Genian EDR

Release 3.0.8

GENIANS, INC.

May 26, 2026

관리자 가이드


DOWNLOAD PDF

CHAPTER

ONE

PHASE 1 - 설치 및 배포

이 장에서는 Genian Insights E를 시스템에 설치하고 관리자가 웹 콘솔 및 CLI 콘솔에 접근하는 과정을 안내합니다.

1.1 설치 전 준비사항

이 장에서는 Genian Insights E를 설치하기 전에 알아야 할 기본 정보를 소개합니다.

1.1.1 구성 요소 이해

Genian Insights E가 동작하려면 다양한 구성 요소가 필요합니다. 이 장에서는 각 구성 요소의 역할 및 설치에 대해 설명합니다.

정책 서버

정책 서버는 Genian Insights E의 모든 데이터 및 설정을 저장하는 중앙 관리 시스템입니다. 일반적으로 정책 서버는 조직의 데이터 센터에 설치 됩니다.

정책 서버의 또 다른 역할은 관리자에게 관리 콘솔을 제공하는 것입니다. 웹 기반 관리 콘솔을 통해 다른 구성 요소를 구성 및 관리 할 수 있습니다. 수집 된 정보를 보고 조직의 보안 정책을 수립 할 수 있습니다.

Genian NAC 서버가 있는 경우, 플러그인 추가로 간편하게 에이전트를 배포할 수 있습니다.

에이전트 관리 서버 역할도 하지만 Genian NAC 서버에는 엔드포인트의 세부 자산정보(IP, H/W, S/W, OS, Patch 등)가 수집되어 있으므로, Genian Insights E와 연동을 통해 지속적인 내부 모니터링이 가능합니다.

Genian Insights E 단독 버전일 경우, 정책 서버에서 에이전트 파일을 다운로드 받아 배포 서버를 통해 배포하거나 실행파일을 직접 실행하여 에이전트를 설치할 수 있습니다.

에이전트

에이전트는 사용자의 PC에 설치된 소프트웨어입니다. PC에서 발생하는 모든 이벤트를 수집하고 이를 정책 서버로 전송합니다.

에이전트는 종료 방지 및 삭제 방지와 같은 자체 보안 기능을 제공합니다.

1.1.2 구축 고려사항

Genian Insights E를 통한 성공적인 Insights E 구축 가이드

본 문서는 Genian Insights E 도입을 통해 단말의 가시성을 확보하고, 위협 대응 역량을 극대화하기 위한 단계별 구축 전략을 기술합니다.

1. 사전 준비 및 환경 분석

성공적인 구축의 첫걸음은 현재 자산의 현황을 파악하고 도입 목적을 명확히 하는 것입니다.

- **자산 및 인프라 파악**: 사내 엔드포인트(Windows, macOS, Linux 등)의 수량과 OS 버전을 확인합니다.
- **네트워크 구성 검토**: 에이전트와 서버 간의 통신 경로 및 방화벽 정책을 점검합니다.
- **보안 정책 수립**: Insights E을 통해 탐지하고자 하는 핵심 위협 요소와 알림 우선순위를 설정합니다.

2. 서버 설치 및 연동

정책 서버를 구축하고 기존 보안 솔루션과의 연동을 진행하는 단계입니다.

- **정책 서버 설치**: On-Premise 또는 Cloud 환경에 Genian Insights E 정책 서버를 구축합니다.
- **기존 시스템 연동**: NAC, SIEM, 또는 전사 통합 보안 관제 시스템과 연동하여 로그 수집 체계를 구축합니다.
- **관리자 권한 설정**: 운영 담당자별로 역할 기반 접근 제어를 설정하여 보안성을 강화합니다.

3. 에이전트 배포 및 가시성 확보

엔드포인트에 에이전트를 설치하여 실시간 데이터를 수집하기 시작합니다.

- **단계적 배포**: IT 부서나 특정 팀을 대상으로 우선 배포(Pilot)한 후 점진적으로 전사 확대를 진행합니다.
- **상태 모니터링**: 에이전트 설치 후 단말 성능(CPU/메모리)에 미치는 영향을 검토합니다.
- **로그 수집 확인**: 프로세스 실행, 파일 변경, 네트워크 연결 등 주요 이벤트의 정상 수집 여부를 확인합니다.

4. 정책 최적화 및 탐지 고도화

Genian Insights E의 분석 기능을 통해 오탐을 줄이고 정탐율을 높이는 과정입니다.

- **위협 관리**: 수집된 이벤트를 분석하여 위협의 우선순위를 정의하고, 불필요한 알림을 최소화하기 위한 예외 처리 정책을 수립합니다.
- **ECO 자체평판시스템**: 지니언스만의 클라우드 기반 평판 데이터베이스인 ECO를 활용하여, 알려지지 않은 파일에 대한 안전성을 실시간으로 검증하고 신뢰도를 확보합니다.
- **맞춤형 규칙 설정**: 기업 고유의 업무 환경과 인프라 특성을 반영하여, 이상 행위 탐지 규칙(XBA)을 정교하게 최적화함으로써 고도화된 위협에 대응합니다.

5. 대응 프로세스 수립 및 운영

위협 발생 시 신속하게 대응할 수 있는 체계를 가동합니다.

- **대응 시나리오 확립**: 위협 수준에 따른 단말 격리 및 프로세스 차단 등 대응 프로세스를 수립합니다.
- **침해사고 분석**: 타임라인 분석 기능을 활용하여 유입 경로 및 확산 범위를 파악합니다.
- **정기 리포팅**: 주간/월간 리포트를 통해 보안 취약점을 지속적으로 개선합니다.

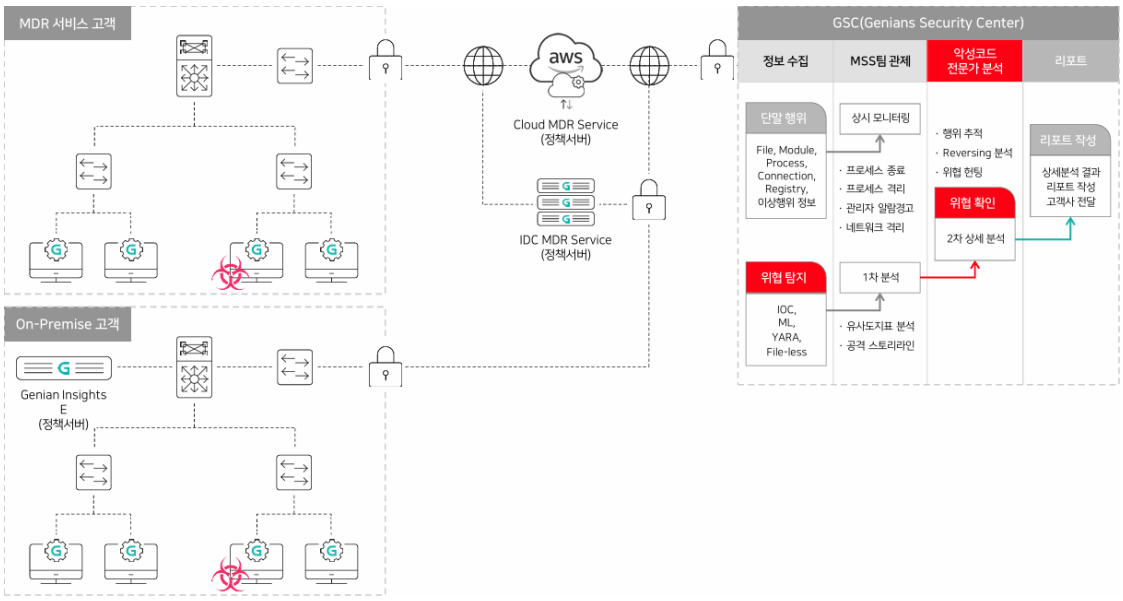
Note: 성공적인 구축을 위한 핵심 팁

- 초기에는 차단보다 **모니터링** 위주로 운영하여 업무 영향도를 최소화하십시오.
- 최신 위협 트렌드에 맞춰 **탐지 룰셋** 을 주기적으로 업데이트하십시오.
- 보안 관제 인력과의 유기적인 **협업 체계** 를 구축하십시오.

정책서버

구성도

Genian Insights E는 On-Premises 및 Cloud 환경에서 수집된 데이터를 기반으로 **지속적인 엔드포인트 감시, 위협 탐지, 전문가 분석, 자동화 대응** 까지 전 과정을 통합 수행합니다. 이를 통해 고도화된 사이버 위협에 선제적으로 대응하고, 보안 운영의 효율성과 신뢰성을 동시에 강화합니다.



1.1.3 네트워크 준비

네트워크에 Genian Insights E 구축을 계획할 때 몇 가지 고려 사항이 있습니다.

- 스위치에 어떻게 연결 하나요?
- 몇 개의 장비가 필요한가요?
- Genian Insights E이 통신하려면 어떤 포트를 열어야 하나요?

유선 연결

Insights E 서버는 Core Switch 포트에 액세스 포트로 직접 연결 되어야합니다.

방화벽 요구 사항

Genian Insights E이 제대로 동작하려면 아래의 포트들이 방화벽으로부터 개방되어야합니다.

[On-Premises]

SRC IP	DST IP	Service	Note
정책서버 IP	유동IP : eco.genians.net(도메인 기반) 고정IP : eco.genians.net (13.124.21.19, 13.124.15.244)	TCP/443	탐지항목 검증(평판서비스)
Client IP	정책서버 IP	UDP/3880 TCP/3879 TCP/3876 TCP/443	Heartbeat 전송(Keep Alive) Plugin 수집정보 전송(Plaintext) Plugin 수집정보 전송(SSL) 인증 정보 전송, 수집샘플 전송, 정책(업데이트) 수신
관리자 PC IP	정책서버 IP	TCP/3910 TCP/9200 TCP/8443	SSH 접속 LOG 관리 Web접속 Web콘솔 접속

Note: 탐지항목에 대한 평판서비스 검증을 위해서는 정책서버가 외부 통신이 가능해야 합니다.

1.2 시스템 요구사항

이 장에서는 Genian Insights E의 안정적인 운영을 위한 서버 및 에이전트의 최소/권장 요구사항을 기술합니다.

1.2.1 정책 서버 요구사항

Table 1: 정책 서버 권장 사양 (단말 1,500대 기준)

항목	권장 사양
CPU	8 Core (2.1GHz 이상)
Memory	64GB RAM 이상
Disk	2TB 이상 (SSD 권장)

1.2.2 에이전트 요구사항

- **Windows**: Windows 7 SP2 이상, 8, 10, 11, 2012, 2016, 2019, 2022, 2025 (32/64-bit)

항목	권장 사양
CPU	Intel(R) Pentium(R) Silver 1.10Ghz 이상
Memory	4GB RAM 이상
Disk	5GB 이상
NIC	10/100 Mbps 1 Port 이상

- **macOS**: Big Sur 11.0 이상
- **Linux**: Linux 에이전트 지원 목록 을 참고 바랍니다.

Note: 대규모 단말(Node) 관리 환경은 데이터 수집량 및 로그 보존 주기에 따라 스토리지 요구량이 변동될 수 있습니다. 시스템의 **안정적인 운영 환경** 을 확보하기 위해, 구축 전 담당 파트너 엔지니어 또는 솔루션기술센터 상담을 통해 환경에 최적화된 리소스 설계를 진행하시기를 권장합니다.

1.3 Insights E 3.0 서버 설치

1.3.1 설치 유형 선택

정책 서버는 물리적으로 하나 이상의 시스템에 정책 및 IOC Database, 로그서버를 운영합니다.

서버 전용
시스템은 서버 단독으로 동작할 수 있습니다. 다만, 대규모 네트워크 환경에서는 성능 및 안정성을 위해 정책 서버와 로그 서버를 분리할 수 있습니다. 서버 분리 구성은 별도의 안내가 필요합니다.

1.3.2 하드웨어 준비

물리적 시스템에 정책 서버를 설치할 수 있습니다.

하드웨어 사양
테스트를 위해 낮은 사양의 일반 서버를 사용할 수 있으나, 일반적으로 사용하는 하드웨어 사양은 아래와 같습니다.

ES300	ES500
Intel Xeon 6333p @ 3.1GHz (6C12T)	Intel Xeon 4510 @ 2.4GHz (12C24T)
Mem: 64G	Mem: 128G
SSD / HDD : 2TB / 4TB	SSD / HDD : 4TB / 12TB
1U	2U
800W Dual Power	750W Dual Power

1.3.3 초기 구성

Genian Insights E는 CLI를 통해 2가지 설치 모드를 제공하며, Interactive Wizard를 이용한 설치 방법을 설명합니다.

Interactive Wizard를 이용한 설치

1. CLI Initial Configuration Tool 화면에서 installation type 에 1을 입력합니다.

```
Genian Insights Initial Configuration Tool

1. Interactive Wizard
2. Manual Configuration

Select installation type :
```

2. server type 에 1을 입력합니다.

```
1. Single Server -Stand Alone

Select Server Type:
```

3. System Language 에 2를 입력합니다.

```
1. English
2. Korean

Select System Language :
```

4. CLI 로그인 계정을 생성합니다.

```
Enter Console Username (31 characters max) [admin] :
```

5. CLI 로그인 패스워드를 생성합니다.

```
Password must contain at least one uppercase letter, lowercase letter, number,␣
↪and special character
Enter Console Password (9 to 30 Characters) :
```

6. 5에서 생성한 패스워드를 한번 더 입력합니다.

```
Try Again:
```

7. Database 계정을 생성합니다.

```
Enter database Username (4-31 characters) :
```

8. Database 패스워드를 생성합니다.

```
Password must contain at least one uppercase letter, lowercase letter, number,␣
↪and special character
Enter DB Password (9 to 30 Characters) :
```

9. 8에서 생성한 패스워드를 한번 더 입력합니다.

```
Try Again:
```

10. 관리콘솔(WEB) 로그인 계정을 생성합니다.

```
Enter Superadmin ID (4-31 characters) :
```

11. 관리콘솔(WEB) 로그인 패스워드를 생성합니다.

```
Password must contain at least one uppercase letter, lowercase letter, number,␣
↪and special character
Enter Superadmin Password (9 to 30 Characters) :
```

12. 11에서 생성한 패스워드를 한번 더 입력합니다.

```
Try Again:
```

13. System timezone 설정을 선택합니다.

```
1. Africa     2. America      3. Antarctica
4. Asia       5. Arcic        6. Australia
7. Europe     8. Indian       9. Pacific

[Timezone] Select Continental :
```

14. System timezone 설정을 선택합니다.

```
[Timezone] Select City (press enter for re-display):
```

15. NTP 서버가 존재하는 경우 서버 Domain 정보를 입력합니다.

```
Enter NTP server:
```

16. 서버 IP로 사용할 IP 정보를 입력합니다.

```
Enter IP Address:
```

17. 서버 IP 의 Netmask 를 설정합니다.

```
Enter Netmask:
```

18. 서버의 Gateway 를 설정합니다.

```
Enter Default Gateway:
```

19. DNS 서버 IP 정보를 입력합니다.

```
Enter DNS Server IP Address:
```

20. 입력이 완료되면 입력한 정보를 최종 확인 후 y를 입력합니다. Database Server Password 변경 과정을 추가로 진행합니다.

```
Configuration Summary
---------------------------------------------------------------
Server Type:                Single Server -Stand Alone
System Language:            Korean
Console Username:           [ID]
Timezone:                   Asia/Seoul
NTP Server:                 pool.ntp.org
Network Interface:          eth0
IP Address:                 [Server IP]
Netmask:                    [Netmask]
Default Gateway:            [Gateway IP]
DNS Server IP Address:      [DNS IP]
Database Server Username:   [ID]
Database Server Password:   ********
Webconsole superadmin ID:   [ID]
Webconsole superadmin Password:  ********
---------------------------------------------------------------

Are you sure to continue (y/n) ? y
```

21. Genian Insights E는 라이선스에 따라 메뉴 구성이 달라집니다. 초기 설치 시 GMODULE로 설치되며, EMODULE인 경우 관리콘솔에서 EMODULE 라이선스를 먼저 등록하고 IOC DB를 구성하는 설정이 추가로 필요합니다.

