

통합 보안 플랫폼 기업, 지니언스

PC 가시성의 모든 것

Genian EDR v2.0

Brand New 2023



Table of Contents

01. 배경 및 필요성

02. Genian **EDR** 제품 소개

03. Genian **EDR** 도입 효과

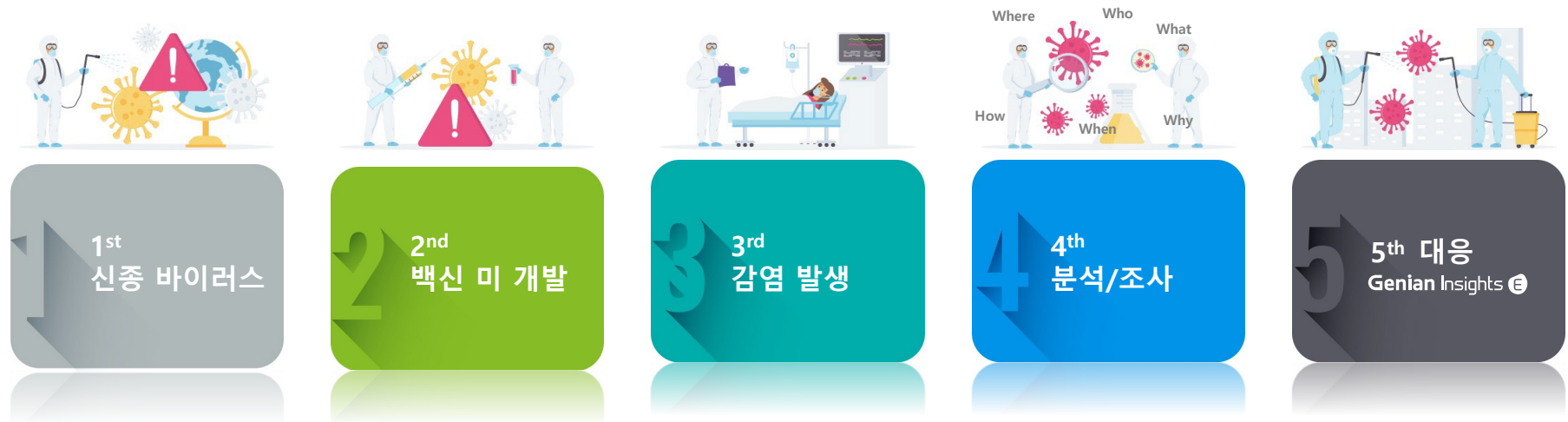
01.

배경 및 필요성

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.

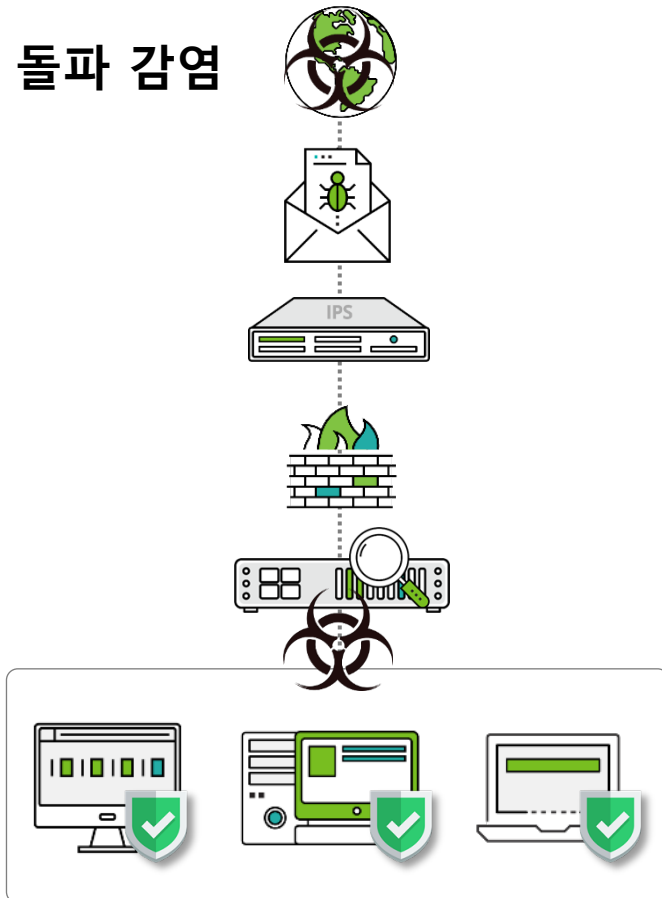
네트워크 경계에 있는 대부분의 보안 솔루션은 내부 자산을 보호하기 위해 구성되어 있으나 엔드포인트의 위협은 계속 증가하고 있습니다.

사용자에게 보내지는 악성 메일, 피싱 사이트, 위/변조 된 홈페이지 접속 등을 통한 악성코드 감염 및 APT 침해는 네트워크 보안 솔루션의 한계를 보여주고 있습니다.

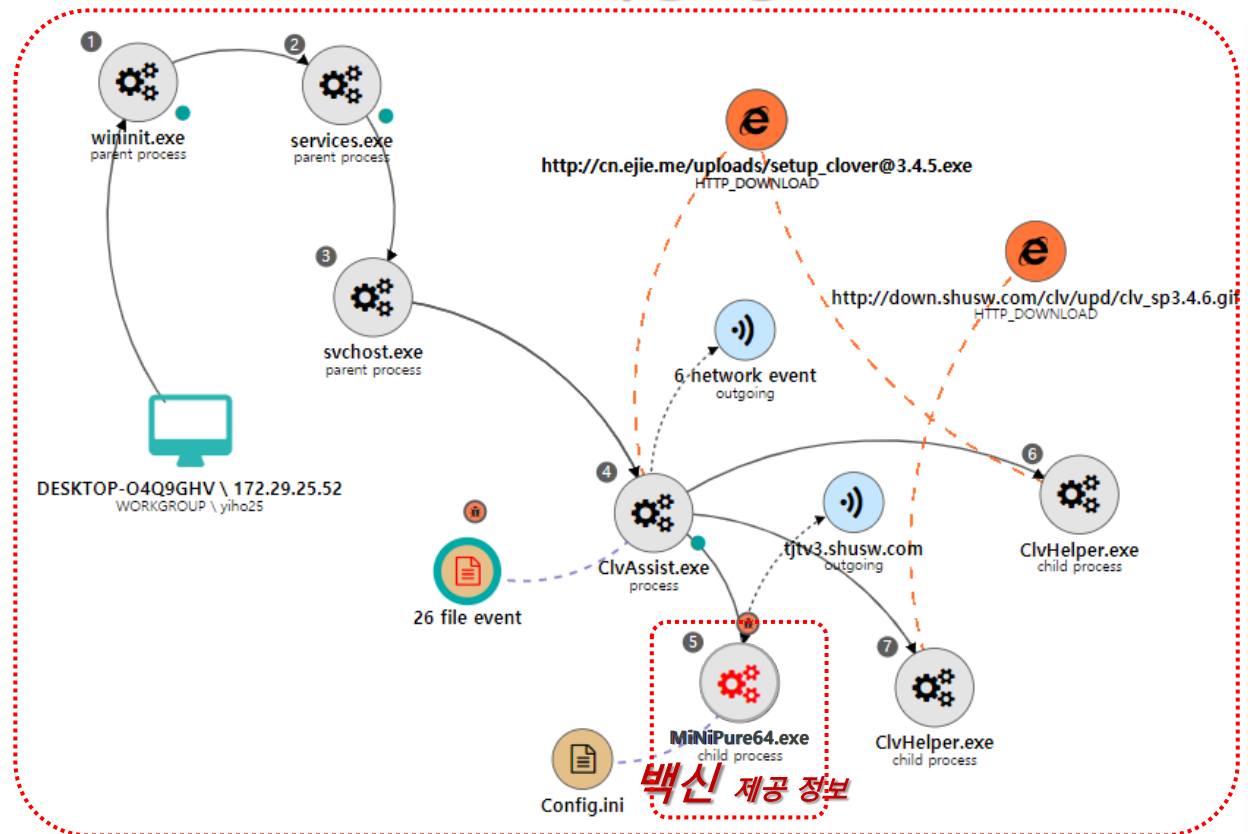
배경 및 필요성

코로나 바이러스의 돌파감염처럼 많은 보안 솔루션이 있음에도 해킹 사고는 줄지 않고 있으며, 백신으로는 역부족인 상황입니다. 백신으로 탐지를 했어도 해당 파일이 언제부터 있었는지, 다른 PC 에도 해당 파일이 있는지, 어떤 정보가 유출이 됐는지, 어떤 파일을 생성했는지 알 수 없습니다.

돌파 감염



EDR 제공 정보

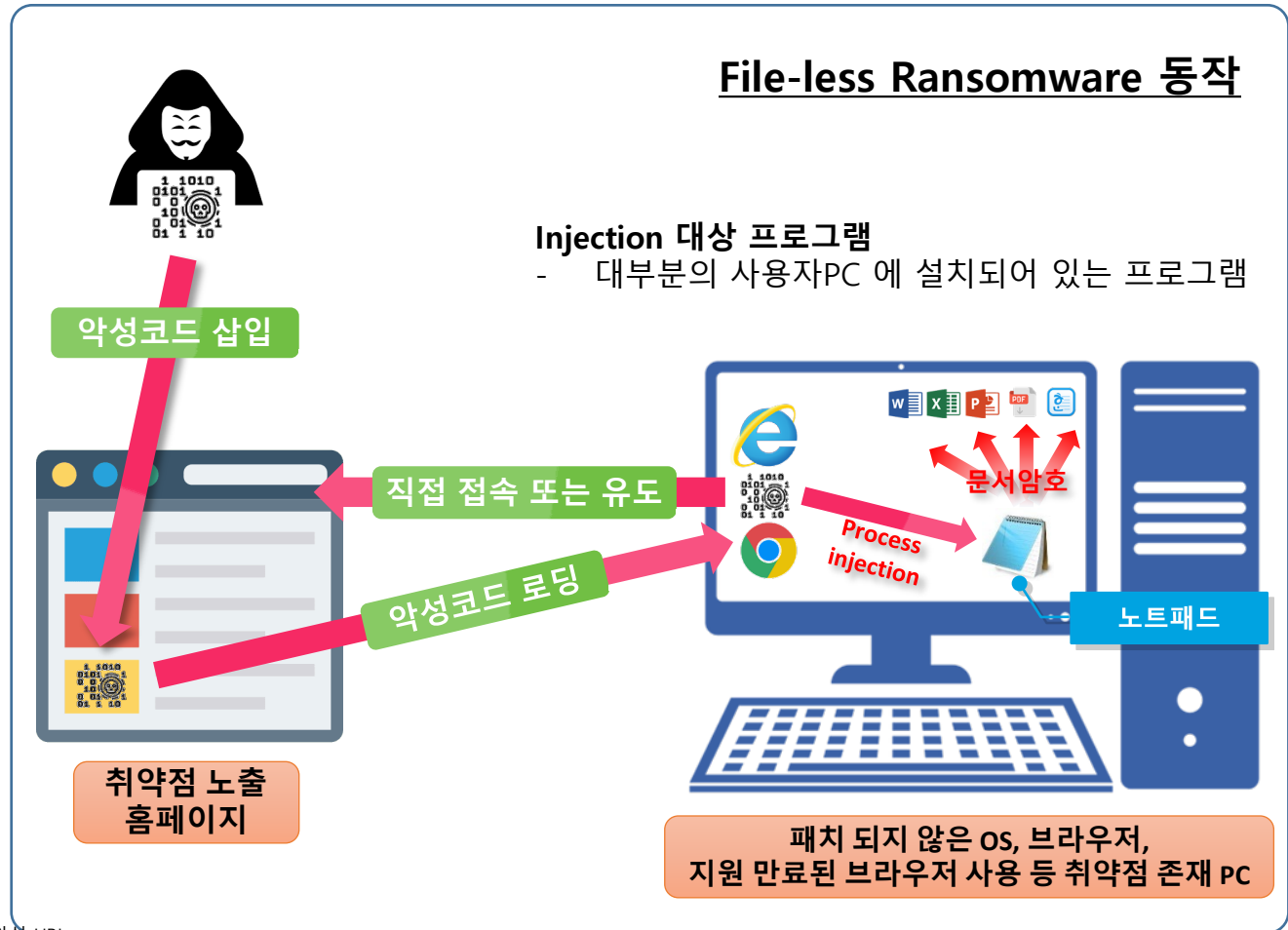


배경 및 필요성

파일만 탐지/대응 하는 시대는 지났습니다. 정상 파일(프로세스)에 의한 이상행위도 탐지할 수 있어야 합니다.



