

보안 전략의 변화

(지니안 인사이드 소개)

목 차

01

변화의 필요성

02

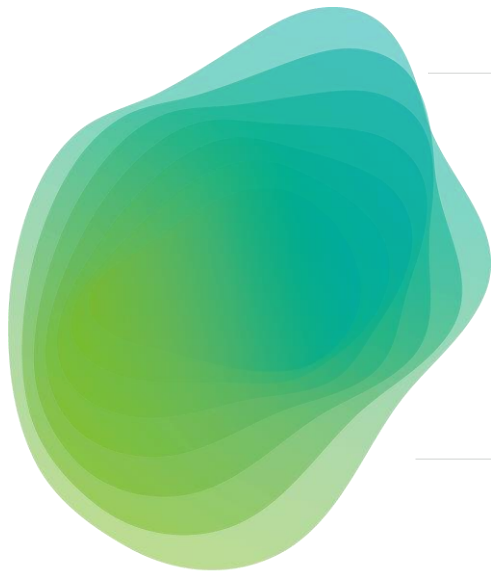
Insights 제품 소개

03

Insights 기능 소개

04

Insights 활용 방안



변화의 필요성

(방어 전략의 한계)

보안 전략의 변화

시스템, Application의 복잡, 다양성 증가
공격의 지능화, 조직화. 사용자보안의식 개선의 한계



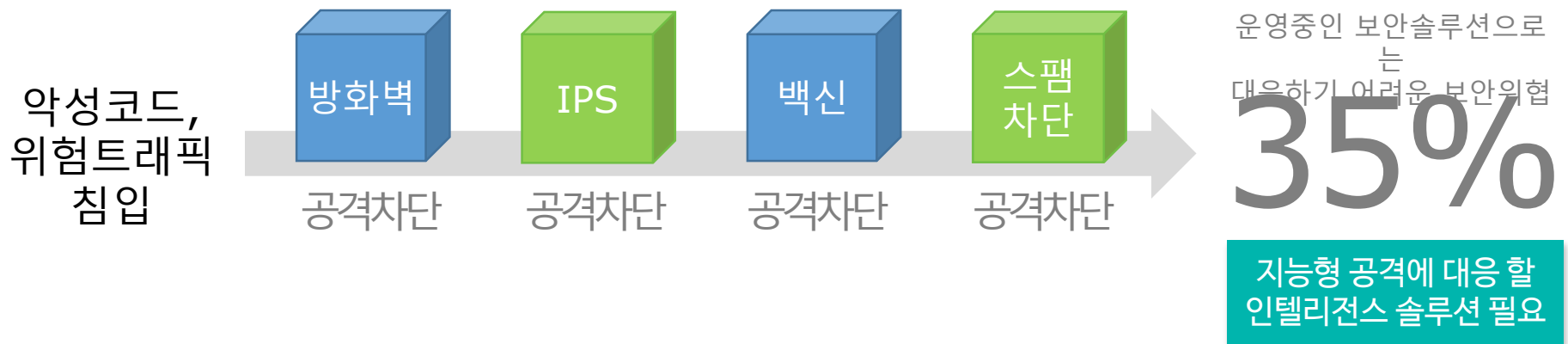
모든 공격 100% 방어는 불가능
방어 위주의 보안 전략의 한계



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



방송사(MBC, KBS)
은행(신한은행, 농협)



최초 공격시작에서 사고 발생까지의 기간

2개월



16년 7월
2,600만건 개인정보유출

8개월



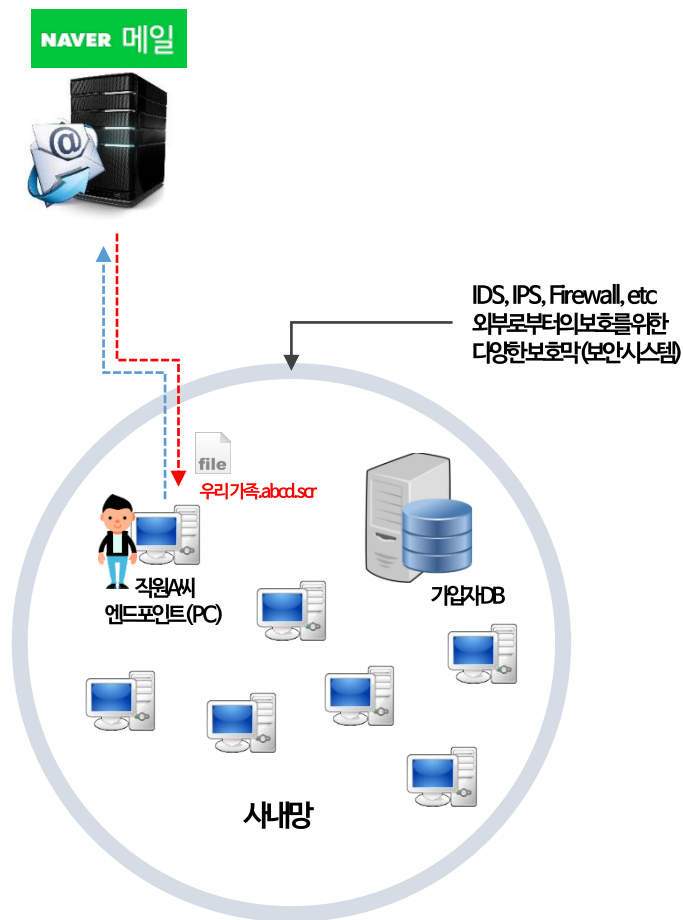
13년 3월
3.20대란 전산망 마비

7개월



11년 4월
전산망 마비

수개월 간 진행 되는 지능형 위협 공격 (인터파크 사례)



쇼핑몰에서 근무중인 A직원



발신자

동생 이메일 주소

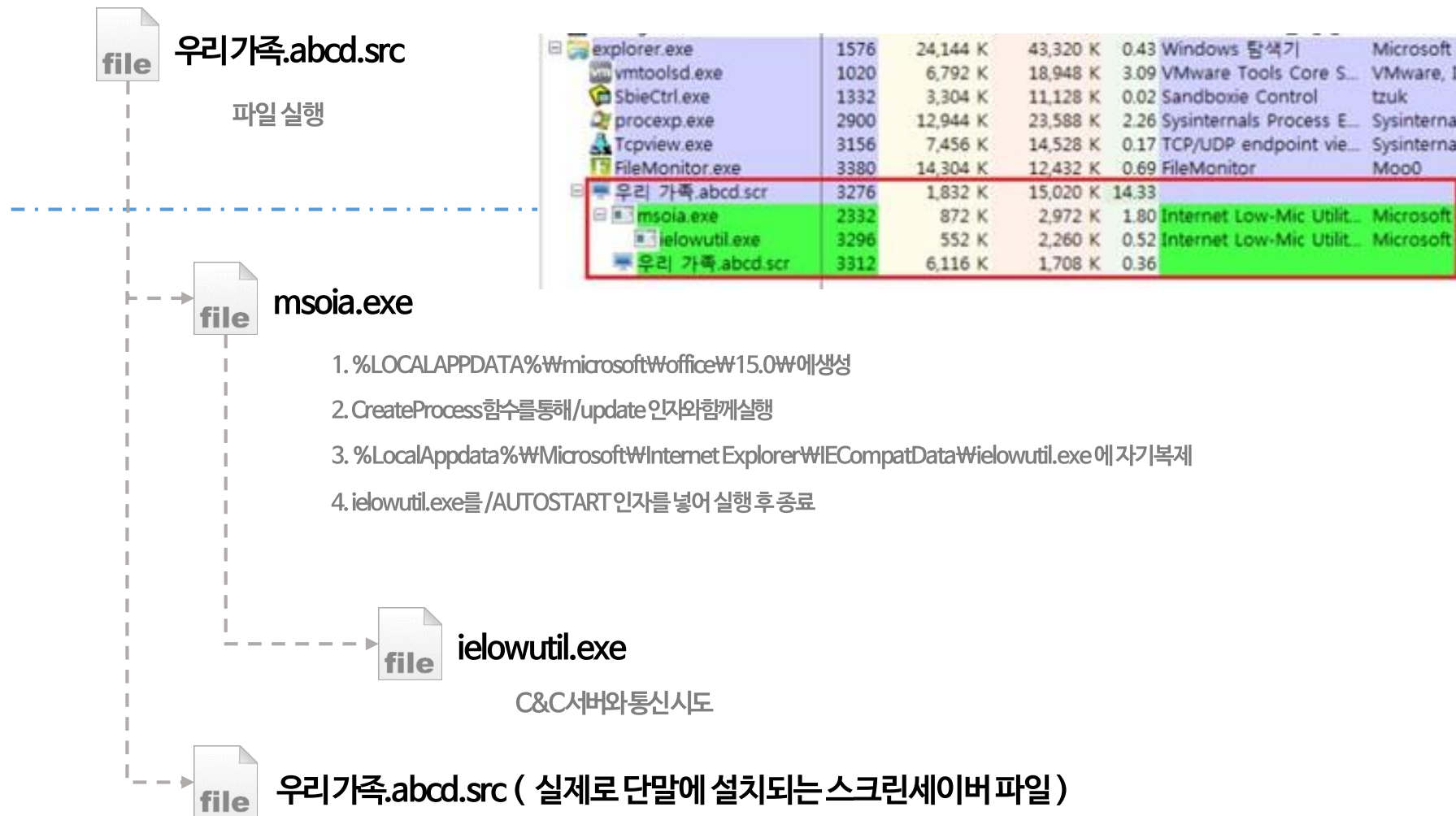
첨부파일



우리 가족.abcd.scr

수개월 간 진행 되는 지능형 위협 공격 (인터파크 사례)

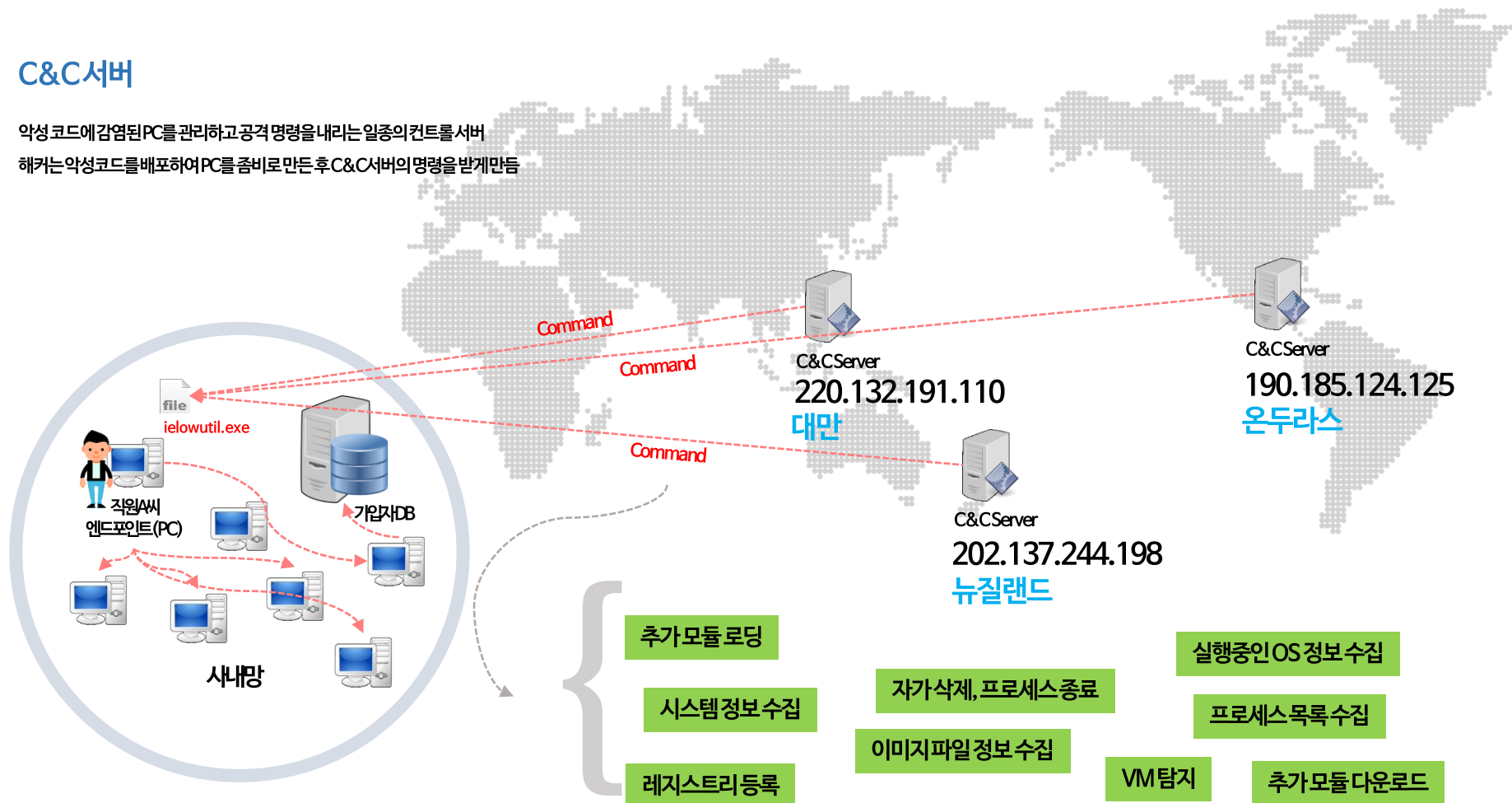
직원 A씨의 엔드포인트 (PC)에서 일어나는 일



수개월 간 진행 되는 지능형 위협 공격 (인터파크 사례)

