



Intelligent EDR, Intelligent Visibility

Genian Insights E v2.0 제품소개서

2021.02 / 지니언스



목 차

-
- 배경 및 필요성
 - Genian Insights E 제품 소개
 - 도입 효과
-

배경 및 필요성



배경 및 필요성

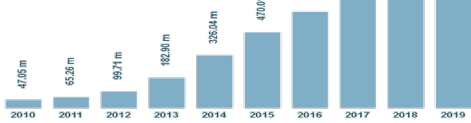
현재 도입/운영 중인 보안 솔루션으로는 더 이상 지능형 위협을 탐지 및 통제할 수 없습니다.

보안담당자 관점의 현황 파악 어려움

- 악성파일 존재 여부 및 피해현황 파악의 한계
- 관리 감독 기관의 피해 상황 보고 요청 대응에 한계

10년간 고유 악성코드 수

누적 9억 개 고유 악성코드
하루 35만개 증가



지능화·고도화 공격 패턴

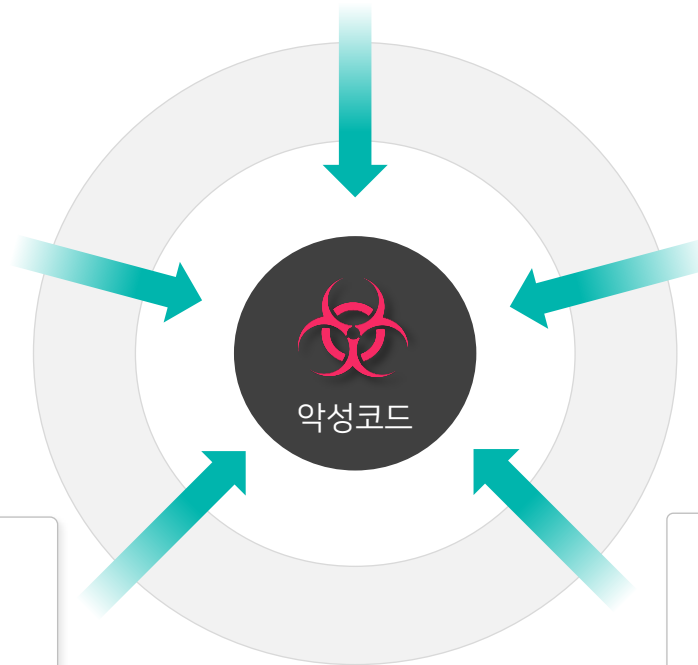
- 파일 없는 악성행위
- 잠복/은닉형 악성행위
- 소프트웨어 취약점 공격
- 웹 취약점 공격

APT 대응 솔루션(샌드박스)

- 암호화된 공격 탐지 불가
- 가상화 환경 내 파일 조합 불가
- 대용량 파일 분석 불가
- 다수의 샌드박스 회피 기법 존재

Anti-Virus의 한계

- 시그니처 기반 블랙리스트 방식
- 신종 악성 코드 및 지능형 지속공격 탐지불가
- 다수의 안티바이러스 회피 기법 존재



배경 및 필요성

점점 다변화, 고도화되고 있는 사이버 공격을 모두 막는 것은 불가능합니다.

의심스러운 활동에 대한 빠른 인지와 행적을 분석하여 감염의 대응책을 마련하고
확산을 막아 피해를 최소화하고 동일 형태의 피해가 발생하지 않도록 할 수 있는 솔루션이 필요합니다.



최종 공격 대상은 결국 엔드포인트 입니다.

네트워크 경계에 있는 대부분의 보안 솔루션은 내부 자산을 보호하기 위해 구성되어 있으나 엔드포인트의 위협은 계속 증가하고 있습니다.
사용자에게 보내지는 악성 메일, 피싱 사이트, 위/변조 된 홈페이지 접속 등을 통한 악성코드 감염 및 APT 침해는 네트워크 보안 솔루션의 한계를 보여주고 있습니다.

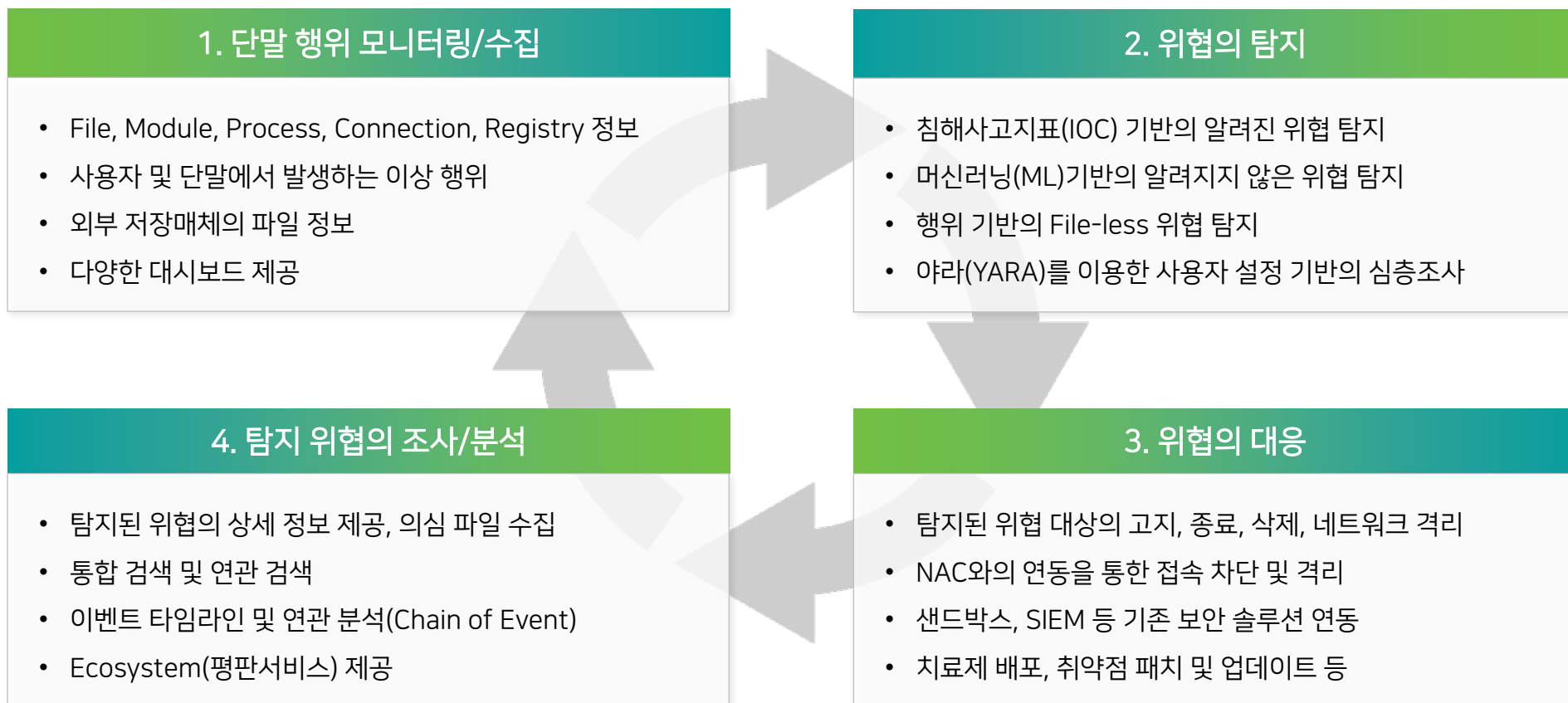
Genian Insights E

제품 소개



1.개요

Genian Insights E는
단말에 대한 지속적인 모니터링 및 정보 수집을 통해 위협의 탐지 및 분석, 대응을 제공하는
단말 이상행위 탐지 및 대응 (Endpoint Detection & Response) 솔루션입니다.



2. Genian Insights E 구성

Genian Insights E는 Insights E 분석 서버, PC에 설치되는 Agent로 구성됩니다.



Insights E Server

- E Module에서 전달된 Event Raw Data의 저장 및 백업
- Data 분석을 통한 위협 및 이상 징후의 탐지
- 탐지된 위협의 상세 내용 분석
- Event 통합 분석 및 시계열 분석, 근원 분석 등
- 분석 내용의 보고서, 위젯, 대시보드 등 시각화 및 표출
- 타 시스템 연동을 위한 Syslog, REST API 제공
- 보안이 강화된 자체 OS 사용



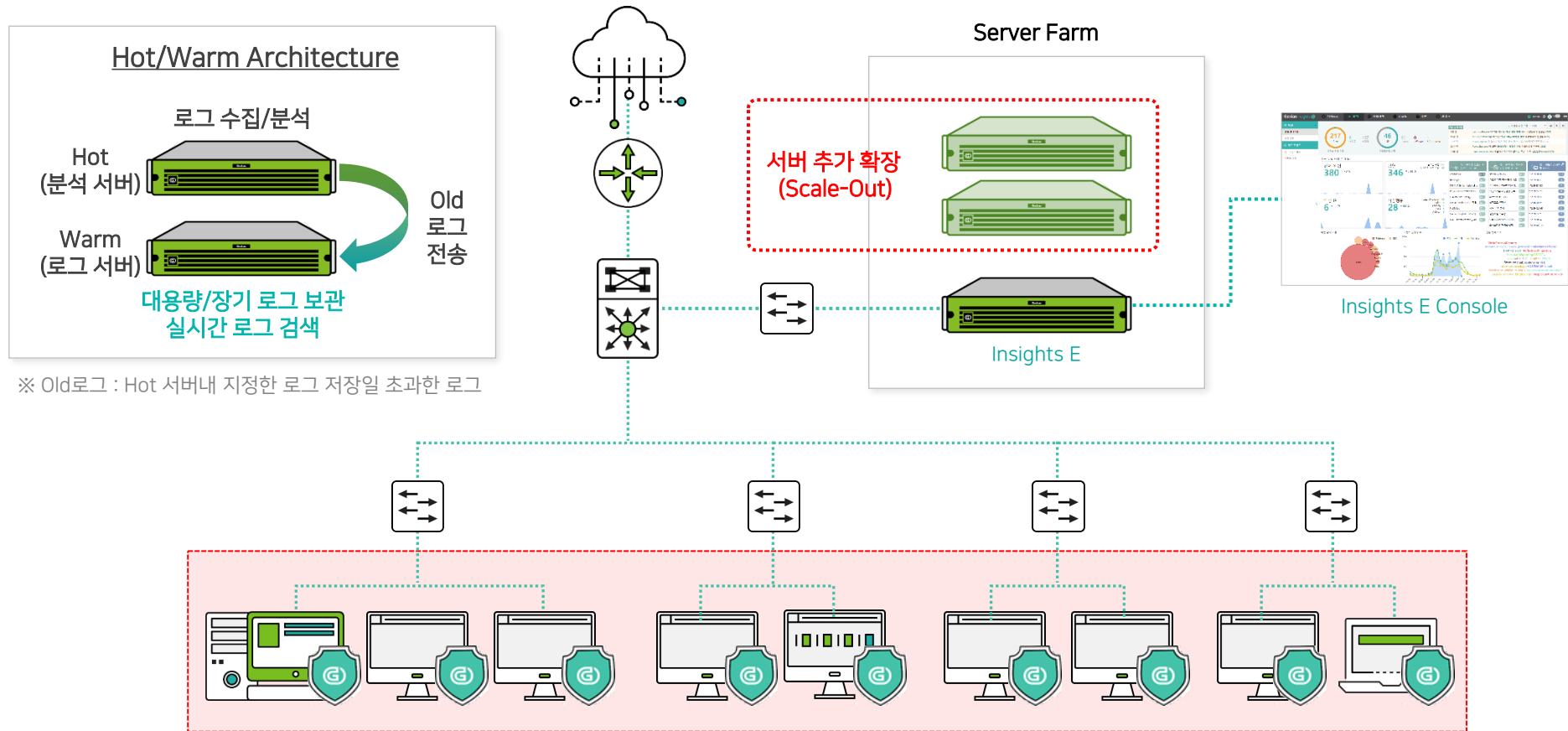
Insights E Agent

- 단말 주요 행위(파일, 프로세스, 네트워크, 레지스트리 등)의 모니터링 및 수집
- 수집된 정보 Server로 전송
- Off-line 에서 수집된 로그 임시 보관 (on-line 에서 서버로 전송)
- 위협 탐지 시 고지, 차단, 종료 등 단말 수준의 대응
- 위협 대상(파일 등)의 격리 및 삭제
- 가벼운 Agent