    EMODULE을 사용하지 않는 경우 21은 생략하고 22을 진행합니다. ioc-updater enable 명령 설정 시 외부 서버와 통신하여 1억건 이상의 IOC DB를 업데이트 합니다.

    데이터 업데이트에는 수 일 이상의 많은 시간이 소요되므로 수동 명령을 통해 초기 데이터를 저장한 후 ioc-updater enable 설정을 하여야 합니다. 수동 명령을 이용한 초기 설치 방법은 IOC Database 설치 페이지를 참고합니다.

22. show config 명령어를 통해 설정 확인 후 장비를 재부팅 합니다.
23. Web Browser에서 "https://정책서버IP:8443/mc" 로 접속합니다.

1.4 Insights E 3.0 에이전트 설치

1.4.1 Linux Agent 설치

에이전트 다운로드 및 설치

1. **관리 > 시스템 > 에이전트 패키지** 에서 에이전트 패키지를 업로드 합니다.
2. Linux OS 계열(deb, rpm)에 맞게 설치 파일을 다운로드 합니다. 이 때, **다운로드 받은 실행 파일의 이름은 변경하지 않도록 합니다.**
3. 다운로드한 설치 파일을 Linux 서버/단말에 업로드 합니다.
4. 설치 파일 권한을 부여합니다.
    - deb 파일 : user@ubuntu:~$ chmod 755 GenianInsights-deb_x.x.x.x.sh
    - rpm 파일 : user@ubuntu:~$ chmod 755 GenianInsights-rpm_x.x.x.x.sh
5. root 권한으로 설치 파일을 실행 합니다.
    - deb 파일 : root@ubuntu:/home/user# ./GenianInsights-deb_x.x.x.x.sh
    - rpm 파일 : root@ubuntu:/home/user# ./GenianInsights-rpm_x.x.x.x.sh

에이전트 패키지 관리

1. 패키지(.gpf) 파일 업로드 시, 버전 정보 및 업로드 시간 등 에이전트 패키지를 관리 할 수 있는 기능을 제공합니다.
2. 업로드된 패키지들은 에이전트 배포 관리에서 배포 버전을 선택하여 사용할 수 있습니다.

에이전트 업데이트

> **Warning:** **관리 > 설정 > 시스템** 의 에이전트 자체 업데이트 설정이 ON 으로 설정돼 있어야 합니다.

에이전트 배포 관리

Genian Insights E는 스크립트를 통한 에이전트 초기 설치 후, 자체 배포관리 시스템을 통해 지속적인 배포 관리 기능을 제공하고 있습니다. **관리 > 시스템 > 에이전트 배포 관리** 에서 배포 관리를 설정을 할 수 있습니다.

1. 에이전트 배포할 그룹을 선택합니다.
2. **작업선택 > {선택 | 전체} 에이전트 업데이트 즉시 수행** 버튼을 통해 즉시 배포가 가능합니다.
3. **배포 설정** 에서 자동 업데이트가 가능합니다.
4. **배포 설정** 에서 에이전트 버전 설정이 가능합니다.

에이전트 업데이트 확인

1. 에이전트 배포 완료 시, 완료된 단말의 상태에 ✓ 표시가 나타납니다.
2. 감사 로그를 통해 배포된 Agent의 설치 및 업데이트 로그를 확인 할 수 있습니다.

Linux 에이전트 설치 확인

1. **분석 > 엔드포인트 목록** 를 선택합니다.
2. 엔드포인트 목록에서 에이전트가 설치된 단말을 확인 할 수 있습니다.

Linux 단말 에이전트 로그 위치

- **Linux에서 터미널 열어서 아래의 위치의 로그파일을 확인합니다.**
  - 설치경로: /opt/genians/insights
  - 로그경로: /opt/genians/insights/logs

Linux 에이전트 지원 목록

Linux OS 계열	지원 버전 범위
Red Hat Enterprise Linux (RHEL)	6, 7, 8, 9
CentOS	6, 7, 8
Rocky Linux	8, 9
Ubuntu	18.04, 20.04, 22.04, 24.04
Fedora	42
SUSE Linux	11, 12 (sp4)
openSUSE	11, 12, 15
Oracle Linux	6, 8

지원 버전 참고사항

문의사항이 있으신 경우, 우측 하단의 챗봇 또는 기술지원센터(tac@genians.com)로 문의해 주시기 바랍니다.

1.4.2 macOS Agent 설치

에이전트 다운로드 및 설치

1. **관리 > 시스템 > 에이전트 패키지** 에서 에이전트 패키지를 업로드 합니다.
2. macOS 아키텍처 상관 없이 설치 파일을 다운로드 합니다. 이 때, **다운로드 받은 실행 파일의 이름은 변경하지 않도록 합니다.**
3. 다운로드한 실행 파일을 직접 더블클릭하여 설치하거나, PMS 등을 통해 설치합니다.

   설치 과정 중 다음과 같은 사용자 권한 요청 창이 표시될 수 있으며, 아래 절차에 따라 진행합니다:

   - **"프로그램 설치 허용"** 버튼 클릭
   - **macOS 사용자 암호 입력**
   - **"소프트웨어 설치"** 버튼 선택하여 설치 완료

에이전트 패키지 관리

1. 패키지(.gpf) 파일 업로드 시, 버전 정보 및 업로드 시간 등 에이전트 패키지를 관리 할 수 있는 기능을 제공합니다.
2. 업로드된 패키지들은 에이전트 배포 관리에서 배포 버전을 선택하여 사용할 수 있습니다.

에이전트 업데이트

Warning: **관리 > 설정 > 시스템** 의 에이전트 자체 업데이트 설정이 ON 으로 설정돼 있어야 합니다.

에이전트 배포 관리

Genian Insights E는 스크립트를 통한 에이전트 초기 설치 후, 자체 배포관리 시스템을 통해 지속적인 배포 관리 기능을 제공하고 있습니다. **관리 > 시스템 > 에이전트 배포 관리** 에서 배포 관리를 설정을 할 수 있습니다.

1. 에이전트 배포할 그룹을 선택합니다.
2. **작업선택 > {선택 | 전체} 에이전트 업데이트 즉시 수행** 버튼을 통해 즉시 배포가 가능합니다.
3. **배포 설정** 에서 자동 업데이트가 가능합니다.
4. **배포 설정** 에서 에이전트 버전 설정이 가능합니다.

에이전트 업데이트 확인

1. 에이전트 배포 완료 시, 완료된 단말의 상태에 ✓ 표시가 나타납니다.
2. 감사 로그를 통해 배포된 Agent의 설치 및 업데이트 로그를 확인 할 수 있습니다.

macOS 에이전트 설치 확인

1. **분석 > 엔드포인트 목록** 를 선택합니다.
2. 엔드포인트 목록에서 에이전트가 설치된 단말을 확인 할 수 있습니다.

macOS 단말 에이전트 로그 위치

- **macOS에서 터미널 열어서 아래의 위치의 로그파일을 확인합니다.**
  - 설치경로: ~/Library/Application Support/GenianInsights
  - 로그경로: ~/Library/Application Support/GenianInsights/agent.log

macOS 지원 목록

macOS	버전
macOS Big Sur	11.0 이상

1.4.3 Windows Agent 설치

Note: Genian Insights E **단독 버전 에이전트** 설치 버전을 기본으로 설명합니다.

에이전트 다운로드 및 설치

1. **관리 > 시스템 > 에이전트 패키지** 에서 에이전트 패키지를 업로드 합니다.
2. Windows 버전(x64, x84)에 맞게 설치 파일(.exe)을 다운로드 합니다. 이 때, **다운로드 받은 실행 파일의 이름은 변경하지 않도록 합니다.**
3. 다운로드한 실행 파일을 직접 더블클릭하여 설치하거나, PMS 등을 통해 설치합니다.

에이전트 패키지 관리

1. 패키지(.gpf) 파일 업로드 시, 버전 정보 및 업로드 시간 등 에이전트 패키지를 관리 할 수 있는 기능을 제공합니다.
2. 업로드된 패키지들은 에이전트 배포 관리에서 배포 버전을 선택하여 사용할 수 있습니다.

에이전트 업데이트

> **Warning:** **관리 > 설정 > 시스템** 의 에이전트 자체 업데이트 설정이 `ON` 으로 설정돼 있어야 합니다.

에이전트 배포 관리

Genian Insights E는 PMS 등을 통해 에이전트 초기 설치 후, 자체 배포관리 시스템을 통해 지속적인 배포 관리 기능을 제공하고 있습니다. **관리 > 시스템 > 에이전트 배포 관리** 에서 배포 관리를 설정을 할 수 있습니다.

1. 에이전트 배포할 그룹을 선택합니다.
2. **작업선택 > {선택 | 전체} 에이전트 업데이트 즉시 수행** 버튼을 통해 즉시 배포가 가능합니다.
3. **배포 설정** 에서 자동 업데이트 또는 분산 업데이트를 통해 분산 배포가 가능합니다.
4. **배포 설정** 에서 에이전트 버전, 자동 업데이트 시간, 분산 업데이트 설정이 가능합니다.

에이전트 업데이트 확인

1. 에이전트 배포 완료 시, 완료된 단말의 상태에 ✓ 표시가 나타납니다.
2. 감사 로그를 통해 배포된 Agent의 설치 및 업데이트 로그를 확인 할 수 있습니다.

Windows Agent 설치 확인

1. **분석 > 엔드포인트 목록** 를 선택합니다.
2. 엔드포인트 목록에서 에이전트가 설치된 단말을 확인 할 수 있습니다.

Windows 단말 에이전트 로그 위치

1. Windows 단말에서 **파일 탐색기** 열기
2. **C:\Program Files\Geni\Insights\logs** 로 이동합니다.

Note: 에이전트 설치와 관련된 인스톨로그는 Windows 디렉토리에 `Installer.INSIGHTS"년월일".log` 로 존재합니다.

Windows 지원 목록

Microsoft Windows OS (32bit/64bit)
Microsoft Windows 7 (SP2 이상)
Microsoft Windows 8
Microsoft Windows 8.1
Microsoft Windows 10
Microsoft Windows 11
Microsoft Windows Server 2012
Microsoft Windows Server 2016
Microsoft Windows Server 2019
Microsoft Windows Server 2022
Microsoft Windows Server 2025

1.4.4 에이전트 삭제

에이전트 삭제는 Genian Insights E 웹 관리 콘솔에서 삭제 기능을 제공합니다.

에이전트 삭제 요청

1. **분석 > 엔드포인트 목록** 에서 삭제를 원하는 단말을 선택합니다.
2. 단말 선택 후, **작업선택 > 에이전트 작업 > 에이전트 삭제** 버튼을 클릭합니다.
3. 웹 관리 콘솔에서 본인 인증을 위해 계정 비밀번호를 확인 후 단말의 에이전트에 삭제 명령을 전달합니다.

에이전트 삭제 확인

삭제 요청한 엔드포인트 상세 정보 > **로그** 탭에서 에이전트 삭제 요청 정보를 확인할 수 있습니다.

에이전트 삭제시 변경 사항

1. **분석 > 위협 모니터링 > 엔트포인트 현황**의 UP, DOWN 된 단말의 수 변경
2. **분석 > 엔드포인트 목록** 리스트 중 삭제된 단말 상태에 삭제 아이콘 생성

1.5 정책 관리

1.5.1 그룹 정책 관리

Genian Insights E는 그룹 별 이벤트 수집, 탐지, 대응 및 에이전트 정책 설정 기능을 제공합니다. 새로운 정책 추가는 **정책 > 그룹 정책 관리**에서 정책 추가 버튼을 통해 새로운 정책 그룹을 생성 할 수 있습니다.

기본 정책

Genian Insights E 서버에 접속하는 모든 엔드포인트는 최초에 **기본정책**을 적용받습니다. 정책은 수집, 탐지, 대응, 에이전트 설정 및 고급 설정에 대한 정책으로 구성됩니다.
에이전트가 적용받는 정책 그룹은 **엔드포인트 목록, 엔드포인트 그룹 관리**에서 **정책 설정**을 통해 변경 가능합니다.

수집

수집 대상 이벤트

항목	수집 이벤트
기본	프로세스 실행, 실행/문서/압축 파일 생성 등 중요 이벤트 수집
지정	파일, 모듈, 네트워크, 레지스트리 이벤트 중 선택된 항목 수집
전체	수집 가능한 모든 이벤트를 수집

파일 수집 목록

정책	설명
실행파일목록수집	실행파일 목록을 수집합니다. 수집된 파일 목록은 FileList 인덱스에서 확인 가능합니다.
지정파일목록인덱싱	'지정 확장자'에 정의된 파일 정보를 인덱싱하여 PC에 저장합니다.
파일크롤링	PC가 유휴 상태일 때 파일 정보를 수집 **문서/압축파일:** 모든 파일의 Signature를 확인하여 문서/압축 파일 정보를 수집합니다. **지정 파일:** '지정 확장자'에 정의된 파일 정보를 수집합니다. **빠른 수집:** 시스템 자원을 적극적으로 사용하여 정보를 빠르게 수집합니다. **실행 파일:** 모든 파일의 Signature를 확인하여 실행파일 목록을 수집합니다. **잠금 화면 수집:** 잠금 화면 상태일 때 크롤링을 수행합니다. **수행 대기 시간:** 설정 시간동안 사용자의 입력이 없는 경우 크롤링을 시작합니다. **크롤링 실행 주기:** 크롤링 완료 후 다시 수행할 주기를 설정합니다. **예외 경로 설정:** 파일 크롤링 예외 경로를 설정합니다.

윈도우 이벤트 수집(ETW)

윈도우 이벤트는 보안상 중요한 다양한 종료의 이벤트를 제공하고 있습니다.
Genian Insights E는 관리자가 원하는 윈도우 이벤트를 등록하면 해당 이벤트를 수집하여 검색할 수 있도록 기능을 제공합니다.

정책	설정
수집 대상 윈도우 이벤트	윈도우 이벤트 뷰어에 기록되는 이벤트 정보 수집, XBA 연동 설정
자연어 설명 수집	이벤트 데이터를 자연어 형태로 수집
json 데이터 수집	이벤트 데이터를 json 형태로 수집

설정된 윈도우 이벤트는 winevt 인덱스에 저장되어 **통합 검색**에서 검색 가능합니다.

탐지

탐지 엔진

엔진	설명
침해지표 (IOC)	최소 신뢰도 10%, IOC,YARA 와 같은 알려진 위협 탐지 시 설정된 신뢰도 이상인 경우에만 탐지하도록 설정 기능을 제공합니다.
머신러닝 (ML)	에이전트에서 전송하는 파일에 대해 머신러닝 탐지 기능을 적용하고, 위협 탐지 시 통합검색 및 엔드포인트 상세 메뉴에 탐지 정보를 제공합니다.
이상행위 (XBA)	**이상행위 룰셋** 설정 기능을 제공합니다.

대응

에이전트 배포방식이 단독버전일 경우 NAC 연동은 지원하지 않습니다.

대응 설정은 아래와 같습니다.

정책	설정
알려진 악성코드 대응	YARA, IOC DB에 등록된 위험 프로세스 탐지 시 대응 설정
NAC 연동	에이전트에서 위협 탐지 시 해당 노드에 부여할 태그 설정
알려지지 않은 악성코드 대응	머신러닝에 의한 탐지 시 대응 설정
악성IP	IOC DB에 등록된 악성 IP로 접속을 탐지 시 대응 설정

에이전트 알림 표시, 프로세스 강제 종료, 파일 삭제 등 정책에 따른 대응 정책 설정을 할 수 있습니다.