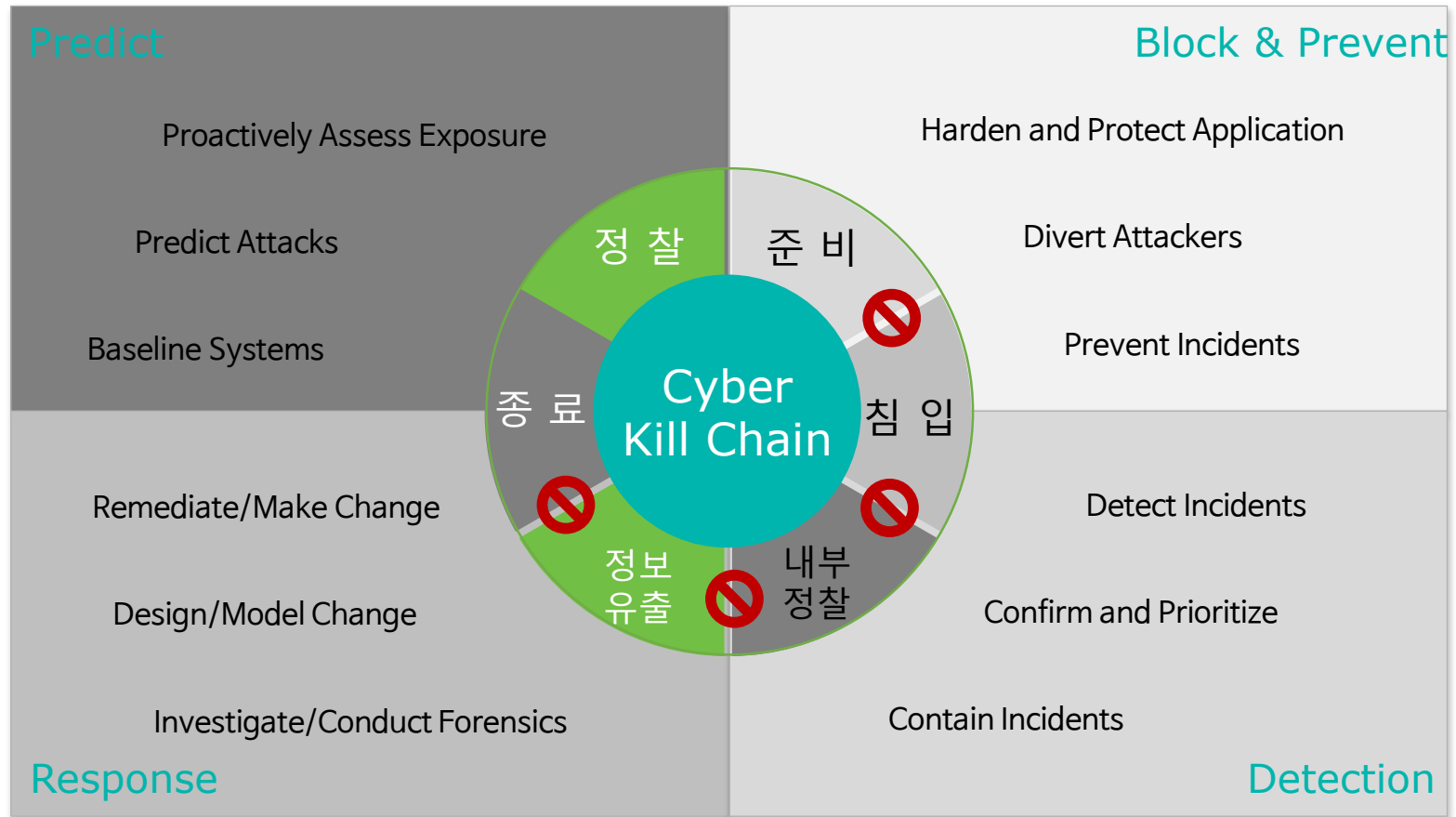
C&C서버

악성 코드에 감염된 PC를 관리하고 공격 명령을 내리는 일종의 컨트롤 서버
해커는 악성코드를 배포하여 PC를 좀비로 만든 후 C&C서버의 명령을 받게 만듦



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 막기 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

노드 정보 (IP + MAC)

사용자 정보

사용자명

부서

사용자 ID

단말 정보

H/W
[CPU, 모니터, 프린터, HDD 등]

S/W
[OS, 버전, 설치S/W, 패치정보 등]

네트워크 서비스 정보

운영중인 서비스

동작중인 네트워크 프로세스

위치 정보

스위치 포트

무선위치 추적

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

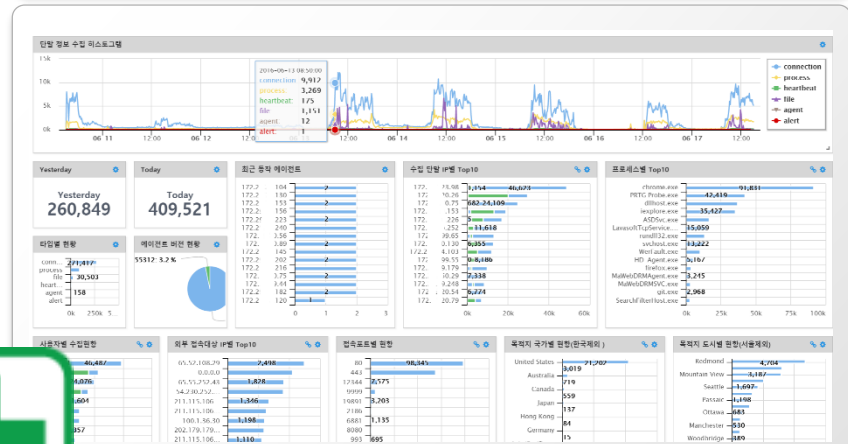
- 단말의 네트워크 인터페이스 탐지 및 제어
- 무선랜 인터페이스에서 탐지된/연결된 AP항목 수집
- 관리자가 지정한 White List 기반의 AP에만 접속 가능한 정책