❖ Genian NAC 사용 시 NAC Agent 에 모듈(plugin-in)을 추가함으로써 EDR Agent 설치 완료

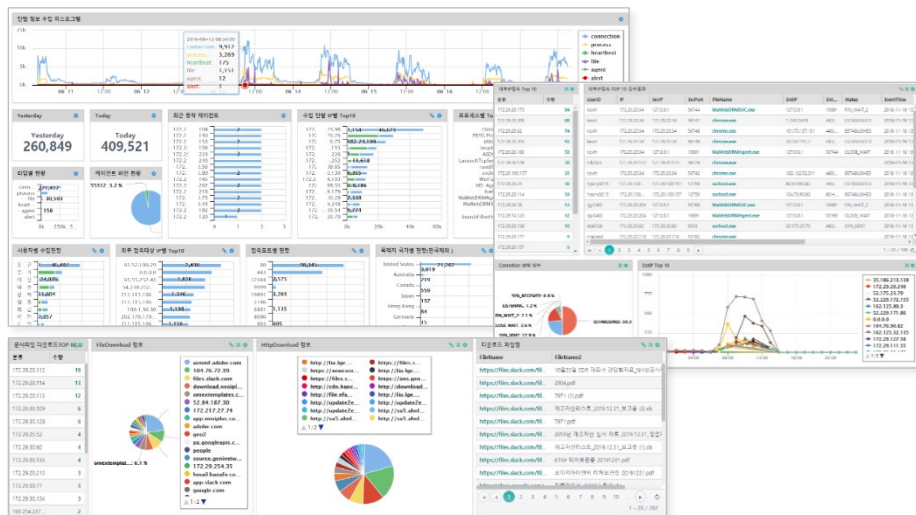
2. Genian Insights E 구성

Genian Insights E 서버, Agent의 간단한 구성입니다.
Scale-Out 기능을 제공하여 확장을 쉽게 할 수 있습니다.



※ Genian NAC 사용 시, NAC Agent 에 플러그인(모듈)을 배포하는 형태로 구축 가능

Agent는 서버로 로그 전송 역할만 수행, 분석 및 탐지는 서버에서 수행합니다.



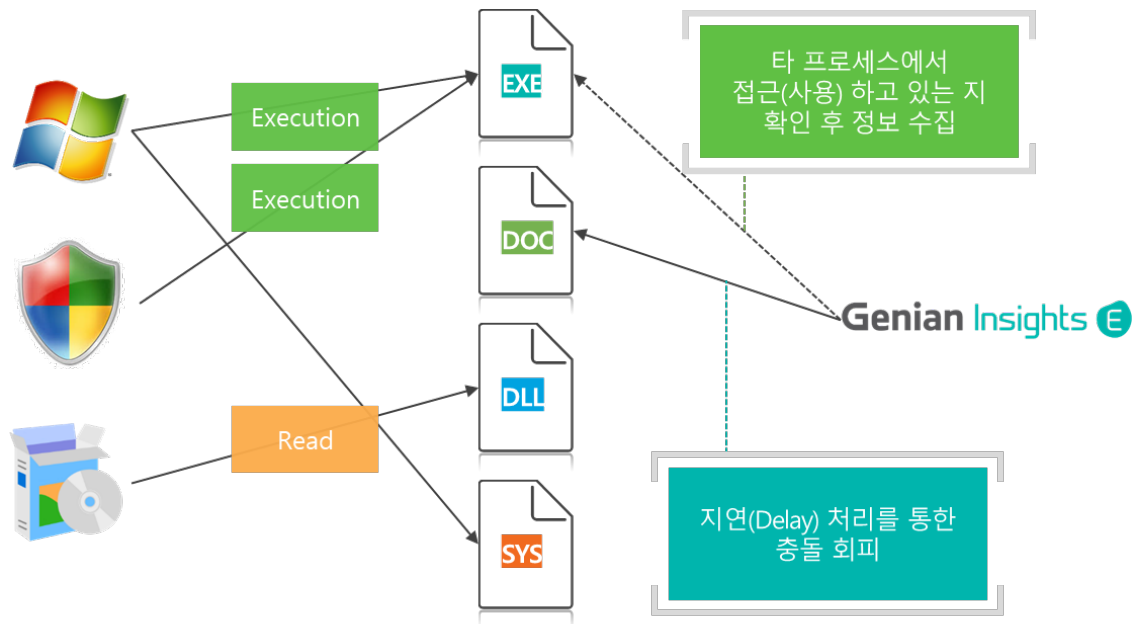
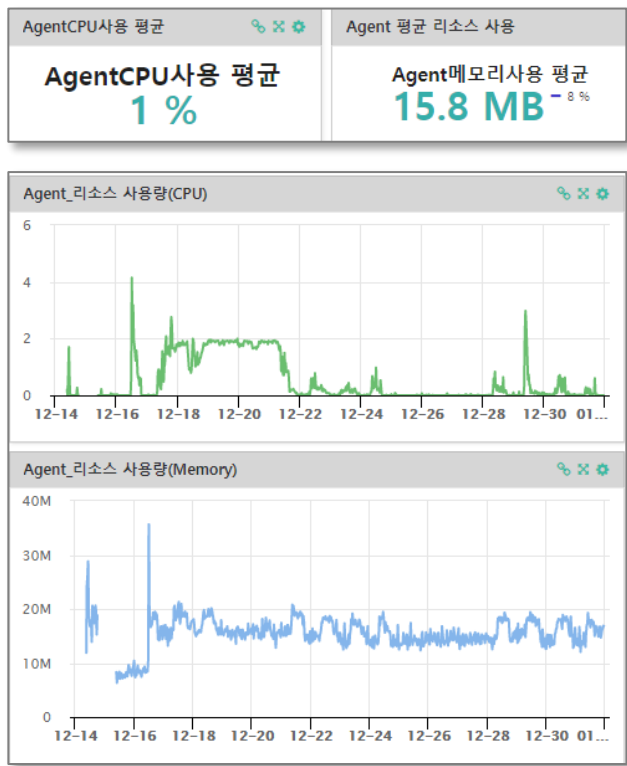
다양한 분석



3. 단말의 부하를 최소화한 수집 및 탐지

Agent는 충돌을 방지하기 위한 충돌 회피 기술이 적용되어 있으며, 최소의 리소스를 사용합니다.

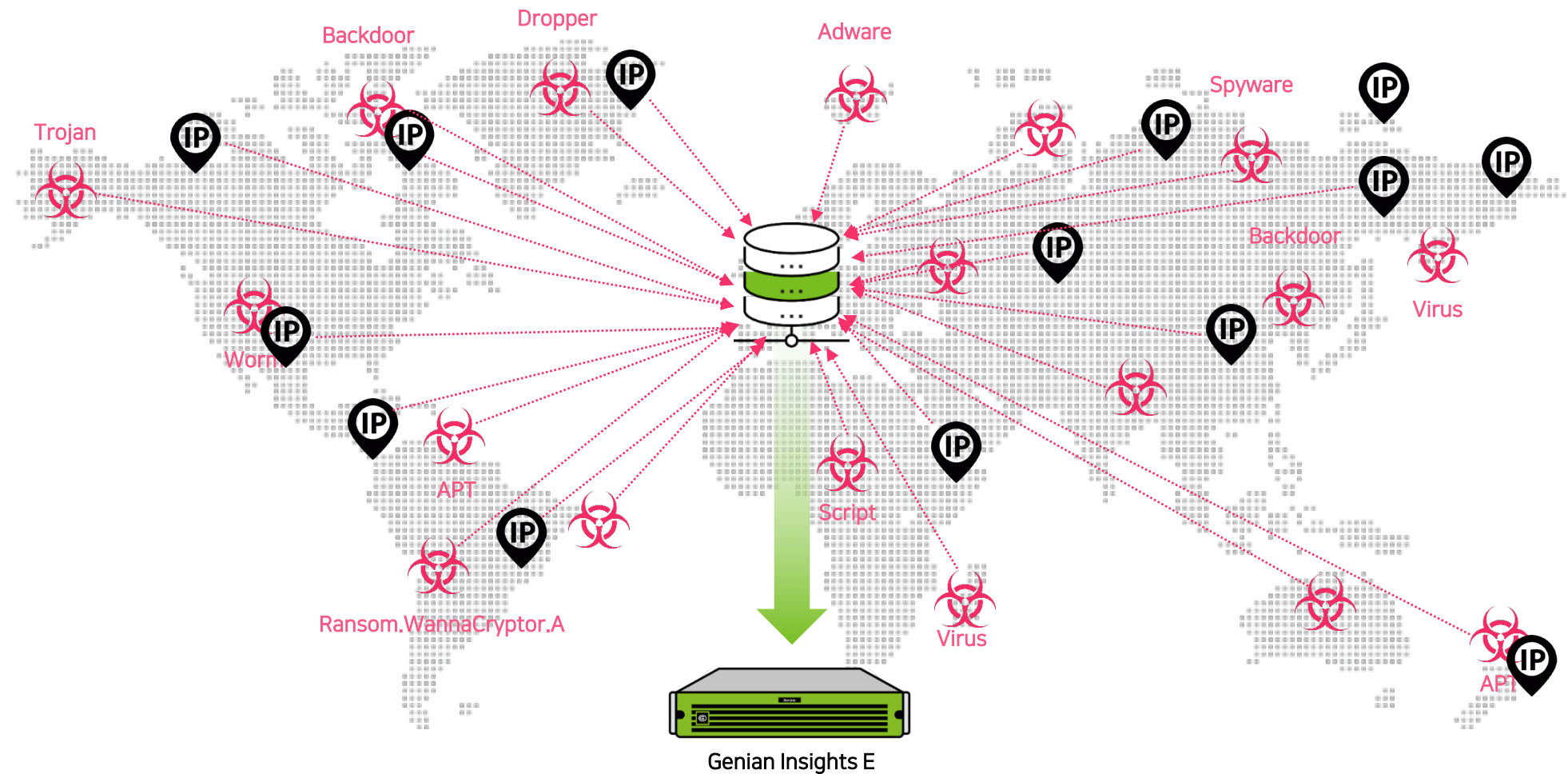
확인 처리 기술(타 프로세스의 접근 확인 후 처리), 지연 처리 기술(지연처리하는 기술) 적용으로 타 프로그램의 동작에 영향을 주지 않는 기술 적용
CPU, MEMORY 사용을 최소화하여 동작하는 Agent



