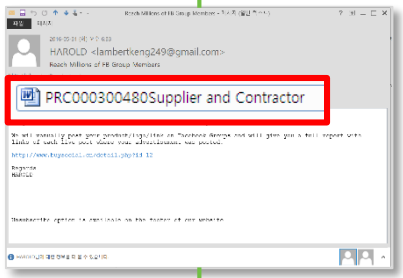
발생시간	사용자IP	호스트명	사용자명	타입	위험도	신뢰도	악성IP	악성파일
2016-09-06 14:19:56	172.29.20.229	YOOJH	유지하	악성프로세스	Low	2%		g2brun.exe
2016-09-06 14:19:56	172.29.20.229	YOOJH	유지하	악성프로세스	Low	4%		StartMenu_Hook.exe
2016-09-06 14:19:55	172.29.20.229	YOOJH	유지하	악성프로세스	Medium	4%		StartMenu8.exe
2016-09-06 14:19:48	172.29.20.229	YOOJH	유지하	악성프로세스	Medium	7%		LiveUpdate.exe
2016-09-01 09:23:31	172.29.20.229	YOOJH	유지하	악성프로세스	Medium	7%		LiveUpdate.exe
2016-09-01 09:23:21	172.29.20.229	YOOJH	유지하	악성프로세스	Low	2%		g2brun.exe
2016-08-31 09:29:22	172.29.20.229	YOOJH	유지하	악성프로세스	Medium	7%		LiveUpdate.exe
2016-08-31 09:29:20	172.29.20.229	YOOJH	유지하	악성프로세스	Low	2%		g2brun.exe
2016-08-31 09:28:54	172.29.20.229	YOOJH	유지하	악성프로세스	Low	2%		obexsrv.exe
2016-08-31 09:28:53	172.29.20.229	YOOJH	유지하	악성프로세스	Low	2%		devmonsrv.exe

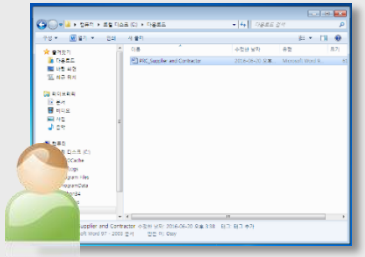
안티바이러스	결과
AegisLab	W32.Adware.Iobit!c
DrWeb	Program.Unwanted.276
GData	Win32.Adware.iObit.A
VBA32	Adware.iObit
ALYac	✔
AVG	✔
AVware	✔
Ad-Aware	✔
AhnLab-V3	✔
Alibaba	✔
Antiy-AVL	✔
Arcabit	✔

활용 - 취약점 공격 대응

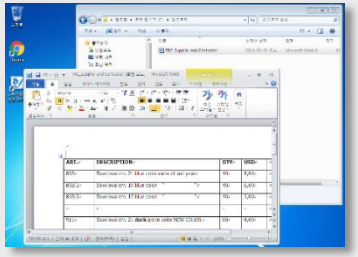
CVE-2014-1761.D / DOC_Dropper 취약점 공격 대응 예