- 유포지 : 악성코드를 직접 유포하는 악성 URL
- 경유지 : 악성코드를 유포하는 유포지로 연결하는 악성스크립트가 삽입된 악성 URL
- Mozi : 2016년 유행한 미라이(Mirai) 악성코드 변종으로 IoT 기기를 감염시켜 DDoS 공격을 수행하는 악성코드
- Emotet : 2014년 독일, 오스트리아, 스위스 등에서 처음으로 발견된 악성코드로 금융 정보 탈취를 목적으로 한 악성코드
- Folina : 원격 템플릿 기능을 활용, MSDT(Microsoft 진단도구) URL을 통해 파워셸을 실행시키는 취약점



02.

Genian EDR 제품 소개

1) 개요

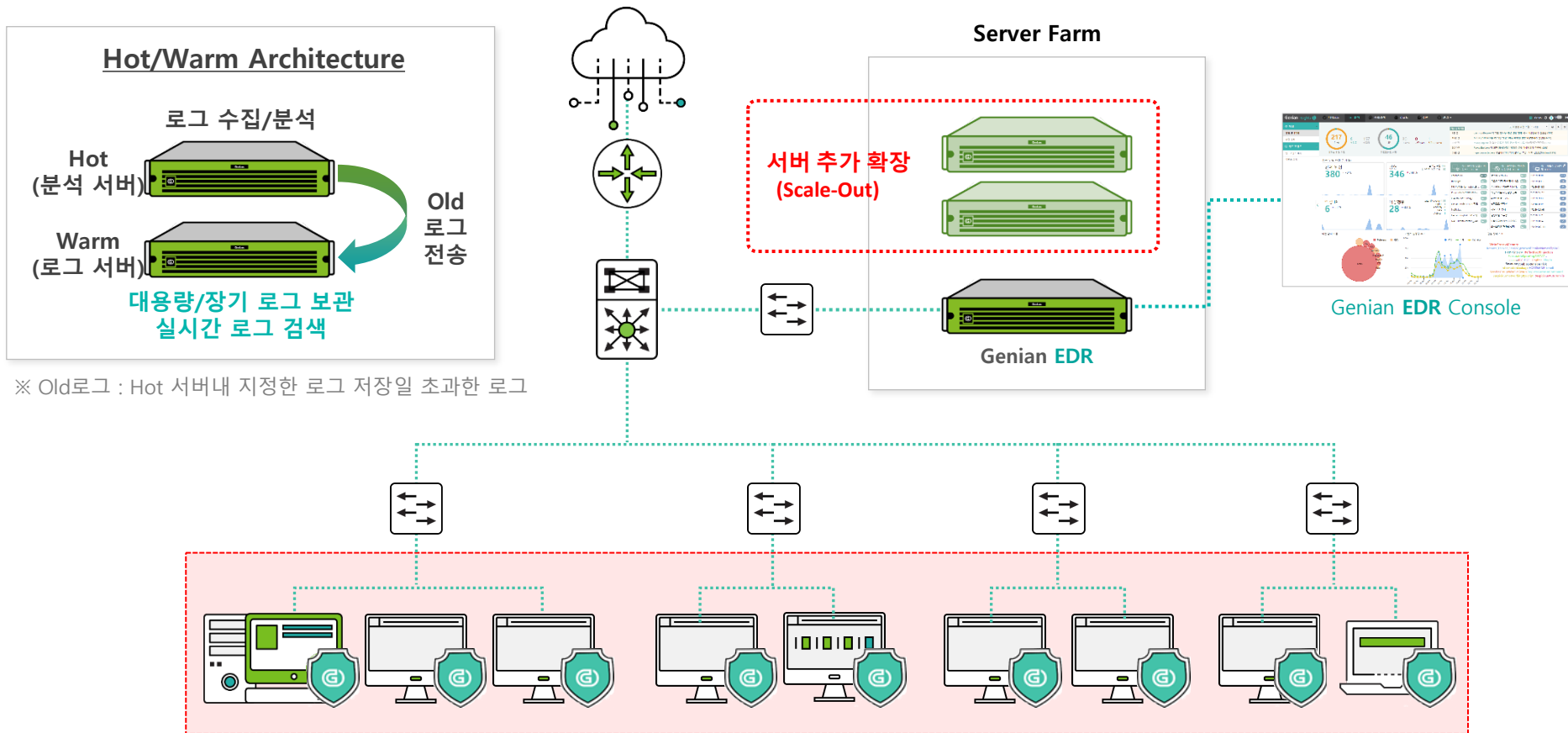
Genian EDR은

단말에 대한 지속적인 모니터링 및 정보 수집을 통해 위협의 탐지 및 분석, 대응을 제공하는 **단말 이상행위 탐지 및 대응 (Endpoint Detection & Response) 솔루션**입니다.



2) Genian EDR 구성

Genian EDR 서버, Agent 의 간단한 구성입니다.
Scale-Out 기능을 제공하여 쉽게 확장 할 수 있습니다.



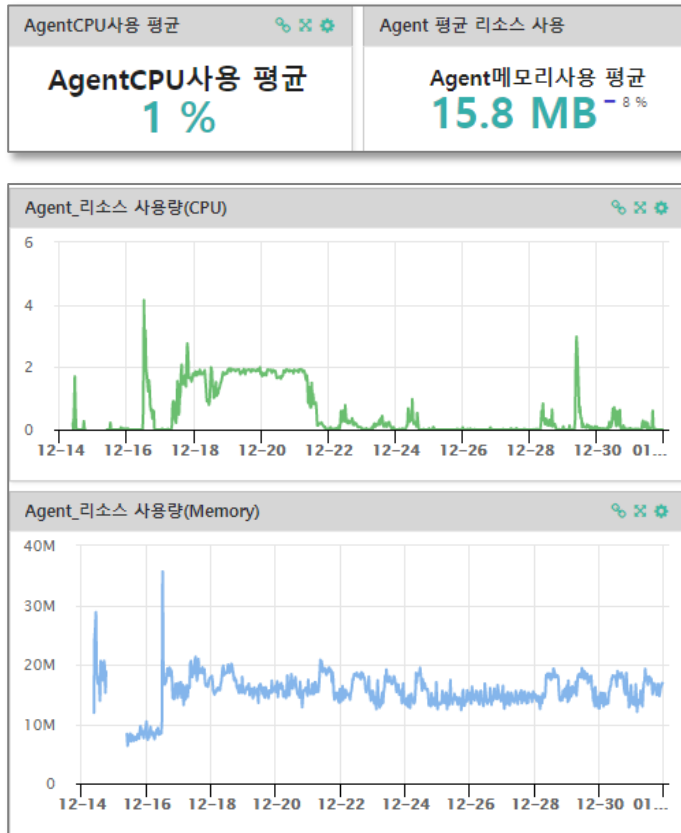
※ Old로그 : Hot 서버내 지정한 로그 저장일 초과한 로그

※ Genian NAC 사용 시, NAC Agent 에 EDR 플러그인(모듈) 형태의 간단한 배포와 인증 정보 자동 연동 기능 제공

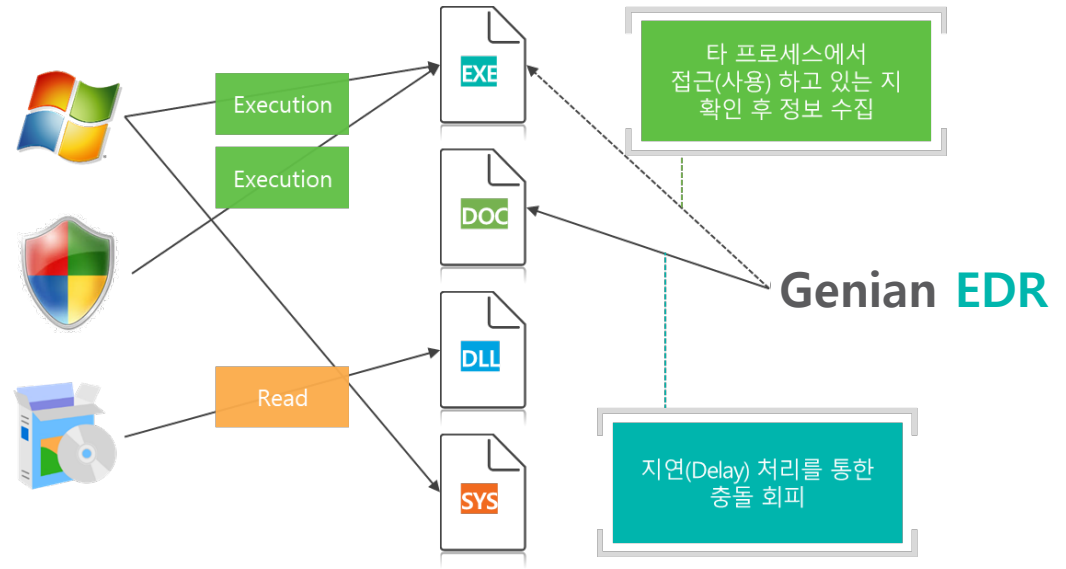
3) Light Agent

Agent는 최소의 리소스를 사용하며, 충돌을 방지하기 위한 충돌 회피 기술이 적용되어 있습니다.

- CPU, MEMORY 최소 사용 동작 및 CPU, Memory 사용을 제한 기능이 있는 Agent
- 확인 처리 기술(타 프로세스의 접근 확인 후 처리), 지연 처리 기술(지연처리하는 기술) 적용으로 타 프로그램의 동작에 영향을 주지 않는 기술 적용

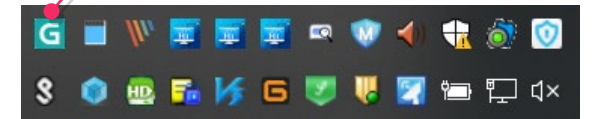


※ 제조사 내부 TEST 결과, 에이전트 100대 평균 리소스 사용률



프로그램명	개요
NAC	Network 접근제어 에이전트
백신관리	백신 중앙관리 에이전트
백신	:000000에서 제공하는 백신 프로그램
DLP	:000000에서 제공하는 정보유출방지프로그램
WPM	자료 영구 삭제 프로그램
SW관리	미 인증 소프트웨어 차단 프로그램
Print0000	출력물보안솔루션
매체제어	:000000에서 제공하는 매체제어 프로그램

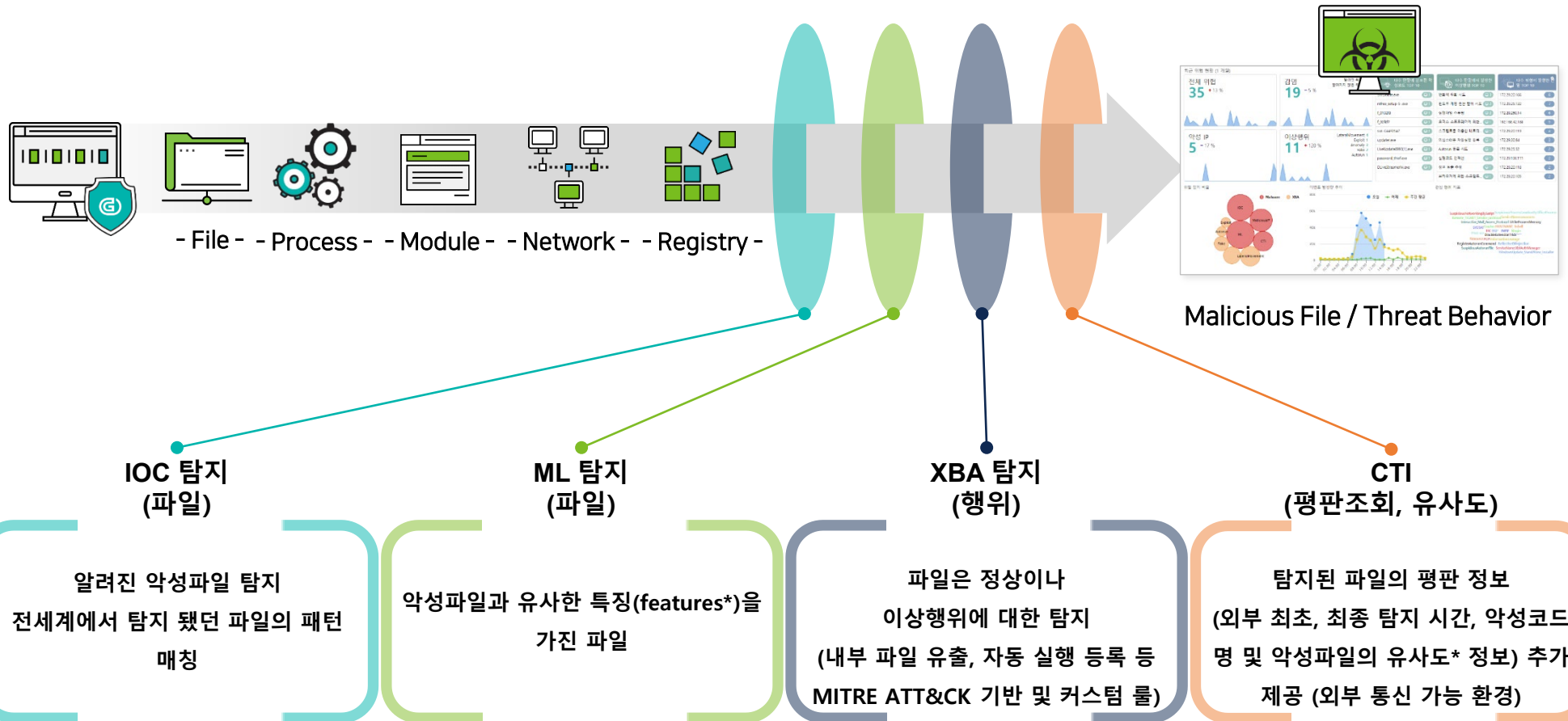
Genian EDR Icon
(On/Off 가능)