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

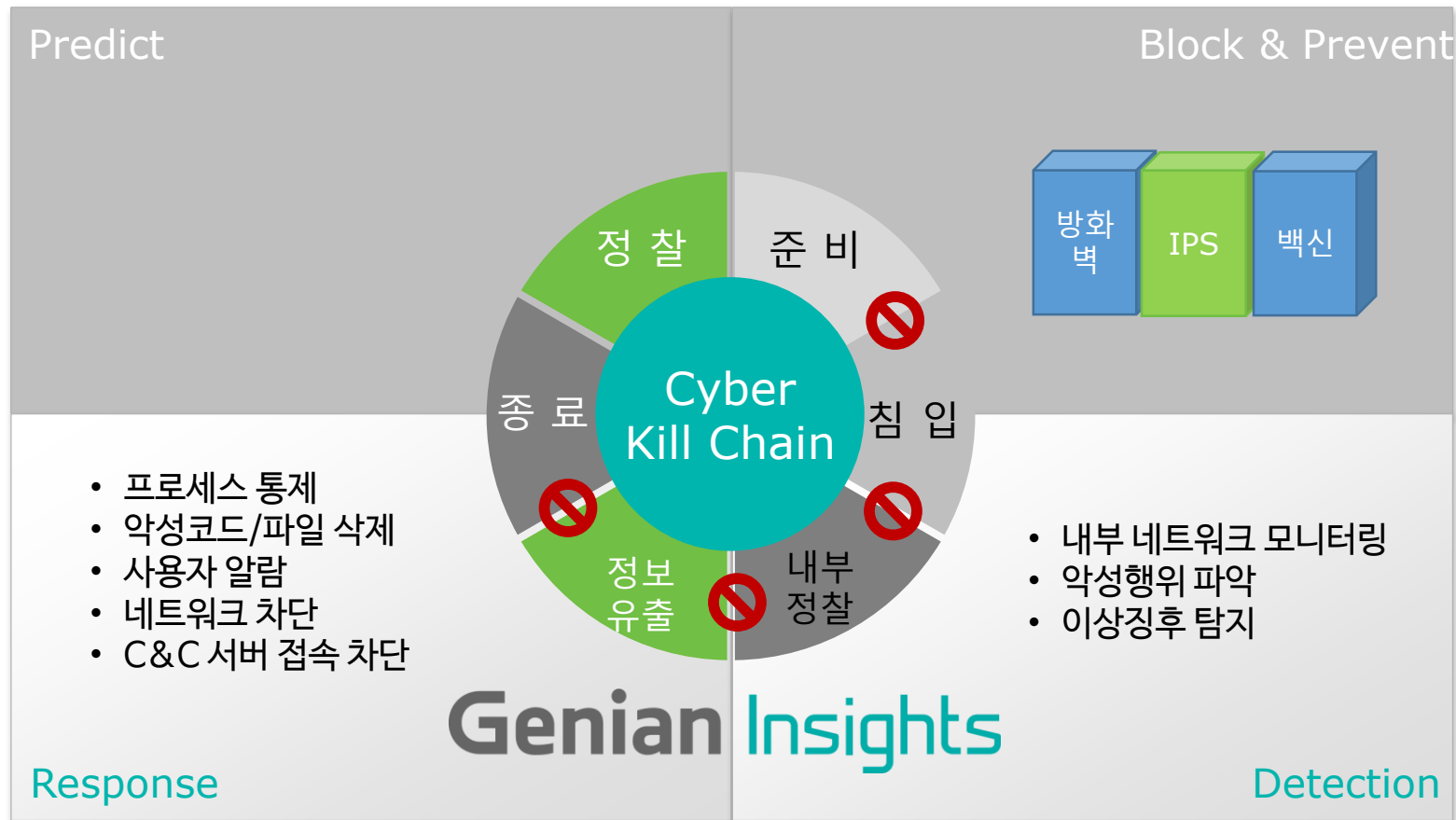


- Process
- Connection
- File
- Heartbeat

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

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

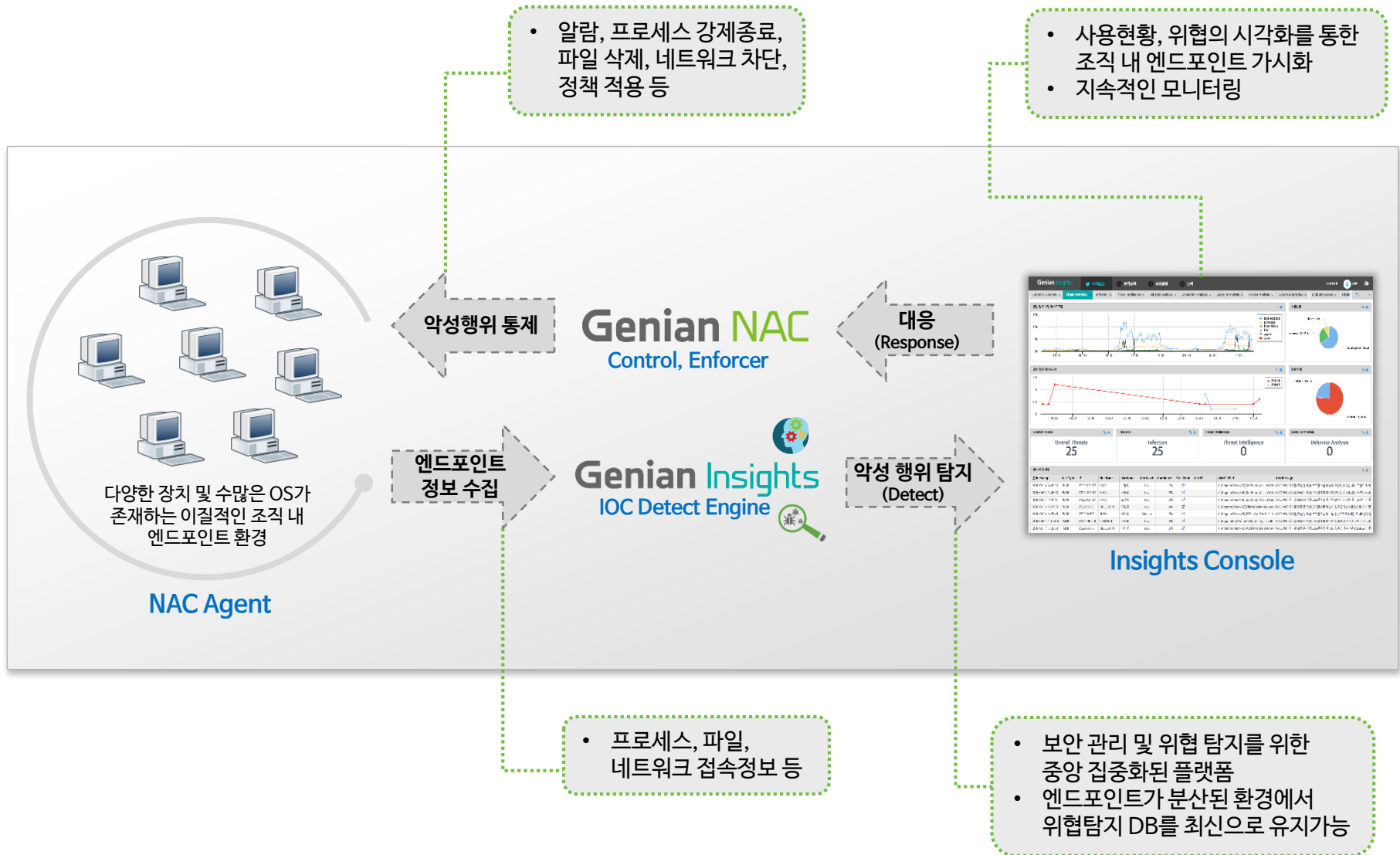
유연한 대시보드

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

모듈별 손쉬운 적용

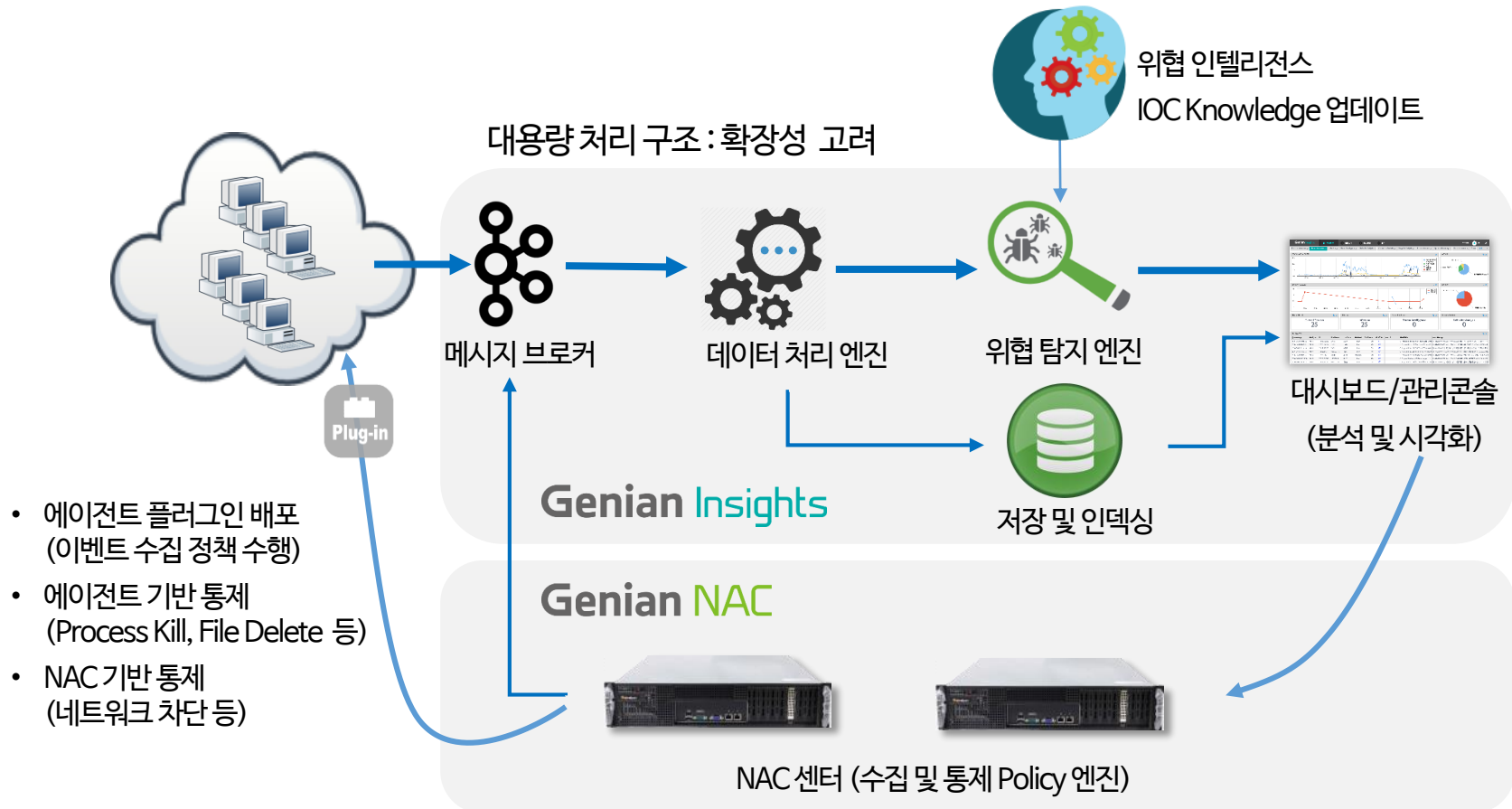
- Genian Insights 기본 통합 관리 분석 기능 외 엔드포인트(E 모듈), 네트워크 행위 분석(N 모듈)등 선택적 적용 가능
- NAC 플러그인 기반 손쉬운 적용

Genian Insights 동작 개요



Genian Insights 구성요소 및 역할

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



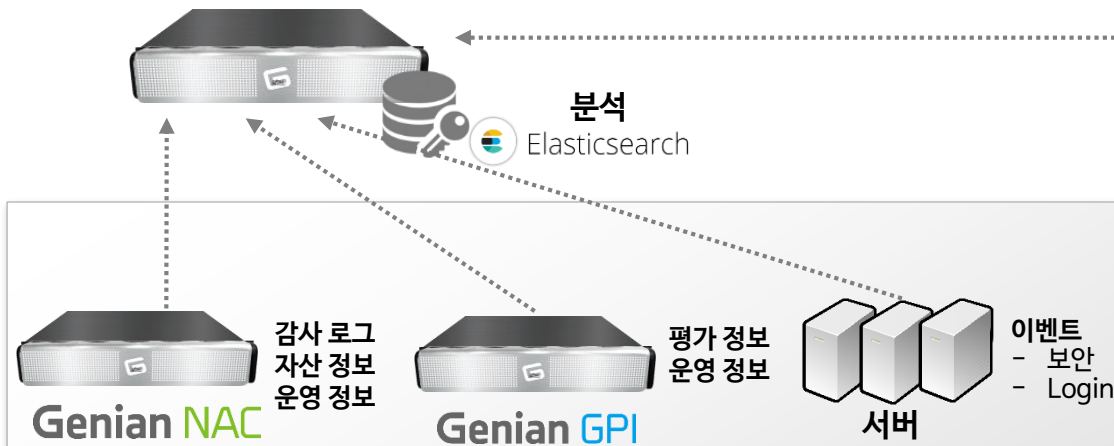


Genian Insights

기능 소개

Genian Insights E 기능 구성

Genian Insights E



통합 분석관리 기능

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



엔드포인트 정보수집

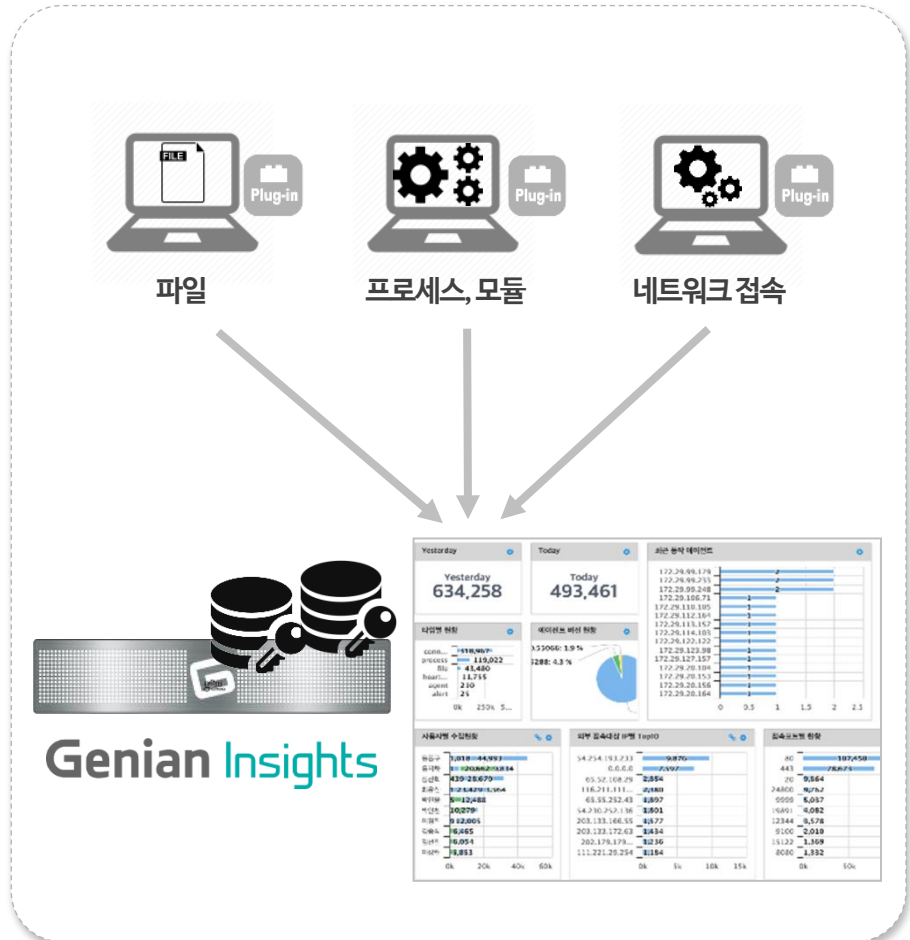
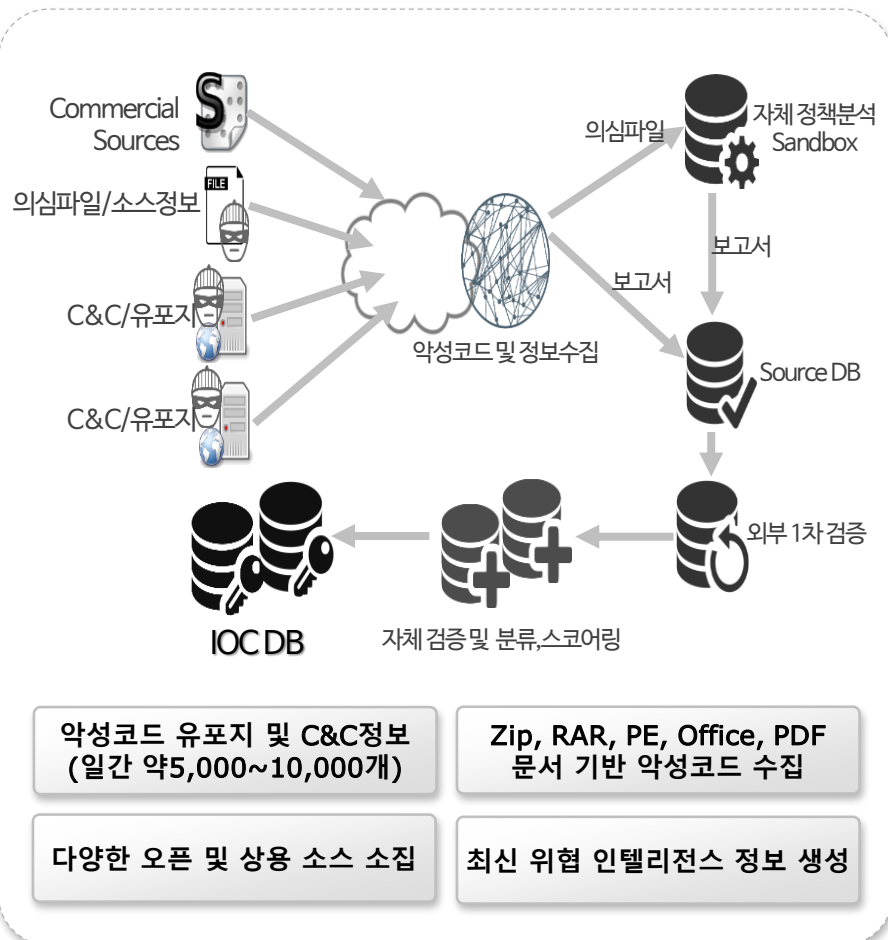
- 프로세스
- 파일
- 접속