Genian Insights 미적용 시

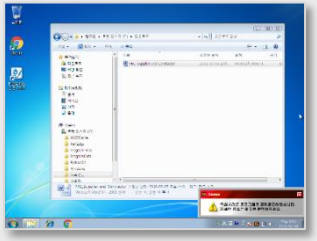




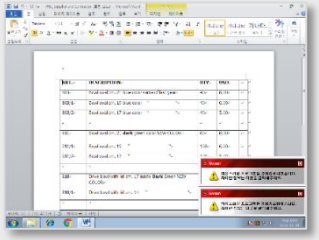
악성코드 감염 파일 다운로드



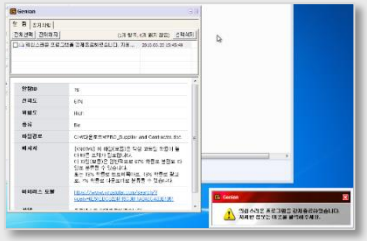
단말 감염



파일 다운로드 시 차단, 알림



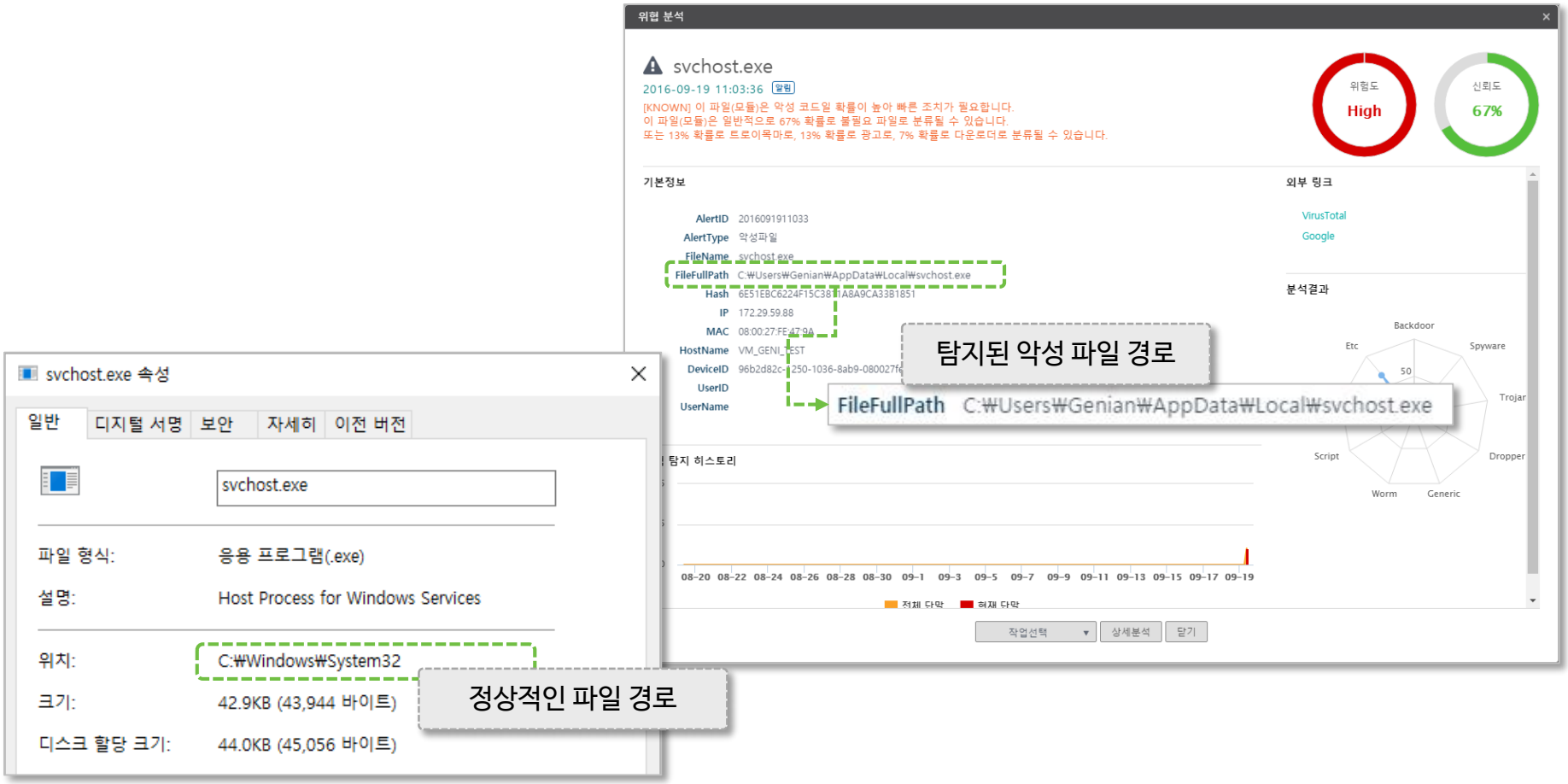
문서 열람 시 차단, 알림



상세정보 열람 : 단말 미감염