다양한 프로그램이 설치된
고객사 PC 환경에서 안정적인 동작

4) 탐지 기술

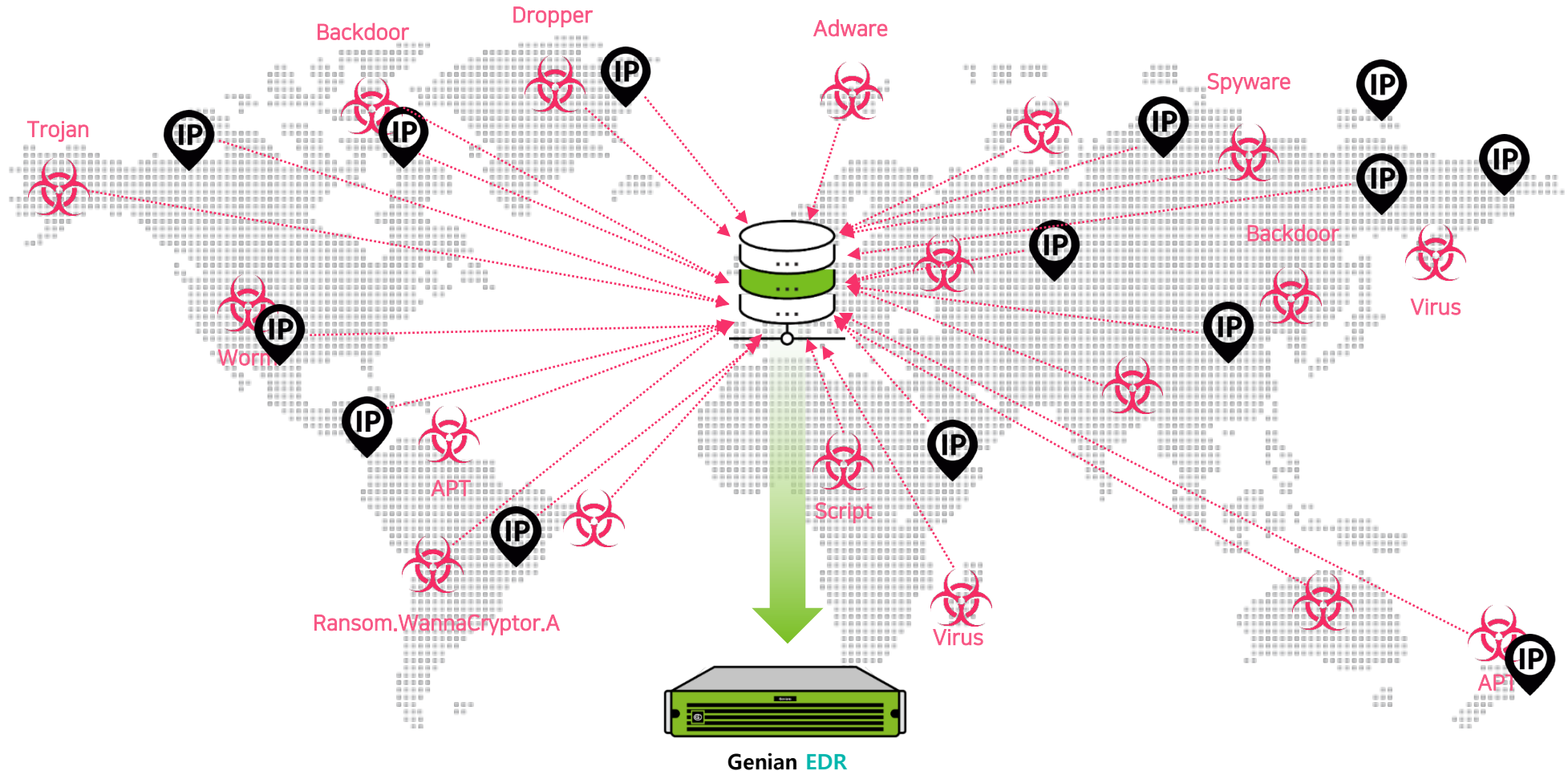
Multi-layer의 탐지 엔진으로 구성이 되어 File 과 이상행위(file-less) 탐지와 함께 분석에 필요한 상세 정보를 제공합니다.



※ PE features : PE 파일은 수십개의 섹션이 있으면 해당 섹션에 특징을 features 라 함
 ※ 유사도 : 탐지된 파일이 어떤 악성코드와 유사한 지에 대한 % 제공 (ssdeep hash)

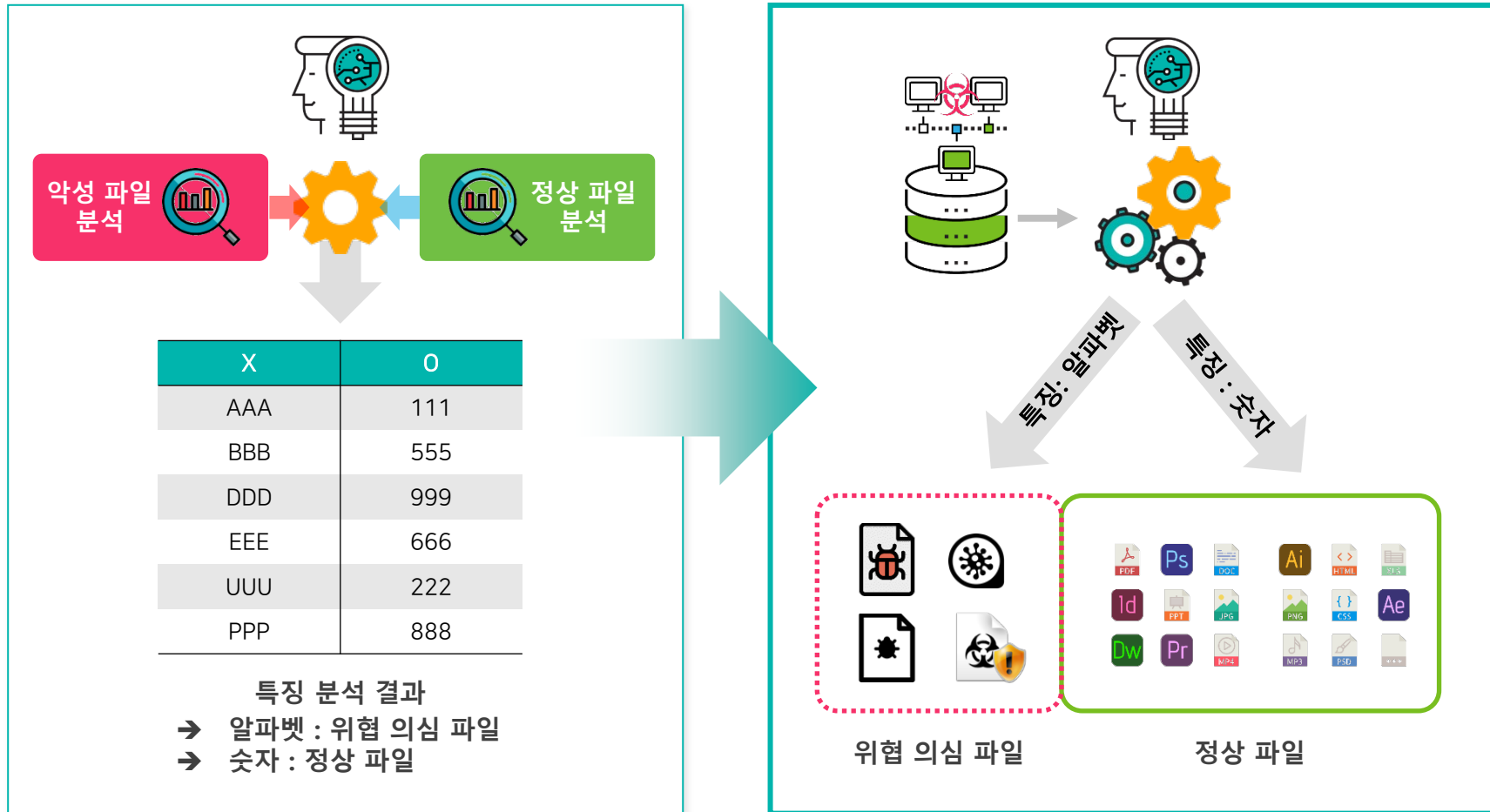
4) 탐지 기술

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.



신규
처리중
해결됨
전체

신규	신뢰도	탐지 시간	탐지 분류	탐지 세부분류	내용	위협 판정	상태	사용자 IP	사용자명	대응	액션
6	30%	2019-12-26 14:22:52	XBA	Anomaly	netsh.exe 에 의한 네트워크 설정 변경 시도 이상...	안전	해결됨	172.29.20.179	이상현		<button>위협 분석</button>
4	30%	2019-12-26 09:26:16	XBA	Anomaly	fswss.exe 에 의한 방화벽 우회 시도 이상행위가 ...	안전	해결됨	172.29.30.110	류지하		<button>위협 분석</button>
4	80%	2019-12-17 14:18:39	XBA	Autorun	eqyrguteroid.exe 에 의한 의심스러운 자동실행 ...			172.29.25.132	이창수		<button>위협 분석</button>
19	30%	2019-12-17 14:18:14	XBA	Anomaly	plugin.exe 에 의한 실행코드 인젝션 이상행위가 ...			172.29.25.132	이창수		<button>위협 분석</button>
	70%	2019-12-17 14:16:13	XBA	Anomaly	cmd.exe 에 의한 자가 삭제 이상행위가 진단됨 (7...			172.29.25.132	이창수		<button>위협 분석</button>
	50%	2019-12-17 14:15:57	XBA	Anomaly	Setup.exe 에 의한 정보 유출 추정 이상행위가 진...			172.29.25...			<button>위협 분석</button>
	95%	2019-12-11 13:41:20	XBA	Fake	ALZip.exe 에 의한 실행파일 스푸핑 이상행위가 진...			172.29.25...			<button>위협 분석</button>
	95%	2019-12-09 16:19:02	XBA	Exploit	net.ps1 에 의한 스크립트를 이용한 네트워크 점...			172.29.25...			<button>위협 분석</button>

위협 요약

탐지 지표 XBA - SYSTEM 에 의한 스텔스 포트 스캐닝 이상행위가 진단됨 (30%)

탐지 엔진 XBA / LateralMovement

수령 프로세스 SYSTEM

이벤트 network / NetworkConnect

태그

요약 내용 스텔스 포트 스캐닝 (StealthPortScanning)

포트 스캐닝은 타겟 PC를 공격하기 전에 정보를 수집하는 고전적인 방법이다. 따라서 포트스캐닝을 탐지하는 것은 Lateral Movement를 탐지하는 중요한 포인트가 된다. nmap 등 일부 포트 스캔 프로그램에서는 탐지를 회피하기 위해 실제로 커넥션을 맺지 않고 포트가 열려있는지 탐지하는 기능을 제공하는데 이러한 기능을 '스텔스 포트 스캐닝'이라고 부른다.

진단사유: 445/TCP, 135/TCP, 139/TCP 등 주요한 포트로 접속하는 INBOUND TCP 커넥션 중에서 SYN, SYN/ACK까지는 진행되었으나, 마지막 ACK가 수신되지 않은 경우 진단

MITRE ATT&CK T1046 - Network Service Scanning

파일 정보

Active HostName GENIANS

IP 172.29.20.119

MAC 00:0E:C6:8F:7B:81

DeviceID 5c5b5f7c-b66d-10...