EDR 기능

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

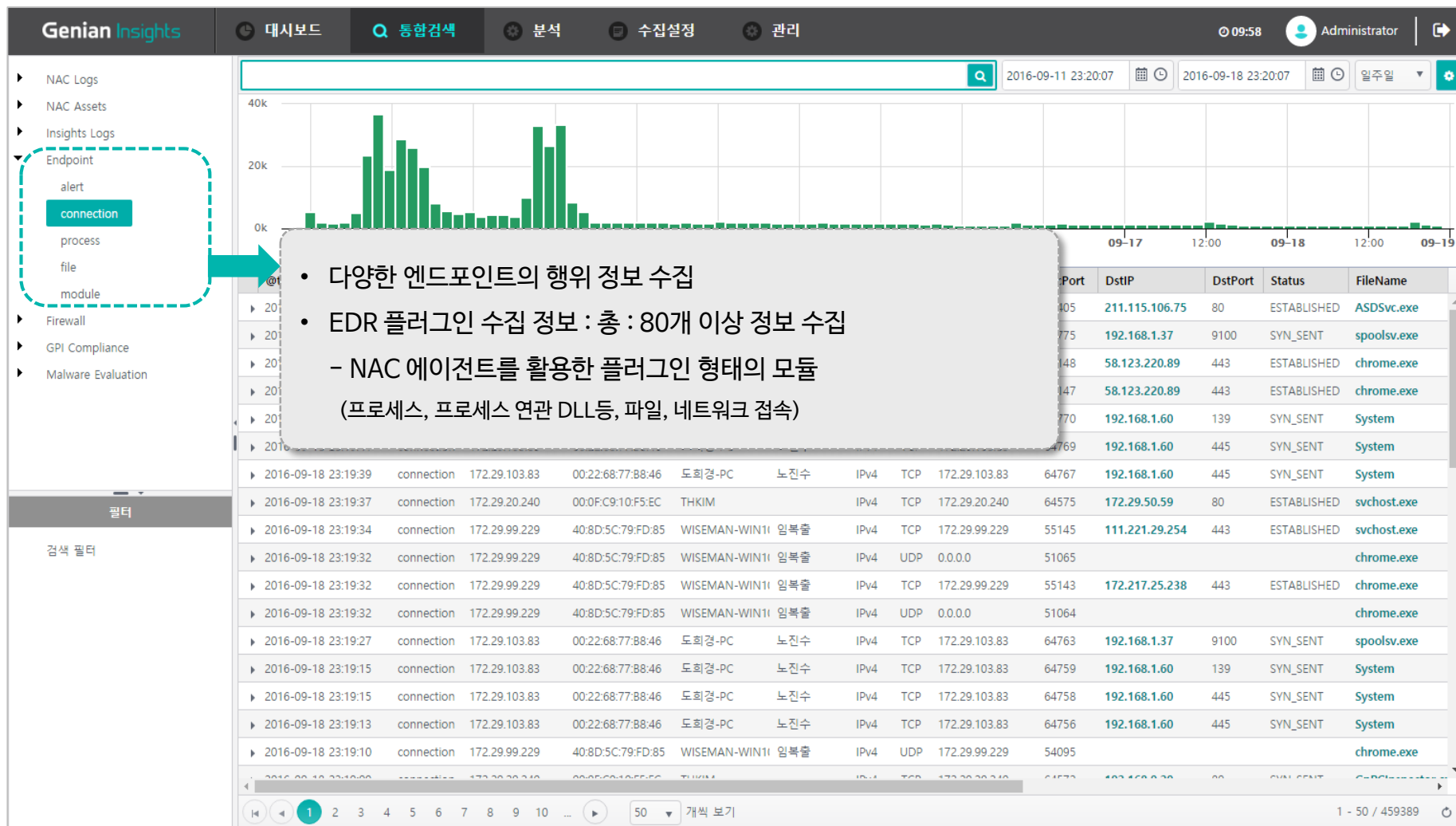
[EDR] 최신 위협 인텔리전스(IOC) 활용

IOC 주기적인 업데이트로 최신 위협 및 침해사고 대응
탐지된 위협에 대한 위험도, 신뢰도 및 유형 정보 제공



[EDR] 이벤트 정보수집

80개 이상의 엔드포인트 정보 수집



[통합 분석관리] 이벤트 정보수집

NAC 정보수집

The screenshot displays the Genian Insights web interface for NAC (Network Access Control) configuration. The left sidebar shows a navigation menu with 'NAC Assets' highlighted. A callout box points to this menu item, stating: "Genian NAC의 정보수집 37개 이상의 항목을 NAC 관리서버와 Sync".

The main content area shows a table of NAC assets with columns: 타입 (Type), 필드명 (Field Name), 출력명* (Output Name*), 필드타입 (Field Type), 기본필드* (Basic Field*), 컨버터* (Converter*), 너비* (Width*), 정렬* (Sort*), and 기본순서* (Default Order*). The table lists various system components like CPU, Memory, Motherboard, and Network interfaces.

Below the asset table, a modal window titled 'Genian Insights' is open, showing a list of collection tasks. The modal has tabs for '대시보드', '통합검색', '분석', '수집설정' (selected), and '관리'. The '수집설정' tab displays a table of collection tasks with columns: 이름 (Name), 수집기 종류 (Collector Type), 모드 (Mode), 상태 (Status), 최종 변경일 (Last Modified), and 수집 건수 (Collection Count). The tasks include '시스템정보수집' (System Information Collection), '프린터' (Printer), '모니터' (Monitor), '저장장치' (Storage Device), '메모리' (Memory), 'CPU', 'OS', '소프트웨어' (Software), '노드/장비정보' (Node/Device Information), and '감사로그' (Audit Log).

A callout box points to the '수집기 SET' (Collector Set) dropdown menu, which lists various collector sets: CS-TEAM, geninetworks, GPI, Guest, mg-nac, mslee, nac99, and '사내NAC' (Intranet NAC), which is highlighted. Below this, there are options for '프로파일' (Profile) and 'JDBC프로파일' (JDBC Profile).

At the bottom right of the modal, a callout box states: "정보수집을 위한 수집기 설정" (Collector setting for information collection).

[통합 분석관리] 이벤트 정보수집

외부시스템 방화벽 정보수집

The screenshot displays the GeniNet Insights web interface. On the left, a sidebar menu lists various management functions, with 'Firewall' highlighted under the 'Endpoint' category. A red arrow points from this menu item to a central text box. This text box contains the text: 'Syslog를 통한 방화벽의 정보 연동' and '84개 이상의 항목에 대해서 연동'. The main interface area is divided into several sections. At the top, there's a header with navigation tabs like '대시보드', '통합검색', '분석', '수집설정', and '관리'. Below this, a table lists various log sources and their configurations, including 'syslog' and 'cisco_message'. A search bar and a '전체' dropdown are also present. In the center, a large bar chart shows data trends over time, with a peak around 2016-09-13. Below the chart, a table displays detailed log entries with columns for timestamp, host IP, severity, protocol, direction, action, source IP, source port, and destination IP. A '상세정보' (Detailed Information) window is open, showing a 'Table' view of selected fields for a specific log entry. This window also includes a '선택 필드' (Selected Fields) section. A red arrow points from the 'Firewall' menu item to the '상세정보' window. At the bottom right of the '상세정보' window, a text box states: '방화벽을 통해 네트워크 접속 상황 파악'.

Genian Insights

대시보드 통합검색 분석 수집설정 관리 09:48 Administrator

사용자관리
관리역할
인덱스관리
NAC Logs
NAC Assets
Insights Logs
Endpoint
Firewall
GPI Compliance
Malware Evaluation
코드관리
커스텀IOC관리
Malware Hash
Malicious IP
Goodware Hash
Good IP
태그관리
환경설정
업데이트 관리
노드정책
제어정책

타입 필드명 출력명* 필드타입 기본필드* 컨버터* 너비* 정렬*

syslog @timestamp date 사용안함 설정안함 100

syslog @version string 사용안함 설정안함 100

syslog action string 사용안함 설정안함 100

syslog ciscotag.raw

syslog cisco_message

syslog cisco_message.raw

syslog connection_count

syslog connection_count.raw

syslog connection_count_max

syslog connection_count_max.raw

syslog connection_id

syslog connection_id.raw

syslog direction

syslog direction.raw

Insights Logs
Endpoint
Firewall
syslog
GPI Compliance
Malware Evaluation

검색 필터
error
관심로그

2016-09-10 07:58:34 2016-09-16 07:58:34 사용자...

1,000k
500k
0k

12:00 09-11 12:00 09-12 12:00 09-13 12:00 09-14 12:00 09-15 12:00 09-16

@timestamp _hostip syslog_severity protocol direction action src_ip src_port dst_ip

2016-09-16 07:58:33 172.29.254.100 informational TCP outbound Built 54.169.222.229 80 172.29.20.199

상세정보

Table JSON

선택 필드

@timestamp 2016-09-15T22:58:33.310Z

_hostip 172.29.254.100

syslog_severity informational

protocol TCP

direction outbound

action Built

src_ip 54.169.222.229

src_port 80

dst_ip 172.29.20.199

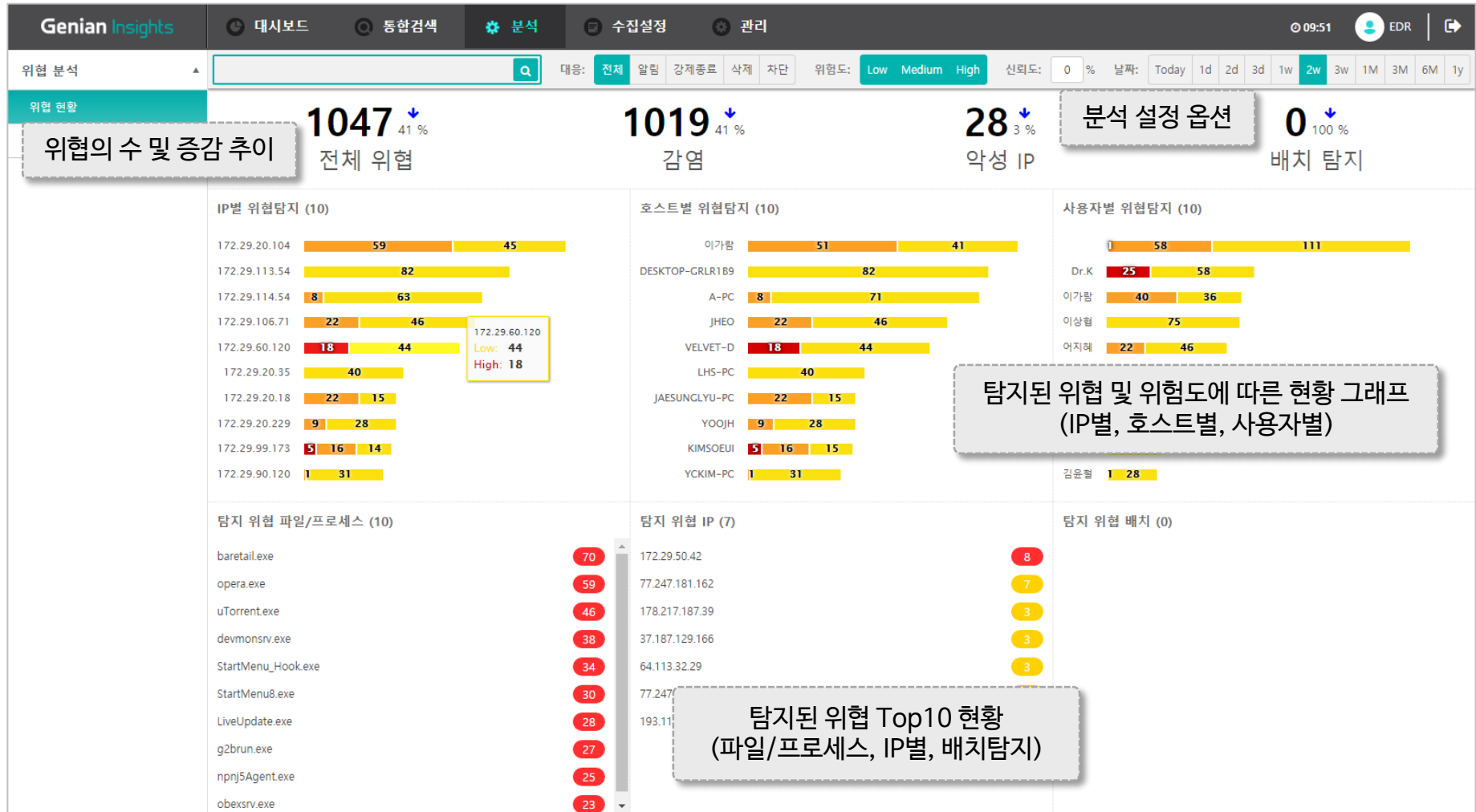
dst_port 57448

cisco_message Built outbound TCP connection 410347615 for outside:54.169.222.229/80 (5)