※ 제조사 내부 TEST 결과, 에이전트 100대 평균 리소스 사용률

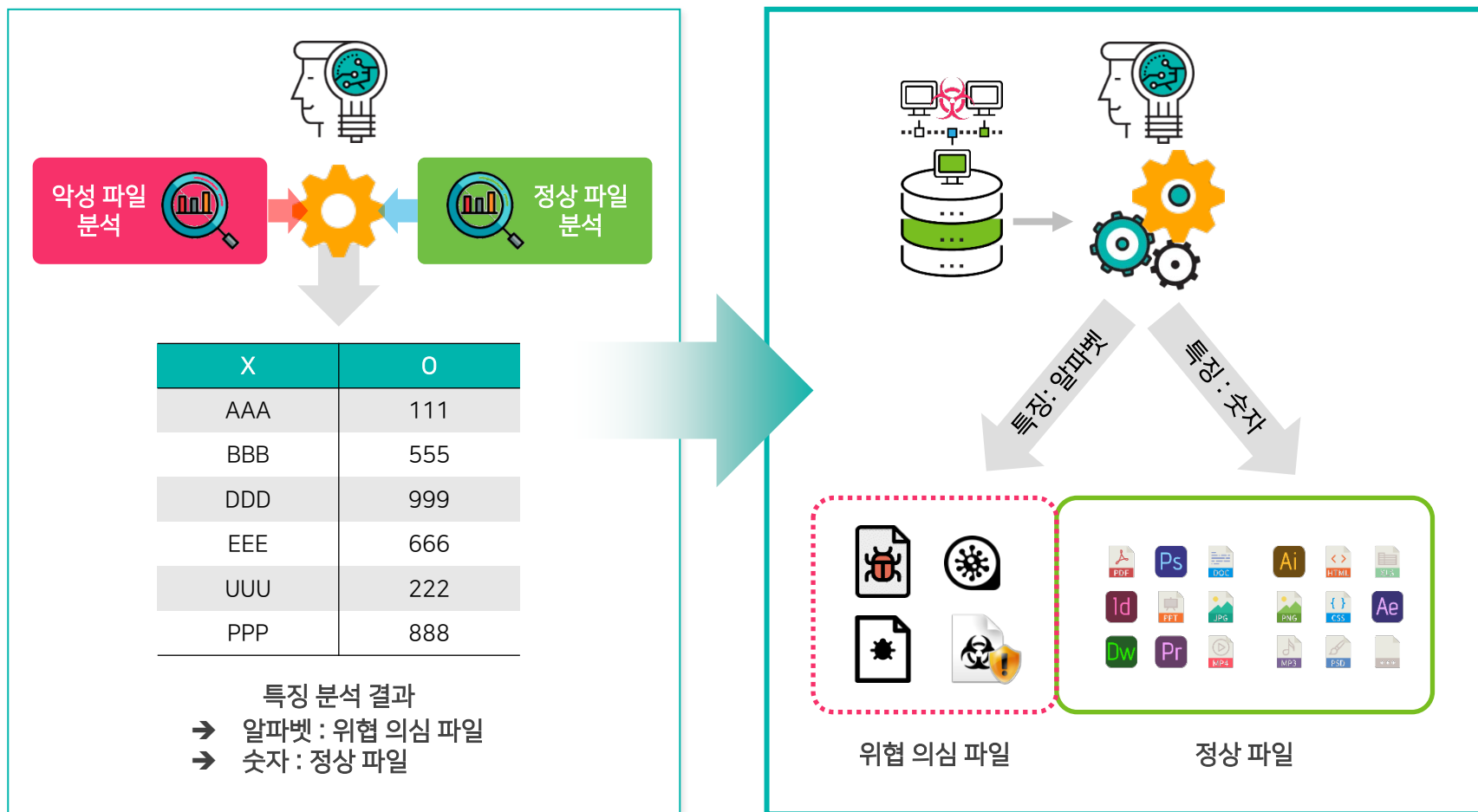
4. 탐지 기술

IOC(Indicator Of Compromise, 침해 지표) : 전 세계에서 탐지된 악성 파일/IP 정보를 DB화하여 알려진 위협을 탐지합니다.



4. 탐지 기술

ML (Machine Learning) : 악성파일/정상 파일의 특징을 학습/분석하여 위협이 의심되는 파일을 탐지합니다.



※ 분기 1회 최신의 머신러닝 모델(파일) 제공

4. 탐지 기술

XBA(X Behavior Analysis) : Fileless 공격 등 비 정상적인 행위를 탐지하는 기술이 적용되어 있습니다.

신규 6

처리중 4

해결됨 19

전체 29

신뢰도	탐지 시각	탐지 분류	탐지 세부분류	내용	위협 판정	상태	사용자 IP	사용자명	액션
30%	2019-12-26 14:22:52	XBA	Anomaly	netsh.exe 에 의한 네트워크 설정 변경 시도 이상...	안전	해결됨	172.29.20.179	이성현	위협 분석
30%	2019-12-26 09:26:16	XBA	Anomaly	fsview.exe 에 의한 방화벽 우회 시도 이상행위가 ...	안전	해결됨	172.29.30.110	류지하	위협 분석
80%	2019-12-17 14:18:39	XBA	Autorun	eqyrguteroid.exe 에 의한 의심스러운 자동실행 ...		처리중	172.29.25.132	이창수	위협 분석
30%	2019-12-17 14:18:14	XBA	Anomaly	plugin.exe 에 의한 실행코드 인젝션 이상행위가 ...		처리중	172.29.25.132	이창수	위협 분석
70%	2019-12-17 14:16:13	XBA	Anomaly	cmd.exe 에 의한 자가 삭제 이상행위가 진단됨 (7...		처리중	172.29.25.132	이창수	위협 분석
50%	2019-12-17 14:15:57	XBA	Anomaly	Setup.exe 에 의한 정보 유출 추정 이상행위가 진...		신규	172.29.25.132		
95%	2019-12-11 13:41:20	XBA	Fake	ALZip.exe 에 의한 실행파일 스무핑 이상행위가 진...		처리중	172.29.25.132		
95%	2019-12-09 16:19:02	XBA	Exploit	net.ps1 에 의한 스크립트를 이용한 네트워크 점...		신규	172.29.25.132		

카테고리

이름

2중 확장자를 이용한 속임수 파일 실행

ADS 실행파일 생성

ADS 프로세스 실행

AppInit_DLL을 이용한 DLL Injection

ApplicationShimming을 이용한 UAC Bypass 시도

Autorun 등록 시도

AV 무적화 시도

Exploit에 의한 프로세스 실행

Hosts 파일 수정

ImageFileExecutionOptions를 이용한 자동실행

LateralMovement - at서비스

LateralMovement - at서비스

LateralMovement - 예약작업

LateralMovement - 원격WMI

LateralMovement - 원격WMI

LateralMovement - 원격서비스

LateralMovement - 원격서비스

LSA 레지스트리를 이용한 자동 실행

netsh.exe를 이용한 자동 실행

psexec을 이용한 내부 확산

RDP 암호 무작위 대입

RLO 특수문자를 이용한 속임수

ShadowCopy 삭제

UAC 우회 - AppAndFeature

UAC 우회 - DLL 하위재킹

UAC 우회 - DLL 하위재킹 (WUSA)

MITRE

2중 확장자를 이용한 속임수 파일 실행

ADS 실행파일 생성

ADS 프로세스 실행

AppInit_DLL을 이용한 DLL Injection

ApplicationShimming을 이용한 UAC Bypass 시도

Autorun 등록 시도

AV 무적화 시도

Exploit에 의한 프로세스 실행

Hosts 파일 수정

ImageFileExecutionOptions를 이용한 자동실행

LateralMovement - at서비스

LateralMovement - at서비스

LateralMovement - 예약작업

LateralMovement - 원격WMI

LateralMovement - 원격WMI

LateralMovement - 원격서비스

LateralMovement - 원격서비스

LSA 레지스트리를 이용한 자동 실행

netsh.exe를 이용한 자동 실행

psexec을 이용한 내부 확산

RDP 암호 무작위 대입

RLO 특수문자를 이용한 속임수

ShadowCopy 삭제

UAC 우회 - AppAndFeature

UAC 우회 - DLL 하위재킹

UAC 우회 - DLL 하위재킹 (WUSA)

위협 요약

탐지 지표

탐지 연신

수행 프로세스

이벤트

태그

요약 내용

MITRE ATT&CK

T1046 - Network Service Scanning

파일 정보

해시 목록

엔드포인트

Active

HostName

IP

MAC

DeviceID

Platform

Domain

LogonID

AuthName

AuthID

AuthDeptNa...

Plugin version

Create time

GENIANS

172.29.20.119

00:0E:C6:8F:73:B1

5c5b577c-b66d-10...

Microsoft Windows

WORKGROUP

SYSTEM

홍정현

hyuny0215

EDR기술팀

3.1.1.2466

2020-01-09 13:12:22

timeout.exe

2019-12-17 14:16:12

ProcessStart

스캔 ID

스캔 시간

스캔 대상

스캔 경로

스캔 ID

스캔 시간

스캔 대상

스캔 경로

timeout.exe

2019-12-17 14:16:12

ProcessStart

스캔 ID

스캔 시간

스캔 대상

스캔 경로

스캔 ID

스캔 시간

스캔 대상

스캔 경로

MITRE ATT&CK

T1046 - Network Service Scanning

MITRE ATT&CK

T1046 - Network Service Scanning

※ 100가지 이상의 이상행위 탐지 규칙 보유
(MITRE ATT&CK 탐지 룰 지속 추가)

4. 탐지 기술

YARA : 관리자가 직접 생성한 패턴 매칭 탐지 기술이 적용되어 있습니다.

YARA - 문자열이나 바이너리 패턴(Hex string)을 기반으로 미리 정의된 시그니처로 악성코드를 분류할 수 있게 하는 도구
: 백신 등 endpoint 에서도 활용하고 있는 탐지 기법

모든 파일, 프로세스에 대해 행위 기반 탐지를 적용하기 위해서는 자원 소모가 많고 무겁게 동작

➔ 먼저 YARA와 같은 정적 시그니처 또는 평판을 가지고 판단

➔ 탐지 시 별도의 자원 소모 없이 즉각 차단하거나 삭제 ➔ **효율적**



The screenshot displays the Genian Insights interface with several overlapping windows. The 'YARA Rule 추가' (Add YARA Rule) window is in the foreground, showing a rule named 'TeslaCrypt' with a custom author and a ransomware pattern. The '이벤트 상세정보' (Event Details) window shows the detection of 'chrome.exe' as 'Malware' with a score of 100%. The 'Genian Insights' main window shows a list of processes, including 'chrome.exe', which is highlighted. A 'YARA Rule 검사' (YARA Rule Check) dialog box is also visible, asking if the user wants to check the rule.

YARA Rule 추가

기본 정보

제공자 CUSTOM

이름* TeslaCrypt

규칙* rule TeslaCrypt : ransom
{
 meta:
 description = "TeslaCrypt"
 author = "Aw3someSc0t7"
 date = "2017-03-07"
 filetype = "binary"
 version = "1.0"
 strings:
 \$a = { 59 6F 75 72 20 64 6F 63 75 6D 65
 74 61 62 61 73 65 73 20 61 6F 64 20 6F
 \$b = { 6D 73 68 74 61 2E 65 78 65 20 23
 2E 31 33 32 2F 3F 53 75 62 6A 65 63 74
 76 65 72 73 69 6F 6E 3D 25 73 26 64 61
 49 44 3D 25 64 26 73 75 62 69 64 3D 25
 \$c = { 72 74 61 6E 74 20 66 69 6C 65 73
 79 70 74 65 64 0A }
 }

알림 메시지 TeslaCrypt 랜섬웨어가 탐지되었습니다.