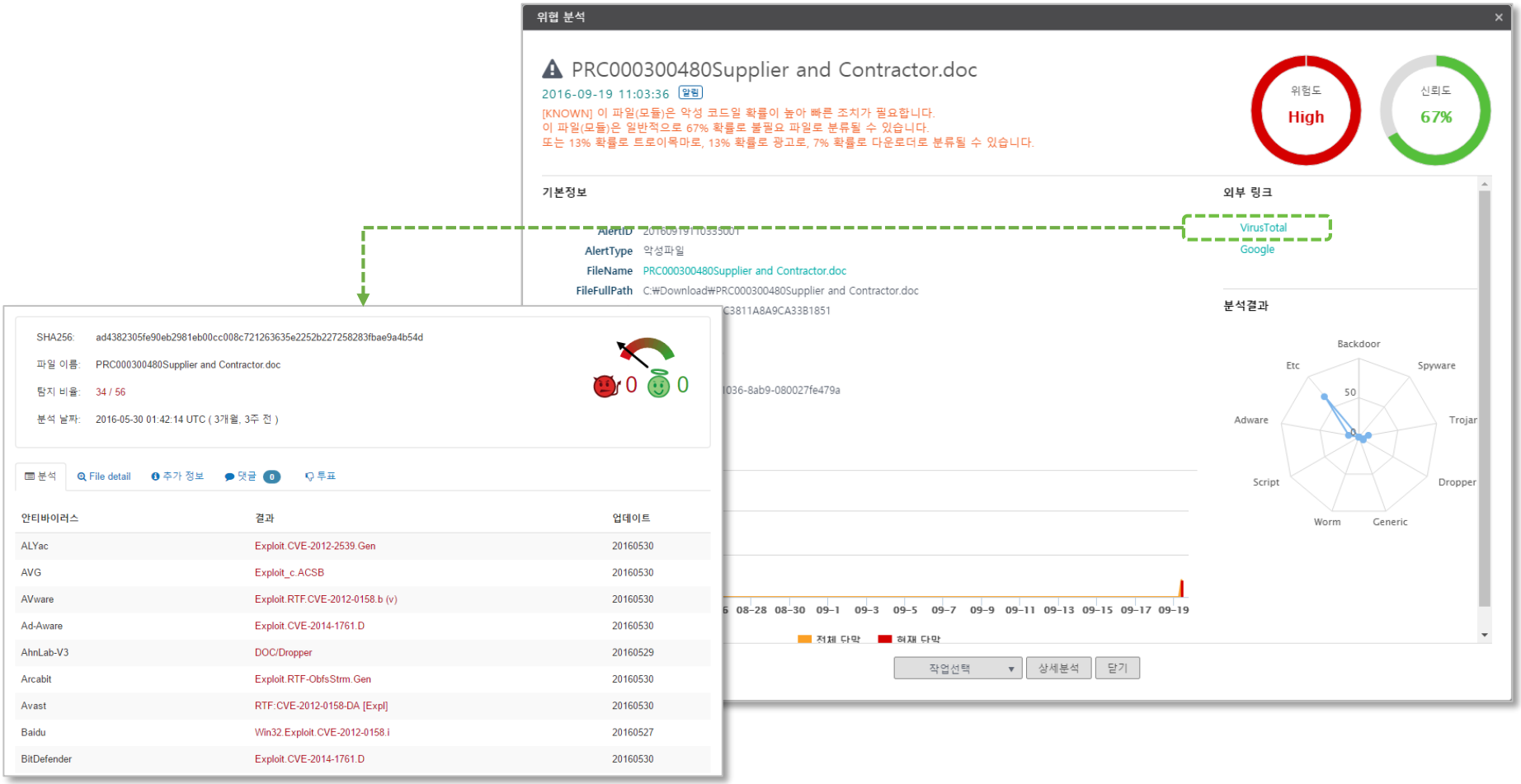
활용 - 취약점 공격 대응

솔루션 적용 시 CVE-2014-1761.D / DOC_Dropper
위변조 파일 다운로드 시 취약점 탐지 화면



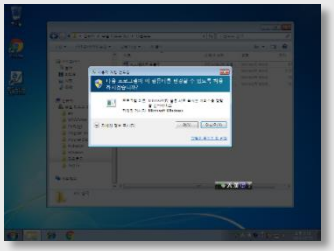
활용 - 취약점 공격 대응

솔루션 적용 시 CVE-2014-1761.D / DOC_Dropper
위협분석 결과 화면 (VirusTotal, google 결과 제공)