에이전트

기본 설정

정책	설정
접속 서버 IP	다중서버 구성 환경인 경우, 서버 부하 분산을 위해 에이전트가 접속해서 정책을 내려받을 서버 IP 또는 도메인 입력
사용자 알림 팝업	악성코드 탐지 후 위협 관리의 대응 방법이 **프로세스 강제종료, 파일 삭제** 시 엔드포인트에 알림 팝업 표시 여부 설정
트레이 아이콘	에이전트 트레이 아이콘을 표시(NAC와 에이전트 아이콘 통합인 경우 사용 안 함)
알림 메시지 팝업	네트워크 격리와 해제 시 엔드포인트에 발생하는 알람 메세지 문구 작성 격리 메세지: 관리자가 관리콘솔에서 엔드포인트에 네트워크 격리 명령을 수행했을 때 엔드포인트에 표시되는 팝업창 문구 해제 메세지: 관리자가 관리콘솔에서 엔드포인트에 네트워크 격리 해제 명령을 수행했을 때 엔드포인트에 표시되는 팝업창 문구
허용 IP	네트워크 격리 시 허용할 IP를 설정 (Genian NAC 와 Genian Insights E서버 IP는 별도로 설정하지 않아도 통신 가능 함)

네트워크 접속 차단

정책	설명
접속 차단 IP 및 Port	네트워크 격리 정책과 상관없이 접속을 차단할 **IP 및 Port** 를 입력합니다. (TCP 포트) Genian Insights E 서버 운영과 연관된 서버는 차단되지 않습니다.

백업

정책	설명
Windows VSS 백업	랜섬웨어 공격에 대비하여 Windows VSS를 이용한 하드디스크 파일 전체에 대한 백업을 진행합니다. VSS 기능 사용 시 랜섬웨어에 의해 스냅샷이 삭제되지 않도록 **정책 > 이상행위 > 이상행위 룰 관리** 화면에서 ShadowCopy 삭제 및 문서 확장자 Rename 초과 정책의 자동대응 설정이 필요합니다.

기타

정책	설명
API Hooking 사용	다양한 이벤트를 모니터링하기 위해 API를 Hooking 합니다. 타 소프트웨어와 충돌이 발생할 수 있으므로 안정성 테스트 후 적용이 필요하며, 설정 `ON/OFF` 시 PC 재부팅이 필요합니다.

1.5.2 정책 백업 및 이력 관리

예약된 시간에 백업하도록 설정하고, 시스템 장애 발생시 백업파일을 이용하여 복원 할 수 있습니다.

백업 설정

예약된 시간에 백업하도록 설정하고, 저장장치에 백업 파일을 보관하도록 설정할 수 있습니다.

지정된 시간에 백업 예약

1. 상단 패널의 **관리>설정** 으로 이동합니다.
2. 왼쪽 환경 설정 패널에서 **백업** 으로 이동합니다.
3. 백업 예약 작업을 위해 백업수행여부를 **On** 으로 설정합니다.
4. 백업을 반복하려면 **백업수행시각** 을 지정합니다.
5. 백업에 필요한 최소 공간을 확보하기 위해 **여유공간보호 임계 값** 을 지정합니다.
6. **수정** 버튼을 클릭합니다.

저장장치 유형 구성

1. 상단 패널의 **관리>설정** 으로 이동합니다.
2. 왼쪽 환경 설정 패널에서 **백업** 으로 이동합니다.
3. 저장장치 를 찾아서 드롭 다운에서 적절한 **저장장치 타입** 을 선택합니다.
4. **수정** 버튼을 클릭합니다.

저장장치 유형	설명 및 설정값
로컬 디스크	정책서버 디스크에 백업을 수행합니다.(별도의 설정 필요없음)
외부 저장장치	정책서버에 USB Type으로 연결된 외장 디스크에 백업을 수행합니다.
CIFS 저장장치	윈도우 공유 기능을 이용하여 CIFS 사용 백업을 수행합니다.
NFS 저장장치	Unix나 Linux file system의 디렉토리를 mount하여 백업을 수행합니다.
FTP SERVER	FTP(File Transfer Protocol)을 통해 백업파일을 전송합니다. (보안상 비밀번호가 평문으로 전달됨으로 권장하지 않음)
SFTP SERVER	SFTP(Secure File transfer protocol)을 통해 백업파일을 전송합니다. (보안상 SSH 기반으로 암복호화를 수행함으로 권장함)

기존 백업 파일에서 복원

시스템 장애가 발생한 경우, 백업 데이터를 복원 할 수 있습니다. 이 복원 프로세스를 수행하려면 CLI 접근 권한이 있어야합니다.

백업 파일 찾기 및 복원

1. 관리콘솔에 로그인 후, 상단 패널에서 **관리** 을 클릭합니다.
2. 왼쪽 패널의 **환경설정> 백업** 으로 이동합니다.
3. **백업 파일 다운로드** 버튼을 클릭합니다.
4. 목록에서 복구할 백업 파일을 복사한 후 접속을 종료합니다.
5. CLI를 통해 정책 서버 콘솔에 접속합니다.
6. **enable** 및 **관리자 비밀번호** 를 입력하여 **Global Mode** 로 이동합니다.
7. "restore <filename> all" 를 입력하여 백업 데이터를 복원합니다.

CHAPTER

TWO

PHASE 2 - 이벤트 수집

Genian Insights E 3.0은 위협 이벤트 뿐만 아니라 엔드포인트에서 발생하는 모든 이벤트를 수집할 수 있습니다.

엔드포인트에서 수집된 이벤트는 관리 > 시스템 > 인덱스 관리 에서 인덱스 설정이 가능합니다.

또한, 이벤트의 양이 방대하고 보안 프로그램에 의해 이벤트가 빈번하게 발생하는 경우, 선별적으로 이벤트 수집 예외설정을 할 수 있습니다.

2.1 수집 인덱스 구조 및 설명

이벤트 수집 관리 및 예외 설정은 **정책 > 이벤트 수집 관리**에서 설정 가능합니다.

2.1.1 엔드포인트 이벤트 수집

단말의 에이전트 설치가 완료되면 엔드포인트에서 발생하는 이벤트를 Insights E 서버로 전송합니다.
Genian Insights E 서버 설정에 따라 중요하다고 판단하는 이벤트(프로세스 실행, 실행/문서/압축 파일 생성)를 수집하며, 더 필요한 정보는 서버 설정에서 변경할 수 있습니다.

엔드포인트에서 수집된 이벤트는 **통합검색**에서 확인 가능합니다. 기본 인덱스는 아래와 같습니다.

- **Endpoint2:** 엔드포인트에서 발생하는 이벤트(file, process, module, network, registry) 정보
- **Alert2:** Threat Detector 에 의해 위협으로 탐지되어 알람이 발생한 정보 및 이상행위탐지(XBA) 엔진에서 탐지한 위협 정보를 이벤트 기반으로 표시
- **Threat2:** Threat Detector 에 의해 위협으로 탐지되어 알람이 발생한 정보 및 이상행위탐지(XBA) 엔진에서 탐지한 위협 정보를 상태 기반으로 표시
- **Inflow:** 파일 유입 정보
- **Volume:** 외부 저장장치 마운트 정보
- **FileMaster:** PE, Script 관리
- **system-info:** Endpoint 목록의 상세화면-리소스 현황에 표시되는 cpu,memory, storage(agent installed drive) 정보
- **system_info:** Endpoint 목록의 상세화면-시스템 정보에 표시되는 장치정보, 운영체제, 저장장치, 네트워크 인터페이스 정보
- **Filelist:** Agent에서 수집한 Endpoint의 파일 목록
- winevt:* Endpoint에서 발생하는 Windows Event 정보
- **artifact:** aritifact 수집 시, 수집한 파일 관련 정보
- **uploadlist:** 서버에 업로드되어 수집 관리 메뉴에 표시되는 파일 목록

- **filestatic-analyze:** 파일 상세 분석 메뉴를 통해 업로드하여 파일 정적 분석 도구를 이용한 분석 결과 저장 정보

윈도우 이벤트(ETW)

정책 > 그룹 정책 관리 > 수집에서 수집 대상 윈도우 이벤트 설정이 가능합니다.

Genian Insights E에서는 관리자가 원하는 윈도우 이벤트를 등록하면 해당 이벤트를 수집하여 검색할 수 있도록 기능을 제공합니다.
관련 이벤트는 `winevt` 인덱스에 저장되어 **통합 검색**에서 검색 가능합니다.

- **WindowEvent:** 엔드포인트에서 발생하는 Windows Event 정보

2.1.2 이벤트 조사

분석 > 조사 > 이벤트 조사 페이지에서는 특정 엔드포인트가 아닌, 전체 엔드포인트에서 발생한 이벤트를 확인하고 분석할 수 있습니다.

이벤트 검색

- 이벤트 조사 화면에서 단일 키워드로 파일에 관련된 모든 필드를 한번에 검색할 수 있습니다. 필드명을 입력하지 않고 검색이 가능한 필드는 검색창 클릭 시 파란색 별표로 표시되어 있습니다.
- 다른 메뉴의 검색창에서는 데이터 검색 시 필드명:데이터 와 같은 형태로 검색해야 하지만 이벤트 조사 화면에서는 키워드 검색이 가능합니다.
- 검색할 키워드에 공백이 포함된 경우 큰따옴표(Double Quatation)로 키워드를 감싼 후 검색합니다.
- `AuthName`, `AuthDeptName`, `HostName` 필드는 키워드 검색 시 full text로 입력해야 합니다. 예를 들어 AuthName 이 홍길동 이라면 검색시 홍길 이라는 단어만 입력한다면 검색되지 않습니다.

이벤트 조사

이벤트 조사 리스트는 전체 엔드포인트에서 발생한 Event 히스토리를 확인할 수 있습니다.

- 설정한 날짜(ex.Today,1d,3d 등)의 히스토리가 차트로 표시되며, 차트 내에서 마우스 클릭하여 드래그 시 이벤트 날짜 기간을 좁혀서 상세 정보를 확인할 수 있습니다.

이벤트 목록 클릭 시 **이벤트 상세정보 화면**이 나타납니다.

- 이벤트 상세 화면에서 예외처리 아이콘 클릭 시, 해당 이벤트를 수집하지 않도록 등록할 수 있습니다.
- 오른쪽 화면에서 도킹 팝업 클릭 시, 별도의 팝업창이 발생합니다.
  이벤트 상세정보 화면에서는 클릭한 항목이 최초에 어떤 프로세스에 의해 실행되었으며, 연결 정보가 존재하는 경우 Destination IP 정보까지 파악할 수 있습니다.
- 플로팅 아이콘 클릭 시 클릭한 항목과 관련이 있는 Process, File, Module, Network, Registry 정보를 최초 발생 시간 기준으로 표시합니다.
  (정책 > 그룹 정책 > 엔드포인트가 포함된 정책의 수집 대상 이벤트 설정에 따라 수집 되지 않은 데이터는 표시되지 않습니다.)
- 이벤트 상세정보에서 선택한 이벤트에 대해 엔드포인트 정보부터 선택한 이벤트가 실행되기까지 직접적인 관련이 있는 이벤트만 보거나,
  이벤트 종류를 기준으로 연관된 이벤트를 모두 표시하도록 설정할 수 있습니다.

이벤트 조사 컬럼 설정

이벤트 조사 화면에서 컬럼 설정을 통해 관리자가 확인하고 싶은 정보만 표시할 수 있습니다.

1. **분석 > 조사 > 이벤트 조사**에서 오른쪽 상단의 설정 아이콘을 클릭하여 컬럼 설정 선택 시 컬럼 설정 화면이 표시됩니다.
2. 표시하고 싶은 컬럼 항목을 오른쪽으로 이동 후 저장 버튼을 클릭 시 관리자가 설정한 컬럼으로 표시됩니다.

2.2 이벤트 수집 관리

Genian Insights E 3.0은 위협 이벤트뿐만 아니라 엔드포인트에서 발생하는 모든 이벤트를 수집할 수 있습니다. 이벤트의 양이 방대하고 보안 프로그램에 의해 이벤트가 빈번하게 발생하는 경우, 선별적으로 **이벤트 수집 예외 설정**을 할 수 있습니다.

또한, 보안 프로그램 및 업무 프로그램 등에 의해 이벤트가 빈번하게 발생하는 경우, 선별적으로 이벤트 수집 예외 설정을 할 수 있습니다.
알려진 보안 프로그램에 대한 예외 처리를 기본으로 제공하며, 기본으로 제공하는 예외 그룹을 바탕으로 그룹 설정을 복사하여 새로운 **예외 처리 규칙**을 추가할 수 있습니다.

2.2.1 이벤트 수집 예외 설정 추가

1. **정책 > 이벤트 수집 관리 > 이벤트 수집 예외 설정** 메뉴로 이동 후 상단의 추가 버튼을 클릭합니다.
2. 이벤트 수집 예외 그룹 추가 팝업창이 발생하며, 이름, 사용 여부 및 복사할 예외 그룹 선택 여부를 확인한 후 생성 버튼을 클릭합니다.
   기본값으로 등록되어있는 프로그램의 예외 항목을 확인하여 복사할 예외 그룹 선택 시 편리하게 수집 예외 설정을 할 수 있습니다.
3. 예외 그룹 추가 후 목록에서 추가한 그룹 이름을 클릭합니다.
4. 이벤트 수집 예외 추가 버튼을 클릭합니다. 아래 화면에서 업무 프로그램 예외에 마우스를 이동하면 이름을 수정할 수 있고, 연필 모양 아이콘 클릭 시 설명을 추가할 수 있습니다.
5. 이벤트 수집 예외 추가 팝업창이 발생하며, 이벤트의 종류(file, process, module, network, registry)를 선택하고 확인 버튼을 선택합니다.
6. 아래와 같이 프로세스 예외처리 추가 시 추가적인 정보를 입력할 수 있는 팝업창이 표시됩니다.
7. 예외처리할 프로세스에 대한 정보를 입력한 후 저장 버튼을 클릭합니다.
8. 수집 예외 상세 화면에서 앞에서 추가한 예외처리 프로세스 정보를 확인할 수 있습니다.
9. 예외 설정 시 오른쪽 상단에 정책 즉시 적용 버튼을 클릭해야 에이전트에 정책이 즉시 전달됩니다.

2.2.2 이벤트 수집 예외 설정 삭제

1. 삭제할 예외 그룹을 선택하면 삭제 버튼이 활성화되어 예외 그룹을 삭제할 수 있습니다.
2. 예외 설정 삭제 시 오른쪽 상단에 정책 즉시 적용 버튼을 클릭해야 에이전트에 정책이 즉시 전달됩니다.

2.3 수집된 로그 확인 방법

Genian Insights E는 단말에서 발생하는 다양한 보안 이벤트를 실시간으로 수집하여 관리자에게 제공합니다.

수집된 로그를 통해 위협의 흐름을 파악하고 심층 분석을 진행하는 방법을 안내합니다.

2.3.1 대시보드를 통한 현황 확인

엔드포인트에서 수집된 위협 정보와 가시성 데이터를 다양한 위젯으로 시각화하여, 보안 현황을 직관적으로 파악할 수 있습니다.

관리자는 목적에 따라 맞춤형 대시보드를 유연하게 구성할 수 있으며, 기본 제공되는 항목 외에도 분석 데이터를 다각도로 가공하여 모니터링할 수 있습니다.