저장 취소

이벤트 상세정보

chrome.exe
process

Process ID 13172 P 11184

Command line
"C:\Program Files
(x86)\Google\Chrome\Application\chrome.exe" --type=renderer
--field-trial-
handle=1948,17522451440039507250,9839541453125366000,13107

Detect type Malware

위험 정보

Detect time 2020-01-02 17:59:00

Detect type MAL YARA

Detect target chrome.exe

Score 100%

Classification Etc

잠재적 유해 프로그램 (PUP/PUA) : Potentially Unwanted Program or Application

파일 정보

File name chrome.exe

File type PE

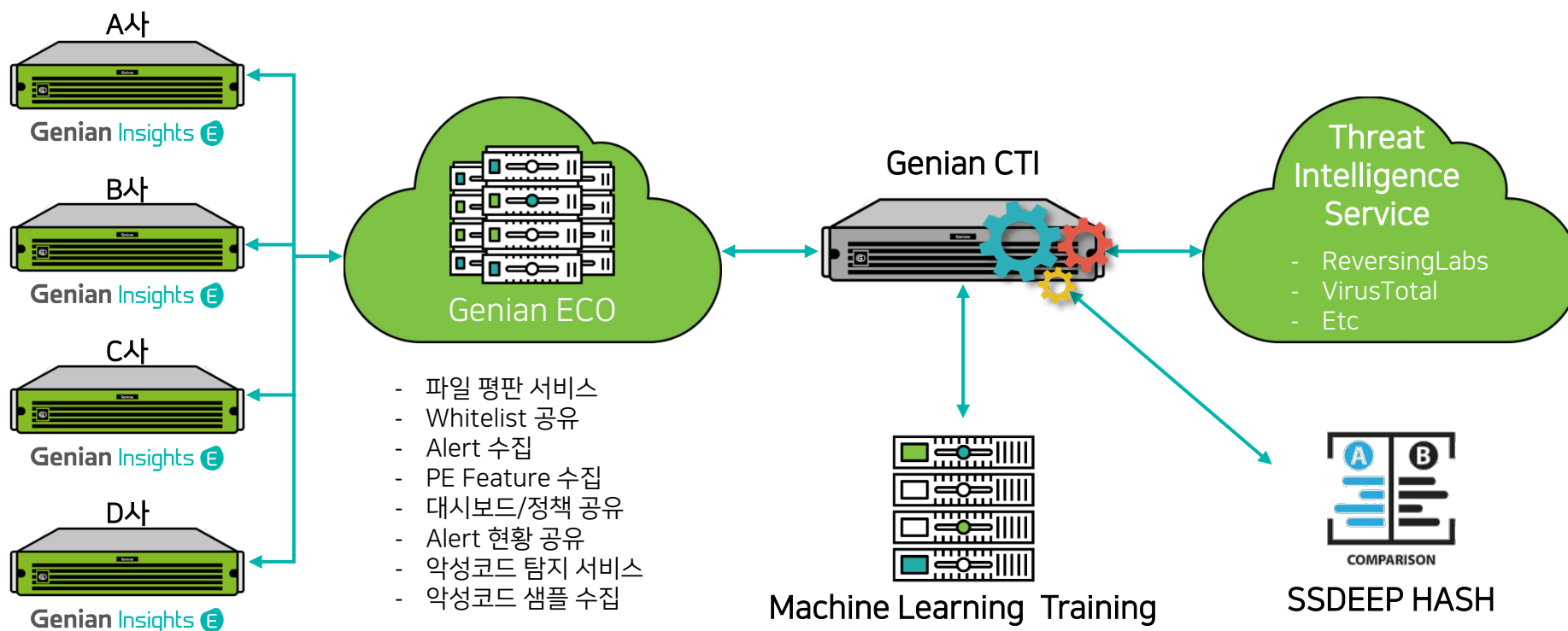
MD5 541fb38e445263f2159ca6c9d12a6778

SHA256 c5be020db6f1803f28e37427975c59379bfb1b084fa48b

4. 탐지 기술

Ecosystem : Genian 자체의 평판시스템을 제공합니다.

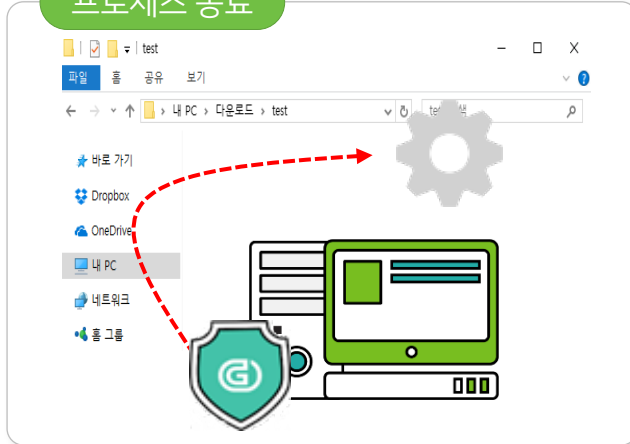
- 오탐 및 최신 악성코드 분석 결과를 고객에게 공유하기 위한 Genian Insights E ECO-SYSTEM 구성
- 파일의 근거 (해당 파일이 어떤 역할을 하는 파일인가? 정말 악성인가?) / 오탐 자동 예외 처리
- 지니언스 고객을 통해 수집된 위협과 예외 처리된 데이터를 수집, 가공하여 Genian Insights E를 사용하는 모든 고객에게 재배포합니다.
- 이를 통해 Genian Insights E를 사용하는 고객들의 오탐을 줄여주며, 위협 혹은 파일 세부 정보 식별이 필요할 때 그 정보를 알려줍니다.



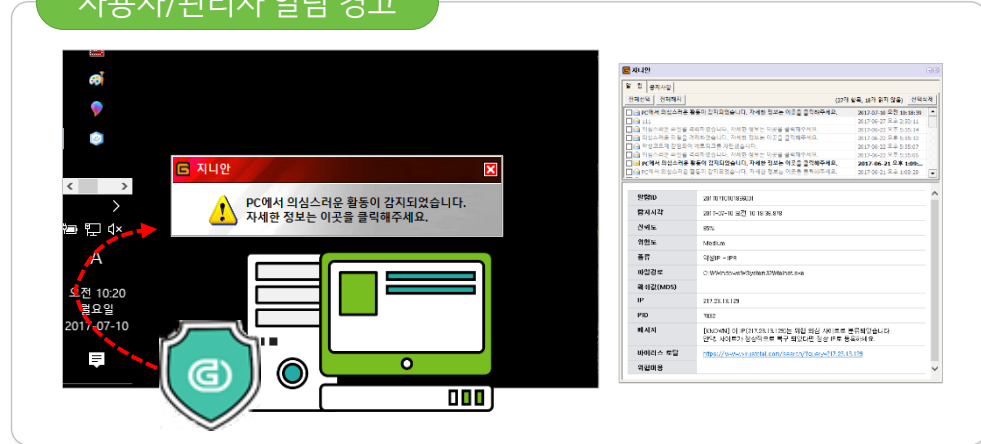
5. 대응

악성 파일에 대한 프로세스 중지, 격리, 사용자/관리자 알람, 네트워크 격리 등의 대응 기능을 제공합니다.

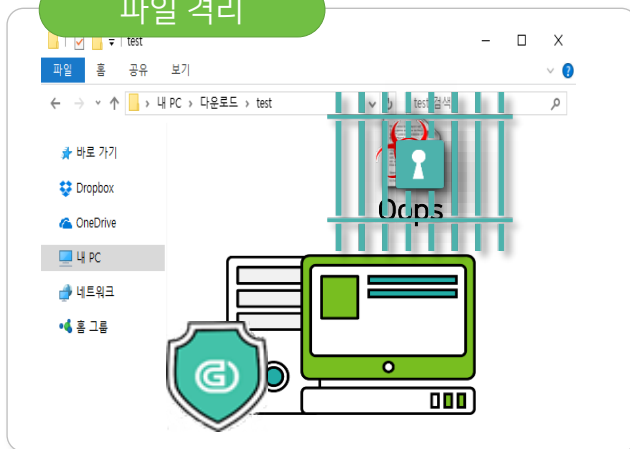
프로세스 종료



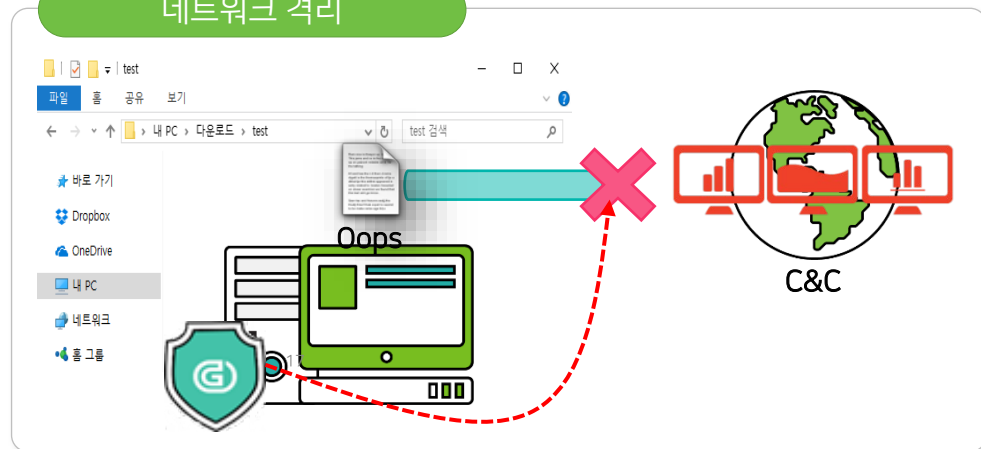
사용자/관리자 알람 경고



파일 격리



네트워크 격리



6. 분석

전체 위협에 대한 요약 정보를 보여주는 위협 모니터링화면을 제공합니다.



6. 분석

탐지된 파일의 위협 정보를 확인할 수 있으며,
이상 행위(Fileless) 탐지 시 연관된 MITRE ATT&CK 링크를 제공합니다.

❖ MITRE ATT&CK : 공격의 기법들을 프로파일링하여, 카테고리별 목록화

기본정보

위험 모니터링: 37ea273266aa2d28430194fca27849170d609d338ab...

위험 관리: 2020-07-07 11:09:52 | Malware / IOC | 상세정보 | 알림 | 삭제 | file_reputation | file_similarity

탐지 지표

탐지 지표: 37ea273266aa2d28430194fca27849170d609d338ab9c6c43c4e6be1bcf51f9.exe 파일이 IOC에 의해 알려진 악성코드로 진단됨 (High/99%)

위험 정보

수행 프로세스: Explorer.EXE

위험 분류: PUA (최종 업데이트 시작: 2020-06-29 17:32:29)

위험명: Win32.PUA.Qjwmonkey

샘플 타입: PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed process / RequestProcessCreate

이벤트: 커맨드라인

커맨드라인: "C:\Users\forest\Downloads\37ea273266aa2d28430194fca27849170d609d338ab9c6c43c4e6be1bcf51f9\37ea273266aa2d28430194fca27849170d609d338ab9c6c43c4e6be1bcf51f9.exe"

요약 내용: 일종의 악성 프로그램의 설치 프로그램의 형태로, 실행 시 내부에 포함되어 있던 바이너리나 쉘, 또는 트로이 목마 등의 악의적인 프로그램이 설치되는 형태의 악성코드

탐지 시각

탐지 시각: 최초 탐지 시각 2020-06-29 17:31:40, 최종 탐지 시각 2020-07-07 11:09:52

File 탐지 정보

악성파일 정보: 파일명 37ea273266aa2d28430194fca27849170d609d338ab9c6c43c4e6be1bcf51f9.exe, 파일경로 C:\Users\forest\Downloads\37ea273266aa2d28430194fca27849170d609d338ab9c6c43c4e6be1bcf51f9\37ea273266aa2d28430194fca27849170d609d338ab9c6c43c4e6be1bcf51f9.exe, 파일타입 PE / Exe, 제품명 downloader, 설명 downloader, 버전 1.0.2.908, 언어 Chinese (Simplified), 아키텍처 x86, EXE 타입 MD5, SHA-256, 전자서명

파일 정보

외부 링크: 37ea273266aa2d28430194fca27849170d609d338ab9c6c43c4e6be1bcf51f9.exe, VirusTotal, malwares.com, Google - File Name, Google - Process Name, Tag 모듈

Fileless(행위) 탐지 정보

탐지 지표: XBA / Autoun.exe에 의한 의심스러운 자동실행 등록 이상행위가 진단됨 (80%)

탐지 엔진: XBA / Autoun

수행 프로세스: kinwuw.exe

의심파일 경로: C:\Users\GENIAN~1\AppData\Local\Temp\kinwuw.exe

파일경로: C:\Users\GENIAN\10\AppData\Roaming\Smart_Clock\SmartClock.exe

파일경로2 (if any): C:\Users\GENIAN\10\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\kinwuw.exe

이벤트: file / FileC

태그: first_seen

커맨드라인: "C:\Users\GENIAN~1\AppData\Local\Temp\kinwuw.exe"

요약 내용: 의심스러운 자동실행 등록 (SuspiciousAutounFile)

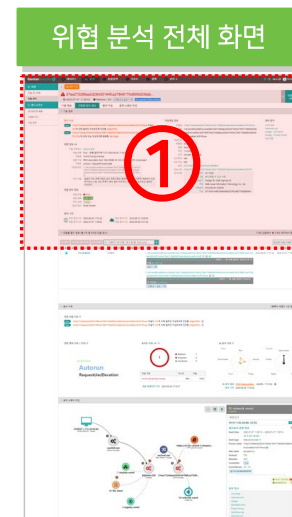
대부분의 악성코드는 다음번 부팅에 다시 실행되기 위해 특정 레지스트리나 시작 프로그램 폴더에 자신을 등록한다. 따라서 부팅시마다 재실행되도록 자신을 등록하는 행위를 집중적으로 모니터링한 악성코드를 효율적으로 탐지할 수 있다.