Platform Microsoft Windows

Domain WORKGROUP

LogonID SYSTEM

AuthName 홍광현

AuthID hyuny0215

AuthDeptNa... EDR기술팀

Plugin version 3.1.1.2466

Create time 2020-01-09 13:12:2

해시 목록

- MITRE 2등 확장자를 이용한 속임수 파일 실행
- MITRE ADS 실행파일 생성
- MITRE ADS 프로세스 실행
- MITRE AppInit_DLL을 이용한 DLL Injection
- MITRE ApplicationShimming을 이용한 UAC Bypass 시도
- MITRE Autoun 등록 시도
- MITRE AV 무적화 시도
- MITRE Exploit에 의한 프로세스 실행
- MITRE Hosts 파일 수정
- MITRE ImageFileExecutionOptions를 이용한 자동실행
- MITRE LateralMovement - at서비스
- MITRE LateralMovement - at서비스
- MITRE LateralMovement - 액작작업
- MITRE LateralMovement - 원격WMI
- MITRE LateralMovement - 원격WMI
- MITRE LateralMovement - 원격서비스
- MITRE LateralMovement - 원격서비스
- MITRE LSA 레지스트리를 이용한 자동 실행
- MITRE netsh.exe를 이용한 자동 실행

연동도

```

graph LR
    Desktop[DESKTOP-33GKBD1] --> Setup[Setup.exe parent process]
    Setup --> Cmd[cmd.exe process]
    Cmd --> Timeout[timeout.exe child process]
    Timeout --> AnotherTimeout[timeout.exe child process]
    
```

MITRE ATT&CK

※ 110가지 이상의 이상행위 탐지 규칙 보유
(MITRE ATT&CK 탐지 를 지속 추가)

기본 룰셋

엔드포인트가 기본적으로 적용받는 룰셋입니다.

랜섬웨어 탐지/제어 정책

카테고리	이름	OS	사용	신뢰도	위협 유형	MITRE ATT&CK Technique
☐	MITRE ShadowCopy 삭제 ?	Windows	☒	90 %	Ransomware	Inhibit System Recovery
☐	MITRE 문서 복사 삭제 임계치 초과 ?	Windows	☒	60 %	Ransomware	Data Encrypted for Impact
☐	MITRE 문서 확장자 Rename 임계치 초과 ?	Windows	☒	60 %	Ransomware	Data Encrypted for Impact

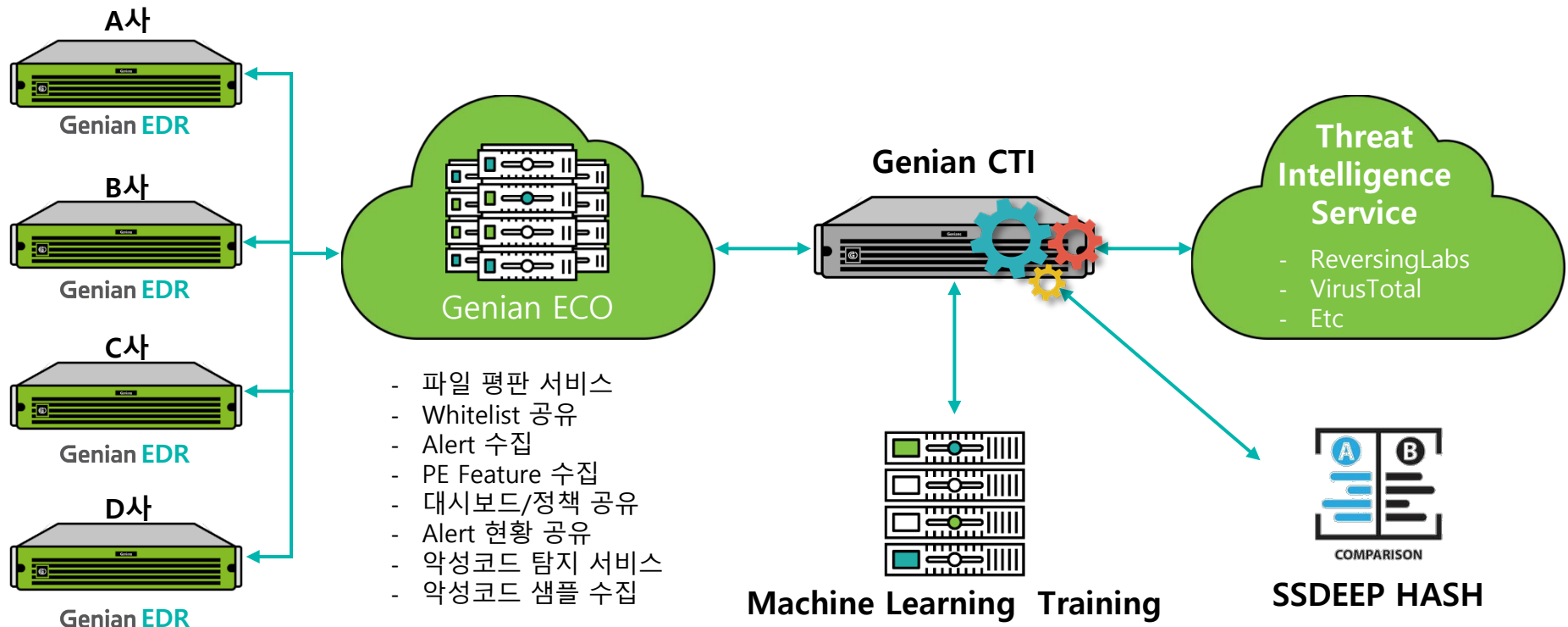
- 기본 제공하지 않는 룰, 필요에 의한 특정 패턴의 룰을 직접 생성 관리



4) 탐지 기술

Ecosystem : Genian 자체의 평판시스템을 제공합니다.

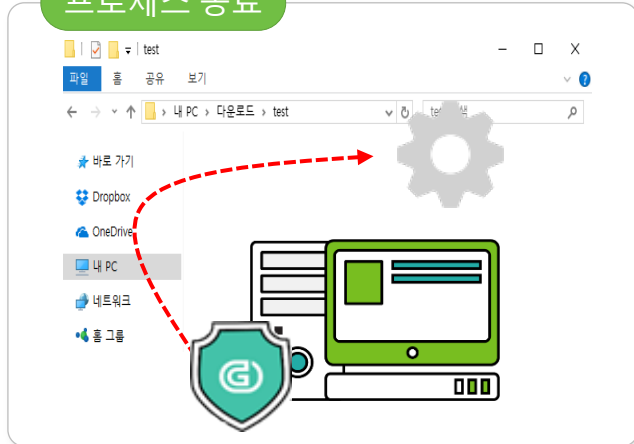
- 오탐 및 최신 악성코드 분석 결과를 고객에게 공유하기 위한 Genian EDR ECO-SYSTEM 구성
- 파일의 근거 (해당 파일이 어떤 역할을 하는 파일인가? 정말 악성인가?) / 오탐 자동 예외 처리
- 지니언스 고객을 통해 수집된 위협과 예외 처리된 데이터를 수집, 가공하여 Genian EDR을 사용하는 모든 고객에게 재배포합니다.
- 이를 통해 Genian EDR을 사용하는 고객들의 오탐을 줄여주며, 위협 혹은 파일 세부 정보 식별이 필요할 때 그 정보를 알려줍니다.



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

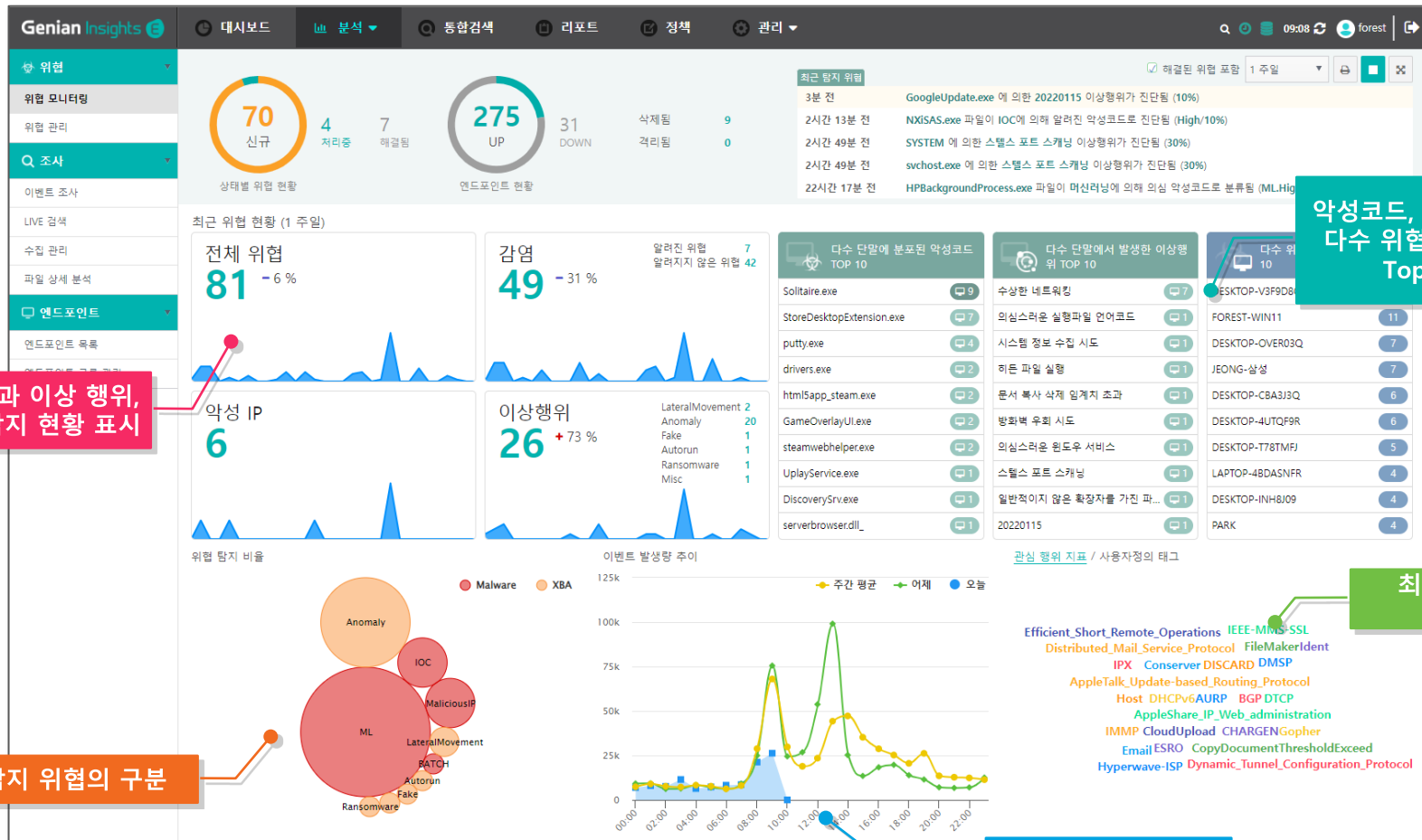


네트워크 격리



6) 분석

전체 위협에 대한 요약 정보를 보여주는 위협 모니터링화면을 제공합니다.