주요 활용 대시보드

- **위협 현황**
  : 특정 프로세스나 IP를 중심으로 전체 행위 흐름을 분석해 이상 징후를 파악할 수 있습니다.
- **외장 저장장치 사용 현황**
  : USB 및 외장 하드 등 이동식 저장매체의 연결 정보와 파일 복사/이동 현황을 실시간으로 추적합니다.
- **원격 접속 현황**
  : 원격 데스크톱(RDP), 터미널(SSH), PuTTY, SecureCRT 등 시스템 접근 제어를 우회하여 내부 시스템에 접속하는 행위를 탐지합니다.
- **취약 버전 SW 사용 현황**
  : 엔드포인트에 설치된 소프트웨어 중 보안 취약점이 발견된 버전을 식별이 가능합니다.
- **ECO 공유 대시보드**
  : 지니언스에서 직접 업데이트하는 클라우드 기반 공유 대시보드입니다. 인터넷이 연결된 환경이라면 최신 위협 트렌드가 반영된 대시보드를 즉시 적용할 수 있습니다.

2.3.2 상세 이벤트 로그 조회

특정 시점에 발생한 세부적인 행위 로그를 확인하기 위해서는 '이벤트 조사' 메뉴를 활용합니다.

- **조회 조건 설정**
  : 특정 기간, 노드 그룹, 위협 유형별로 필터를 적용하여 원하는 데이터를 선별합니다.
- **이벤트 목록 확인**
  : 탐지 시간, 특정 사용자 및 프로세스, 위협 행위 등의 기본 정보를 확인합니다.
- **상세 정보 분석**
  : 특정 로그를 클릭하여 스토리라인, 커맨드 라인, 파일 해시, 부모/자식 프로세스 관계 등 상세 데이터를 분석합니다.

2.3.3 타임라인 기반 분석

Genian Insights E는 수집된 로그를 시간 흐름에 따라 시각화하여 제공함으로써 사고의 유입 경로를 파악하는 데 유용합니다.

- **행위 추적**
  : 위협이 발생하기 전후로 어떠한 파일 생성이나 네트워크 연결이 있었는지 타임라인 순으로 추적합니다.

CHAPTER

THREE

PHASE 3 - 이벤트 조사 및 활용

3.1 대시보드

대시보드 작성에 어려움이 있는 경우 Genian Ecosystem에 등록되어있는 여러 대시보드를 가져오거나, 관리자 간에도 대시보드를 공유할 수 있습니다.

3.1.1 ECO공유 대시보드 추가

엔드포인트에서 많은 정보를 수집하고 있지만 관리자가 필요한 정보를 대시보드로 생성하는 데 어려움이 있습니다. Genian Insights E 서버가 Ecosystem과 통신이 되는 환경이라면 Ecosystem에 생성되어 공유되고 있는 대시보드를 추가할 수 있습니다.

ECO 공유 대시보드를 사용하기 위해서는 eco.genians.net 과 통신이 되어야 하고, **관리 > 설정 > 환경설정 > 시스템** 의 기본 설정에서 인터넷연결 on, Ecosystem 연동 여부가 on 으로 설정되어야 합니다.

1. 관리콘솔 로그인 후 대시보드 메뉴로 이동, 오른쪽 상단 **옵션** 메뉴에서 **공유 대시보드 추가** 를 클릭합니다.
2. 공유 대시보드 추가 팝업창이 표시되며, ECO 공유 대시보드 탭을 클릭합니다. 대시보드 추가 버튼을 클릭합니다.
3. 2에서 추가한 대시보드를 확인할 수 있습니다.

3.1.2 관리자 공유 대시보드 추가

관리자 간 대시보드를 공유할 수 있습니다.

1. A관리자는 관리콘솔 로그인 후 대시보드 메뉴로 이동, 공유하고싶은 대시보드를 선택하여 옵션에서 대시보드 공유 를 클릭하면 사용자 공유 대시보드에 등록됩니다.
2. 대시보드 공유 확인 팝업창이 발생하며, 확인 버튼을 클릭합니다. 공유된 대시보드는 탭이름에 공유 아이콘이 표시됩니다.
3. B관리자는 옵션에서 공유 대시보드 추가 를 클릭하면 사용자 공유 대시보드 탭에서 A 관리자가 공유한 대시보드를 확인하여 추가할 수 있습니다.

3.2 리포트 등록 및 전송

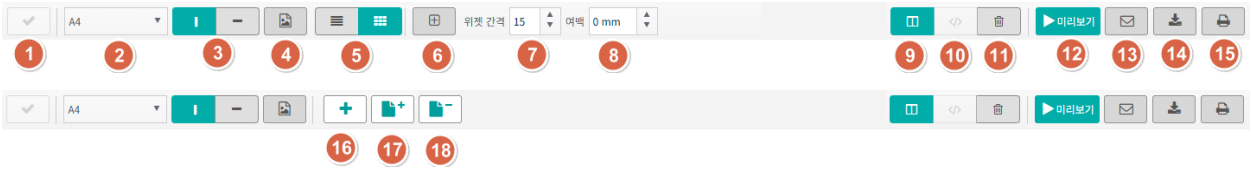
Genian Insights E3.0은 대시보드 데이터를 기준으로 리포트를 작성, 관리자 메일로 전송하거나 pdf 파일 저장 및 리포트 인쇄 기능을 지원합니다.

3.2.1 리포트 등록

1. 관리콘솔에 로그인 후 대시보드 메뉴에서 리포트로 등록할 대시보드를 선택합니다. 화면 오른쪽 상단의 설정 옵션에서 리포트로 등록을 클릭합니다.
2. 리포트 등록 확인창이 발생하면 확인 버튼을 클릭합니다.
3. 리포트 대메뉴로 이동하며, 해당 페이지에서 각종 출력설정을 할 수 있습니다.

3.2.2 리포트 설정

1. 리포트 메뉴에서 리포트 관련 각종 설정을 할 수 있습니다.



번호	항목	설명
1	**저장**	리포트 메뉴 내에 구성된 모든 설정 항목들을 저장합니다.
2	**용지 크기**	출력할 리포트의 용지 규격(A4 등)을 선택합니다.
3	**레이아웃(방향)**	데이터를 출력할 방향(세로 또는 가로)을 설정합니다.
4	**리포트 표지 선택**	생성할 리포트에 전용 표지를 설정할 수 있습니다.
5	**목록 정렬**	위젯을 한 줄에 하나씩 배치하거나, 여러 개를 병렬로 배치하도록 설정합니다.
6	**빈박스 추가**	위젯이 페이지 구분선에 걸치는 경우, 빈 박스를 삽입하여 출력 간격을 조절합니다.
7	**위젯 간격**	배치된 개별 위젯 간의 간격을 세밀하게 설정합니다.
8	**여백**	리포트 용지의 바깥쪽(상하좌우) 여백을 설정합니다.
9	**썸네일**	여러 페이지로 구성된 리포트의 전체 레이아웃을 미리 확인합니다.
10	**코드 보기**	리포트 구성 코드를 확인하거나 직접 편집할 수 있습니다. (사용자 추가 리포트 전용)
11	**리포트 삭제**	현재 편집 중이거나 선택된 리포트 양식을 삭제합니다.
12	**미리보기**	설정이 모두 반영된 최종 리포트 결과물을 사전에 검토합니다.
13	**이메일 전송**	리포트를 메일로 전송합니다. 주소 직접 입력 또는 관리자 계정 연동이 가능합니다.
14	**내려받기**	구성된 리포트를 PDF 파일 형식으로 로컬 PC에 저장합니다.
15	**인쇄**	현재 리포트를 프린터를 통해 즉시 출력합니다.
16	**Element 추가**	신규 리포트 작성 시 테이블, 텍스트, 이미지, 그래프 등을 편리하게 추가합니다.
17	**커스텀 리포트 추가**	사용자의 목적에 맞는 새로운 리포트 페이지를 추가합니다.
18	**커스텀 리포트 삭제**	추가로 생성했던 커스텀 리포트 페이지를 삭제합니다.

2. 리포트 페이지가 여러장인 경우, 각 페이지의 구분은 주황색 실선으로 표시됩니다.

3. 위젯이 페이지 구분선과 맞물리게 될 경우 빈박스를 활용하여 페이지를 구분합니다. 빈박스는 리포트로 전송하거나 출력 시 공백으로 표시됩니다.
4. element 추가 후 추가한 element를 클릭하면 컴포넌트 설정창이 표시되며, 설정창에서 세부적인 내용을 수정할 수 있습니다.
5. 컴포넌트 타입을 Dashboard 로 선택 시, 관리콘솔에 등록된 Dashboard 탭 ID 또는 위젯 ID를 입력하여 리포트로 등록할 수 있습니다.

3.2.3 리포트 전송

Note: 리포트를 메일로 전송하기 위해서는 **관리 > 설정 > 환경설정 > 시스템** 메뉴의 메일서버 설정 이 되어 있어야 합니다.

1. 리포트 화면에서 메일 버튼 클릭 시 메일 주소를 입력할 수 있는 팝업창이 표시됩니다.
2. 추가 버튼을 클릭하여 메일주소를 직접 입력할 수 있으며, 메일주소 입력 후 전송 버튼을 클릭합니다.
3. **관리 > 시스템 > 사용자 메뉴** 에서 사용자 계정 정보에 이메일 주소가 입력되어 있는 경우, 받는사람 텍스트 박스에 텍스트 입력 시 목록을 선택할 수 있도록 표시됩니다.
4. 앞에서 입력한 메일에서 보고서를 확인할 수 있습니다.

3.3 통합검색 검색 활용법

에이전트 및 수집기 설정을 통해 수집한 이벤트는 통합검색 메뉴에서 확인할 수 있습니다.

3.3.1 로그 검색 방법

이벤트의 종류에 따라 로그가 각각 다른 인덱스에 저장되며, 인덱스 선택 후 로그를 검색할 수 있습니다.

1. **통합 검색** 메뉴로 이동, 왼쪽 트리에서 로그를 검색할 인덱스를 선택합니다.
2. 검색창에 직접 검색할 쿼리를 입력하거나, 로그 상세뷰에서 검색하고자 하는 값을 클릭하면 자동으로 쿼리 입력기에 데이터 칩이 생성됩니다.
   쿼리 입력기에 직접 입력하는 경우, 로그 검색은 Lucene 문법을 사용합니다. (더 자세한 문법은 Lucene Documentation에서 확인할 수 있습니다.)

   ex) Insights Logs에서 사용자ID가 'admin' 인 값을 검색하고자 하는 경우

   통합검색 > Insights Logs 선택 후 쿼리 입력기에서 logUserId:"admin" 입력 후 검색 버튼 클릭 시 사용자 ID 가 admin 인 값만 검색되며 쿼리는 하이라이트로 표시됩니다.

Genian Insights E 서버에서 발생하는 감사기록은 Insights Logs 인덱스에 저장되며, 로그 ID별 상세항목은 아래와 같습니다.

로그 ID	이름	내용
100	관리자접속	관리자 로그인 상태 관련 로그
110	그룹	엔드포인트 그룹 생성, 수정, 삭제 로그
118	업데이트	라이선스 업데이트 로그
120	CLI	CLI 접속 관련 로그
121	데이터 동기화	정보, 사용자, 부서 등 데이터 동기화 로그

Table 1 – continued from previous page

로그 ID	이름	내용
130	에이전트	에이전트 동작 상태, 플러그인 업데이트 관련 로그
132	시스템	엔드포인트의 시스템 동작 상태(절전, 로그온, 로그오프. 디스크 사용량) 관련 로그
140	에이전트액션	엔드포인트 위협 대응 결과, 프로세스 덤프 수집, 파일 수집, YARA Rule 검사 관련 로그
150	시스템	백업, 인덱스 정리, 미동작 엔드포인트 삭제, Trendmicro 연동 결과, 서버의 서비스 구동
160	정책	관리콘솔의 정책 즉시 적용, 엔드포인트 정책 수신 관련 로그
200	설정변경	관리콘솔의 각종 설정 변경 관련 로그
300	사용자관리	관리콘솔의 사용자 생성, 삭제 및 관리역할, 사용자 정보 변경 관련 로그
400	인덱스관리	관리콘솔의 인덱스관리 설정 관련 로그
500	수집기관리	관리콘솔의 수집기 설정 관련 로그
600	프로파일관리	관리콘솔의 수집기 설정 프로파일 및 서버 프로파일 관련 로그
700	검색관리	검색필터 관련 로그
750	위협관리	위협관리(위협판정, 담당자 설정 등..) 상태 관련 로그
770	CTI관리	PE File 삭제시, 삭제 정보에 대한 감사로그
790	수집관리	수집관리 메뉴의 파일 수집 상태 관련 로그
800	IOCDB	IOC DB 업데이트 관련 로그
810	위협	위협 탐지 관련 로그
815	장비태그설정	IOC 장비 태그 설정 로그
820	알림메시지	엔드포인트에 알림 메시지 표시 로그
825	프로세스 강제종료	위협 탐지 시 프로세스 강제종료 수행 로그
826	프로세스 강제종료(수동)	관리자가 직접 프로세스 강제종료 수행 로그
830	파일삭제	위협 탐지 시 파일삭제 수행 로그
831	파일삭제(수동)	관리자가 직접 파일 삭제 수행 로그
835	샘플수집	실행 파일 샘플 수집 로그
836	샘플수집(수동)	실행 파일 샘플 수동 수집 로그
837	수집	파일 샘플 수집 로그
838	수집(수동)	파일 샘플 수동 수집 로그
841	네트워크 격리(수동)	관리자가 직접 네트워크 격리 명령 수행 로그
850	이상징후	이상징후 탐지 로그
870	이상행위	이상행위 룰 관리 및 예외정책 설정 관련 로그
900	대시보드	관리콘솔의 대시보드 관련 로그
912	리포트	관리콘솔의 리포트 메뉴 변경사항 관련 로그
999	기타	GenianNac로그 생성, 삭제 관련 로그

3.3.2 검색 기록 저장 및 즐겨찾기

1. 통합검색 화면 검색창에서 데이터 입력 및 검색 후 즐겨찾기 버튼을 클릭하면 화면에 표시된 검색조건이 자동으로 입력된 즐겨찾기 추가 화면이 표시됩니다.
2. 즐겨찾기 저장 후 검색필터 클릭 시 추가했던 즐겨찾기 목록 및 최근 검색 기록을 확인할 수 있습니다.(각각 최대 50건) 최근 검색 기록은 브라우저 캐시가 삭제되면 기록도 삭제됩니다.

3.4 Live 검색 활용법

에이전트가 가지고 있는 Database를 대상으로 실시간으로 파일을 검색할 수 있습니다.

검색 대상을 선택 후 검색할 파일의 조건을 설정하고 검색 요청을 수행하면 에이전트가 가지고있는 Database(FileList, FileMaster, DocList) 에서 조건에 맞는 데이터를 검색 후 결과를 표시합니다.

또한 주요 레지스트리의 Key, Values, Data 를 대상으로 검색조건과 일치하는 레지스트리를 빠르게 검색하는 기능을 제공합니다.

3.4.1 파일 신규 검색

1. **분석 > 조사 > Live 검색** 페이지에서 신규 검색 버튼을 클릭합니다.
2. 검색 타입 선택에서 빠른 파일 검색을 선택하고 다음을 클릭합니다.
3. 아래 조건에 따라 검색 대상을 선택합니다.

구분	설명
전체 엔드포인트	Insights 서버에 등록된 전체 엔드포인트를 대상으로 파일 검색을 수행합니다.
엔드포인트 그룹	**분석 > 엔드포인트 > 엔드포인트 그룹 관리** 에 등록된 특정 그룹을 대상으로 파일 검색을 수행합니다.
조직	**관리 > 설정 > 사용자 관리 > 정보 동기화** 를 통해 부서 정보가 등록되어 있는 경우 해당 부서를 대상으로 파일 검색을 수행합니다.