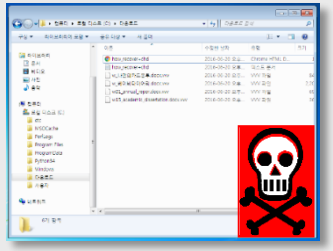


활용 - 랜섬웨어 대응

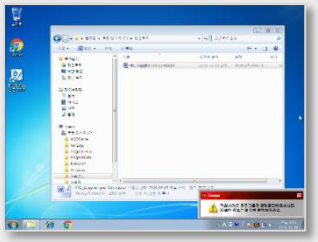
Genian Insights 미적용 시



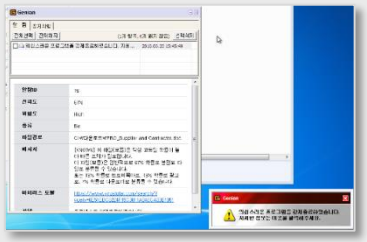
악성코드 감염 파일 다운로드



파일 감염/암호화



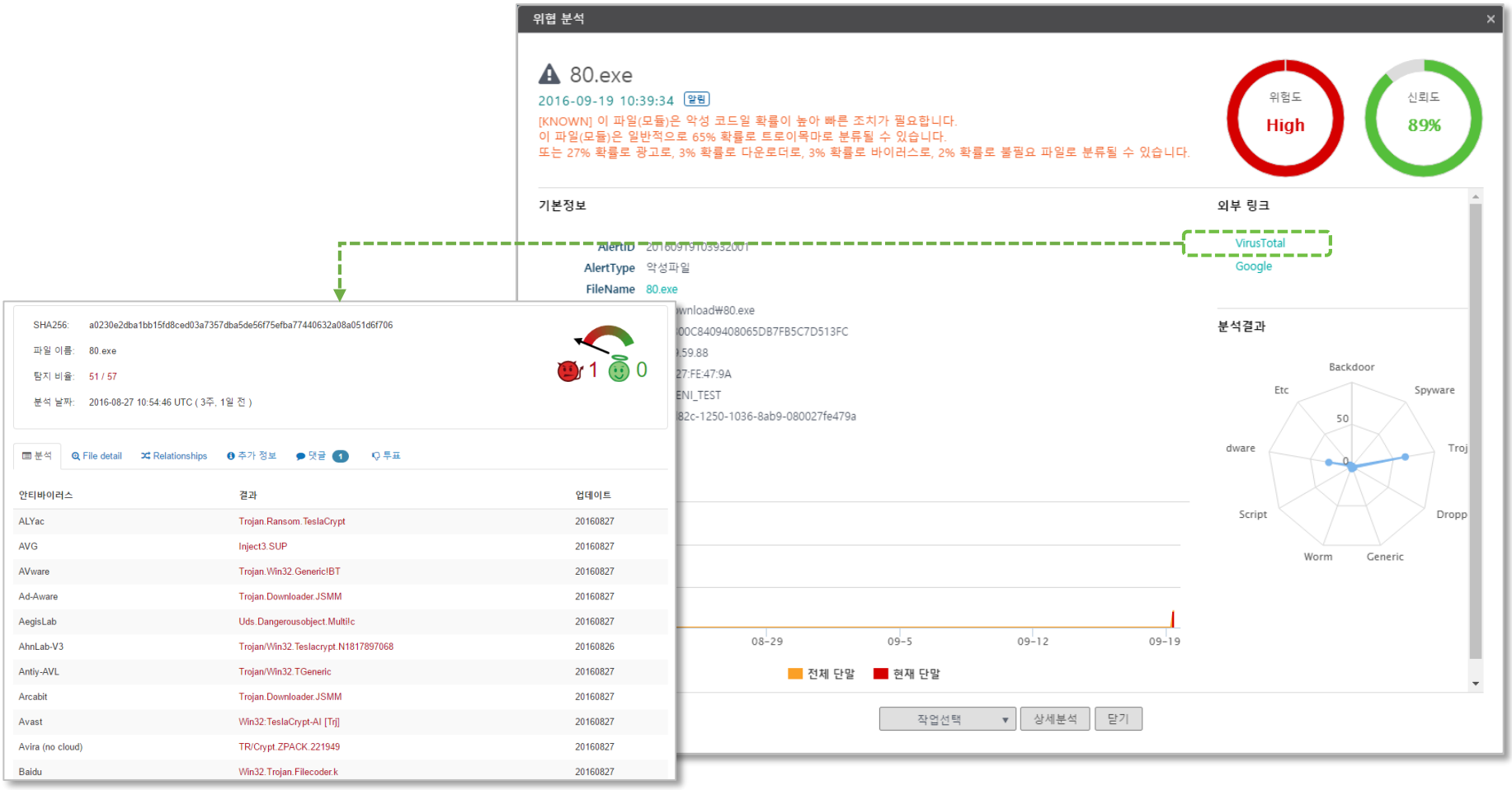
파일 다운로드 시 차단, 알림



상세정보 열람 : 단말 미감염