전단서: Autoun 및 서비스 관련 레지스트리 혹은 시작 프로그램 폴더에 다음과 같은 파일이 등록되는 경우

- 스크립트 파일
- 스크립트에 의해 Autoun이 등록되는 행위
- 전자서명되지 않은 %programfiles% 외의 파일이 등록되는 경우 (Whitelisted 등록된 파일 제외)
- 시작프로그램 폴더에 ink가 아닌 실행파일이 직접 생성되는 경우

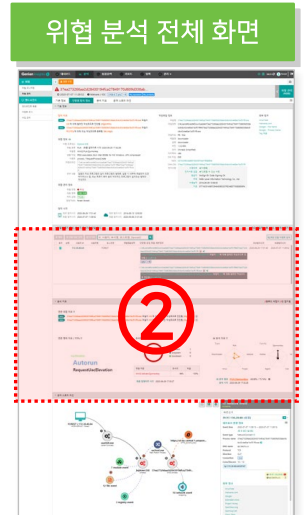
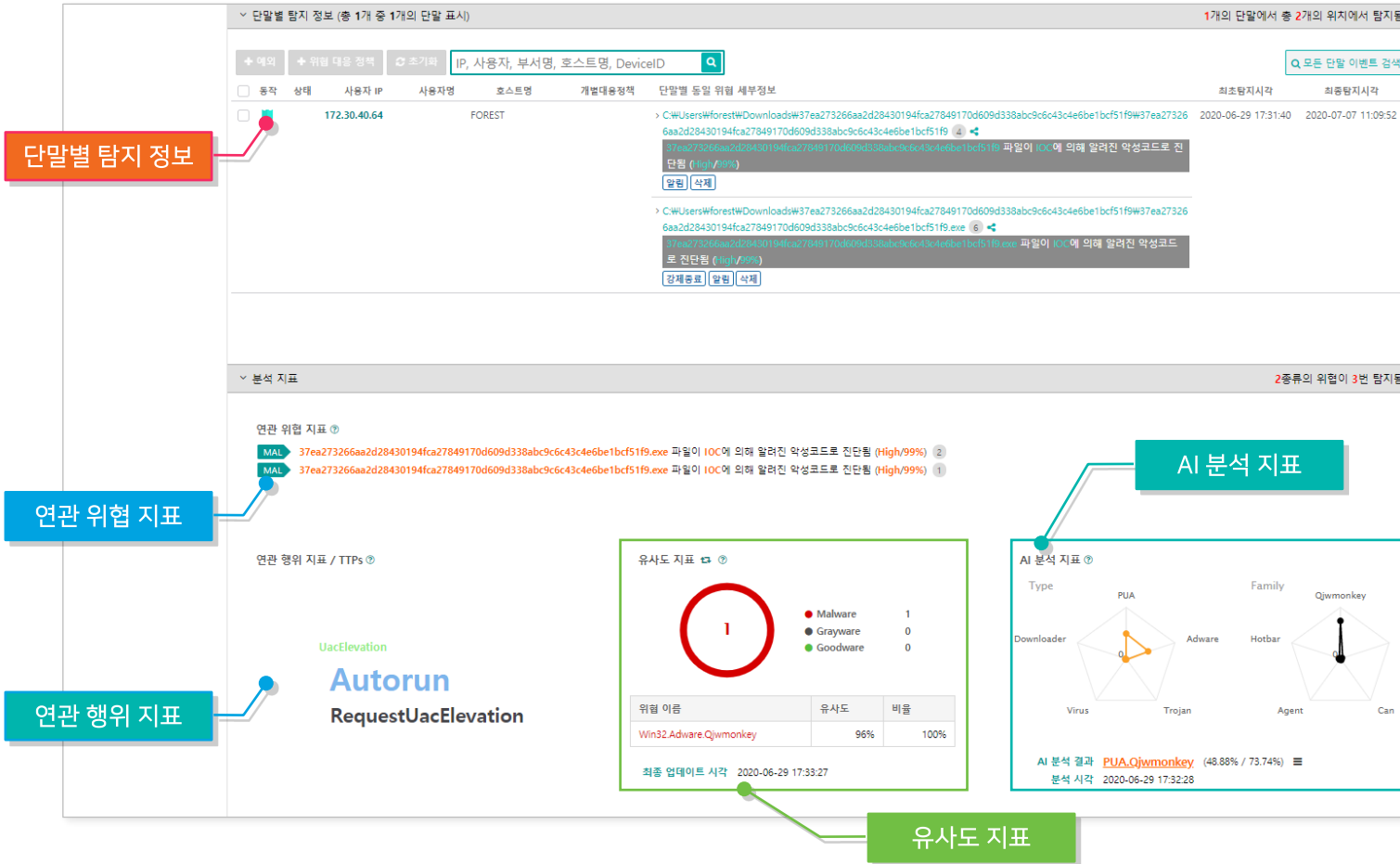
MITRE ATT&CK 링크

MITRE ATT&CK: T1060 - Registry Run Keys / Startup Folder

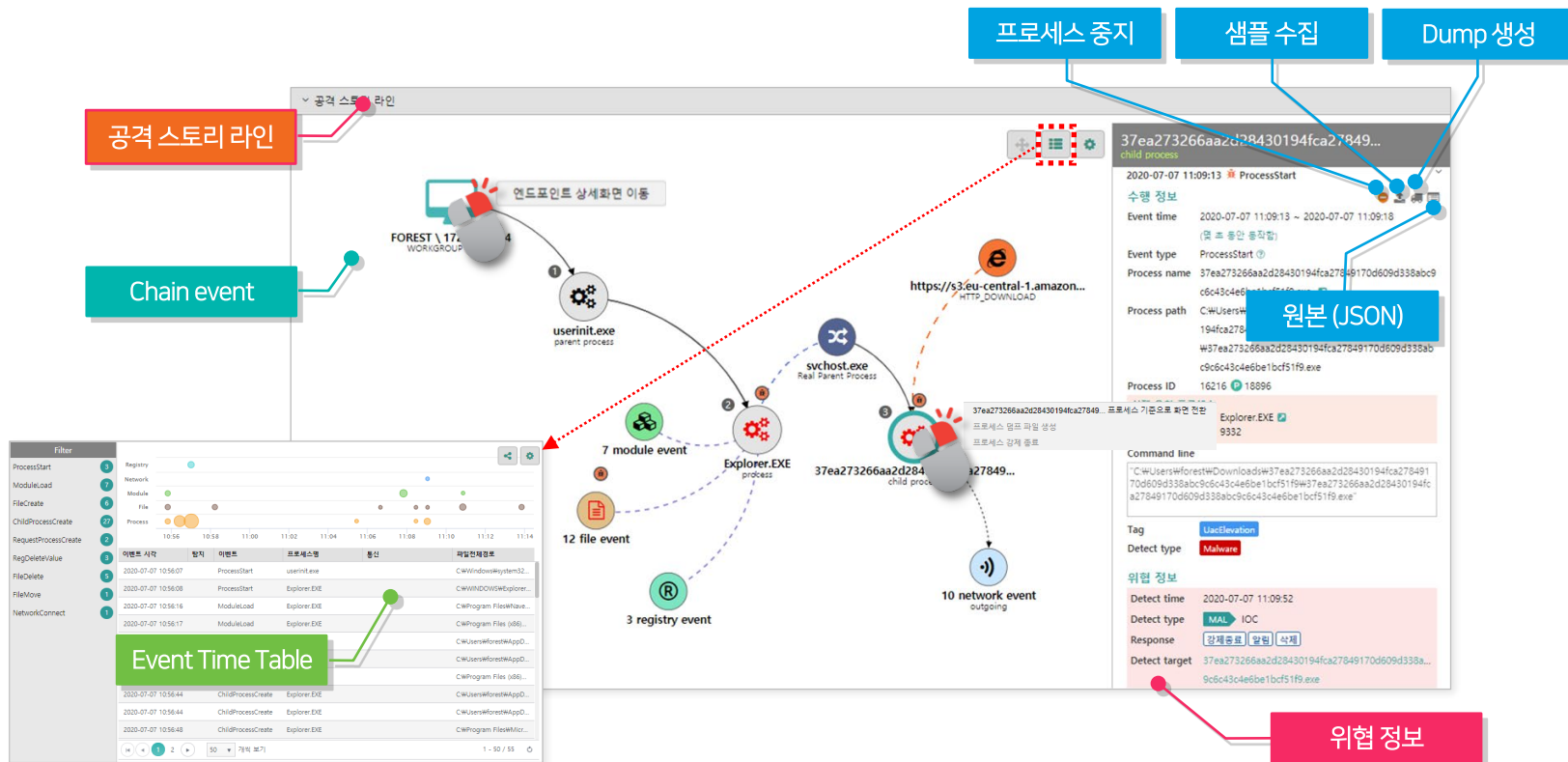


6. 분석

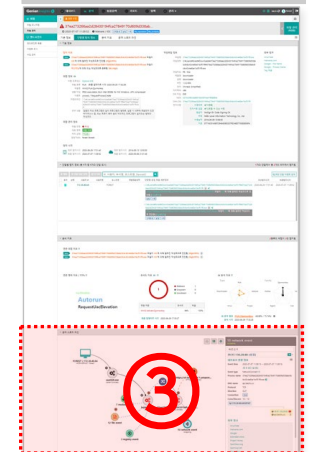
단말 별 탐지정보, 연관지표, 행위, 유사도 등 분석에 도움이 되는 다양한 정보를 제공합니다.



공격 스토리 라인에서는
파일/프로세스의 실행 관계를 표시하며, 프로세스 제어, 파일 수집 등의 제어 기능을 제공합니다.



위협 분석 전체 화면



※ 위협 탐지와 관계없이 수집한 모든 로그에 대해서 위와 같은 Chain Event를 제공합니다.

6. 분석

분석 후 위협에 대한 안전/악성 판단 후 자동 대응을 할 수 있습니다.

The screenshot displays the Genians security management interface. The main window shows details for a threat named 'rkfree_setup-5-.exe'. A modal titled '위협 관리' (Threat Management) is open, allowing for the configuration of response actions based on the threat's status.

위협 관리 (Threat Management) Modal:

- 위험 관리:** rkfree_setup-5-.exe 위협을 관리합니다. 동일한 위협에 대해서 자동화 된 대응을 할 수 있습니다.
- 관리 설정 (Management Settings):**
 - 담당자ID:** forest
 - 위협 판정 (Threat Judgment):** ☒ 악성 (Malicious), ☐ 안전 (Safe), ☐ 보류 (Pending). 악성 여부를 담당자가 판단하여 설정합니다.
 - 대응 정책 (Response Policy):** 기본정책 (Default Policy). 동일한 위협 발생시 대응 정책을 설정합니다.
 - 자동해결 (Auto Resolution):** ☒. 향후 동일한 위협 발생시 자동으로 [해결됨] 상태로 변경합니다.
 - 메모 (Memo):** 메모 입력 (Memo Input).
- 오탐 보고 (False Positive Report):** Genian Cloud에 오탐지 보고합니다. (Report to Genian Cloud).
- Buttons:** 설정완료 (Save), 초기화 (Reset), 취소 (Cancel).
- 히스토리 (History):** Comment를 입력합니다. (Add Comment).
 - 2020-01-08 13:00:10 담당자가 forest으로 변경되었습니다.
 - 2020-01-08 13:00:10 위협 관리상태가 "처리중"으로 변경되었습니다.