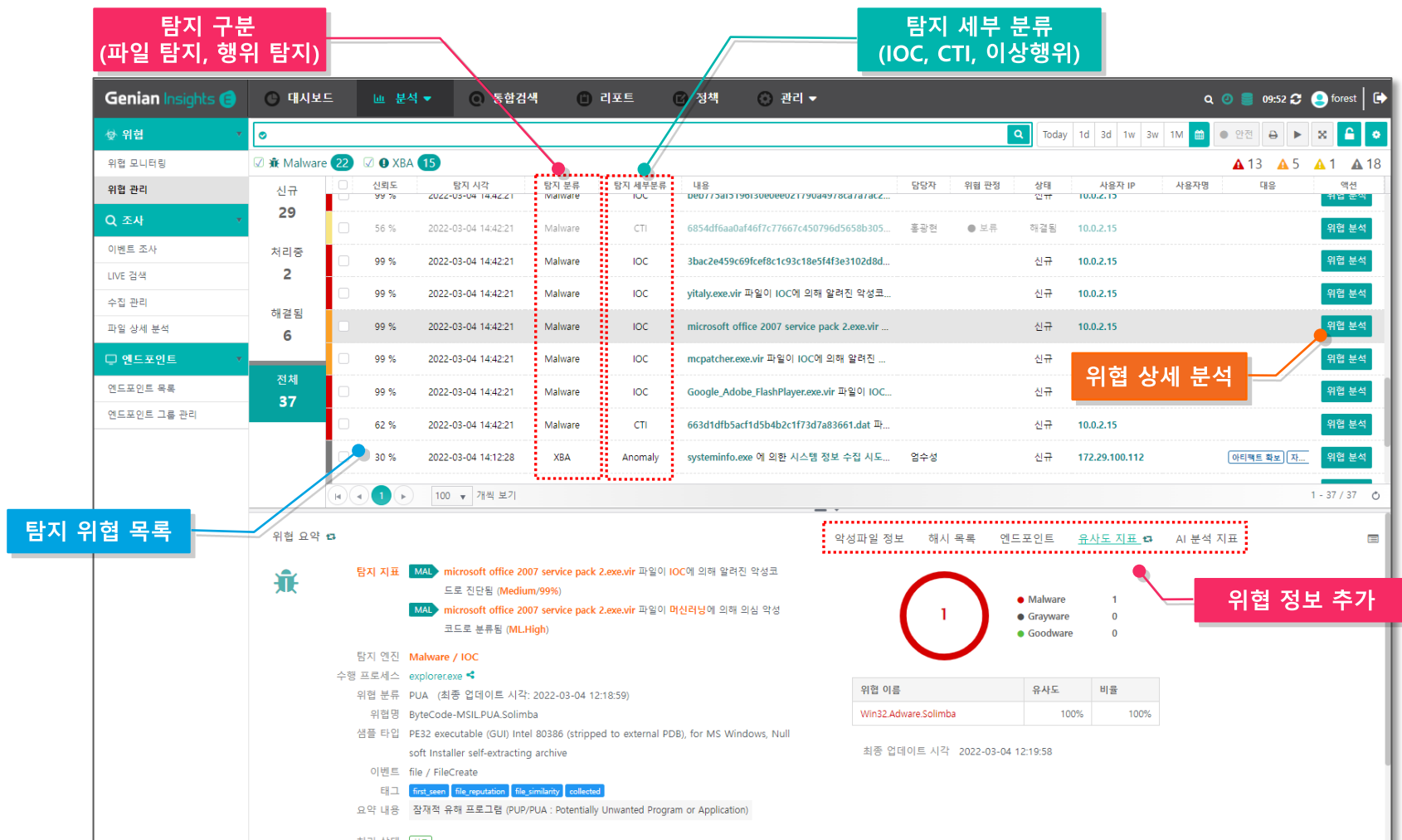


악성코드, 이상 행위,
다수 위협 발생 PC
Top 10

최근 급증한
이벤트

전체 수집 로그 양

탐지된 위협 목록에서의 요약 정보와 상세 분석을 할 수 있는 기능을 제공합니다.



6) 분석

위협 상세 분석에서는 탐지된 파일의 위협 정보와 이상 행위(Fileless) 탐지 시 연관된 MITRE ATT&CK 링크를 제공합니다.

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

기본정보

위협 모니터링: 37ea273266aa2d28430194fca27849170d609d338ab...

위협 관리: 2020-07-07 11:09:52 | Malware / IOC | [강제종료] [말함] [삭제] | file_reputation | file_similarity

탐지 지표

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

37ea273266aa2d28430194fca27849170d609d338ab9c6c43c4e6be1bcf51f9.exe 파일이 머신러닝에 의해 의심 악성코드로 분류됨 (ML:High)

위협 정보

수행 프로세스: Explorer.EXE

위협 분류: PUA (최종 업데이트 시각: 2020-06-29 17:32:29)

위험성: Win32.PUA.Qjwmonkey

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

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

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

탐지 시각

탐지 시작: 2020-06-29 17:31:40

최종 탐지 시각: 2020-07-07 11:09:52

최종 탐지 시각: 2016-09-13 12:55:00

파일 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: 37ea273266aa2d28430194fca27849170d609d338ab9c6c43c4e6be1bcf51f9

전자서명: XBA

Fileless(행위) 탐지 정보

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

탐지 엔진: XBA / Autorun

수행 프로세스: knwuwvx.exe

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

파일경로: C:\Users\GENIAN\1\AppData\Local\Temp\knwuwvx.exe

파일경로2 (if any): C:\Users\GENIAN\1\AppData\Local\Temp\knwuwvx.exe

이벤트: file / FileC

태그: first_seen

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

요약 내용: 의심스러운 자동실행 등록 (SuspiciousAutorunFile)

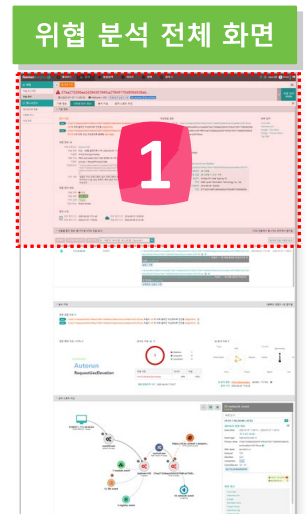
대부분의 악성코드는 다음번 부팅에 다시 실행되기 위해 특정 레지스트리나 시작 프로그램 폴더에 자신을 등록한다. 따라서 부팅시마다 재실행되도록 자신을 등록하는 행위를 집중적으로 모니터링하면 악성코드를 효율적으로 탐지할 수 있다.

전단사유: Autorun 및 서비스 관련 레지스트리 혹은 시작 프로그램 폴더에 다음과 같은 파일이 등록되는 경우

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

MITRE ATT&CK 링크

T1060 - Registry Run Keys / Startup Folder



6) 분석

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

단말별 탐지 정보 (총 1개 중 1개의 단말 표시)

1개의 단말에서 총 2개의 위치에서 탐지됨

단말별 탐지 정보

연관 위험 지표

연관 행위 지표

분석 지표

2종류의 위험이 3번 탐지됨

연관 위험 지표

연관 행위 지표 / TTPs

UacElevation

Autorun

RequestUacElevation

유사도 지표

AI 분석 지표

AI 분석 결과 PUA.Qjwmonkey (48.88% / 73.74%)

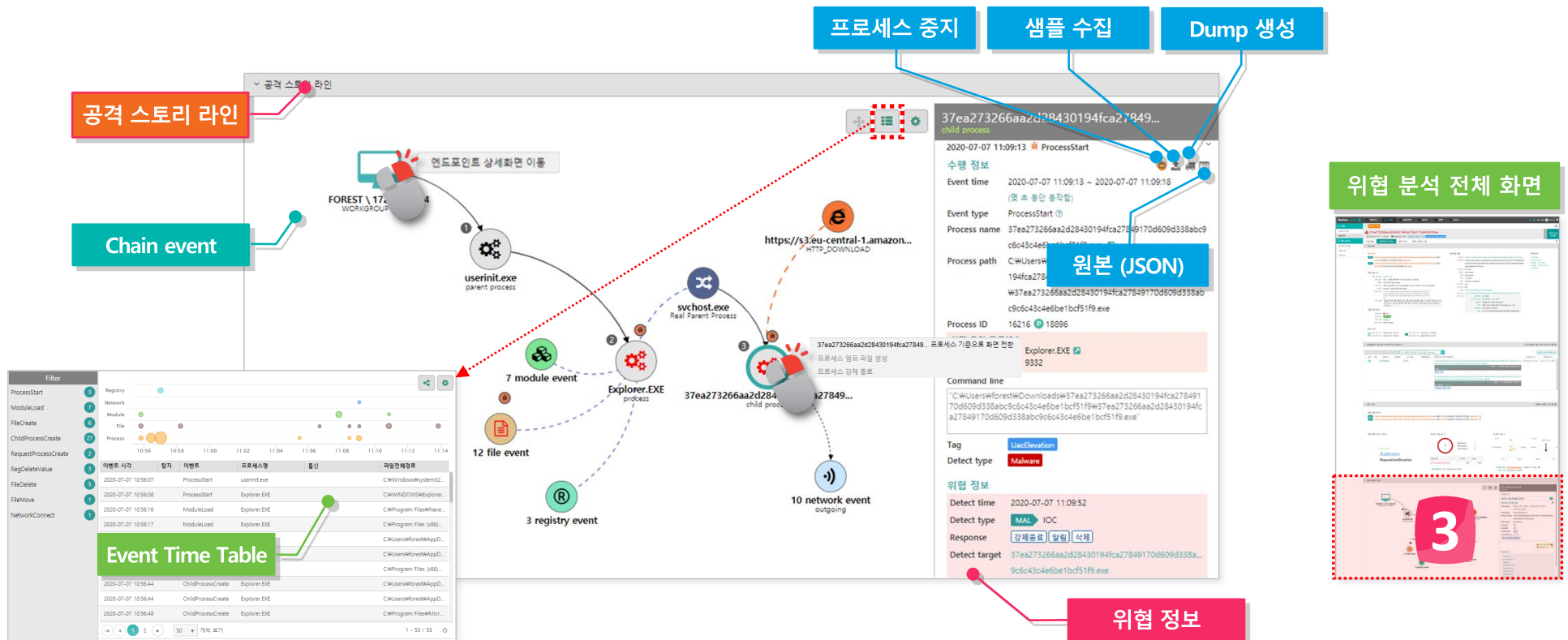
분석 시작 2020-06-29 17:32:28

유사도 지표



6) 분석

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



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

6) 분석

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

rkfree_setup-5.exe

2019-12-24 15:52:51 | Malware / IOC | first_seen | file_reputation | file_size

기본 정보 | 단일별 탐지 정보 | 분석 지표 | 공격 스토리 라인

기본 정보

탐지 지표

- MAL rkfree_setup-5-.exe 파일이 IOC에 의해 알려진 악성 파일입니다.
- MAL rkfree_setup-5-.exe 파일이 머신러닝에 의해 의심 악성 파일입니다.

위협 정보

수행 프로세스 NDSync.exe

위협 분류 Hacktool

위협명 Win32.Hacktool.Revealerkeylogger

샘플 타입 PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed

이벤트 file / FileCreate

요약 내용 컴퓨터 시스템 및 네트워크를 공격하기 위해 해커가 사용할 수 있는 프로그램. 그 자체로는 악의적인 의도가 없는 프로그램.

처리 상태 처리중

탐지 시각

최초 탐지 시각 2019-12-24 15:52:51

최종 탐지 시각 2019-12-24 15:52:51

최초 탐지 시각 2013-08-13

최종 탐지 시각 2019-03-08

위험 관리

rkfree_setup-5-.exe 위협을 관리합니다.
동일한 위협에 대해서 자동화 된 대응을 할 수 있습니다.

신규 | 처리중 | 해결됨

안전 판정

관리 설정

위협 판정

☐ 악성 ☒ 안전 ☐ 보류

악성 여부를 담당자가 판단하여 설정합니다.

메모

메모 입력

메모를 입력합니다.

오탐 보고

☒ 오탐 보고

Genian Cloud에 오탐지 보고합니다.

설정완료 초기화 취소

제조사 오탐보고

위험 관리

rkfree_setup-5-.exe 위협을 관리합니다.
동일한 위협에 대해서 자동화 된 대응을 할 수 있습니다.

신규 | 처리중 | 해결됨

악성 판정

관리 설정

담당자ID forest

위협 판정

☒ 악성 ☐ 안전 ☐ 보류

악성 여부를 담당자가 판단하여 설정합니다.

대응 정책

대응 정책

동일한 위협 발생시 대응 정책을 설정합니다.

자동해결

☒ 자동해결

발표 동일한 위협 발생시 자동으로 [해결됨] 상태로 변경합니다.

메모

메모 입력

메모를 입력합니다.

설정완료 초기화 취소

악성 자동 대응

코멘트

Comment를 입력합니다.

추가

History

Comment를 입력합니다.

추가

2020-01-08 13:00:10 담당자가 forest으로 변경되었습니다.

2020-01-08 13:00:10 위협 관리상태가 "처리중"으로 변경되었습니다.

감사로그

서명날짜 2013-08-07 21:52

지문 7D52F92D69F124

E352A27F1E09AA

708F9DEB

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 14:00:00	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 14:19:52	FileCreate	msiexec.exe		a99b40d.msi	
2020-01-02 14:19:51	FileCopy	msiexec.exe		a99b087.msi	
2020-01-02 14:19:51	FileCreate	msiexec.exe		a99b40d.msi	
2020-01-02 14:19:51	RegSetValue	msiexec.exe			
2020-01-02 14:19:51	RegCreateKey	msiexec.exe			

검색 결과

등록된 검색 조건

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

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

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.