방화벽을 통해
네트워크 접속 상황 파악

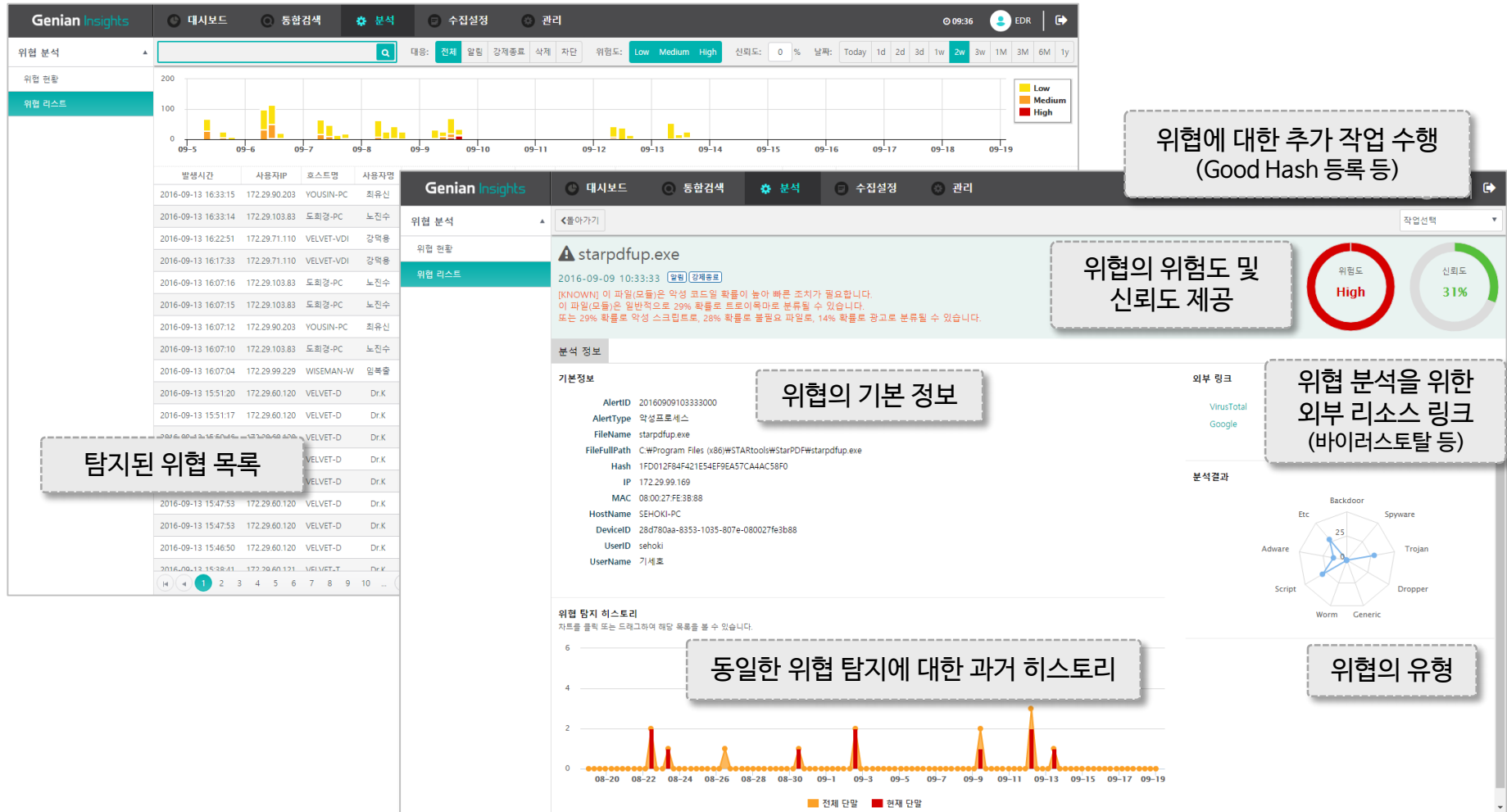
[EDR] 위협분석 - 현황

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



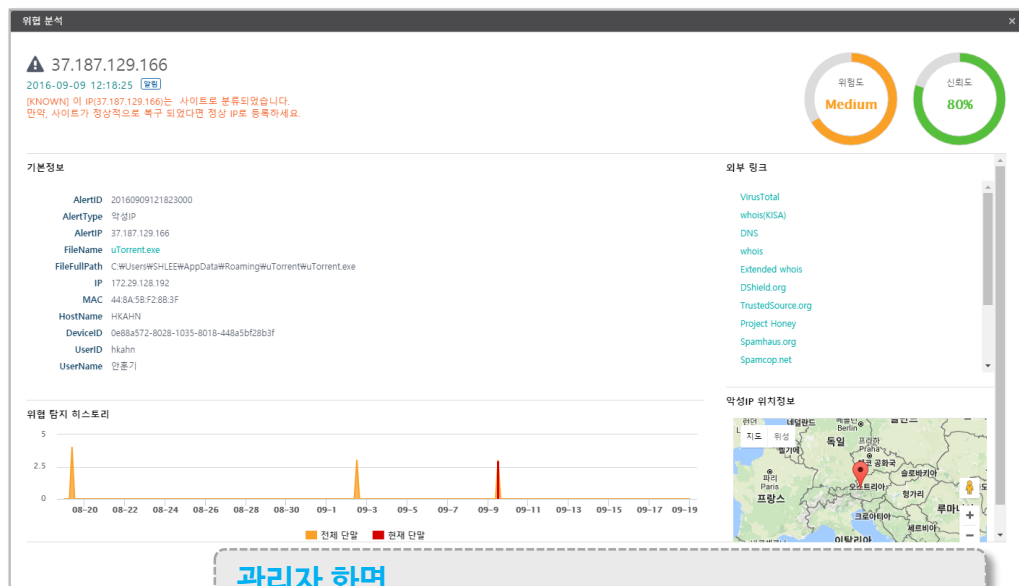
[EDR] 위협분석 - 목록 및 상세

탐지된 위협의 목록과 개별 위협에 대한 상세 분석 정보 제공



[EDR] 엔드포인트 위협 식별 및 대응

이상 행위 악성 IP 접속 프로세스



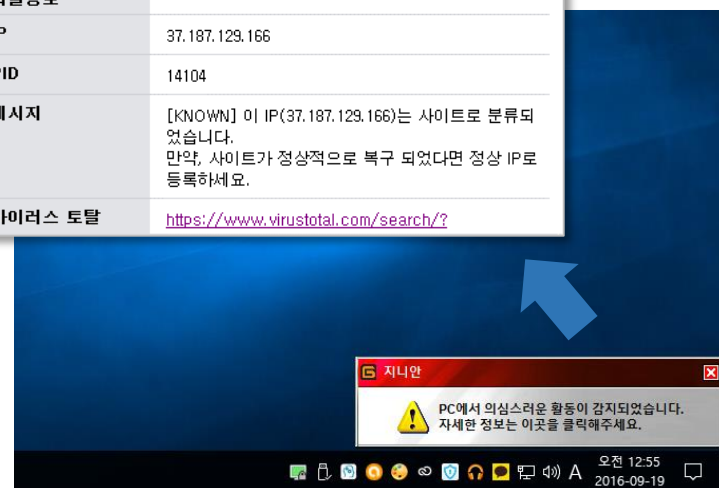
관리자 화면

특정 프로세스가 C&C서버로 의심되는 IP주소로 연결되는 이상 행위 발생

사용자 화면

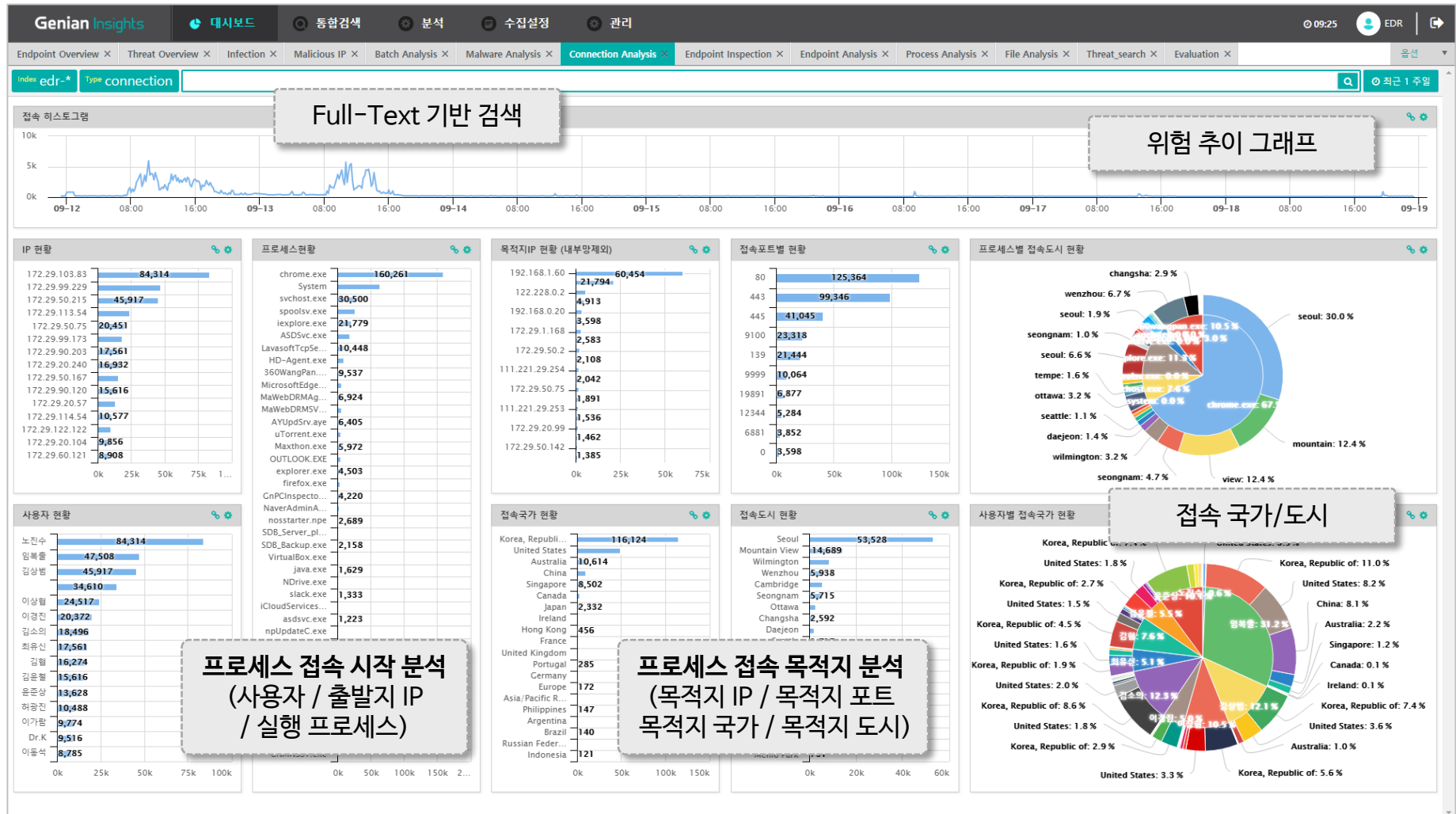
해당 행위가 발생한 단말에서 Process Kill 이후 경고창을 발생하도록 설정