Callouts and Labels:

- 안전 판정 (Safety Judgment):** Points to the '안전' (Safe) radio button.
- 악성 판정 (Malicious Judgment):** Points to the '악성' (Malicious) radio button.
- 대응 방법 (Response Method):** Points to the '기본정책' (Default Policy) dropdown.
- 악성 자동 대응 (Malicious Auto Response):** Points to the '자동해결' (Auto Resolution) checkbox.
- 코멘트 (Comments):** Points to the '히스토리' (History) section.
- 감사로그 (Audit Log):** Points to the '히스토리' (History) section.

6. 분석

조건 없이 파일 명 하나만으로도 파일의 생성, 변경 정보를 확인할 수 있으며, 검색 기록 불러오기, 즐겨찾기 기능으로 동일한 검색을 쉽고 빠르게 할 수 있습니다.

❖ FileDownload.exe 다운로드 ➔ C 에서 D 드라이브로 복사 ➔ D 드라이브에서 이름 변경

FileDownload.exe

이벤트 시각

탐지

이벤트

이벤트 요약

2020-07-31 14:00:10	FileMove	Explorer.EXE 프로세스가 D:\FileDownload.exe 파일을 D:\FileDownload_이름 변경.exe 파일로 이동시켰습니다.
2020-07-31 14:00:02	FileCreate	Explorer.EXE 프로세스가 D:\FileDownload.exe 파일을 생성했습니다.
2020-07-31 14:00:02	FileCopy	Explorer.EXE 프로세스가 C:\Users\forest\Downloads\FileDownload.exe 파일을 D:\FileDownload.exe 파일로 복사했습니다.
2020-07-31 13:59:50	HttpDownload	https://the.earth.li/~sgtatham/putty/0.74/w64/putty.exe 에서 C:\Users\forest\Downloads\FileDownload.exe 파일이 Http로 다운로드
2020-07-31 13:59:49	FileCreate	chrome.exe

조건 없이 파일명으로만 어디서 다운받았는지, 어디로 복사됐는지,어떤 이름으로 변경됐는지 확인 가능

검색 조건	해석
IP:172.29.20.0/24 AND FileName:abc.exe OR NOT FilePath:windows AND FileSize:>100000 AND Score:[50 TO 100]	172.29.20.0/24 PC에서 파일 위치가 windows가 아니고 파일 크기가 1MB 이상이며, 파일 스코어가 50~100점 사이의 abc.exe 파일 존재 유무 검색

최근 검색을 한 기록은 별도로 보관되어 다시 불러오기로 검색이 가능하며, 자주 쓰이는 검색 조건은 " 즐겨찾기 " 로 등록, 재 검색 가능함
 (ProcName:msiexec.exe AND !FilePath("C:\Windows\Installer" OR "C:\Windows\Temp" AND EventSubType:"FileCreate") AND !EventSubType:ProcessStart) AND (IP:"172.29.20.218")

(ProcName:msiexec.exe AND !FilePath("C:\Windows\Installer" OR "C:\Windows\Temp" AND EventSubType:"FileCreate") AND !EventSubType:ProcessStart) AND (IP:"172.29.20.218")

이벤트 시각

탐지

이벤트

프로세스명

통신

파일명

레지스트리

2020-01-02 14:19:54	ChildProcessCreate	msiexec.exe		regsvr32.exe
2020-01-02 14:19:53	ChildProcessCreate	msiexec.exe		regsvr32.exe
2020-01-02 14:19:53	ChildProcessCreate	msiexec.exe		regedit.exe
2020-01-02 14:19:53	ModuleLoad	MSIExec.exe		MSI8A76.tmp
2020-01-02 14:19:53	FileCreate	msiexec.exe		MSI8A76.tmp
2020-01-02 14:19:53	FileCopy	msiexec.exe		a99b40d.msi
2020-01-02 14:19:52	FileCreate	msiexec.exe		a99b087.msi
2020-01-02 14:19:51	RegSetValue	msiexec.exe		a99b40d.msi
2020-01-02 14:19:51	RegCreateKey	msiexec.exe		

검색 결과

등록된 검색 조건

최근 검색 기록

Infoinsightse

cmd

Tag:*

Tag:FolderShare

RegKeyPath:"HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\LanmanServer\Shares"

(ProcName:msiexec.exe AND !FilePath("C:\Windows\Installer" OR "C:\Windows\Temp" AND EventSubType:"FileCreate") AND !EventSubType:ProcessStart) AND (IP:"172.29.20.218")

(ProcName:msiexec.exe AND !FilePath("C:\Windows\Installer" OR "C:\Windows\Temp" AND EventSubType:ProcessStart) AND (IP:"172.29.20.218")

검색 기록 불러오기

즐거찾기

공유폴더설정레지스트리

아웃룩 첨부파일 검색

강속파일검색

프로세스를 통한 파일 다운로드 검색

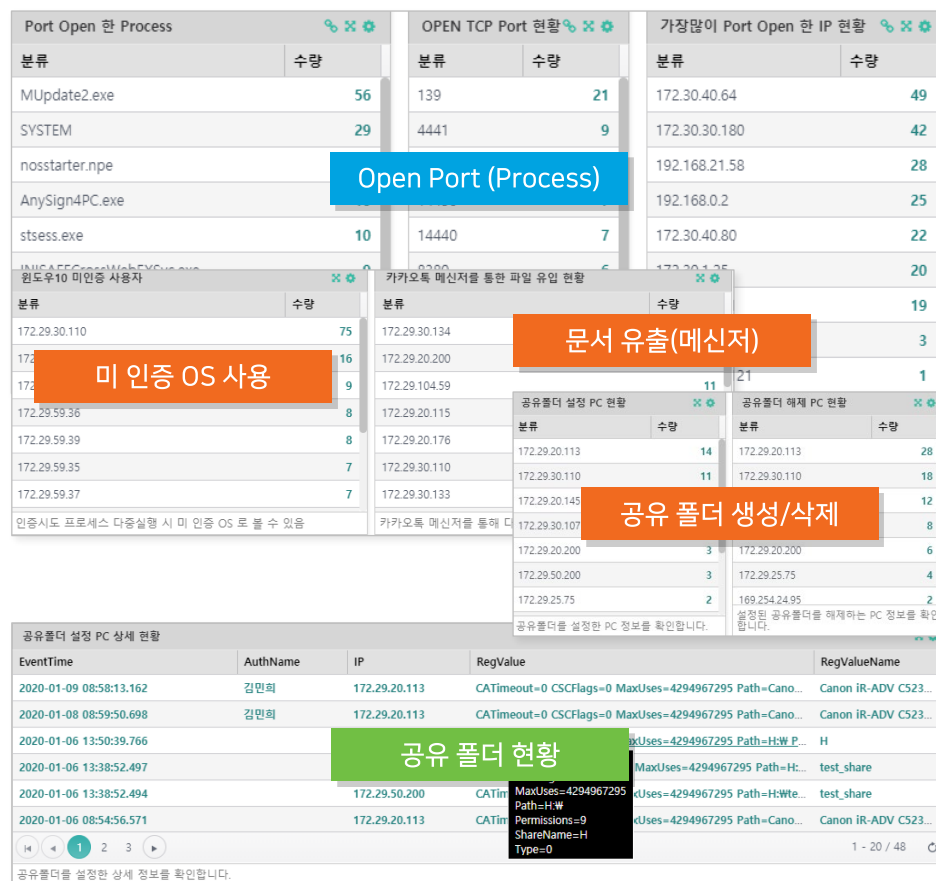
자주 쓰는 검색 조건 저장

❖ 3개월 로그 39억 8천만 건 상황에서의 2가지 조건 검색 속도 : 약 3초

6. 분석

대시보드는 다양한 커스터마이징을 통해 엔드포인트의 가시성을 극대화 합니다. (Endpoint Discovery)

문서에 대한 업/다운로드, 아웃룩 메일 첨부 문서 송/수신, 공유 폴더를 통한 파일 유출, 공유 폴더 현황(설정, 삭제), 윈도우 미 인증 PC, 메시지를 통한 문서 유입/유출, 외장 저장장치를 통한 문서 유입/유출 등



6. 분석

편리하고 유용한 로그 검색

한번 검색한 결과에 다시 검색 탭을 추가해서 단계별 상세 검색을 할 수 있습니다.

초기 검색 (넓은 범위의 검색)
FileName:pptx

2차 검색 (초기 검색 + 추가 조건)
기존 검색 조건 자동 승계 AND EventSubType:FileUpload

3차 검색 (2차 검색 + 추가 조건)
2차 검색 조건 자동 승계 AND ProcName:kakaotalk.exe

정확한 정보를 모르는 상태에서의 특정 로그를 확인하기 위해 범위를 좁혀 가면서 검색을 해야 합니다.
여러 번 검색을 한다면 기존 검색 결과를 지우고 재 검색을 하는 게 아닌 기존 검색결과도 같이 보면서 검색을 해야 효율적으로 사용할 수 있습니다.

6. 분석

Into the unknown : TAGs

수집한 로그의 의미를 알 수 있도록 Tag를 설정하여 원하는 Tag 검색으로 복잡한 파일 경로, 레지스트리 등의 검색을 쉽고 빠르게 할 수 있습니다.

검색조건 (Raw data 검색)

RegKeyPath:"HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\LanmanServer\Shares"

검색조건 (tag 검색)

Tag:FolderShare

Tag:FolderShare

Process

File

Module

Network

Registry

2019-12-19 00:00:00

20

이벤트 시각	탐지	이벤트	프로세스명	통신	파일명	레지스트리 경로	사용자 IP
2019-12-19 11:07:21		RegDeleteValue	svchost.exe			HKEY_LOCAL_MAC...	172.29.20.218
2019-12-19 11:07:21		RegDeleteValue	svchost.exe			HKEY_LOCAL_MAC...	172.29.20.218
2019-12-19 10:57:29		RegSetValue	svchost.exe			HKEY_LOCAL_MAC...	172.29.20.218
2019-12-19 10:57:29		RegSetValue	svchost.exe			HKEY_LOCAL_MAC...	172.29.20.218
2019-12-19 10:57:05		RegDeleteValue	s				229.20.218
2019-12-19 10:57:05		RegDeleteValue	sv				229.20.218

같은 검색 결과

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\LanmanServer\Shares 경로의 레지스트리에 공유 폴더 테스트 2 : CATimeout=0
CSCFlags=0
MaxUses=4294967295
Path=C:\Users\forest\Documents\공유 폴더 테스트
Permissions=9
Remark=222
ShareName=공유 폴더 테스트 2
Type=0
값이 설정되었습니다.

Protocol UDP	#NTP
RemotePort 123	
Protocol TCP	#SNPP
RemotePort 444	
Protocol TCP	#IMAP4
RemotePort 993	
EventSubType ProcessStart	#Bluetooth
ProcName fsquirt.exe	
FilePath C:\Users\com\AppData\Local\Microsoft\Windows\NetCache\Content.Outlook\WMMK3QYA7W\의뢰_지니언스_1912_(002).zip	#OutlookAttachmentAdd
RegKeyPath HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\LanmanServer\Shares\Security	#FolderShare
RegKeyPath HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles\{106A2C18-21C1-489F-AED2-851935A45A10}	#AP
CmdLine C:\WINDOWS\system32\svchost.exe -k netsvcs -p -s XblAuthManager	#ServiceName:XblAuthManager,ServiceStart

EventTime	Tag	EventSubType	ProcName
2020-01-10 11:15:18.371	ServiceStart	ProcessStart	svchost.exe
2020-01-10 11:15:08.511	ServiceStart	ProcessStart	svchost.exe
2020-01-10 11:15:05.760	ServiceStart	ProcessStart	svchost.exe
2020-01-10 11:15:05.458	WindowsFirewall WindowsDefender	RegSetValue	svchost.exe
2020-01-10 11:15:05.457	WindowsFirewall WindowsDefender	RegSetValue	svchost.exe
2020-01-10 11:15:05.453	WindowsFirewall WindowsDefender	RegDeleteValue	svchost.exe
2020-01-10 11:15:05.451	WindowsFirewall WindowsDefender	RegDeleteValue	svchost.exe
2020-01-10 11:15:05.240	ServiceStart	ProcessStart	svchost.exe
2020-01-10 11:15:04.689	WindowsUpdate	ProcessStart	TiWorker.exe
2020-01-10 11:15:04.658	ServiceStart	ProcessStart	TrustedInstaller.exe
2020-01-10 11:15:04.620	ServiceStart	ProcessStart	FlashPlayerUpdateSer...
2020-01-10 11:15:04.617	ServiceStart	ProcessStart	svchost.exe
2020-01-10 11:15:04.599	ServiceStart	ProcessStart	svchost.exe
2020-01-10 11:14:47.848	DocSave	FileCreate	EXCELEXE
2020-01-10 11:14:43.915	ServiceStart	ProcessStart	sppsvc.exe

7. Agent 관리

설치된 Agent 현황을 파악할 수 있습니다.