Genian Insights | 대시보드 | 분석 | 통합검색 | 리포트 | 정책 | 관리

검색조건 (Raw data 검색)

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

Tag 조건 검색

Tag:*

검색조건 (tag 검색)

Tag:FolderShare

Tag 종류

이벤트 시작 | 사용자IP | 탐지 | 이벤트 상세 분류 | 이벤트 요약

이벤트 시작	사용자IP	탐지	이벤트 상세 분류	이벤트 요약	사용자정의 태그	사용자명	호스트명
2022-12-26 09:20:48.334	172.29.100.74	RegSetValue	HKEY_USERSWS-1-5-21-580710875-3074094699-2807007434-1001WSof...	LastLaunchedApplis...			FOREST
2022-12-26 09:20:48.333	172.29.100.74	RegSetValue	HKEY_USERSWS-1-5-21-580710875-3074094699-2807007434-1001WSof...	LastLaunchedApplis...			FOREST
2022-12-26 09:20:48.190	172.29.30.159	ProcessStart	services.exe 프로세스에 의해 svchost.exe 프로세스가 시작되었습니다.	ServiceStart		구...	LAPTOP
2022-12-26 09:20:48.163	172.29.30.159	ProcessStart	services.exe 프로세스에 의해 svchost.exe 프로세스가 시작되었습니다.	ServiceStart		구...	LAPTOP
2022-12-26 09:20:47.606	172.29.30.159	RegSetValue	HKEY_USERSWS-1-5-21-2299071116-4030902283-2756338911-1001WS...	Autonun		구...	LAPTOP
2022-12-26 09:20:47.605	172.29.30.159	RegDeleteValue	HKEY_USERSWS-1-5-21-2299071116-4030902283-2756338911-1001WS...	Autonun		구...	LAPTOP
2022-12-26 09:20:46.821	10.35.100.52	ProcessStart	TouchpointAnalyticsClient.exe 프로세스에 의해 cmd.exe 프로세스가 시작...	cmd		구...	DESKTO
2022-12-26 09:20:43.437	172.29.30.159	TerminateProcess	msedge.exe 가 identity_helper.exe를 종료했습니다.			구...	LAPTOP
2022-12-26 09:20:41.933	10.35.100.52	DocOpen	Hwp.exe 프로세스가 C:\Users\Wskjja\Downloads\W20221200383-00_166...	DocOpen			DESKTO
2022-12-26 09:20:39.043	192.168.0.54	FileCreate	GoogleUpdate.exe 프로세스가 C:\Program Files (x86)\Google\W\Policies...	DirCreate			SECUM/
2022-12-26 09:20:38.237	192.168.10.24	ProcessStart	services.exe 프로세스에 의해 bookingDesktopAppUpdate.exe 프로세스...	ServiceStart		김...	DESKTO
2022-12-26 09:20:38.237	192.168.0.54	ProcessStart	services.exe 프로세스에 의해 svchost.exe 프로세스가 시작되었습니다.	ServiceStart			SECUM/
2022-12-26 09:20:35.100.52	10.35.100.52	HttpDownload	https://www.g2b.go.kr:8081/ep/co/fileDownload.do?fileTask=NOTIFY&...	ZoneIdentifier			DESKTO
2022-12-26 09:20:25.023	10.35.100.52	ProcessStart	TouchpointAnalyticsClient.exe 프로세스에 의해 schtasks.exe 프로세스가 ...	TaskScheduler			DESKTO
2022-12-26 09:20:24.123	172.29.109.22	NetworkConnect	svchost.exe 프로세스가 172.29.62.67:54065 로 TCP : Incoming 통신을 했...	WUDD\Windows_Update_Delivery_Optimization			SEONG\

Tags

7) Agent 관리

설치된 Agent 현황 파악

Genian Insights 대시보드 분석 통합검색 리포트 정책 관리

조건 검색

조직도

단말기 선택 후 제어 옵션 활성화

단말기 리소스

엔드포인트 히스토리

Agent 현황

동작	상태	호스트명	사용자 IP	MAC	플랫폼	사용자명	부서명
☒	UP	WIN11-TEST	10.0.2.123	08:00:27:3C:FA:ED	Microsoft Windows 10 Professional x64		
☒	UP	FOREST_VM_2016	10.0.2.16	08:00:27:D3:7F:72	Microsoft Windows 2016 x64		
☒	UP	HEART	172.29.111.192	10:E7:C6:E8:82:CE	Microsoft Windows 10 Professional x64	신	기술지
☒	UP	SHREWD	172.29.123.102	00:E0:81:35:D2:2F	Microsoft Windows 10 Professional x64	shrewd	
☒	UP	HYUNY			Microsoft Windows 10 Home x64		
☒	UP	DESKTOP-CBA3J3Q	172.29.30.158	00:E0:4C:68:01:BF	Microsoft Windows 10 Professional x64	Super Admini...	
☒	UP	DESKTOP-5C6AUQV	172.29.30.76	00:E0:4A:69:C4:93	Microsoft Windows 10 Professional x64	조	사업1팀
☒	UP	DESKTOP-POD1VJC	172.30.20.202	10:E7:C6:E8:82:D4	Microsoft Windows 10 Professional x64		

단말기 리소스

PC 리소스

Agent 리소스

엔드포인트 히스토리

8) 수집관리

위협/의심파일(PE)은 선택에 따라 자동/수동 수집하고 필요시 artifact 를 수집하는 기능을 제공합니다.

탐지된 위협 파일은 사용자 PC 에서 자동/수동 업로드 (위협이 아닌 지정한 PE 파일 수동 수집 기능 제공)
필요시 특정 사용자 PC 의 artifact 수집

Artifact 수집

타입 (File, Threat, Artifact 등)

자동/수동 수집 위협(의심)파일

샘플파일 다운로드

수집 정보 목록

Artifact 항목

상세 정보

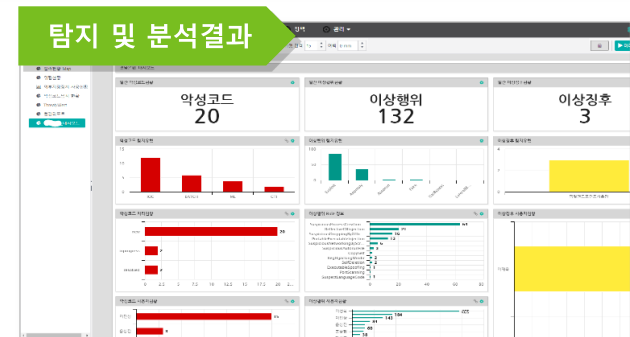
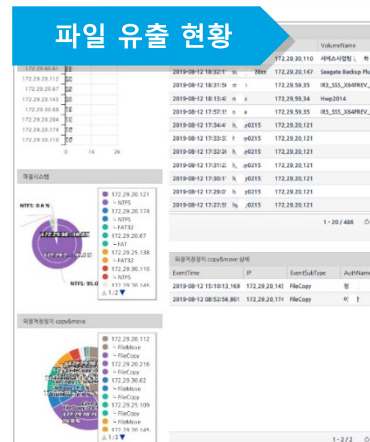
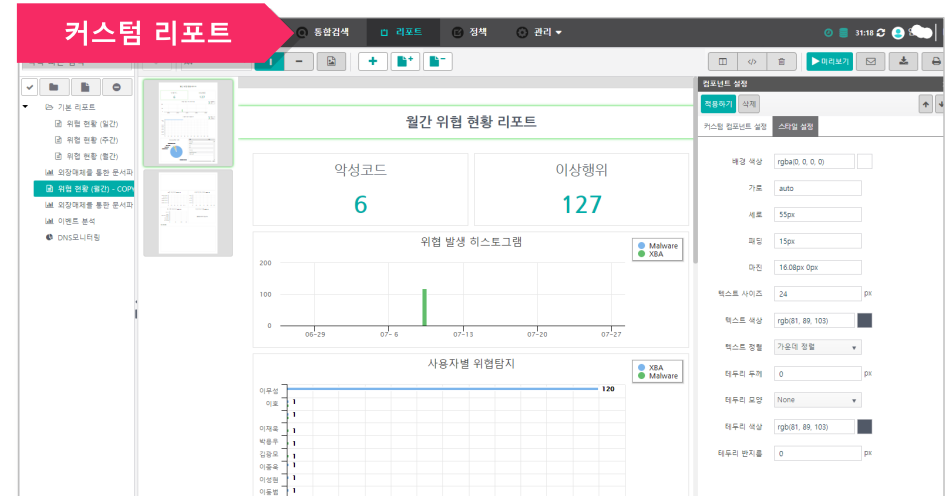
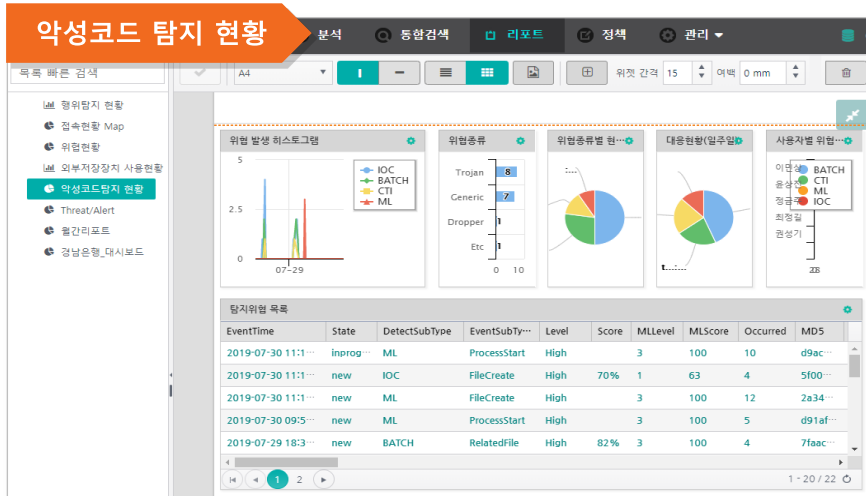
Artifact

포렌식 분석을 위하여 특정 시점(위협 발생 시)의 다양한 정보를 수집하여 관리자가 쉽게 확인 할 수 있는 화면을 제공합니다.

(시스템 정보, 브라우저 방문 기록, 자동 실행 목록, 윈도우 이벤트, prefetch 파일, 파일시스템, 레지스트리 하이버)

9) 리포트

기본 제공 리포트와 대시보드를 리포트로 변환할 수 있습니다.
리포트는 관리자가 직접 생성/수정할 수 있도록 다양한 옵션을 제공합니다.



파일의 상세 정보, 문자열, 위협정보, PE정보, 전자서명, 최근 1달간 파일의 히스토리 정보 등



Genians

11) Live 검색

현재 PC 내에 존재하는 파일, 레지스트리를 검색하여 결과를 보여줍니다.

사용자 PC 내의 파일, 레지스트리를 다양한 조건 검색

Genian Insights EDR

+ 신규 검색 | 지난 검색 결과 찾기

[신규 검색] 버튼을 클릭하여 새로운 검색을 시작하거나 이전 검색 결과를 확인 할 수 있습니다.

Live 검색

검색 항목 선택 (File, Registry)

Agent 선택 (전체, 그룹 별)

검색 조건 설정

검색 결과

파일명이 GsAgent.exe와 같으면

2021-09-23 10:21:10 ~ 검색 항목명 2021-09-23 (완료됨)

빠른 파일 검색 | 6 / 15

9 종파 | 0 시작 | 0 실패 | 6 종료 | 15 전체

5개의 엔드포인트에서 건이 검색됨

파일명 Top10

파일명	Count
gsagent.exe	6
gsagent.exe	1

IP Top10

IP	Count
172.30.10.59	3
172.28.111.192	1
172.28.123.104	1
172.30.28.251	1
192.168.0.16	1

사용자 Top10

사용자	Count
인도식	6
인도식	1

검색 결과 테이블

검색 시간	IP	사용자ID	사용자명	부서명	파일명	파일사이즈	파일바이트
2021-09-23 12:49:06	192.168.0.16				GsAgent.exe	1.9 MB	2.0.16.564
2021-09-23 10:21:10	172.28.123.104				GsAgent.exe	1.9 MB	2.0.16.564
2021-09-23 10:21:10	172.30.111.192	dishin	인도식	기술직팀	GsAgent.exe	1.9 MB	2.0.16.564
2021-09-23 10:21:09	172.30.10.59				GsAgent.exe	1.9 MB	2.0.16.564
2021-09-23 10:21:09	172.30.10.59				gsagent.exe	1.1 MB	2.0.16.564
2021-09-23 10:21:09	172.30.10.59				GsAgent.exe	1.5 MB	2.0.16.564
2021-09-23 10:20:57	172.30.20.251	sue11041			GsAgent.exe	1.9 MB	2.0.16.564

상세정보

파일 정보

검색 시작: 2021-09-23 10:21:10

파일명: GsAgent.exe

파일사이즈: 1.9 MB (2,035,256 bytes)

파일경로: C:\Program Files\Genian\Genian\GsAgent.exe

파일설명: Genian Insights E Agent for Windows

파일버전: 2.0.16.564

대부분의 파일명: 2.0.16.564

생성 시작: 2021-06-17 17:16:16

수정 시작: 2021-09-14 16:18:42

사용자 정보

IP: 172.28.123.104

호스트명: HYUNV0215

도메인: WORKGROUP

로그온ID: [redacted]

사용자명: [redacted]

12) VSS 관리

윈도우의 Window shadow copy 백업/복원 (Volume Shadow Copy Services) 서비스를 관리합니다.