   예제에서는 검색 대상 중 전체 엔드포인트를 선택합니다.

4. 검색 조건 추가버튼을 클릭 후 검색 조건 (항목 및 조건, 설정) 을 입력하고 조건 연산을 선택, 저장합니다.

항목	설명
조건 연산	AND - 두 개 이상의 조건을 사용할 때, 조건을 모두 만족시켜야 그룹에 포함됩니다. OR - 두 개 이상의 조건을 사용할 때, 많은 조건들 중 하나만 만족시켜도 그룹에 포함됩니다.

5. 4에서 설정한 조건이 화면에 표시되고, 검색 시작* 버튼을 클릭합니다.

   파일 검색 만료일을 선택한 후 검색 시작 버튼을 클릭하면 검색이 시작됩니다.

6. 빠른 파일 검색 모드로 수행된 결과를 확인 합니다.

지난 검색 결과 찾기 검색바를 이용하여 검색 조건에 해당하는 검색 결과를 찾을 수 있습니다.

검색 결과는 7일간 유지되며, 결과 삭제를 원하지 않는 경우 잠금 아이콘을 이용하여 삭제하지 않도록 설정할 수 있습니다.

3.4.2 파일 수집

1. LIVE 검색을 통해 검색 결과가 있고, 파일 종류가 PE 또는 SCRIPT 파일이면 해당 파일을 서버로 수집할 수 있습니다. 검색 결과 상세화면에서 수집할 파일 목록을 선택하면 파일 수집 버튼이 활성화 됩니다.
2. 수집이 완료되면 **분석 > 조사 > 수집 관리** 화면에서 파일을 다운로드 받을 수 있습니다.
3. LIVE 검색 파일 수집 기능은 오용에 따른 민감 정보 유출 방지를 위해 수집 대상을 PE, SCRIPT 파일로 제한하고 있으나,

advance 설정 > 프론트엔드 설정 > 파일 수집 대상 제한 여부 를 `off` 로 변경하면 DOC_LIST 인덱스에 포함된 파일도 수집할 수 있습니다.

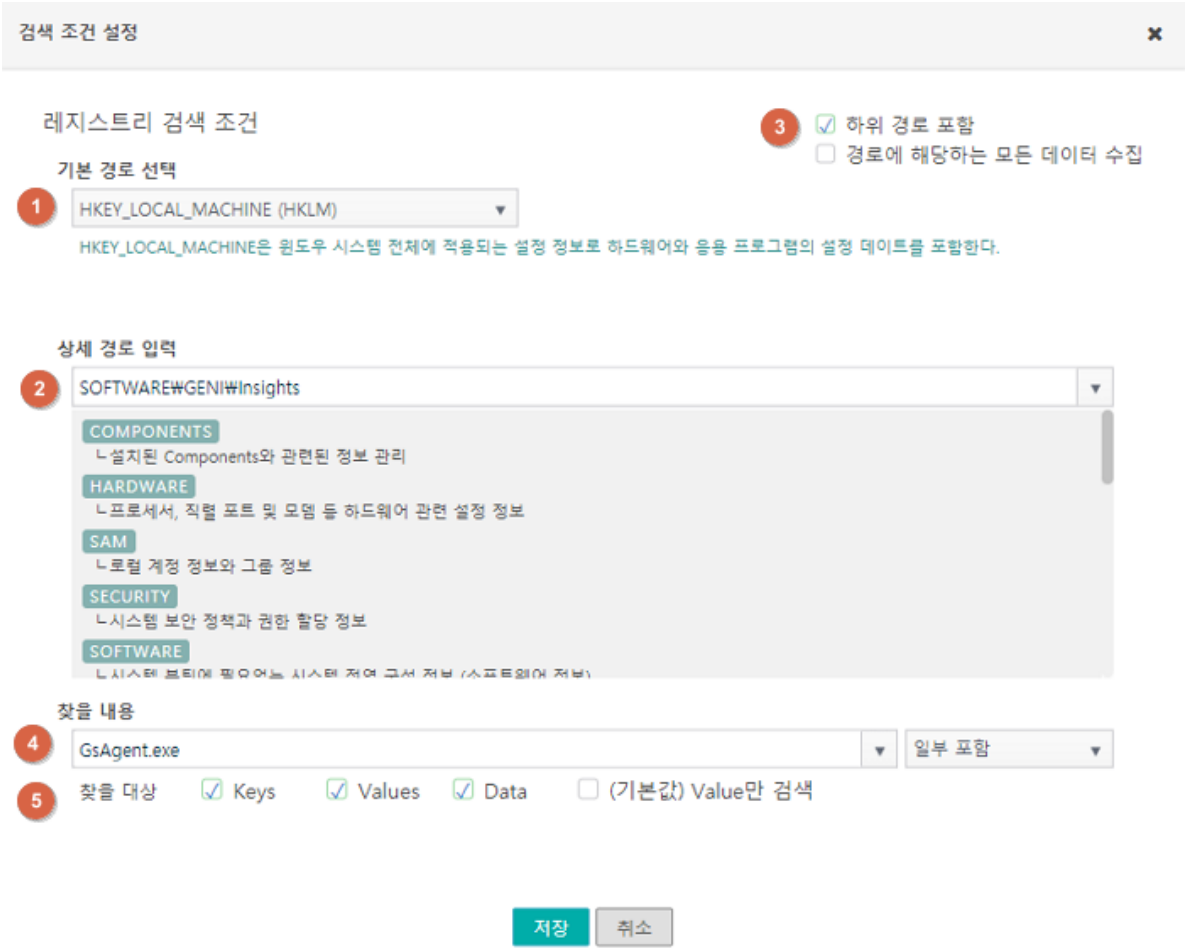
3.4.3 레지스트리 신규 검색

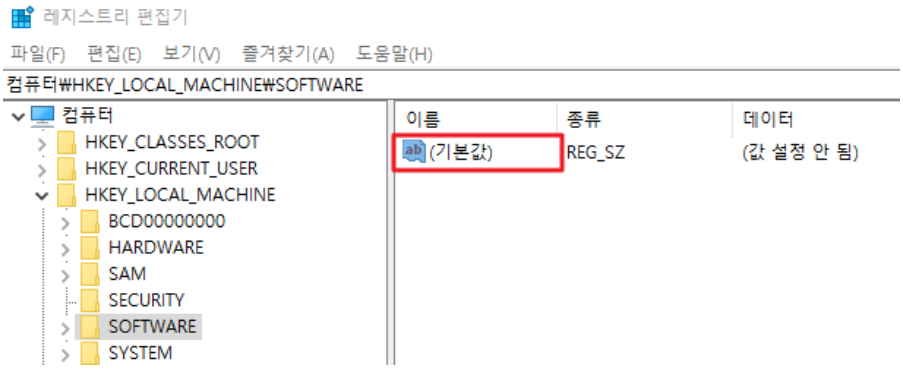
1. **분석 > 조사 > Live 검색** 페이지에서 신규 검색 버튼을 클릭합니다.
2. 검색 타입 선택에서 빠른 파일 검색을 선택하고 다음을 클릭합니다.
3. 아래 조건에 따라 검색 대상을 선택합니다.

구분	설명
전체 엔드포인트	Insights 서버에 등록된 전체 엔드포인트를 대상으로 파일 검색을 수행합니다.
엔드포인트 그룹	**분석 > 엔드포인트 > 엔드포인트 그룹 관리** 에 등록된 특정 그룹을 대상으로 파일 검색을 수행합니다.
조직	**관리 > 설정 > 사용자 관리 > 정보 동기화** 를 통해 부서 정보가 등록되어 있는 경우 해당 부서를 대상으로 파일 검색을 수행합니다.

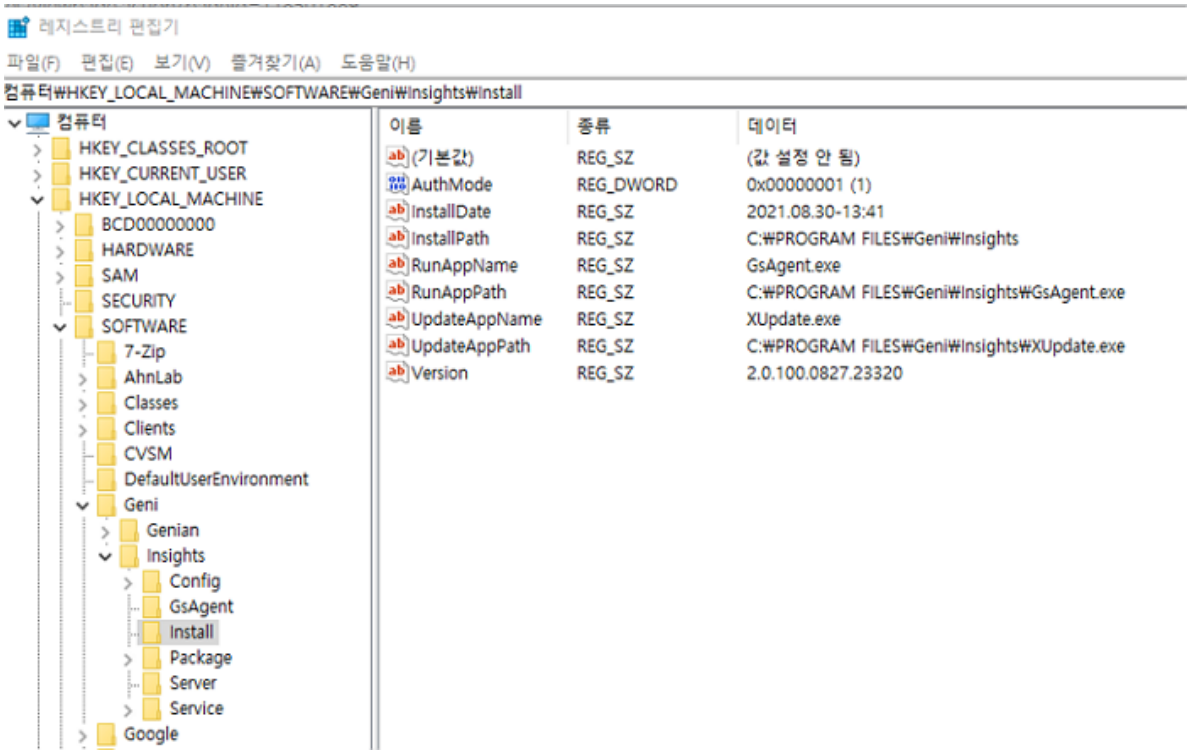
예제에서는 검색 대상 중 전체 엔드포인트를 선택합니다.

4. 검색 조건 추가버튼을 클릭 후 레지스트리 검색 조건을 설정합니다.



번호	구분	설명
1	기본 경로 선택	기본 경로 5 개 항목 중 검색할 경로를 선택합니다.HKEY_CLASSES_ROOT (HKCR), HKEY_CURRENT_USER(HKCU), HKEY_LOCAL_MACHINE(HKLM), HKEY_USERS(HKU), HKEY_CURRENT_CONFIG(HKCC)
2	상세 경로 입력	1의 기본 경로를 선택하면 하위에 사용할 수 있는 상세 경로 COMPONENTS 를 예제 박스에서 선택하거나, 직접 입력합니다.
3	하위 경로 포함	선택 시 레지스트리 경로 하위의 경로도 검색 대상에 포함합니다. (단, 엔드포인트 별 100개까지 수집)
3	경로에 해당하는 모든 데이터 수집	선택 시 찾을 내용과 상관없이 선택한 경로에 해당되는 Key, Value, Data를 모두 수집합니다. (단, 엔드포인트 별 100개까지 수집)
4	찾을 내용	찾을 내용을 입력하고 일부 포함 또는 정확하게 일치하는 경우만 찾을 지 선택합니다.
5	찾을 대상	찾을 대상을 선택합니다. (기본값) Value 만 검색의 경우 아래와 같은 항목을 검색합니다. 

설정 예)



기본 경로: HKEY_LOCAL_MACHINE ,상세경로: SOFTWARE\GENI\Insights , 찾을 내용: GsAgent.exe , 찾을 대상: Key, Values, Date 로 설정 후

하위 경로 포함 선택 시: HKEY_LOCAL_MACHINE\SOFTWARE\GENI\Insights\Install, RunAppName:GsAgent.exe 를 찾을 수 있음

경로에 해당하는 모든 데이터 수집 선택 시(찾을 내용과 대상은 disable 됨): HKEY_LOCAL_MACHINE\SOFTWARE\GENI\Insights\Config 부터 Service 까지 모든 데이터 중 100 개까지 수집

5. 4에서 저장한 조건이 표시되며, 필요한 경우 추가 버튼을 클릭하면 조건 설정 화면으로 이동합니다. 화면에서 조건 설정 후 저장 시 OR 조건으로 설정됩니다.

   조건 확인 후 검색 시작 버튼을 클릭합니다.

레지스트리 검색 만료일을 선택 한 후 검색 시작 버튼을 클릭하면 검색이 시작됩니다.

6. 레지스트리 검색 수행 결과를 확인합니다.

   지난 검색 결과 찾기 검색바를 이용하여 검색 조건에 해당하는 검색 결과를 찾을 수 있습니다.

   검색 결과는 7일간 유지되며, 결과 삭제를 원하지 않는 경우 잠금 아이콘을 이용하여 삭제하지 않도록 설정할 수 있습니다.

3.4.4 검색 결과

1. LIVE 검색 목록에서 검색이 완료된 목록을 클릭, 상세 화면으로 이동합니다.

   전체 클릭 시 개별 엔드포인트에서 검색된 결과가 표시되며, 엔드포인트별 최대 100개까지 확인할 수 있습니다.

결과	설명
준비	검색 대상(검색을 시작하지 않은) 엔드포인트 수
시작	검색 요청을 수신한 엔드포인트 수
실패	검색 실패를 수신한 엔드포인트 수
완료	검색이 완료된 엔드포인트 수
전체	결과 전송과 상관없이 검색 대상 전체 엔드포인트 수

2. 검색 결과 입력창에서는 파일 or 레지스트리 검색 타입에 따라 아래와 같은 키워드 검색이 가능합니다.

검색 가능 keyword
부서코드, 부서명, 인증사용자 ID, 인증사용자 명, 파일명, 파일 설명, 파일경로, MD5, SHA256, IP 정보 RegDataSize, RegDataType, RegKeyPath, RegNewKeyPath, RegValue, RegValueName

3. 파일 검색 의 경우 통계 차트 아이콘 클릭 시 파일명, IP, 인증사용자 기준 TOP 10 차트 및 데이터를 확인할 수 있습니다.
4. 레지스트리 검색 의 경우 통계 차트 아이콘 클릭 시 결과 타입 분류, 레지스트리 경로 TOP 10, 레지스트리 값 TOP 10, IP 기준 TOP 10 차트 및 데이터를 확인할 수 있습니다.