Agent On/Off 상태, IP, MAC, 사용자 정보, OS 정보, 부팅 시각, 정책 수신 시각, 데이터 전송 시각을 제공하며, 단말기 선택 후 네트워크 차단, Agent 재 기동, YARA Rule 검사를 수동으로 할 수 있습니다.

Genian Insights 대시보드 분석 통합검색 리포트 정책 관리

조건 검색

엔드포인트

단말기 선택 후 제어 옵션 활성화

단말기 리소스

단말기 리소스

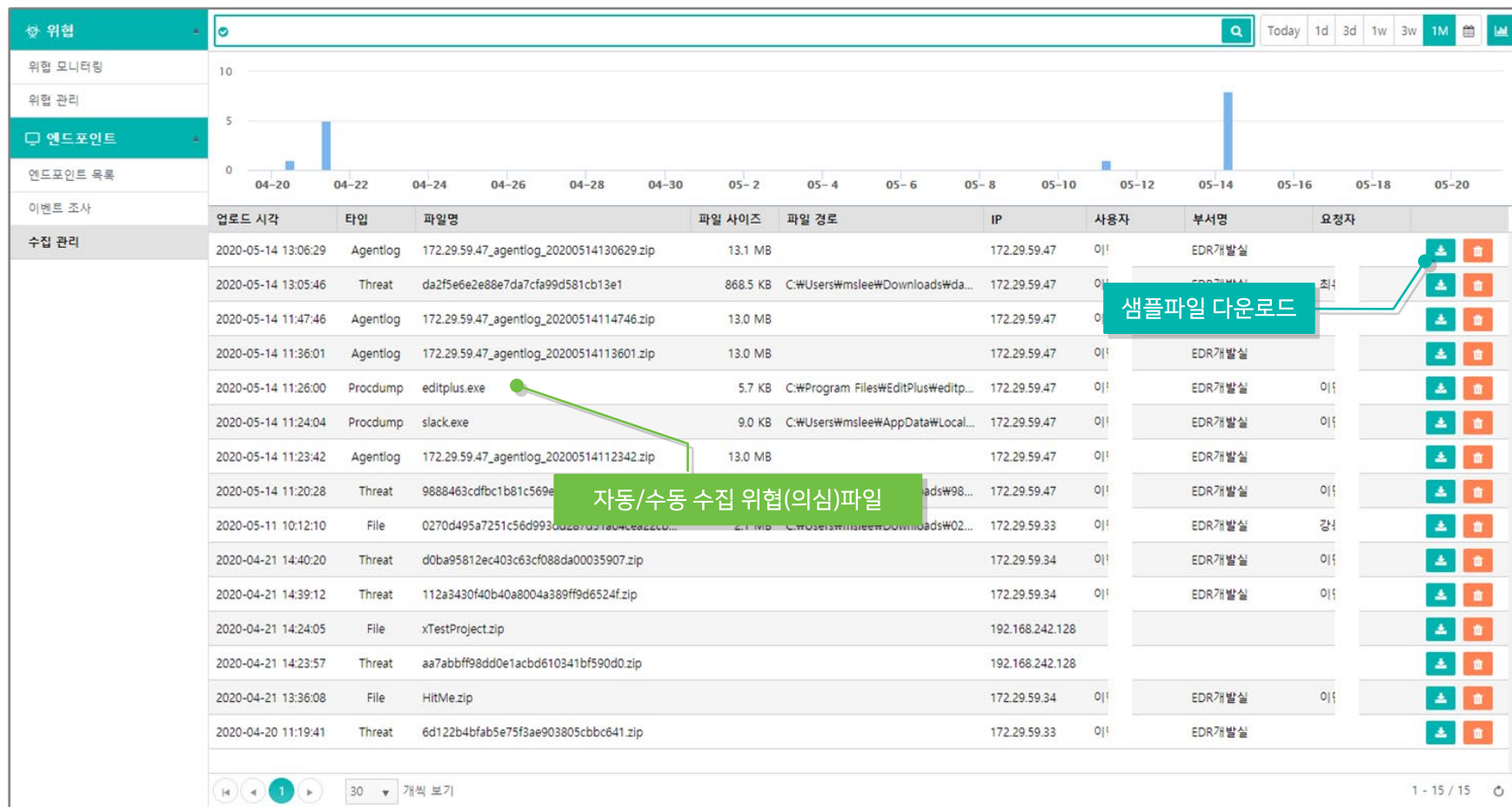
엔드포인트 히스토리

단말기	상태	액션	사용자 IP	MAC	사용자명	부서명	호스트명	부팅 시각	정책 수신 시각	데이터 전송 시각	PC 리소스 사용량	Agent 리소스 사용량
172.29.20.176	UP	172.29.20.176	E0:D5:5E:A5:D2:CA				DESKTOP-E68VV7A	2020-07-27 09:02:34	2020-07-27 09:05:48	2020-07-27 13:17:52	CPU 6.35% MEM 65.14% DISK 32.85%	CPU 0% MEM 0.14% DISK 0.03%
172.29.20.200	DOWN	172.29.20.200	1C:1B:0D:88:BF:7A				DESKTOP-IV8KHRE	2020-07-16 09:00:54	2020-07-27 12:33:12	2020-07-27 13:17:51	CPU 15.85% MEM 49.29% DISK 62.22%	CPU 0% MEM 0.3% DISK 0.23%
172.29.20.205		172.29.20.205	00:E0:4C:62:7A:80							2020-07-27 13:17:40	CPU 18.25% MEM 41.11% DISK 42.11%	CPU 0% MEM 0.24% DISK 0.15%
172.29.20.219		172.29.20.219	1C:1B:0D:4F:35:34							2020-07-27 13:17:49	CPU 10.42% MEM 42.64% DISK 60.75%	CPU 0% MEM 0.33% DISK 0.12%
172.29.20.224		172.29.20.224	00:E0:4C:36:00:85							2020-07-27 13:18:10	CPU 9.72% MEM 23.26% DISK 49.86%	CPU 1% MEM 0.14% DISK 0.14%
172.29.25.161		172.29.25.161	C4:D9:87:31:FE:9D							2020-07-27 13:17:55	CPU 20.29% MEM 76.5% DISK 61.67%	CPU 1% MEM 0.35% DISK 0.05%
172.29.25.78		172.29.25.78	F8:63:3F:22:48:CE							2020-07-27 13:18:12	CPU 13.09% MEM 71.33% DISK 81.48%	CPU 0% MEM 0.22% DISK 0.19%

8. 수집관리

위험파일, 의심파일(PE)은 선택에 따라 자동/수동 수집하며, 관리자가 선택한 일반 PE 파일을 수동으로 수집할 수 있습니다.

탐지된 위험 파일은 추가 분석을 위해 사용자 PC 에서 EDR 서버로 파일을 전송, 관리할 수 있는 기능을 제공합니다.



10. 연동

Syslog, SNMP, Rest API 를 지원하고 있어 타 시스템과의 연동을 다양하게 할 수 있습니다.

※ Syslog, SNMP 설정

The screenshot shows the Genian Insights web interface. On the left is a sidebar with navigation options like '사용자 관리' (User Management), '속성 관리' (Attribute Management), and '환경설정' (Settings). The main area displays two configuration windows. The top window is 'Syslog 설정' (Syslog Settings), which includes fields for '서버 IP' (Server IP), '전송포트' (Transmission Port), '인덱스 선택' (Index Selection), '타임존' (Timezone), and 'Syslog 메시지' (Syslog Message). The bottom window is 'SNMP 설정' (SNMP Settings), which includes a '사용여부' (Usage) toggle, 'Username', 'Auth Password', and 'Priv Password' fields. Both windows have '저장' (Save) and '취소' (Cancel) buttons.

※ REST API

The screenshot shows the REST API interface. It lists several endpoints: 'sitemap : 사이트맵 API', 'sysadmin : 시스템 관리 API', 'threats : Threat 처리 API', and 'Implementation Notes'. The 'threats : Threat 처리 API' section is expanded, showing endpoints like 'POST /threats/command', 'GET /threats/download', and 'GET /endpoints'. The 'GET /endpoints' endpoint is selected, showing its implementation notes and a detailed response message. The response is a JSON object with fields like 'values', 'empty', 'size', 'entrySet', and 'keySet'. Below the response, there is a table of parameters for the endpoint.

Parameter	Value	Description	Parameter Type	Data Type
page	1	페이지 인덱스(1부터 시작)	query	Integer
pageSize	200	페이지별 Row수	query	Integer
sort		정렬조건 JSON (field, dir)	query	string
active		동작여부 (0:동작안함, 1:동작중)	query	string
DeviceID		Device Id	query	string
Version		Version	query	string
Platform		Platform	query	string
PlatformCode		Platform코드	query	string
IP	192.168.0.13	IP	query	string
MAC		MAC	query	string
ServerIP		서버IP	query	string

10. 연동

기타 다른 형태의 연동도 별도의 패치 작업 없이 플러그인 추가로 간단히 가능합니다.
(연동 플러그인 개발 후 패치 없이 적용)

The screenshot shows the Genian Insights web interface. The top navigation bar includes '대시보드', '분석', '통합검색', '리포트', '정책', and '관리'. The left sidebar has a tree view with categories like '인덱스 관리', '시스템 관리', and '업데이트 관리'. The main content area displays a table of installed and available plugins. A red dashed box highlights the table, and a red arrow points from it to a diagram of a server with a 'Plugin' being added. The diagram is labeled '연동 플러그인' (Integration Plugin).

이름	패키지	사용여부	상태	버전	동작방식	설명
DummySchedulePlugin	dummyschedule	☐		1.0.0.14336	schedule	python plugin 테스트를 위한 dummy schedule plugin
DummyRestApiPlugin	dummyrestapi	☒	⚙️	1.0.0.14336	restapi	외부 연동을 위한 restapi 테스트를 위한 dummy plugin
AhnlavV3	ahnlavv3	☒	🔴	1.0.0.14312	schedule	Ahnlav V3 정보를 주기적으로 조회
SamsungsdsAMS	samsungsds	☒	⚙️	1.0.0.14221	schedule	AMS를 이용한 위협 분석 요청 및 결과 조회
SecudiumSuspiciousIP	secudiumhip	☒	🔴	1.0.0.14221	schedule	secudium suspicious ip 정보를 주기적으로 조회
SecudiumIOC	secudiumioc	☒	⚙️	1.0.0.14221	schedule	secudium ioc 정보를 주기적으로 조회
SecudiumSuspiciousURL	secudiumurl	☒	🔴	1.0.0.14221	schedule	secudium suspicious url 정보를 주기적으로 조회