사용자 PC 의 데이터를 디스크 내의 특정 용량 이내, 몇일, 백업 수행 시간 설정으로 snapshot 저장

백업

Windows VSS 백업

사용

사용안함

VSS 실행 옵션

랜섬웨어 공격에 대비하여 Windows VSS(Volume Shadow Copy Service)를 사용한 하드디스크 파일 전체에 대한 백업을 진행합니다. (1일 1회)

본 기능 사용 시에는 랜섬웨어에 의해 스냅샷이 삭제되지 않도록 정책 > 이상행위 관리 > 이상행위 를 관리 화면에서 "ShadowCopy 삭제" 및 "문서 초 Rename 임계치 초과" 등의 '자동대응' 을 설정하시기 바랍니다.

백업에 사용할 최대 용량 (MB)

6000 MB

백업에 사용할 최대 용량을 설정합니다. (0: 사용안함)

백업에 사용할 최대 용량 (%)

5 %

백업에 사용할 하드디스크 용량의 퍼센트를 설정합니다. (0: 사용안함)

보관할 백업의 수*

5 개

보관할 백업의 수를 설정합니다. (1 - 64)

수행 대기 시간*

600 초

설정 시간 동안 사용자 입력이 없으면 백업이 진행됩니다. (300 - 3600)

수행 시간

Off

지정된 시간 중에 사용자 입력이 없으면 백업이 진행됩니다.

ShadowCopy 생성

```
[FOREST] C:\Program Files\Geni\Insights> shadowcopy /create
스냅샷 생성에 성공하였습니다. (패키지ID : 1)

생성된 스냅샷 정보 :
패키지ID    볼륨    스냅샷ID    생성일    상태
-----
1           C:\    {e1fc0cfe-c647-4741-a5a3-bbd9114328b9}  2021-01-21 17:28:32  SUCCESS
1           D:\    {53bd8491-df53-46e2-80fb-95d930e6bbb1}  2021-01-21 17:28:38  SUCCESS
1           E:\    {fee06af8-bf17-4e9f-9505-762c869fefcd}  2021-01-21 17:28:45  SUCCESS

[FOREST] C:\Program Files\Geni\Insights>
```

```
[DESKTOP-2E60RNR] C:\Program Files\Geni\Insights> shadowcopy /create C:
스냅샷 생성에 성공하였습니다. (패키지ID : 4)

생성된 스냅샷 정보 :
패키지ID    볼륨    스냅샷ID    생성일    상태
-----
4           C:\    {4b2db4a0-0c09-4135-8d52-eb07ac4a89aa}  2021-01-21 18:25:51  SUCCESS

[DESKTOP-2E60RNR] C:\Program Files\Geni\Insights> shadowcopy /restore /all 4
스냅샷 {4b2db4a0-0c09-4135-8d52-eb07ac4a89aa} 이 "C:\vss\{4b2db4a0-0c09-4135-8d52-eb07ac4a89aa}" 에 마운트되었습니다.
의 복원 작업이 시작되었습니다.
복원 작업은 백그라운드로 진행되며, 복원 완료 시 결과가 감사 로그에 기록됩니다.

[DESKTOP-2E60RNR] C:\Program Files\Geni\Insights>
```

ShadowCopy 복원

▶ 2021-02-15 17:17:18	192.168.0.19	CC:3D:82:34:D1:E0	ShadowCopy 복원 완료 (총 35 파일 복원됨). VOLUME='D:\'
▶ 2021-02-15 17:17:18	192.168.0.19	CC:3D:82:34:D1:E0	ShadowCopy 복원 시작. VOLUME='D:\'
▶ 2021-02-15 17:17:17	192.168.0.19	CC:3D:82:34:D1:E0	명령 전송됨. COMMAND='shadowcopy /restore /all 3', SESSIONID='forest_20210215171620808', ID='fore...
▶ 2021-02-15 17:16:33	192.168.0.19	CC:3D:82:34:D1:E0	ShadowCopy 스냅샷 생성 성공 (D:\).
▶ 2021-02-15 17:16:32	192.168.0.19	CC:3D:82:34:D1:E0	명령 전송됨. COMMAND='shadowcopy /create D:', SESSIONID='forest_20210215171620808', ID='forest', I...

Genians

31

13) 안티랜섬웨어 기능

윈도우 볼륨 새도우 카피보다 효율적이고 고도화된 안티랜섬웨어 기능을 제공합니다.

실시간 탐지 및 백업과 복원 기능 제공 (추가 라이선스 필요함)

안티랜섬 기능 사용 **사용** **사용안함**

에이전트 자체 업데이트 기능을 통하여 안티랜섬 기능이 설치됩니다. 에이전트 자체 업데이트 기능을 사용하지 않는 경우에는 PMS등의 외부 배포를 이용하여 안티랜섬 기능 사용 시에는 랜섬웨어에 의해 안티랜섬 기능이 정지되지 않도록 **정책 > 에이전트 > 자체 보호** 기능을 **사용**으로 설정해야 합니다.

운영모드 **Active 모드**

Monitoring 모드 : 랜섬웨어가 행위기반 진단되더라도 대응(강제종료, 삭제 등)하지 않습니다.
Active 모드 : 랜섬웨어를 행위기반 진단하고 대응(강제종료, 삭제 등)합니다.
Active 모드 사용 시에는 랜섬웨어에 의하여 변조된 파일들이 올바르게 복구 될 수 있도록 하기 이상행위 틀들에 대한 대응정책 > 이상행위 관리 > 이상행위 틀셋 관리 화면에서 "문서 복사 삭제 임계치 초과" 및 "문서 확장자 Rename 임계치 초과"를 설정합니다.

실시간 보호 **사용** **사용안함**

랜섬웨어를 실시간 모니터링하고 행위기반 탐지합니다.

파일백업 **사용** **사용안함**

보호대상 파일이 변조될 경우 백업하고, 랜섬웨어가 행위기반 진단되면 백업합니다.

백업률도 보호 **사용** **사용안함**

백업된 파일 및 관련 파일이 랜섬웨어에 의해 훼손되지 않도록 보호합니다. 수동 복원 등 꼭 필요한 상황에서만 off하시기 바랍니다.

MBR 보호 **사용** **사용안함**

일부 랜섬웨어는 파일 암호화 행위 이외에 마스터 부트 레코드(MBR)을 변조하여 시스템 부팅 자체를 방해하는 행위를 진행합니다. MBR 보호 기능을 통하여 MBR 변조 행위를 방지합니다.

예외 프로세스 설정 **+ 추가**

예외 프로세스 전체 경로	설정

예외 프로세스 전체 경로를 설정합니다.

백업 이전

감염된 파일

랜섬웨어 감염 직전 실시간 백업

랜섬웨어 감염 후

자동 복원

랜섬웨어 실시간 대응 후

☐	MITRE	안티랜섬 MBR 보호 기능에 의한 MBR 쓰기 차단	90 %	Ransomware	Data Encrypted for Impact
☐	MITRE	안티랜섬 실시간 보호 기능에 의한 프로세스 실행 차단	90 %	Ransomware	Data Encrypted for Impact
☐	MITRE	안티랜섬 실시간 보호 기능에 의한 행위기반 탐지	90 %	Ransomware	Data Encrypted for Impact

14) QoS 기능

Agent 업그레이드, 이벤트 전송 시 QoS 기능으로 네트워크 부담 없이 배포, 전송할 수 있습니다.

다양한 옵션 및 그룹 관리를 통해 agent 업그레이드 및 이벤트 전송 시 네트워크에 부담을 주지 않는 옵션

The screenshot displays the Genian Insights EDR interface with several key sections highlighted to demonstrate QoS functionality:

- Agent 자동 업그레이드 (Agent Automatic Upgrade):** A blue arrow points to the '에이전트 배포 관리' (Agent Deployment Management) menu item in the left sidebar.
- 에이전트 배포 QoS (Agent Deployment QoS):** An orange arrow points to the '에이전트 배포 QoS' settings section, which includes a table of agent groups and their deployment status.
- 이벤트 전송 QoS (Event Transmission QoS):** A green arrow points to the '이벤트 전송 QoS' settings section, which includes a table for event transmission QoS settings.
- 다양한 옵션 (Various Options):** A pink arrow points to the '배포 설정' (Deployment Settings) section, which includes options for agent version, automatic upgrade, and event transmission.
- 네트워크 환경이 열악한 지점 등 적용에 용이함 (Easy application in areas with poor network environment, etc.):** A text box highlights the '이벤트 전송 QoS' settings, noting that the QoS can be set to 0 to prevent network congestion.

에이전트 배포 관리 (Agent Deployment Management) Table:

완료	동작	상태	에이전트 버전	호스트명	액션
☐			2.0.21.1227-25658	WIN11-TEST	
☐			2.0.21.0110-25962	DESKTOP-IL6DL8C	
☐			2.0.21.1227-25658	SHREWD	
☐			2.0.21.0110-25962	DESKTOP-CBA3J3Q	

이벤트 전송 QoS (Event Transmission QoS) Table:

수집	탐지	대응	에이전트
이벤트 전송 QoS	0	KB/s	

네트워크 환경이 열악한 지점 등 적용에 용이함 (Easy application in areas with poor network environment, etc.):

이벤트 전송 QoS를 0로 설정하면 이벤트 전송 시 네트워크 부하를 줄여줍니다. (0 - 8096)
QoS가 0인 경우 QoS가 OFF되어 이벤트가 빠르게 전송되고, 0 이상인 경우 지정된 Bps만큼 느리게 전송됩니다.

15) 연동

Syslog, SNMP, Rest API 를 지원, 타 시스템과 다양한 연동을 지원합니다.

※ Syslog, SNMP 설정

The screenshot displays the Genian Insights web interface with the '관리' (Management) tab selected. The left sidebar contains navigation options: 사용자 관리 (User Management), 속성 관리 (Attribute Management), 환경 설정 (Environment Settings), and 외부 연동 (External Integration). The main content area shows the 'Syslog 서버 설정' (Syslog Server Settings) dialog box, which includes fields for '사용' (Use) toggle, '서버 IP' (Server IP), '프로토콜' (Protocol) dropdown (set to UDP), '전송 포트' (Transmission Port) dropdown (set to 514), '중계 서버 IP' (Relay Server IP), '인덱스 선택' (Index Selection), '타임존' (Timezone) dropdown (set to Asia), and '필터 설정' (Filter Settings). Below this, the 'SNMP Agent 설정' (SNMP Agent Settings) section shows the '사용 여부' (Use) toggle set to 'On'. It includes fields for 'Username' (insights), 'Auth Password', and 'Priv Password', each with a strength indicator. A blue callout box labeled 'Syslog 설정' is positioned over the Syslog settings, and another labeled 'SNMP 설정' is positioned over the SNMP settings.

※ REST API

The screenshot shows the REST API documentation page for Genian Insights. The page lists several APIs: 'sitemap : 사이트맵 API', 'sysadmin : 시스템 관리 API', and 'threats : Threat 처리 API'. The 'threats : Threat 처리 API' section is expanded, showing endpoints like 'POST /threats/command', 'GET /threats/download', and 'GET /threats/endpoints'. The 'GET /threats/endpoints' endpoint is highlighted, showing its 'Implementation Notes', 'Parameters', 'Response Class', and 'Response Message'. A blue callout box labeled 'API 조회 가능' (API Queryable) is overlaid on the 'GET /threats/endpoints' section. The 'Response Message' section displays a JSON response with fields like 'page', 'pageSize', 'sort', 'active', 'DeviceID', 'Version', 'Platform', 'PlatformCode', 'IP', 'MAC', and 'ServerIP'.

15) 연동

Syslog, SNMP, Rest API 외의 다양한 연동이 될 수 있도록 연동 플러그인(모듈)을 개발하여 적용할 수 있습니다.

연동 플러그인 적용으로 서버 업그레이드 불필요

Genian Insights
대시보드
분석
통합검색
리포트
정책
관리
09:59
이

인덱스 관리
En
jint2
Al
t2
Th
t2
Int
Vo
e
File
NA
NA
sp
In
Sy
Tr
File
NA
수집

시스템 관리
서버 관리
세션 관리
업데이트 관리
시스템 OS
IOC 업데이트
ML모델 업데이트
유사도해시 업데이트
서버 플러그인 관리

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
☐ AhnlabV3	ahnlabv3	☒	⚙️	1.0.0.14312	schedule	Ahnlab 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

모듈 연동 목록 외 다수

- FireEye AX
- Trendmicro sandbox
- Secudium (IOC)
- CheckPoint SandBlast (Sandbox)
- ReversingLabs A1000 (Sandbox)
- Samsung AMS (Sandbox)
- C-TAS (KISA IOC)

연동 플러그인

03.