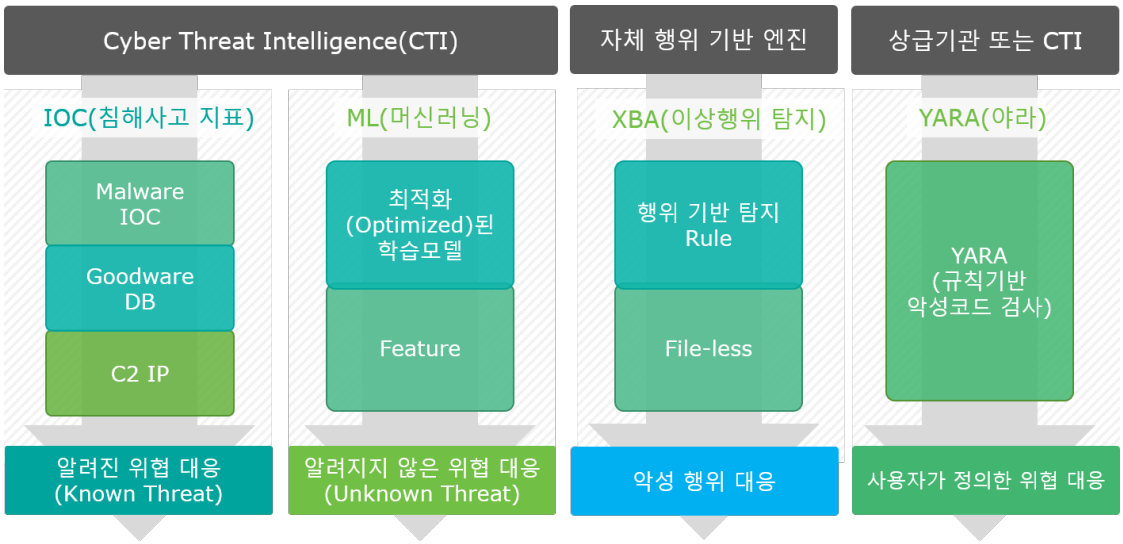
CHAPTER

FOUR

PHASE 4 - 위협 탐지

Genian Insights E 3.0은 **위협의 종류** 에 따라 다양한 탐지 모듈을 이용하여 위협을 탐지, 대응합니다.

File 기반의 위협 은 크게 **악성코드** 로 분류되며, 악성코드는 **알려진 위협** 과 **알려지지 않은 위협** 으로 세분화 할 수 있습니다.
File-less 기반의 위협 은 **이상행위** 로 분류되며, 행위기반 이상탐지 엔진에 의해 탐지됩니다.



이 장에서는 다양한 위협 탐지 기술에 대해 설명합니다.

4.1 ANTIRANSOM 행위기반 탐지

안티랜섬은 고도화되는 랜섬웨어 위협으로부터 기업의 자산과 업무 연속성을 보호합니다.

기존의 시그니처(Signature)에 의존하는 기존 보안 체계의 한계를 넘어, 행위기반 탐지 기술을 통해 신/변종 랜섬웨어를 실시간으로 차단하는 솔루션입니다.

안티랜섬 적용을 통해 랜섬웨어의 행위기반 탐지 및 차단은 물론 백업과 복원까지 진행합니다.

행위기반 탐지로 Fileless 및 정상 프로세스의 메모리에 인젝션되는 형태의 랜섬웨어도 탐지가 가능하며,
랜섬웨어 행위가 발생한 프로세스를 연계분석하여 대응합니다.

4.1.1 안티랜섬 주요 기능 및 동작 방식

안티랜섬 모듈은 단순 시그니처 기반 차단을 넘어, **행위 기반 탐지** 와 **실시간 백업 및 복원** 을 핵심 가치로 합니다. 고도화된 랜섬웨어 위협에 대응하기 위한 주요 기능과 동작 방식은 다음과 같습니다.

1. 주요 기능

- **실시간 보호 및 행위 기반 탐지**: 실시간 I/O 모니터링 드라이버를 통해 프로세스의 모든 행위를 분석합니다. 이를 통해 Fileless 공격이나 정상 프로세스 메모리에 인젝션되는 지능형 위협까지 정밀하게 탐지합니다.
- **실시간 파일 백업**: 보호 대상 파일(문서, 압축파일, 이미지 등 지정된 확장자)이 변조되기 직전, 해당 프로세스를 일시 중지하고 원본 파일을 안전한 경로(`C:\Program Files\Geni\AntiRansom\backup`)로 즉시 복사합니다.
- **백업 폴더 및 데이터 보호**: 백업된 데이터가 랜섬웨어에 의해 2차 훼손되지 않도록 강력한 자체 보호 기능을 수행합니다.
- **MBR 보호**: 시스템 부팅을 방해하기 위해 마스터 부트 레코드(MBR)를 변조하거나 파괴하려는 시도를 실시간으로 차단합니다.

2. 동작 방식

설정된 운영 모드에 따라 탐지 후 다음과 같은 단계로 대응을 수행합니다.

1. **모니터링 단계**: Insights E 에이전트가 시스템 내 I/O 및 프로세스 행위를 지속적으로 감시합니다.
2. **탐지 및 백업**: 랜섬웨어 의심 행위가 발견되는 즉시, 파일이 암호화되기 전 실시간 백업을 우선 수행합니다.
3. **대응 및 복원 (운영 모드별 차이)**:
    - **Monitoring 모드**: 행위 탐지 시 로그 기록만 수행하며, 강제 종료나 복원 등의 대응은 자동으로 수행하지 않습니다.
    - **Active 모드 (수동 복원)**: 탐지 즉시 해당 프로세스를 강제 종료하고 실행 파일을 삭제합니다. 이후 관리자가 위협을 분석하여 '악성'으로 판정하는 시점에 복원을 진행합니다.
    - **Active 모드 (자동 복원)**: 탐지 시 프로세스 차단은 물론, 백업된 데이터를 이용해 변조된 파일을 즉시 원상태로 복구합니다.

3. 기술적 특징 및 장점

- **정밀한 차단 범위**: 랜섬웨어 본체뿐만 아니라, 랜섬웨어에 의해 생성(Drop)된 파일이나 유포지로 사용된 실행 파일까지 추적하여 일괄 차단 및 삭제합니다.
- **시스템 안정성 확보**: 정상 프로세스 내부에 악성 스레드가 생성된 경우, 프로세스 전체를 종료하지 않고 **악성 스레드만 선별하여 종료** 함으로써 업무 중단을 최소화합니다.
- **효율적인 자원 관리**: 모든 데이터를 상시 백업하는 대신 변조 행위 발생 시점에만 대상 파일을 백업하므로 디스크 공간을 효율적으로 사용하며, 설정된 정책에 따라 백업 파일을 자동 최적화(삭제)합니다.

Note: 안정적인 서비스 운영을 위해 초기 도입 시에는 모니터링 모드로 운용하며 업무 환경에 적합한 예외 프로세스를 식별할 것을 권장합니다.

4.1.2 안티랜섬 행위기반 탐지 예외 프로세스 설정 방법

안티랜섬 모듈과 타 프로세스 간의 호환성 이슈를 방지하거나 특정 프로세스의 성능 저하가 우려될 경우, **행위기반 탐지 예외 프로세스**로 등록하여 보다 안정적인 업무 환경을 구축할 수 있습니다.

정책 별 설정

1. [정책] > [그룹 정책 관리] > [그룹 정책 목록] > 정책 선택
2. [안티랜섬] 탭의 '기본 설정'에서 행위기반 탐지 예외 프로세스 설정
3. 파일 경로 or 해시 or 전자서명 기반으로 예외 설정 가능

글로벌 설정

1. [관리] > [설정] > [환경설정] > [탐지 및 대응] 메뉴로 이동
2. '안티 랜섬'에서 행위기반 탐지 예외 프로세스 설정
3. 파일 경로 or 해시 or 전자서명 기반으로 예외 설정 가능

4.2 IOC 기반 탐지

IOC(Indicator Of Compromise, 침해지표) 는 전 세계에서 발생 및 기록되는 침해사고의 흔적들을 수집하고 이 정보들을 별도의 DB로 관리하고 있으며,
Insights E 정책서버는 외부의 IOC DB 서버와 주기적으로 통신하여 최신 위협 정보를 업데이트 하고 있습니다.
폐쇄망 환경에서는 정책서버에 월 단위의 IOC DB를 직접 업데이트 할 수 있습니다.

엔드포인트에서 파일, 프로세스에 대한 이벤트가 발생하면 정책서버의 위협탐지(Threat Detector) 엔진이 IOC DB에 해당 파일의 Hash값이 등록되어 있는 지 확인합니다.
파일정보가 등록되어 있는 경우, 해당 파일은 **알려진 위협** 으로 분류되며, IOC에 등록된 신뢰도, 위험도, 악성코드의 종류 정보를 확인할 수 있습니다.

IOC DB에 파일 정보가 등록되어 있지 않다면, 머신러닝 정보를 확인합니다.

4.2.1 IOC에 등록되지 않은 데이터 처리 방법

Genian Insights E는 IOC(Indicators of Compromise) Database를 이용하여 알려진 위협에 대한 탐지 및 대응이 가능합니다.
IOC Database의 경우 정기적으로 업데이트되지만 알려지지 않는 악성 프로그램이나 악의적인 IP를 관리자가 직접 등록하여 탐지하는 **사용자정의 IOC 관리** 기능을 제공하고 있습니다.
해당 악성 프로그램은 MD5 Hash 값을 등록하여 탐지할 수 있습니다.

Genian Insights E 설정을 통해 에이전트 설치 시 수집한 정보에서 프로그램에 대한 MD5 HASH 값을 확인 가능합니다.

MD5 Hash 값 확인 방법

1. **통합검색 > Endpoint** 메뉴로 이동, 에이전트에서 수집한 프로세스 정보가 표시되며, 등록하고자 하는 파일의 목록을 더블클릭 합니다.
2. 선택 가능 필드 항목 중, MD5 Hash 정보를 확인할 수 있습니다.

확인한 정보로 Hash 값을 등록하는 방법은 아래 해당하는 목록으로 이동하여 확인할 수 있습니다.

Malware Hash

1. 정책 > 사용자정의 IOC 관리 > Malware Hash 메뉴로 이동 후 상단의 추가 버튼을 클릭합니다.
2. 해시값은 필수로 입력하고 기타 필요한 정보 입력 후 저장 버튼을 클릭합니다.

항목	설명
대응여부-탐지	Malware Hash 탐지 시 관리자 페이지의 분석 탭 대응 컬럼에 관련 정보 태그만 표시하며, 사용자 PC에 특별한 Action을 수행하지 않습니다.
대응여부-탐지및대응	Malware Hash 탐지 시 관리자 페이지의 분석 탭 대응 컬럼에 관련 정보 , 태그 및 Genian NAC에서 설정한 Action (관리자 커스텀 태그) 을 수행합니다. 대응 설정은 Threat Detector 플러그인 설정을 따릅니다.
사전실행차단	Malware Hash로 등록된 데이터를 에이전트에서 가지고 있다가 hash가 일치하는 파일이 실행될 경우 즉시 차단하게 되며, 사용자 PC에 차단 알림 메시지를 표시합니다.

Malware Hash 수정

1. 정책 > 사용자정의 IOC 관리 > Malware Hash 메뉴로 이동 후 수정할 hash 목록의 값을 클릭합니다.
2. hash 값을 제외한 정보를 수정할 수 있습니다.
3. hash 수정 페이지에서 외부 링크 버튼 클릭 시 미리 등록된 검색 사이트에서 해당 hash 값에 대한 정보를 조회할 수 있습니다.

Malware Hash 삭제

1. 정책 > 사용자정의 IOC 관리 > Malware Hash 메뉴로 이동 후 삭제할 hash 목록의 체크박스를 선택합니다. 버튼이 활성화 되면 클릭합니다.
2. 확인 팝업창이 발생하며 확인 버튼을 클릭합니다.

Malicious IP

Malicious IP 추가

1. **정책 > 사용자정의 IOC 관리 > Malicious IP** 메뉴로 이동 후 상단의 추가 버튼을 클릭합니다.
2. 구분을 통해 단일, 서브넷, 주소 범위를 선택할 수 있습니다. IP는 필수로 입력하고 기타 필요한 정보 입력 후 저장 버튼을 클릭합니다.

항목	설명
대응여부-탐지	Malicious IP 탐지 시 관리자 페이지의 분석 탭 대응컬럼에 관련 정보 만 표시하며, 사용자 PC에 특별한 Action을 수행하지 않습니다.
대응여부-탐지 및 대응	Malicious IP 탐지 시 관리자 페이지의 분석 탭 대응컬럼에 관련 정보, 태그 및 설정한 Action (관리자 커스텀 태그) 을 수행합니다. 대응 설정은 Threat Detector 플러그인 설정을 따릅니다.

Malicious IP 수정

1. **정책 > 사용자정의 IOC 관리 > Malicious IP** 메뉴로 이동 후 수정할 IP 목록을 클릭합니다.
2. IP를 제외한 정보를 수정할 수 있습니다.

Malicious IP 삭제

1. **정책 > 사용자정의 IOC 관리 > Malicious IP** 메뉴로 이동 후 삭제할 IP 목록의 체크박스를 선택합니다. 버튼이 활성화 되면 클릭합니다.
2. 확인 팝업창이 발생하며 확인 버튼을 클릭합니다.

Goodware Hash

IOC(Indicator Of Compromise, 침해지표)에 등록되어 탐지되었으나, 정상적인 파일로 판단되지만 IOC Database 업데이트가 되지않아 오탐(False Positive)이 발생하는 경우 관련 정보를 관리자가 직접 등록하여 예외처리 할 수 있습니다.

Goodware Hash 추가

1. **정책 > 사용자정의 IOC 관리 > Goodware Hash** 메뉴로 이동 후 상단의 추가 버튼을 클릭합니다.
2. hash(MD5) 값은 필수로 입력하고 기타 필요한 정보 입력 후 저장 버튼을 클릭합니다.

Goodware Hash 수정

1. **정책 > 사용자정의 IOC 관리 > Goodware Hash** 메뉴로 이동 후 수정할 MD5 hash목록을 클릭합니다.
2. hash(MD5) 값을 제외한 정보를 수정할 수 있습니다.
3. Goodware Hash 수정 페이지에서 외부 링크 버튼 클릭 시 미리 등록된 검색 사이트에서 해당 MD5 hash 값에 대한 정보를 조회할 수 있습니다.

Goodware Hash 삭제

1. **정책 > 사용자정의 IOC 관리 > Goodware Hash** 메뉴로 이동 후 삭제할 MD5 hash 목록의 체크박스를 선택합니다. 버튼이 활성화 되면 클릭합니다.
2. 확인 팝업창이 발생하며 확인 버튼을 클릭합니다.

Good IP

Good IP 추가

1. **정책 > 사용자정의 IOC 관리 > Good IP** 메뉴로 이동 후 상단의 추가 버튼을 클릭합니다.
2. 구분에서 단일, 서브넷, 주소 범위를 설정할 수 있습니다.
   단일 버튼을 클릭합니다. IP는 필수로 입력하고 기타 필요한 정보 입력 후 저장 버튼을 클릭합니다.
3. 또한 Network Event일 **경우 분석 > 위협 관리 > 공격 스토리 라인**에서 사용자 정의 `Good IP`로 등록 버튼을 클릭해 Good IP를 추가할 수 있습니다.

Good IP 수정

1. **정책 > 사용자정의 IOC 관리 > Good IP** 메뉴로 이동 후 수정할 IP 목록을 클릭합니다.
2. IP를 제외한 정보를 수정할 수 있습니다.

Good IP 삭제

1. **정책 > 사용자정의 IOC 관리 > Good IP** 메뉴로 이동 후 삭제할 IP 목록의 체크박스를 선택합니다. 버튼이 활성화 되면 클릭합니다.
2. 확인 팝업창이 발생하며 확인 버튼을 클릭합니다.

4.3 ML 기반 탐지

엔드포인트에서 수집되는 정보 중 파일의 종류가 실행 파일(PE)인 경우, 해당 파일의 특징(Feature)을 추출합니다.
이 특징(Feature) 정보는 머신러닝에 의한 악성코드 탐지에 사용됩니다.

해당 파일이 조회가 된다면 **알려진 위협** 으로 분류되며, 정보가 없다면 **알려지지 않은 위협** 으로 분류됩니다.

알려진 위협과 알려지지 않은 위협은 관리자가 미리 설정한 정책(대응 방법)에 따라 에이전트에서 알람, 프로세스 강제 종료, 파일 삭제를 수행합니다.