연동 플러그인

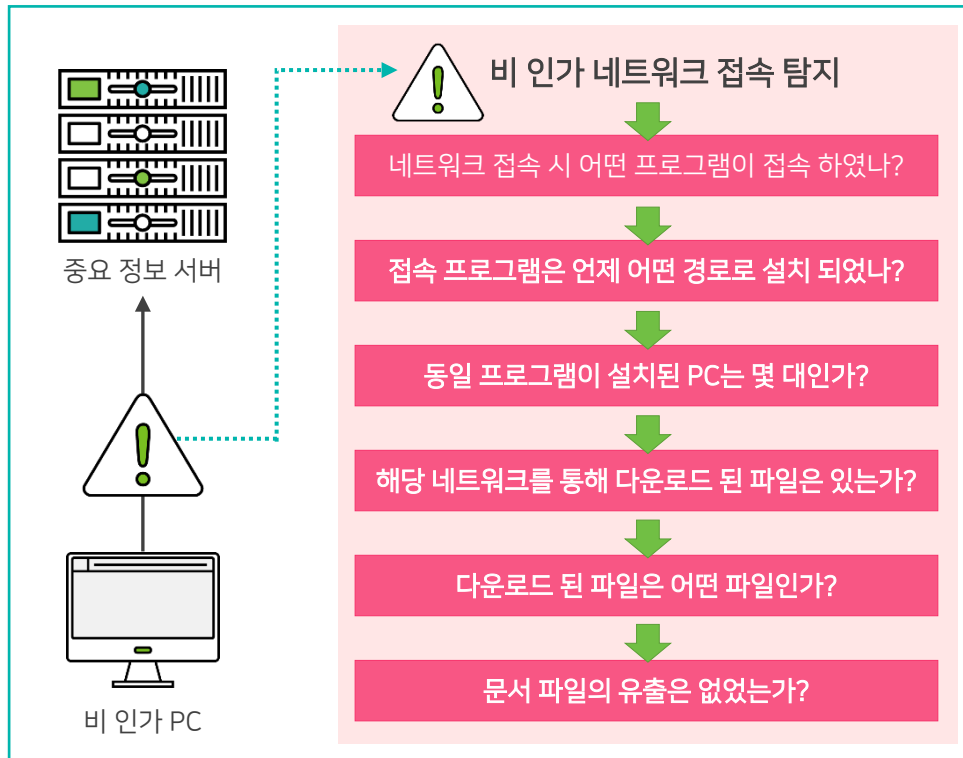
Plugin

도입 효과

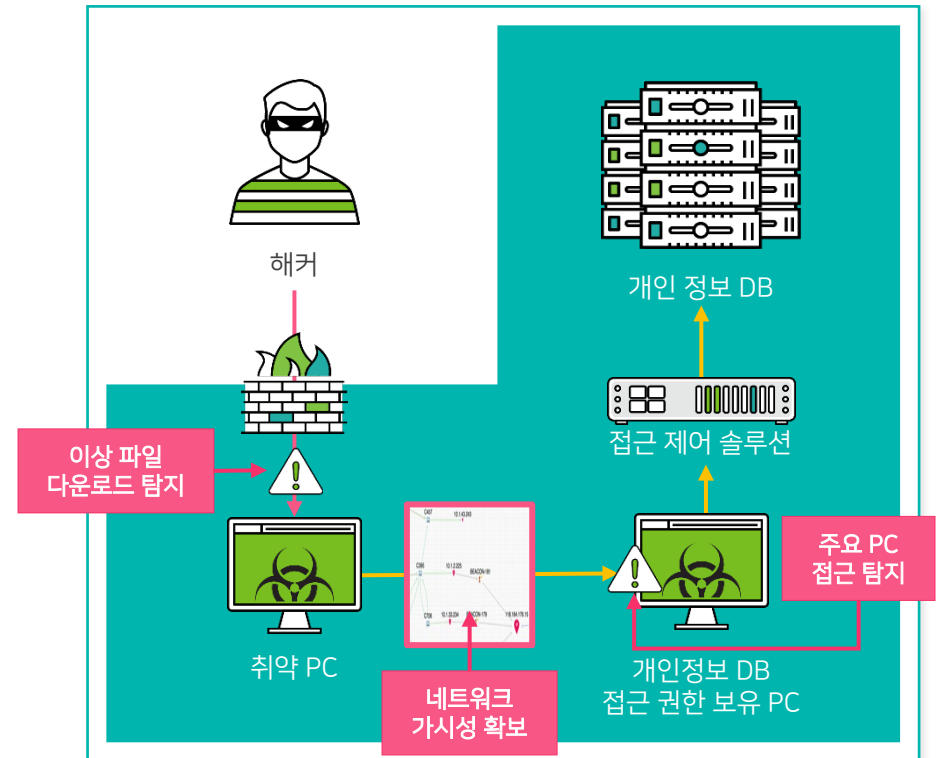


침투 경로와 행위에 대한 파악

단말에 침투한 파일이 언제, 어떻게 유입/실행이 됐으며, 어떤 네트워크 통신과 어떤 행위를 했는지에 대한 정보를 바탕으로 이상 파일/행위에 대한 탐지와 대응을 쉽게 할 수 있습니다.



Unknown → Known



Unknown → Known

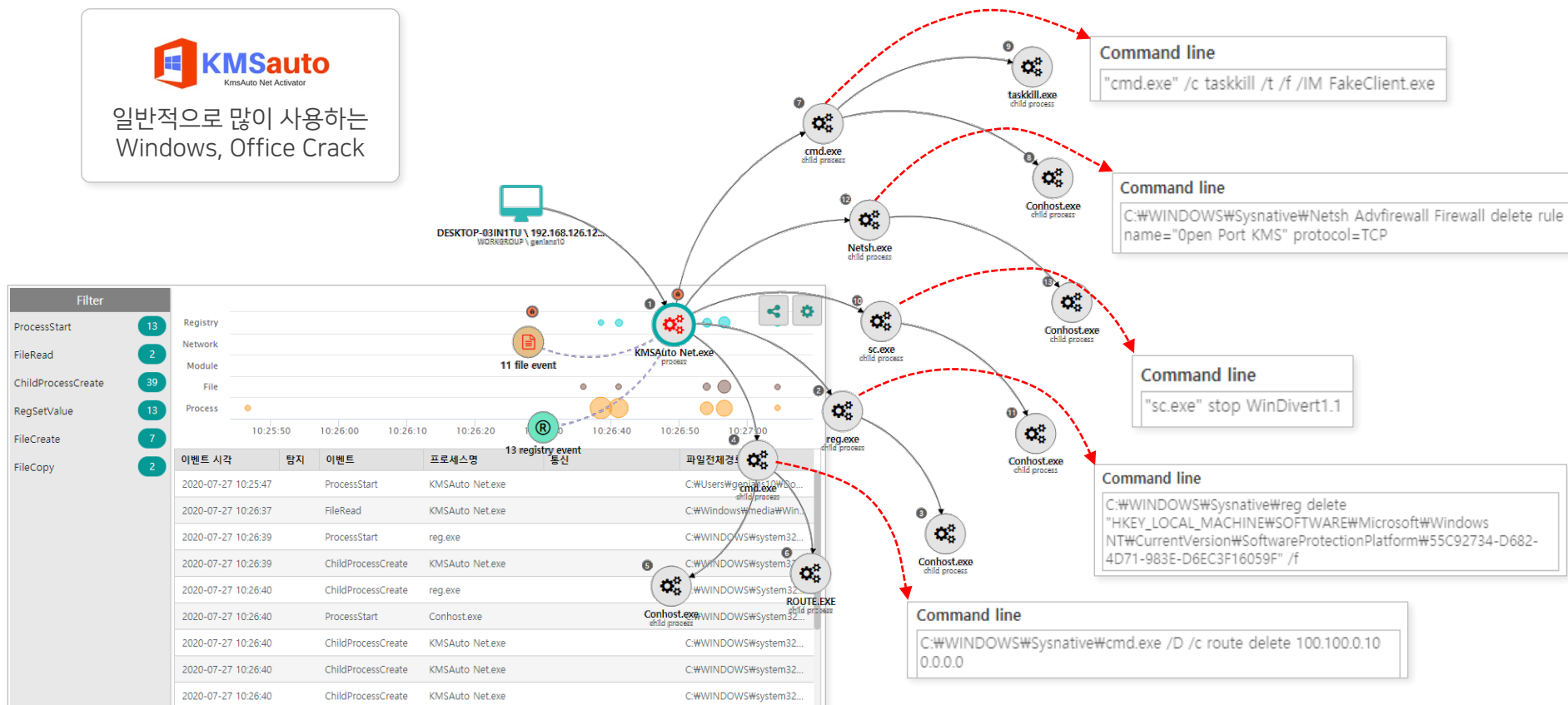
침투 경로와 행위에 대한 파악

리버스 엔지니어링(Reverse Engineering)없이 프로그램의 동작을 확인할 수 있습니다.

특정 프로세스 킬(KILL), 서비스 중지, 파일 생성, 방화벽 정책 삭제, 레지스트리 삭제, 라우팅 삭제 등



일반적으로 많이 사용하는
Windows, Office Crack



내부 보안 정책 점검

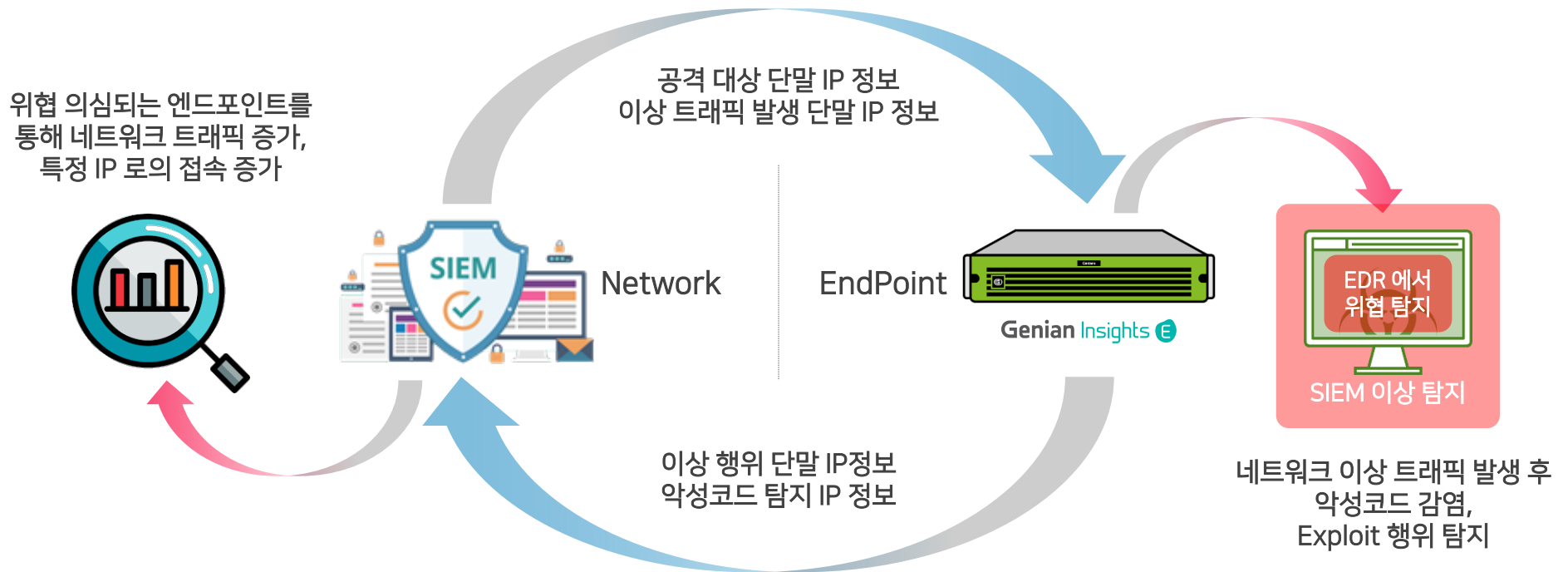
기존에 확인이 어려웠던 엔드포인트 보안 정책의 적합성을 확인할 수 있습니다.

폐쇄망 PC의 외부 통신, 내부 중요 시스템 접속 차단 PC의 통신 이력, USB 사용 금지 PC의 USB 사용 이력, 허용되지 않은 DNS 변경, 프록시 사용, 공유폴더 사용 여부, 테더링 사용, 개인 클라우드 사용 등 사용자 PC에서 적용되는 정책이 정상적으로 적용되고 있는지 확인 가능



네트워크와 엔드포인트의 연관성

네트워크 상의 위협 의심 정보를 연동하여, 네트워크 상의 이상 행위가 엔드포인트에서의 악성 행위나 악성파일 생성으로 이어졌는지 분석할 수 있습니다. 상호 연동으로 반대 상황도 분석이 가능합니다.





Thank you!