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/



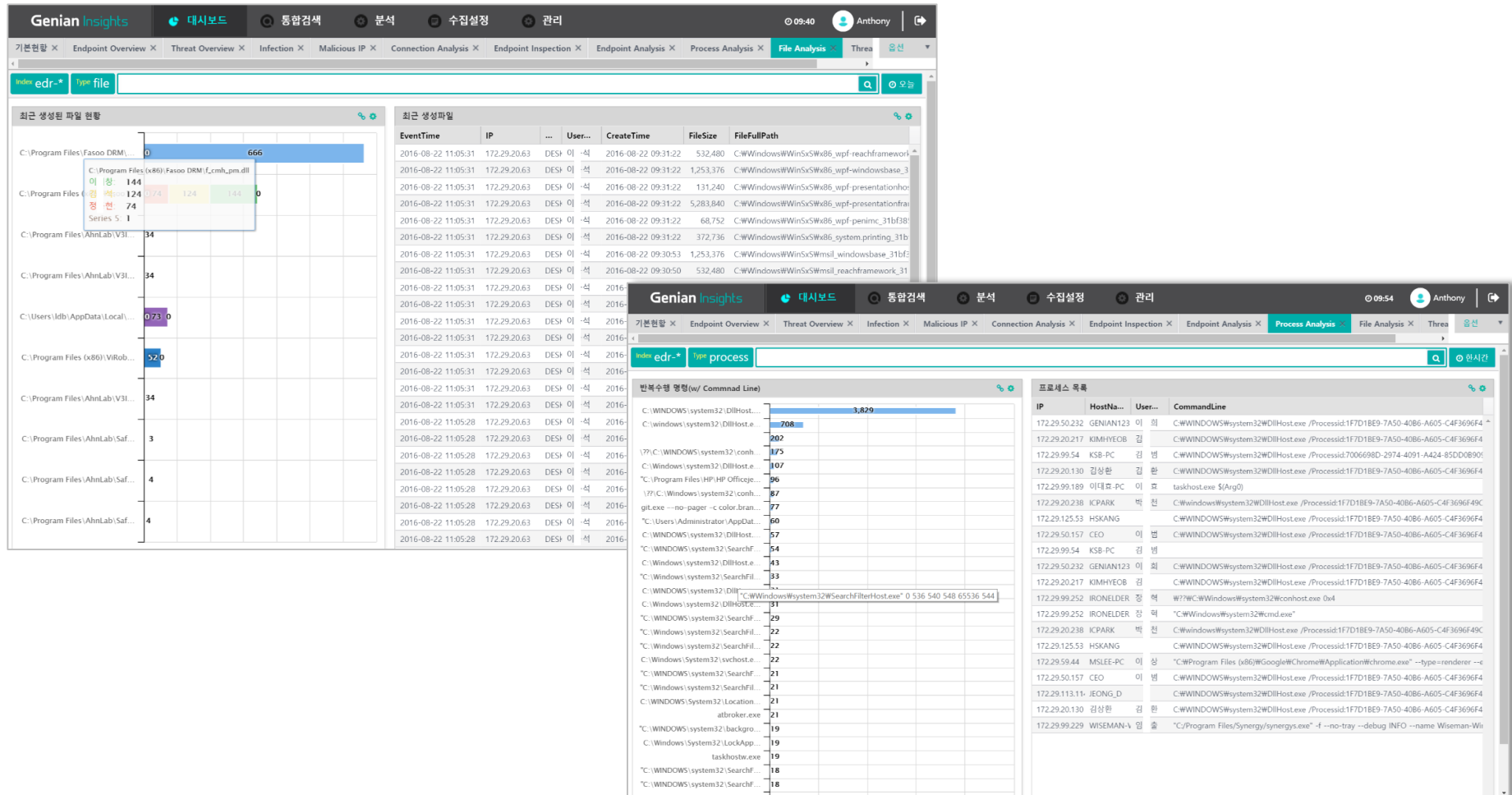
[EDR] 대시보드

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

Genian Insights

대시보드

통합검색

분석

수집설정

관리

사용자관리

관리역할

인덱스관리

NAC Logs

NAC Assets

Insights Logs

Endpoint

Firewall

GPI Compliance

Malware Evaluation

코드관리

커스텀IOC관리

Malware Hash

Malicious IP

Goodware Hash

Good IP

태그관리

환경설정

화면설정

시스템설정

업데이트 관리

노드정책

+

-

Q

☐	해시	파일명	등록일시	등록자 아이디	메모
☐	9536396430A0A1FB1A61A6564AEF07A8	ToggleDesktop.exe	2016-09-05 16:24:25	edr	IObit
☐	76B53798822A7229DCBED364285D2452	g2brun.exe	2016-09-05 16:26:00	edr	나라장터
☐	9537D95D36D47C838B645673E201850A	BuildIndex.exe	2016-09-05 16:28:07	edr	IObit
☐	C31120CCEAFB15C90B0EECE761A7C86	LiveUpdate.exe	2016-09-05 16:28:20	edr	IObit
☐	F9F87BA9B953D2A9B396A092626A758D	UniCRSLocalServer.exe	2016-09-06 19:42:58	edr	
☐	4D600B3FB6C8EBBCDC38CA1DCEDB27B2	innosvc7.exe	2016-09-06 19:43:21	edr	Innorix File Transfer Service
☐	82F5E8957DC64AD9C3E16C200E0A77EB	StartMenu8.exe	2016-09-06 23:19:09	edr	IObit
☐	BB319A6240A810FD09E63CDBB3E6AF30	LiveUpdate.exe	2016-09-06 23:19:28	edr	IObit
☐	337FA50FFDED5E2BC94B36BF625A8681	LiveUpdate.exe	2016-09-07 19:35:32	edr	IObit
☐	45BCD6113DE37F0C839731352B84CB24	AutoUpdate.exe	2016-09-07 19:48:48	edr	IObit
☐	B3121B21EF03A9FAC9094D3C630F612C	npmonz.exe	2016-09-08 07:05:15	edr	nProtect Netizen 4
☐	BB71C3B43578376C11147AAF779890	IObitDownloader.exe			
☐	2BDD6B31BD9A6DEC8BC850E4230FAE04	AUpdate.exe			
☐	2CC19C0E6DC09F14AD3B7C47DB31AB2E	SPUpdate.exe			
☐	F9C06769E4000431317372970A305D03	SHTTPSandBoxMonitor.10035.exe			
☐	800EA2BDE231C78C82BC5D48737C9483	StartMenu_Hook.exe	2016-09-08 09:07:39	edr	IObit
☐	A0BD5290FE8119458E54AC2370800294	pinomate.exe	2016-09-08 09:10:25	edr	pinomate.exe는 Peering Portal, Inc.에서 제공하는
☐	6D61E8191DB6BCF4328F810DA86C3B0A	UninstallPromote.exe	2016-09-08 09:23:52	edr	IObit
☐	96B61B8E069832E6B809F24EA74567BA	vcredist_x64.exe	2016-09-08 20:16:09	edr	Wireshark

제공되는 IOC 외에 국내에서 발생하는 위협에 대해 지니네트웍스 R&D 센터 분석정보 및 자체 수집 IOC 정보 추가 등록 가능

[통합 분석관리] 정보검색

수집된 정보에 대한 통합검색

Genian Insights

대시보드

통합검색

분석

수집설정

관리

09:48 Administrator

NAC Logs

NAC Assets

Insights Logs

Endpoint

Firewall

GPI Compliance

Malware Evaluation

LOG_TYPESTR:에러

2016-08-19 17:48:03

2016-09-19 17:48:03

한달

Full Text 검색

개인화 및 엑셀 내보내기 지원

드릴다운 방식의 타임라인 차트 지원

(원하는 구간을 드래그 또는 그래프를 클릭 하여 세부 정보 탐색 가능)

컬럼 설정

컬럼 초기화

엑셀 내보내기

필터 추가

필터 수정

2016-08-29 20:52:48

타임차트: 2

Time	Server	Log Type	로그ID	Managing Device	IP Address	MAC Address	Username	Full Name	Department	Description
2016-09-19 03:02:22	mslee	에러	데이터동기화		172.29.50.40	00:25:90:25:E0:2C				데이터 소스 서버 접속실패. DATASOU
2016-09-19 02:01:15	mslee	에러	GENIAN장비	기술연구소-50	172.29.50.40	00:25:90:25:E0:2C				센서설정 수신실패. ERRMSG='SOAP 1
2016-09-18 03:02:21	mslee	에러	데이터동기화		172.29.50.40	00:25:90:25:E0:2C				데이터 소스 서버 접속실패. DATASOU
2016-09-18 02:01:14	mslee	에러	GENIAN장비	기술연구소-50	172.29.50.40	00:25:90:25:E0:2C				센서설정 수신실패. ERRMSG='SOAP 1
2016-09-17 07:49:18	nac99	에러	GENIAN장비	23	172.29.50.99	40:8D:5C:A7:C7:91				위험이벤트 전송실패. ERRMSG='Error
2016-09-17 07:48:50	nac99	에러	GENIAN장비	23	172.29.50.99	40:8D:5C:A7:C7:91				노드 활성화상태 동기화실패. ERRCOD
2016-09-17 07:48:39	nac99	에러	GENIAN장비	23	172.29.50.99	40:8D:5C:A7:C7:91				센서설정 수신실패. ERRMSG='Error -1
2016-09-17 07:48:10	nac99	에러			172.29.50.99	40:8D:5C:A7:C7:91				데이터베이스 오류. ERRMSG='Lost coi
2016-09-17 07:46:45	nac99	에러			172.29.50.99	40:8D:5C:A7:C7:91				데이터베이스 오류. ERRMSG='Lost coi
2016-09-17 07:46:44	nac99	에러			172.29.50.99	40:8D:5C:A7:C7:91				데이터베이스 오류. ERRMSG='Lost coi
2016-09-17 07:46:37	nac99	에러			172.29.50.99	40:8D:5C:A7:C7:91				데이터베이스 오류. ERRMSG='Lost coi
2016-09-17 07:37:03	nac99	에러	GENIAN장비	23	172.29.50.99	40:8D:5C:A7:C7:91				ERRMSG='Error
2016-09-17 07:36:15	nac99	에러			172.29.50.99	40:8D:5C:A7:C7:91				'Lost coi
2016-09-17 06:47:48	nac99	에러	GENIAN장비	23	172.29.50.99	40:8D:5C:A7:C7:91				ERRMSG='Error
2016-09-17 06:04:29	nac99	에러			172.29.50.99	40:8D:5C:A7:C7:91				데이터베이스 오류. ERRMSG='Lost coi
2016-09-17 03:02:22	mslee	에러	데이터동기화		172.29.50.40	00:25:90:25:E0:2C				데이터 소스 서버 접속실패. DATASOU