머신 러닝에 의해서도 탐지되지 않는 경우, Reversing Labs, VirusTotal 등의 외부 인텔리전스(CTI:Cyber Threat Intelligence Service)에 등록된 파일인 지 한번 더 조회하는 절차를 수행합니다.

4.4 XBA 기반 행위 탐지

File-less 기반의 위협은 **이상행위** 로 분류되며, 이상행위 탐지(XBA:X Behavior Analysis) 엔진에 의해 탐지합니다.
행위기반 이상탐지 엔진은 미리 정의한 이상행위 정책을 가지고 있으며, 엔드포인트에서 이상행위 감지 시 즉시 탐지 및 대응이 가능합니다.
MITRE ATT&CK(Adversarial Tactics, Techniques, and Common Knowledge-공격자 관점의 전술, 기술, 절차를 프레임워크로 제공하는 지식 베이스) 공격 기법 탐지 및 관련 정보를 제공합니다.

4.4.1 이상행위 탐지 정책 설정 방법

모든 엔드포인트는 이상행위 룰셋에 등록된 기본 룰셋을 적용받습니다.
특정 엔드포인트에 별도의 이상행위 룰 적용이 필요한 경우 룰셋을 추가하여 해당 엔드포인트가 속한 그룹 정책에 별도로 생성한 룰셋을 적용받도록 설정할 수 있습니다.

이상행위 탐지 설정

기본 룰셋

항목	설명
카테고리	Insights E Rule 과 MITRE ATT&CK Rule 을 지원합니다.
이름	미리 정의된 진단명 입니다.
OS	이상행위 진단이 가능한 OS 이며, 현재는 windows 만 지원합니다.
사용	이상행위 진단 룰 사용 여부 옵션입니다. (기본값: on)
이벤트 타입	이상행위 진단 시 이벤트 타입(file, Module, Network, process, Registry)에 따라 진단하는 정책이 달라집니다.
신뢰도	내부적으로 정의되어있는 신뢰도 입니다.
위협 유형	위협 유형은 8개의 카테고리(Anomaly,Autorun,Exploit,Fake,LateralMovement,Ransomware,Rootkit,UacBypass)로 분류됩니다.
MITRE ATT&CK Technique	MITRE ATT&CK(Adversarial Tactics, Techniques, and Common Knowledge-공격자 관점의 전술, 기술, 절차를 프레임워크로 제공하는 지식 베이스) 정보를 제공합니다. MITRE ATT&CK Technique 정보가 있는 경우 클릭 시 해당 정보 site로 이동합니다.
자동 대응	이상행위 룰에 의한 이상행위 탐지 시 자동으로 대응할 방법(알림, 프로세스 강제종료, 대응 안함)을 설정합니다.
예외	이상행위 룰은 기본으로 진단을 하도록 설정이 되어 있으나, 이상행위 룰을 사용하지 않을 예외 규칙 설정을 할 수 있습니다. **정책 > 이상행위 관리 > 진단 예외 설정** 에서 예외 규칙을 작성하고 예외처리를 반영할 룰을 선택하거나, 이상행위 룰 관리 상세 화면에서 직접 예외처리 규칙을 설정할 수 있습니다.
설명	이상행위 규칙에 대한 관리자 memo를 입력합니다.

룰셋 추가

기본 룰셋 이외에 특정 엔드포인트만 적용 or 제외해야할 규칙이 있는 경우 예외가 적용된 룰셋을 추가할 수 있습니다.

1. 추가 버튼을 클릭, 복사할 룰셋 선택 후 생성 버튼을 클릭합니다.
2. 다르게 적용할 룰셋을 수정한 후 저장 및 상단의 정책 즉시 적용 버튼을 클릭합니다.
3. **정책 > 그룹 정책 관리 > 그룹 정책 목록** 메뉴 내 생성된 정책의 상세 화면에서 1에서 생성한 이상행위 룰셋을 선택 후 저장 및 정책 즉시 적용을 수행합니다.

이상행위 탐지 시 대응

이상행위 정책에 의한 탐지 시, 오탐 및 빈번한 알람이 발생할 수 있어서 기본 대응은 관리콘솔에서 관리자만 인지할 수 있도록 되어 있습니다.
단말(PC)에 알림이 필요하거나, 이상행위 발생 프로세스의 종료가 필요한 경우 자동대응 설정을 통해 위협 대응을 할 수 있습니다.

1. 대응설정을 할 이상행위 룰 이름을 클릭, 상세 설정에서 자동대응을 선택합니다.
2. 자동대응 선택 시 왼쪽 상단에 저장 버튼을 클릭해야 변경사항이 반영되며, 저장 완료 후 오른쪽 상단의 정책 즉시 적용 버튼을 클릭해야 에이전트에 정책이 전달 됩니다.
3. 자동대응 설정한 이상행위가 탐지되면 **분석 > 위협 관리** 메뉴에서 해당 위협의 요약 정보에 자동 대응 정책 항목을 확인할 수 있습니다.

이상행위 탐지 예외 설정

이상행위 엔진은 관리콘솔에 미리 정의된 이상행위 규칙을 탐지합니다.

오탐을 줄이기 위해 탐지 전에 미리 예외 정책을 설정하거나, 오탐이 된 이후 위협 관리를 통해 예외 처리할 수 있습니다.

탐지 전 진단 예외 설정

진단 예외 설정 생성

1. **정책 > 이상행위 관리 > 진단 예외 설정** 메뉴로 이동 후 상단의 추가 버튼을 클릭합니다.
2. 규칙 명, 동작모드 및 예외 규칙 설정 후 저장 버튼을 클릭합니다.

-	항목	설명
예외 적용 방식	전체	모든 엔드포인트에 진단 예외 정책을 적용합니다.
예외 적용 방식	미적용대상 설정	예외처리를 적용하지 않을 대상을 설정합니다.
예외 적용 방식	적용대상 설정	예외처리를 적용할 대상을 설정합니다.

정책 적용 대상은 IP 또는 부서 정보 입력을 통해 설정할 수 있습니다. 정책 예외처리 대상 설정 후 나머지 상세 정보를 입력 후 저장 버튼을 클릭합니다.
3. 사용자가 등록한 예외 설정을 목록에서 확인할 수 있으며, 오른쪽 상단 메뉴 옆 정책 즉시 적용 버튼을 클릭합니다.
4. 정책 적용 팝업창이 표시 되며, 확인 버튼을 클릭하면 엔드포인트에 즉시 적용됩니다.

진단 예외 설정 수정

1. **정책 > 이상행위 관리 > 이상행위 룰 관리 > 진단 예외 설정** 메뉴로 이동 후 수정 할 규칙명을 클릭합니다.
2. 규칙 수정 후 저장 버튼을 클릭합니다.
3. 오른쪽 상단 메뉴 옆 정책 즉시 적용 버튼을 클릭합니다.
4. 정책 적용 팝업창이 표시 되며, 확인 버튼을 클릭하면 엔드포인트에 즉시 적용됩니다.

진단 예외 설정 삭제

1. **정책 > 이상행위 관리 > 이상행위 룰 관리 > 진단 예외 설정** 메뉴로 이동 후 삭제 할 목록의 체크 박스를 선택합니다. 삭제 버튼이 활성화되면 클릭합니다.

진단 예외 설정 엑셀 내보내기

1. **정책 > 이상행위 관리 > 이상행위 룰 관리 > 진단예외설정** 메뉴로 이동 후 왼쪽 상단의 저장 버튼을 클릭, 내보내기 메뉴를 클릭합니다.
2. 1에서 목록을 선택하지 않으면 현재 등록된 목록 전체를 내보내며, 목록 선택 시 선택한 항목만 내보내기 할 수 있습니다.

진단 예외 설정 엑셀 가져오기

1. **정책 > 이상행위 관리 > 이상행위 룰 관리 > 진단예외설정** 메뉴로 이동 후 왼쪽 상단의 저장 버튼을 클릭, 가져오기 메뉴를 클릭합니다.
2. 관리자 페이지에 등록된 목록에 엑셀 목록을 덮어 쓰거나 등록된 목록 삭제 후 엑셀 파일에 등록된 목록만 등록할 수 있습니다.
3. **기존 데이터 유지** 는 서버에 A라는 데이터가 존재하고, 엑셀 파일에 동일하게 A 데이터가 존재했을 때 기존 데이터 유지를 선택하고 파일을 업로드 하면 기존 데이터 유지 카운트가 표시됩니다.

탐지 후 진단 예외 설정

오탐으로 진단된 이상행위는 관리콘솔에서 관리자가 직접 예외처리 할 수 있습니다.

1. **분석 > 위협 > 위협관리** 메뉴로 이동 합니다.
2. 위협으로 탐지된 목록 중 예외처리 할 이상행위 탐지목록의 오른쪽 화면에 위협 분석 버튼을 클릭합니다.
3. 탐지된 위협에 대한 상세 정보 화면이 표시되며, 오른쪽 상단의 위협 관리 (신규) 버튼을 클릭합니다.
4. 위협 관리 상세 화면이 펼쳐지며, 내가 담당하기 버튼을 클릭합니다.
5. 위협 판정에서 안전 라디오 버튼을 선택하면 진단 예외 설정-진단 예외 규칙 추가 파란색 버튼이 활성화 됩니다. 진단 예외 규칙 추가 버튼을 클릭합니다.
6. 오탐으로 진단되었던 프로세스 명 또는 파일 경로 또는 의심 파일 경로가 자동으로 작성된 진단 예외 규칙 추가 팝업창이 발생하며, 규칙명을 자유롭게 입력 후 저장 버튼을 클릭합니다.
7. 진단 예외 규칙 추가 버튼 아래 설정 완료 버튼을 클릭하여, 예외 설정을 완료합니다.
8. 오른쪽 상단에 정책 즉시 적용 버튼이 깜빡이며, 클릭하여 예외 정책을 에이전트에 즉시 적용하도록 합니다.
9. 다음에 예외설정과 동일한 행위가 발생하는 경우, 이상행위로 진단에서 예외처리 됩니다.
10. 위협 관리 화면에서 예외처리한 내용은 **정책 > 이상행위 관리 > 이상행위 룰 관리 > 진단 예외 설정** 메뉴로 이동, 목록에서 확인할 수 있습니다.

4.5 YARA 기반 탐지

YARA는 문자열이나 바이너리 패턴(Hex string)을 기반으로 악성코드를 검색, 분류할 수 있게 해주는 도구로,
문자열과 바이너리 패턴만을 이용해서 파일의 시그니처를 찾는 것뿐만 아니라 특정 Entry Point 값을
지정하거나,File Offset, Virtual Memory Address를 제시하고
정규 표현식을 이용하여 효율적인 패턴 매칭이 가능합니다.

Genian Insights E는 관리자가 직접 작성한 YARA Rule을 통해 빠르고 효율적으로 엔드포인트의 위협을 탐지할 수 있습니다.

4.5.1 YARA Rule 등록 방법

YARA는 악성코드 시그니처를 이용해서 악성 코드의 종류를 식별하고 분류하는 목적으로 사용하는 도구입니다.
악성코드의 시그니처는 파일, 프로세스에 포함되어 있는 텍스트 문자열 또는 바이너리 패턴으로 되어 있으며, Genian Insights E는 YARA를 이용하여 악성코드 샘플에 포함된 패턴을 탐지 및 대응이 가능합니다.
YARA는 관리자가 직접 파일 또는 프로세스에서 확인하고자 하는 패턴 정보가 담긴 YARA Rule 작성하고, 개별 엔드포인트에 YARA Rule 검사 명령을 수행하는 형태로 동작합니다.

YARA Rule 등록 및 검사 명령 수행 방법은 아래와 같습니다.

YARA Rule 추가

1. **정책 > YARA Rule 관리 > YARA Rule** 메뉴로 이동 후 상단의 추가 버튼을 클릭합니다.
2. 이름과 규칙은 필수로 입력하고 저장 버튼을 클릭합니다.

항목	설명
이름	YARA Rule 정책 이름을 입력합니다. 최대 128자까지 입력할 수 있습니다.
규칙	파일 또는 프로세스에서 확인하고자 하는 패턴 정보가 담긴 YARA Rule 을 작성합니다. 최대 12000자까지 입력할 수 있습니다.

YARA Rule의 최소한으로 갖춰야 할 형태는 아래와 같습니다.

```
rule 룰_이름
{
condition:
Boolean 값
}
```

YARA Rule 수정

1. 정책 > YARA Rule 관리 > YARA Rule 메뉴로 이동 후 수정할 YARA Rule을 클릭합니다.
2. Rule 수정 후 저장 버튼을 클릭합니다.

YARA Rule 삭제

1. 정책 > YARA Rule 관리 > YARA Rule 메뉴로 이동 후 삭제할 YARA Rule 목록의 체크박스를 선택합니다. 버튼이 활성화 되면 클릭합니다.

YARA Rule 사용여부

1. 정책 > YARA Rule 관리 > YARA Rule 메뉴로 이동 후 사용여부를 수정할 YARA Rule 목록의 체크박스를 선택합니다. 작업 선택에서 사용 여부를 선택합니다.
   사용여부 선택 시 변경 사항이 즉시 반영됩니다.

YARA Rule 정책 적용

YARA Rule 작성 후 개별 엔드포인트에 대해 검사 명령을 수행하여야 합니다.

1. **분석 > 엔드포인트 > 엔드포인트 목록** 메뉴로 이동 후 검사 명령을 수행 할 목록을 클릭합니다.
2. 엔드포인트 상세 목록 화면에서 작업선택, `YARA Rule 검사` 를 클릭합니다. 목록 중 전체 Rule 또는 선택한 Rule 중 클릭합니다.
   아래 예제에서는 선택한 Rule 적용방법에 대해 서술합니다.
3. 선택한 Rule 클릭 시 **정책 > YARA Rule 관리**에서 생성했던 정책 중 사용 여부가 사용함 인 정책 목록이 표시됩니다.
4. YARA Rule 검사 여부에 대해 **분석 > 엔드포인트 > 엔드포인트 목록** 메뉴에서 표시된 그림과 같이 톱니바퀴 모양의 아이콘이 파란색으로 활성화 되어 있습니다.
5. **분석 > 엔드포인트 > 엔드포인트 목록** 에서 `IP`를 클릭하여 로그 탭으로 이동 시, 에이전트에서 위협 탐지 후 처리한 결과 및 YARA Rule 관련 로그를 확인 할 수 있습니다.
6. **분석 > 위협 관리** 에서 `YARA Rule 탐지 목록` 을 클릭하면 상세 화면에 어떤 파일을 탐지했는 지 확인 할 수 있습니다.
   자세한 정보는 목록 오른쪽의 위협 분석 버튼을 클릭하여 상세 화면으로 이동하여 확인할 수 있습니다.
7. YARA Rule 탐지한 파일을 격리 또는 위협 파일로 등록하고자 하는 경우 오른쪽 위협 관리에서 대응 방법을 선택합니다.

CHAPTER

FIVE

PHASE 5 - 위협 분석

엔드포인트에서 수집한 이벤트를 바탕으로, 위협 탐지엔진에 의해 위협이 탐지되면 관리콘솔에서 위협 상세 정보를 확인할 수 있습니다.

분석 > 위협 모니터링 에서 확인할 수 있는 정보는 아래와 같습니다.