Genian EDR 도입 효과

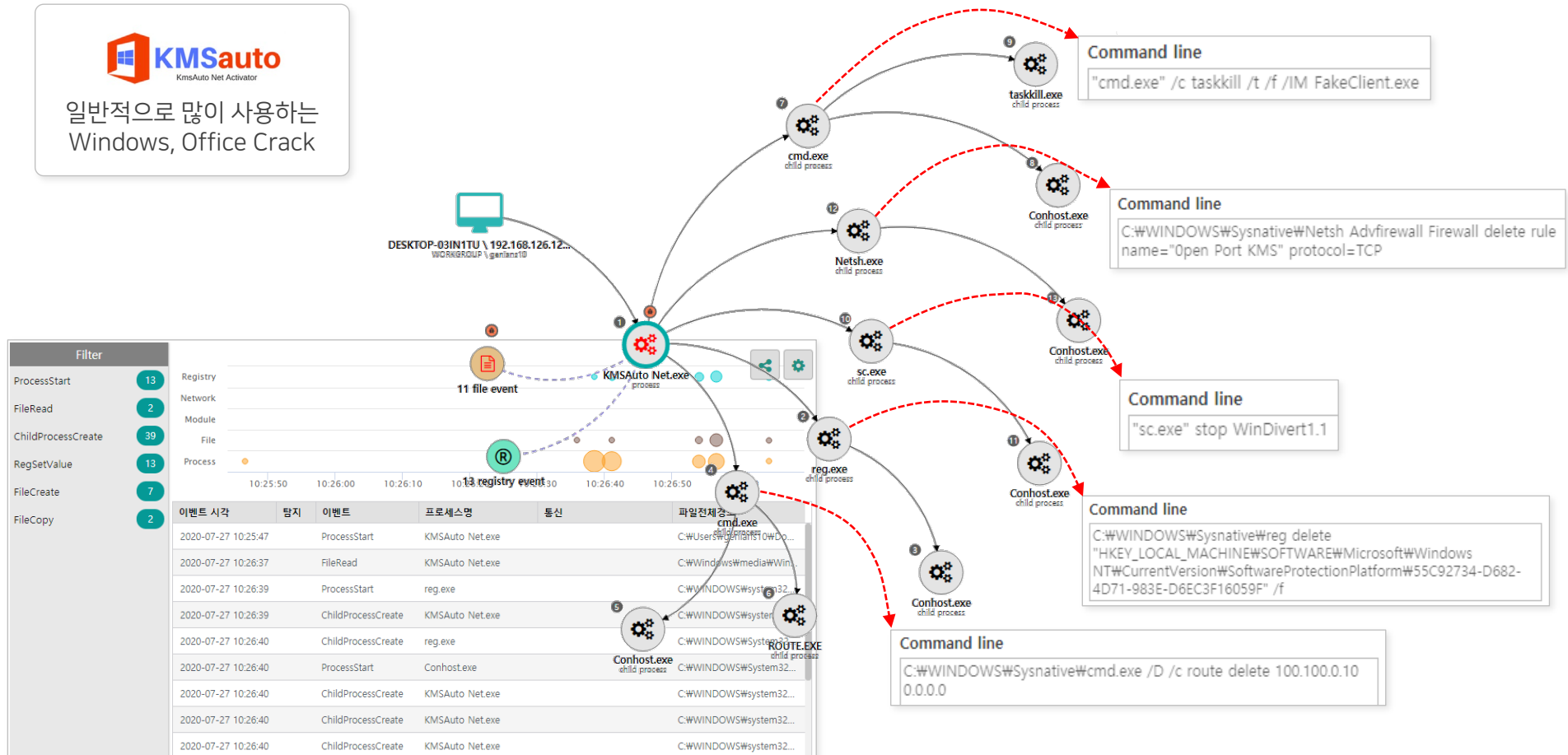
침투 경로와 행위에 대한 파악

리버스 엔지니어링(Rreverse 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



엔드포인트의 다양한 정보 제공

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

위협 탐지를 위해 수집한 로그는 원하는 다양한 형태의 대시보드로 구성하여 사용자 PC 내에서 발생하는 행위를 쉽게 모니터링
내부 정책 위반, USB 등의 저장 장치를 통한 문서 이동, 내부 시스템 접속, AP 접속 현황 등 기존 확인할 수 없던 정보 제공

DATA(데이터)

INFORMATION(유용한 정보)

Event time 2022-11-17 13:26:17

Event type FileCreate

Process name POWERPNTXEXE

Create file E:\[발표]발표자료\202212\과학기술정보보호회의_세미나\EDR탐지사례_Endpoint_ZT.pptx

Tag DocSave

Custom Tag 사용자정의 태그를 입력하세요.

파일 정보 (PPTX 문서 생성)

File name EDR탐지사례_Endpoint_ZT.pptx

Size 31.9 MB

File type DOC

Event time 2022-11-17 13:38:48

Event type ChildProcessCreate

Process name powershell.exe

Process path C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Process ID 16084

Child process PING.EXE (ping 실행)

Command line "C:\Windows\system32\PING.EXE" 168.126.63.1

Event time 2022-11-17 14:35:52

Event type FileUpload

Process name KakaoTalk.exe

Source file C:\Users\admin\Desktop\정민\EDR\TEST\카톡 업로드 테스트.pptx

Target IP 121.53.205.50

Custom Tag 사용자정의 태그를 입력하세요.

파일 정보 (카톡 파일 업로드)

File name 카톡 업로드 테스트.pptx

Size 605.3 KB

File type DOC

Event time 2022-11-18 10:38:29

Event type FileCopy

Process name Explorer.EXE

Source file D:\TEST\활용사례.pptx

Target file E:\연동문서\활용사례.pptx

Custom Tag 사용자정의 태그를 입력하세요.

파일 정보 (문서 복사)

File name 활용사례.pptx

Size 2.9 MB

File type DOC

네트워크 연결 정보

Event time 2022-12-15 11:11:24 ~ 2022-12-15 12:21:03 (1시간 9분 동안 발생함)

Events time 2022-12-15 11:11:24 ~ 2022-12-15 12:21:03 (1시간 9분 동안 발생함)

Event type NetworkConnect

Process name putty.exe

Protocol TCP

Direction OUT

Connection 성공

Conn/Disconn 2 / 2

192.168.10.2457113

192.168.10.25422

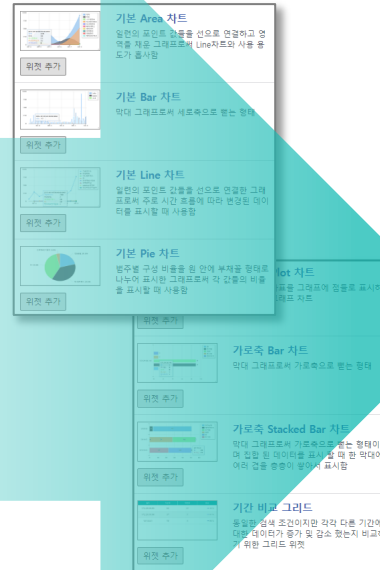
(putty.exe 서버 접속)

RegValueName 공유

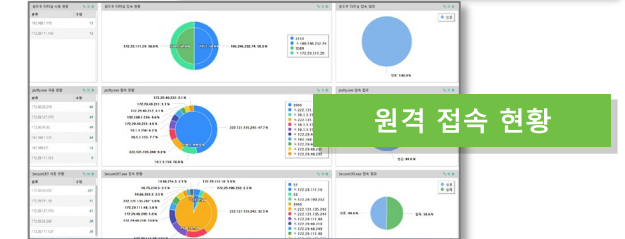
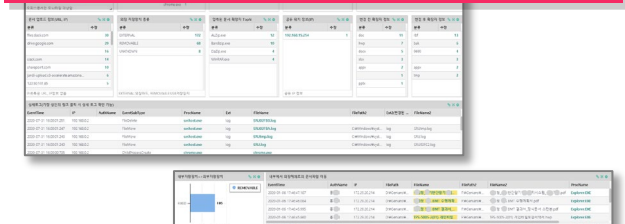
RegValue CATimeout=0 CSCFlags=2048 MaxUses=3 Path=D:\공유

유 Permissions=860 Remark= ShareName=공유

Type=0 (공유폴더 설정)

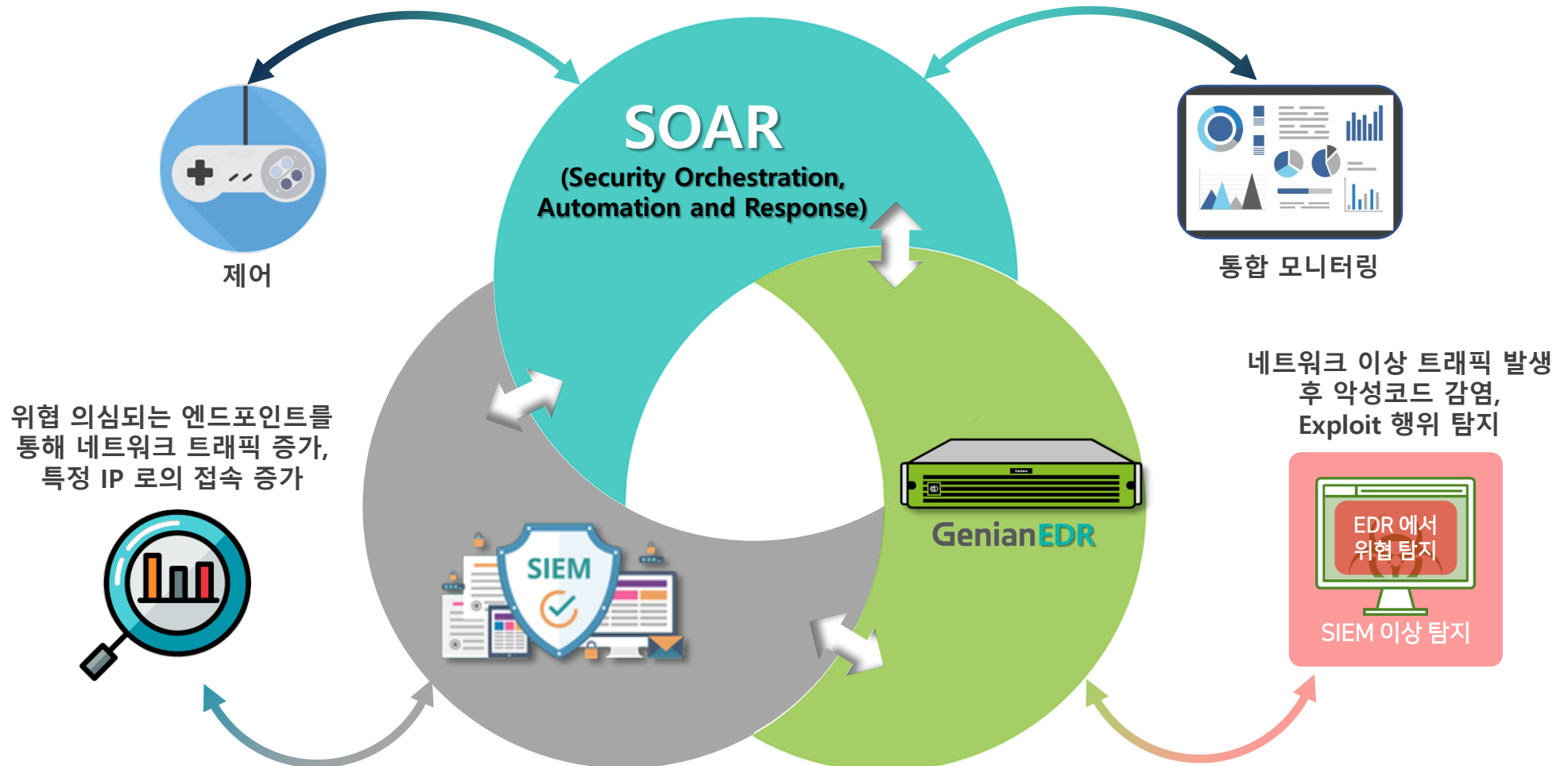


문서 통합 분석
(업로드, 외장 장치, 압축, 공유폴더, 확장자 변경)



● 네트워크와 엔드포인트의 연관성, 그리고 SOAR

SIEM, SOAR 연동하여, 네트워크 상의 이상 행위가 엔드포인트에서의 악성 행위나 악성파일 탐지와 연관이 있는 지에 대한 분석과 자동 대응 및 모니터링을 할 수 있습니다.



통합 보안 플랫폼 기업 지니언스

PC 가시성의 모든 것

Genian EDR v2.0

THANK YOU :)