1

2

3

50

개씩 보기

1 - 50 / 139

필터

검색 필터

Error Logs

Risk Logs

Sensor Down

Warn Logs

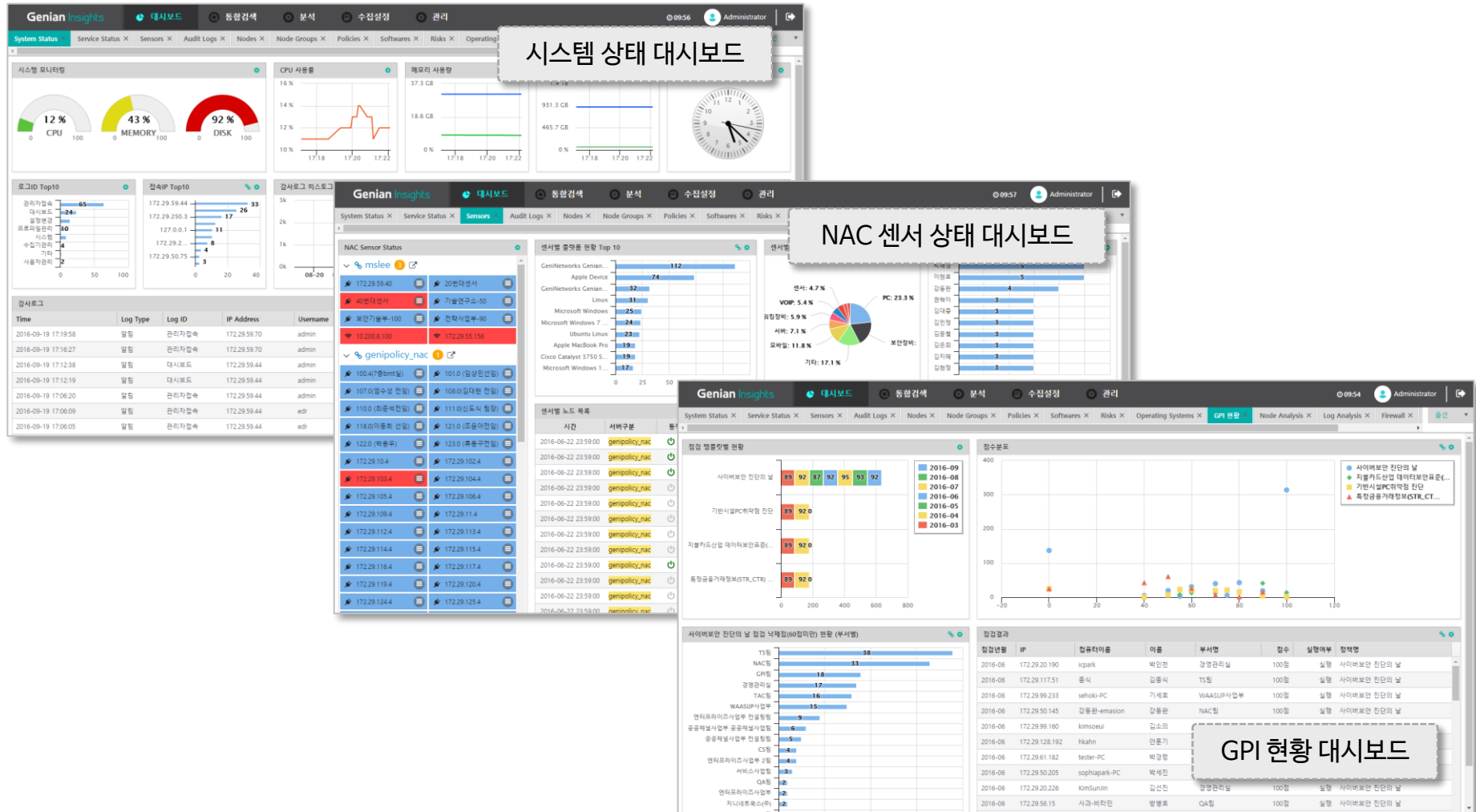
에이전트 손상

사용자 정의 검색 필터

검색 데이터에 따른 세부 정보 산출

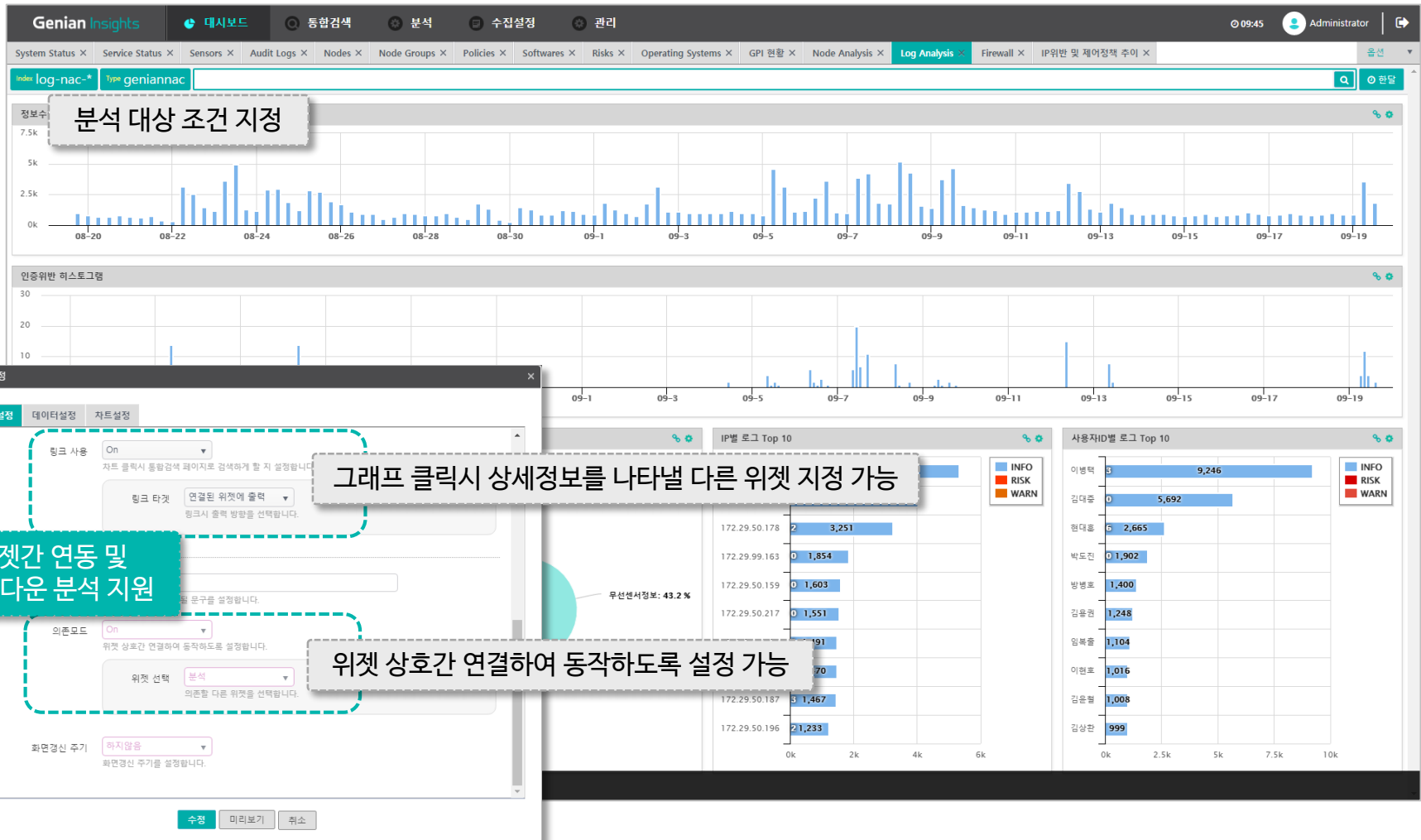
[통합 분석관리] 대시보드

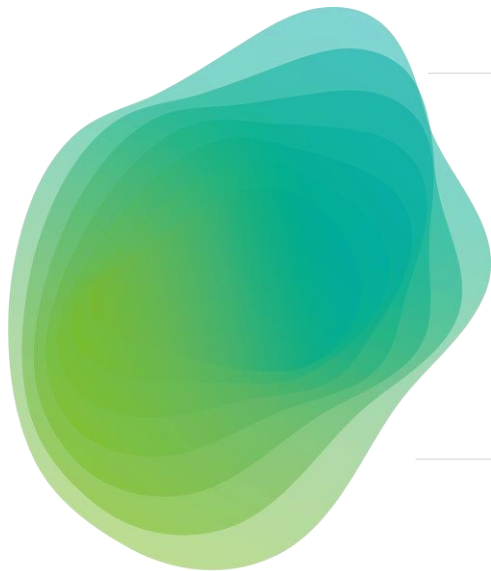
용도에 따른 다양한 분석 대시보드 설정 가능



[통합 분석관리] 위젯 기능 소개

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

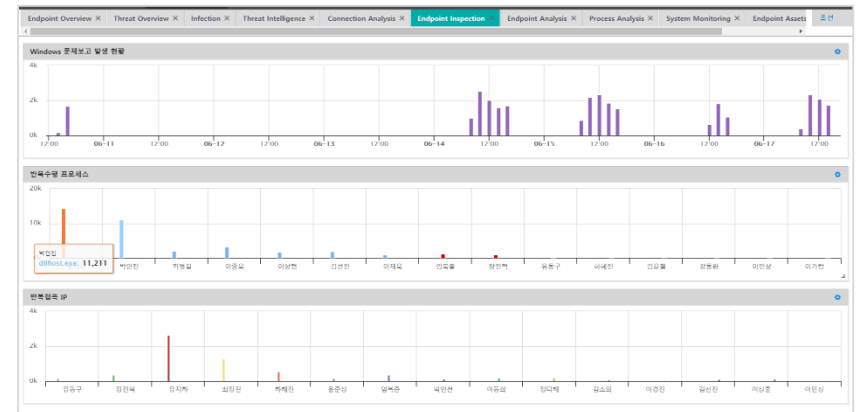




Genian Insights

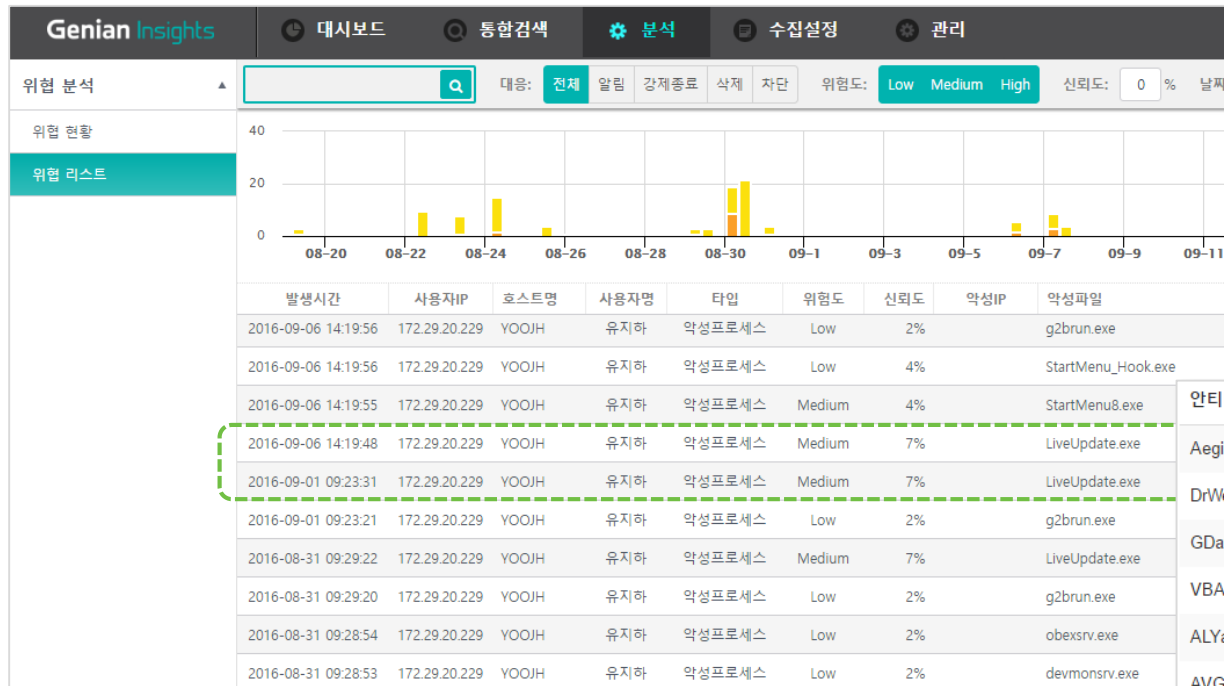
활용 예

사용자 단말의 동작 이상 유무 사전 파악



활용 - 기존 보안솔루션 미탐지 공격 대응

안티바이러스 솔루션 미탐지 프로세스 탐지 및 대응 가능



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	✓

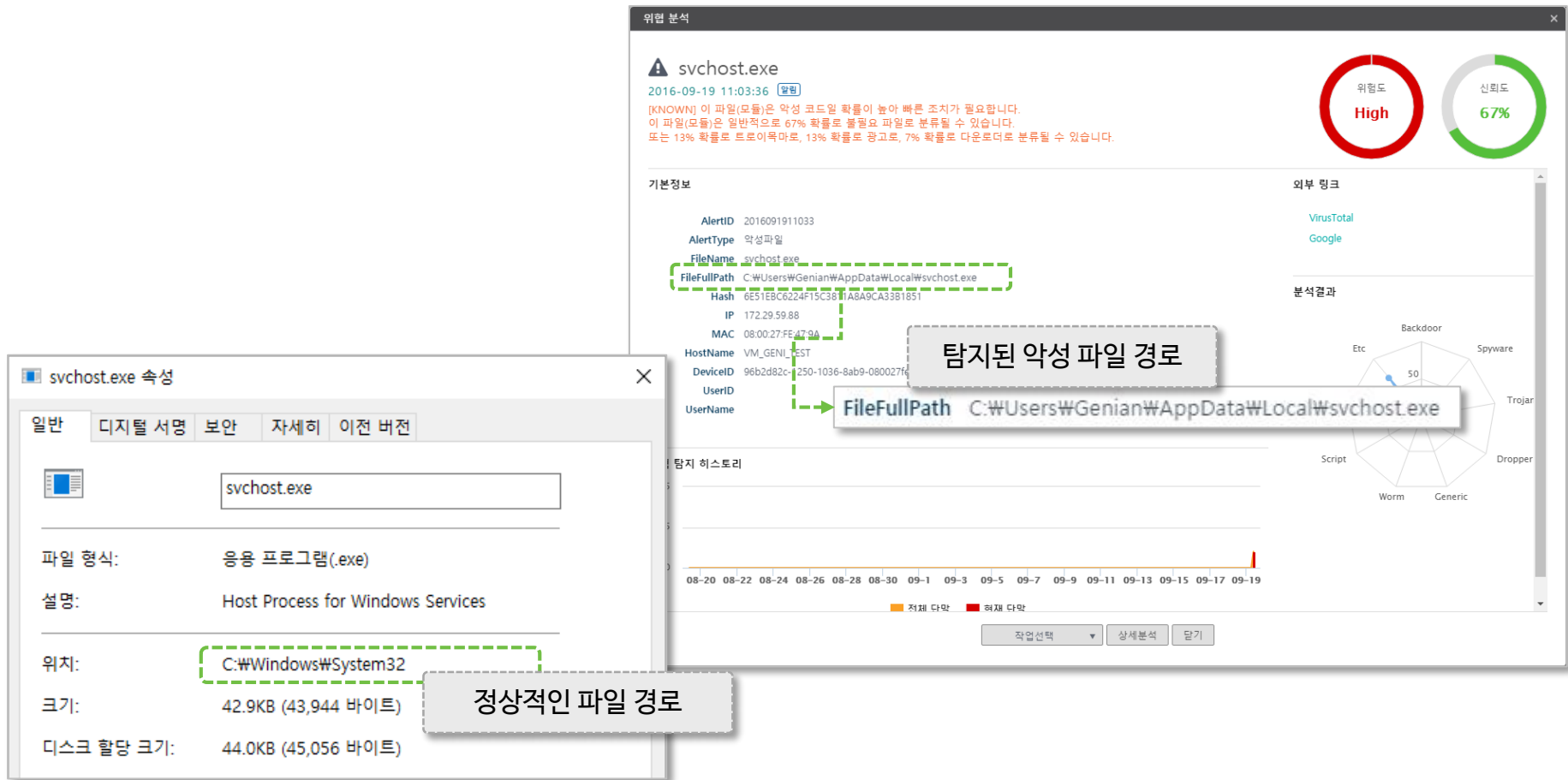
활용 - 취약점 공격 대응

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



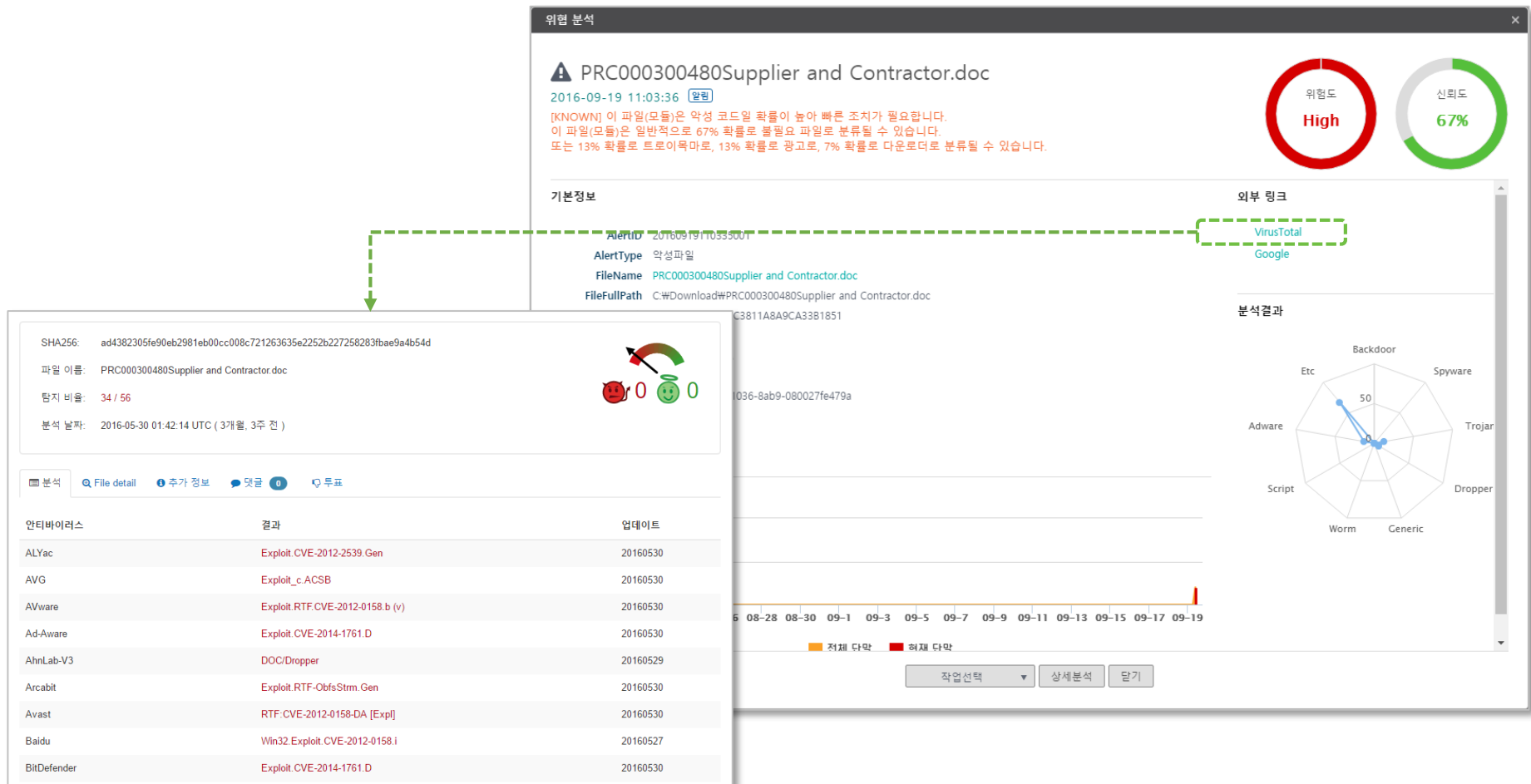