활용 - 랜섬웨어 대응

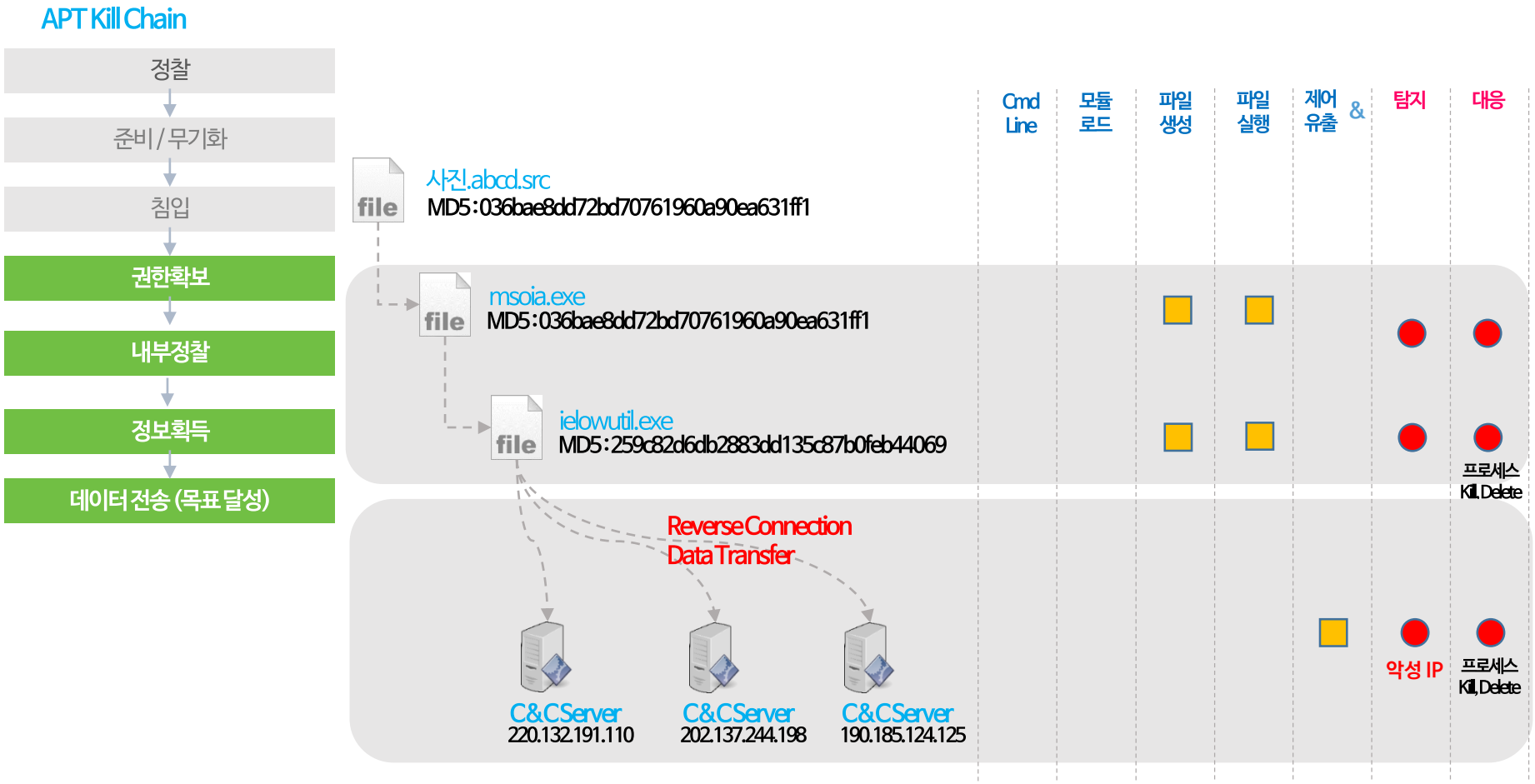
솔루션 적용 시 랜섬웨어 악성코드 위협분석 결과 화면 (VirusTotal, google 결과 제공)



활용 - I사 APT 사고발생 대응

실제 APT 공격상황에서 Genian Insights 활용

공격 Chain의 고리를 끊을 수 있는 지능형 솔루션



Thank you!

Tel : 031-422-3823
Mail : geni@geninetworks.com