활용 - 취약점 공격 대응

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



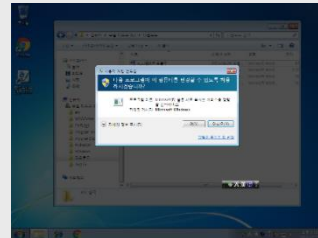
활용 - 취약점 공격 대응

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

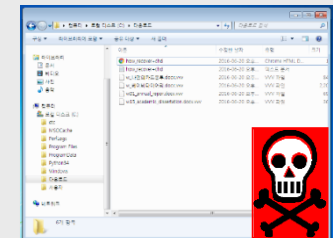


활용 - 랜섬웨어 대응

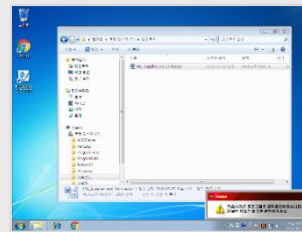
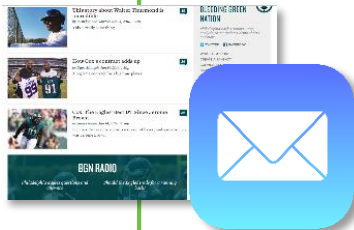
Genian Insights 미적용 시



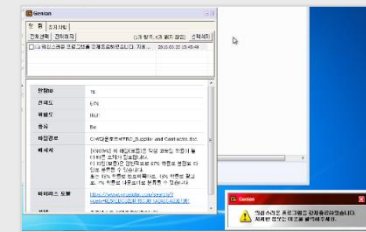
악성코드 감염 파일 다운로드



파일 감염/암호화



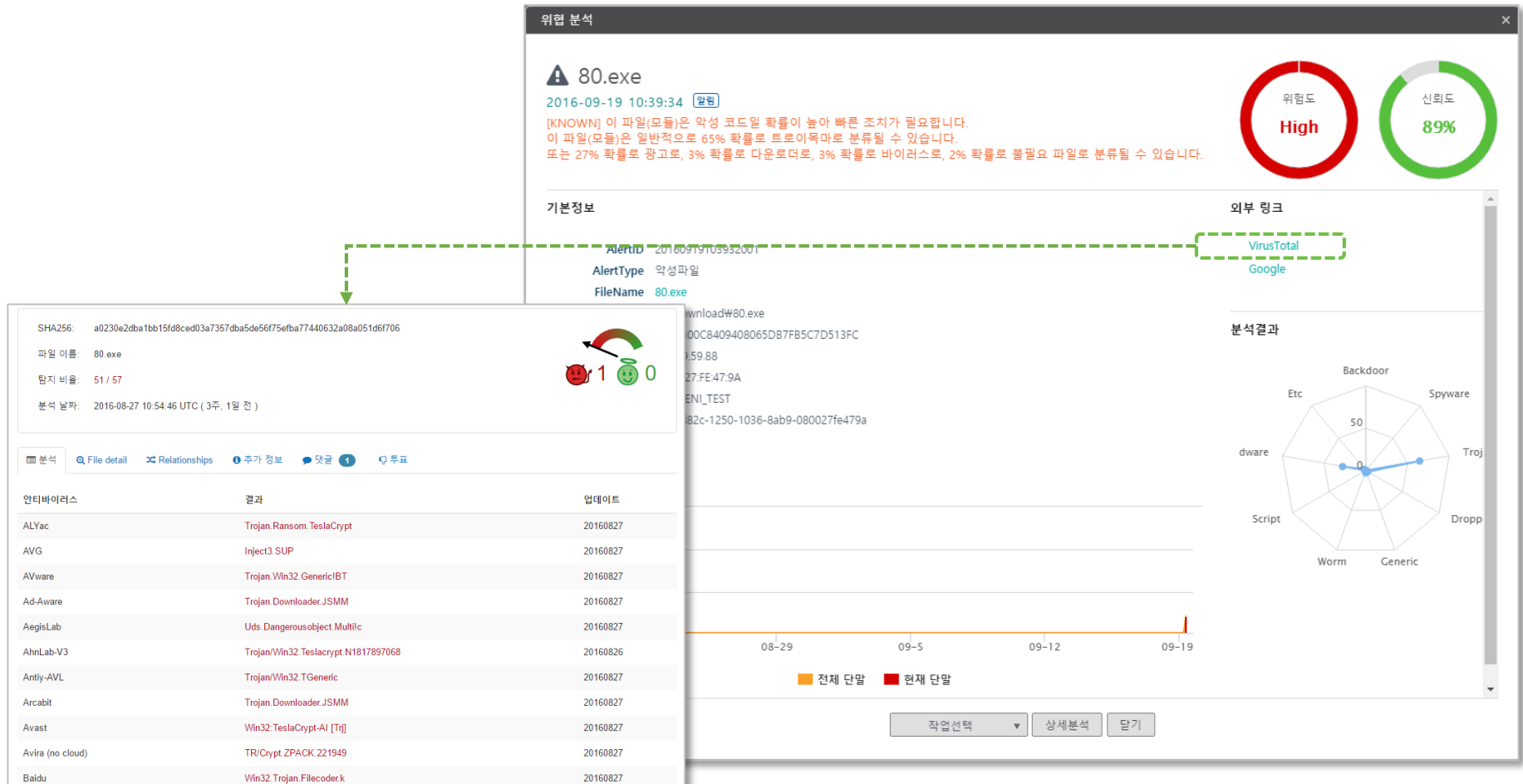
파일 다운로드 시 차단, 알림



상세정보 열람 : 단말 미감염

활용 - 랜섬웨어 대응

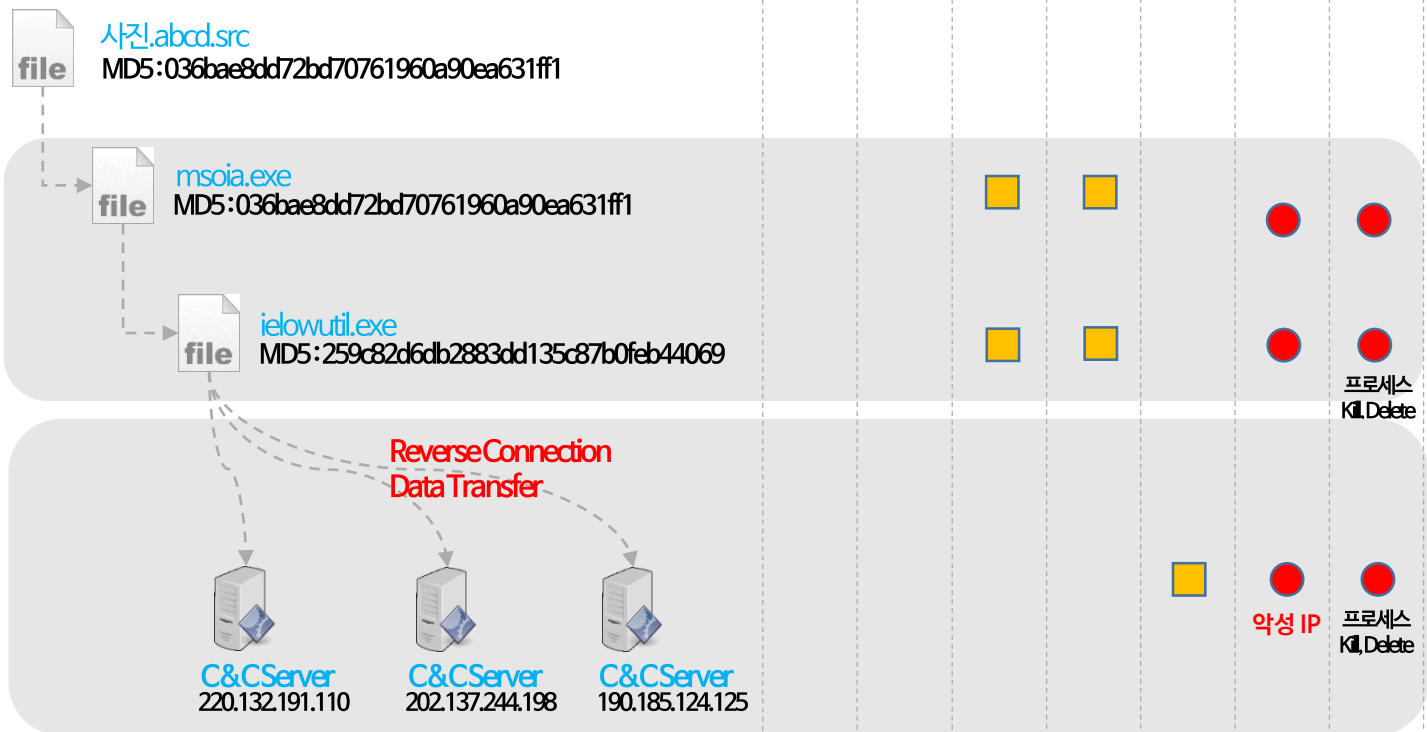
솔루션 적용 시 랜섬웨어 악성코드 위협분석 결과 화면 (VirusTotal, google 결과 제공)



활용 - I사 APT 사고발생 대응

실제 APT 공격상황에서 Genian Insights 활용
공격 Chain의 고리를 끊을 수 있는 지능형 솔루션

APT Kill Chain





Thank you!

Tel : 031-422-3823

Mail : geni@geninetworks.com