항목	설명
상태별 위협 현황	• **신규:** 신규로 탐지된 위협 숫자 입니다. • **처리중:** 담당자가 위협 관리에서 '내가 담당하기' 버튼을 클릭하여 검토하고 있는 위협 숫자 입니다. • **해결됨:** 담당자가 위협 관리에서 '내가 담당하기' 버튼을 클릭하여 위협 판정(악성/안전/보류)을 완료 한 숫자 입니다. • 해결됨 숫자는 **해결된 위협 포함** 을 선택해야 표시 됩니다.
엔드포인트 현황	• **UP:** 에이전트가 설치된 엔드포인트 중 동작(UP)중인 엔트포인트 수 입니다. • **DOWN:** 에이전트가 설치된 엔드포인트 중 동작안함(DOWN)상태인 엔트포인트 수 입니다. • **삭제됨:** 에이전트가 삭제된 엔드포인트 수 입니다. • **격리됨:** 네트워크 차단(격리) 상태인 엔드포인트 수 입니다. 엔드포인트가 차단(격리) 상태여도 Insights E 서버와 통신이 가능합니다.
최근 탐지 위협	최근 5건의 위협 발생 정보를 표시합니다. (1시간 이내이면 노란색 백그라운드)
위협 표시 설정	**해결된 위협 포함:** 위협 탐지 시 관리자 확인이 완료된 위협까지 포함하여 표시할 지를 설정합니다. **검색 날짜:** 최소 오늘부터 최대 1개월까지의 위협 현황을 검색합니다. 날짜 검색 범위는 아래와 같습니다. (ex: 현재시각이 2021-06-06 13:00 인 경우) • **오늘:** 2021-06-06 00:00 ~ 2021-06-06 23:59 • **어제:** 2021-06-05 00:00 ~ 2021-06-05 23:59 • **이번주:** 2021-06-04 00:00 ~ 2021-06-10 23:59 • **지난주:** 2021-05-28 00:00 ~ 2021-06-03 23:59 • **1일:** 2021-06-05 00:00 ~ 2021-06-06 23:59 • **1주일:** 2021-05-30 00:00 ~ 2021-06-06 23:59 • **1개월:** 2021-05-06 00:00 ~ 2021-06-06 23:59 **기타 기능:** • **인쇄:** 위협 모니터링 화면을 인쇄합니다. • **자동갱신:** 위협 모니터링 화면을 1분마다 갱신합니다. • **전체화면보기:** 위협 모니터링 화면을 전체 화면으로 표시합니다.
위협통계-최근 위협 현황	• **전체 위협:** 파일/프로세스(IOC, 머신러닝,YARA), 악성IP, 배치 탐지 전체 항목에 대한 탐지 숫자 입니다. • **감염:** 위협 파일/프로세스(IOC, 머신러닝,YARA, 배치탐지) 에 대한 탐지 숫자 입니다. • **악성IP:** 악성IP로 등록된 정보를 탐지한 숫자 입니다. • **이상행위:** 이상행위 정책에 의해 탐지된 위협 숫자 입니다. • **배치:** 배치를 탐지한 숫자 입니다. (배치탐지란 에이전트가 PC 정보를 전송한 후 IOC DB가 업데이트 되면 일정 기간(default: 3일)동안 수집한 정보를 확인하여 새로 업데이트 된 위협이 있는 지 분석하는 역할을 합니다. 매일 02:00 수행, 06:00 이내에 종료) **해결된 위협 포함** 여부에 따라 탐지 숫자가 달라집니다.
다수의 단말에 분포된 악성코드 TOP 10	악성코드의 MD5를 기준으로 목록이 표시되며, 숫자 박스는 해당 악성코드가 발생한 단말 수를 표시합니다.
다수 단말에 분포된 이상행위 TOP 10	이상행위정책을 기준으로 목록이 표시되며, 숫자 박스는 해당 이상행위정책을 탐지한 단말 수를 표시합니다.
다수 위협이 발생한 단말 TOP 10	인증사용자명/호스트명/IP/부서명 으로 위협(악성코드+이상행위) 탐지 수를 표시합니다. 설정 아이콘 클릭 시 표시 기준을 선택할 수 있습니다. 탐지 시 갯수에 따라 숫자 바탕의 색이 달라집니다. (8개이하-옅은색, 8개이상-짙은색)
위협 탐지 비율	탐지된 위협의 종류(IOC, CTI, ML, MaliciousIP, YARA, 이상행위 분류별) 가 1가지 이상인 경우 위협 발생 비율을 표시합니다.
이벤트 발생량 추이	endpoint2 인덱스를 기준으로 오늘, 어제, 주간 평균 이벤트 발생량을 그래프로 표시합니다.
관심 행위 지표	endpoint2 인덱스에 기록된 Tag 정보를 표시합니다. (자주 발생하지 않는 순으로 크게

5.1 수집된 아티팩트 분석

Genian Insights E는 XBA 진단 시 **아티팩트 자동 수집 기능**을 제공하고 있습니다.

5.1.1 아티팩트 수집 설정

아티팩트 수집 설정은 **관리 > 설정 > 탐지 및 대응** 중 **아티팩트 수집 대상**에서 설정 가능합니다.

수집 대상은 아래와 같습니다.

수집 대상	설명
system 정보	시스템 정보 수집
Autorun	자동실행 항목 수집
브라우저 방문 기록	브라우저 방문 기록 수집
레지스트리	레지스트리 하이브 수집
윈도우 이벤트	윈도우 이벤트 로그 수집
Prefetch 파일	Prefetch 파일 수집
FileSystem 정보	의심 파일 수집

Registry, File, Process은 아티팩트 자동 수집 대상입니다.

5.1.2 아티팩트 샘플 수집

샘플 수집

1. **분석 > 위협 관리**에서 이상행위로 탐지된 위협 목록 중 아티팩트 수집 요청이 가능한 위협의 위협 분석 버튼을 클릭합니다. 상세 화면에서 아티팩트 수집 버튼을 클릭합니다.
2. **분석 > 엔트포인트 목록**에서 원하는 단말 목록 선택 후 **작업선택 > 아티팩트 수집** 버튼을 클릭합니다.
3. **분석 > 엔트포인트 그룹 관리**에서 원하는 그룹 목록 선택 후 **작업선택 > 아티팩트 수집** 버튼을 클릭합니다.

수집된 아티팩트 확인

수집된 아티팩트는 **분석 > 수집 관리**에서 확인 가능합니다.

1. 아티팩트 수집 시, 수집 관리 목록에서 데이터 로드 버튼을 클릭합니다. 수집 데이터 로드가 끝난 후 `G-Report` 버튼이 생성됩니다.
2. `G-Report` 버튼 클릭 시 G-Report 창이 생성되며, 아티팩트 수집된 데이터를 리포트 형태로 확인할 수 있습니다.

5.2 단말별 탐지 이력 분석

탐지된 위협이 다수의 단말에서 탐지된 경우 단말별 탐지 정보에서 단말 목록을 확인할 수 있습니다. 10개 단말까지 표시되며, 더 많은 단말에서 탐지된 경우 모든 단말 이벤트 검색 버튼을 클릭하면 해당 위협이 탐지된 모든 단말 목록을 확인할 수 있습니다.

항목	설명
상태	엔드포인트의 동작 상태를 표시합니다.
사용자 IP	IP 를 표시합니다.
사용자명	위협 탐지 단말이 Genian NAC에 의해 인증받은 사용자인 경우, 인증사용자 명을 표시합니다.
호스트명	위협 탐지 단말의 호스트명을 표시합니다.
개별대응정책	악성 파일 또는 악성IP에 대해 즉시 대응 또는 예외처리가 필요한 경우 위협관리 화면에서 설정할 수 있습니다.
단말별 동일 위협 세부정보	동일한 파일이 여러번 탐지 될 경우 탐지 경로 및 탐지 정보, 대응결과를 표시합니다.
최초탐지시각	해당 단말에 위협이 최초로 탐지된 시각을 표시합니다.
최종탐지시각	해당 단말에 위협이 마지막으로 탐지된 시각을 표시합니다.

5.3 파일 상세 분석

5.3.1 파일 상세 분석

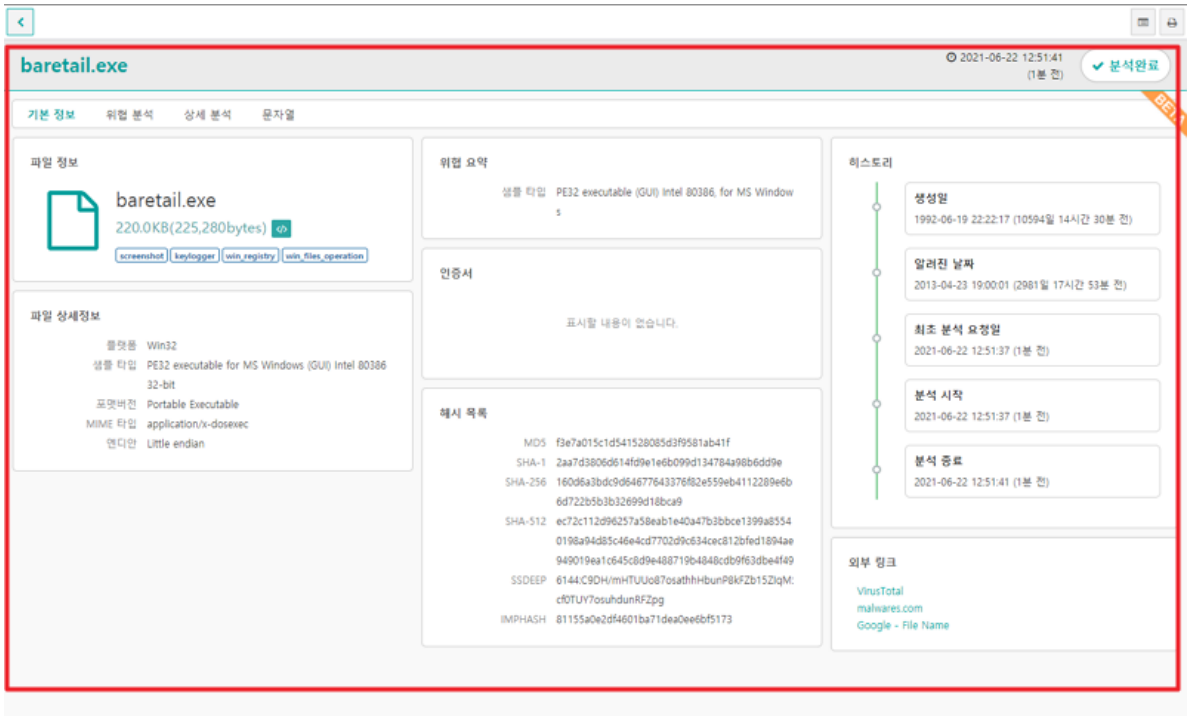
악성 파일로 탐지되지 않은, 의심스러운 PE 파일에 대해 파일 정적 분석 기능을 제공합니다.

파일 정적 분석은 분석할 파일을 직접 드래그하여 업로드하거나, 위협 관리에서 파일 상세 분석 요청 버튼으로 분석 요청이 가능합니다.

업로드된 파일은 여러 탐지엔진 (IOC, ML, YARA, 유사도지표 및 AI 분석지표) 에서 위협 파일 여부를 한 번 더 검사하고, 파일 Header 정보가 포함된 다양한 분석 정보를 제공합니다.

파일 정적 분석 수행 절차

1. **분석 > 조사 > 파일 상세 분석** 메뉴 내 파일업로드 탭으로 이동합니다.
2. 정적 분석을 수행할 PE 파일을 드래그하여 서버에 업로드합니다. (파일 업로드 최대 용량 50MB)
3. 업로드된 파일 목록 확인 후 분석 시작 버튼을 클릭합니다.
4. "분석 요청에 성공했습니다" 메시지가 발생하고, 페이지 새로 고침 시 분석 중인 파일이 목록에 표시됩니다.
5. 분석이 완료된 목록을 클릭하면 기본정보, 위협 분석, 상세 분석, 문자열 화면이 표시됩니다.



항목	설명
기본정보-파일 정보	파일 이름, 파일 크기, 해당 파일에 YARA 관련 TAG 정보를 표시합니다. (/usr/geni/data/yara 폴더 내 capabilities.yar 파일에 정의된 YARA 규칙 검사). hex 데이터는 1000줄 단위로 표시하며, 더보기를 통해 추가로 확인할 수 있습니다.
기본정보-파일 상세정보	플랫폼 정보, 샘플 타입 등 상세정보가 있는 경우 표시합니다.
기본정보-위협 요약	위협 요약 정보가 있는 경우 표시합니다.
기본정보-인증서	인증서 정보가 있는 경우 표시합니다.
기본정보-해시 목록	파일에 대한 해시값 (**MD5, SHA-1, SHA256, SHA512, SSDEEP, IMAPHASH**)을 표시합니다.
기본정보-히스토리	파일 생성일과 분석 요청, 분석 완료 시간을 표시합니다.
기본정보-외부 링크	악성 파일/프로세스, 악성 IP 를 분석하기 위한 외부링크를 표시합니다.
위협 분석-위협 지표	탐지된 위협이 있는 경우 표시합니다.
위협 분석-위협 정보	IOC DB 또는 파일평판조회하여 결과가 있는 경우 위협 정보를 표시합니다.
위협 분석-YARA 검사 결과	정책 > YARA Rule관리 에 등록된 규칙 검사 결과가 있는 경우 표시합니다.
위협 분석-유사도 지표	유사도 지표 분석 결과가 있는 경우 표시합니다.
위협 분석-AI 분석 지표	ML로 탐지되고 AI 분석 결과가 있는 경우 표시합니다.
상세 분석-PE 정보	PE 정보를 표시합니다.
상세 분석-PE Header	PE Header 정보를 표시합니다.
상세 분석-전자서명	전자서명이 되어있는 경우 전자서명 정보를 표시합니다.
문자열-관심 문자열	문자열에서 **이메일, http, IP 주소** 3가지 항목을 검색하며, 정보가 있는 경우 관심 문자열에 정보를 표시합니다.
문자열-문자열 검색	파일 내부의 string 값을 추출하며, 문자열 길이에 따라 검색이 가능합니다.

6. 상세 분석 파일을 대상으로 파일의 이동 경로를 확인할 수 있습니다.

   파일 상세 분석에서 분석 파일을 업로드하고 파일 분석이 완료되면 **연관 파일 히스토리** 탭에 해당 파일 이벤트의 **SHA256 값** 을 이용하여, `endpoint2` 인덱스에 동일한 SHA256에 대한 이벤트 정보를 가지고 있는 사용자 정보 목록 및 파일 이동 경로를 표시합니다.

7. 분석을 위해 업로드한 파일은 **분석 > 조사 > 수집관리** 메뉴의 파일 목록에서 확인할 수 있습니다.

5.4 분석 지표 설명 (위험도, 신뢰도 등)

분석 지표에서는 연관 위협 지표와 연관 행위 지표, 유사도지표, AI 분석 지표 정보를 표시합니다.

항목	설명
연관 위협 지표	위협이 마지막으로 탐지된 단말과 해당 단말에서 발생한 모든 위협 탐지 정보를 표시합니다.
연관 행위 지표	위협과 연관된 모든 프로세스의 이벤트에 Tag 정보가 존재하는 경우 해당 Tag를 연관 행위 지표 정보로 표시하고, 클릭 시 이벤트 조사 목록으로 이동합니다.
유사도지표	의심악성파일 탐지 시 알려진 악성파일의 변종인지 여부를 Ecosystem을 통해 조회하고, 유사도 정보를 표시합니다. 새로고침 아이콘 클릭 시 Ecosystem에 최신 정보를 한번 더 조회합니다.
AI 분석 지표	ML에서 탐지한 정보로 악성코드의 위협분류 및 위협명을 예측한 지표를 제공합니다. • **Type:** 악성코드의 위협 종류(Adware, Trojan, Virus 등..)에 대한 분석 지표 • **Family:** 악성코드의 FamilyName에 대한 분석 지표 • **분석시각:** AI 지표를 만들어낸 시각

5.5 공격 스토리라인 분석

에이전트는 엔드포인트에서 실행하는 file, process, module, network, registry 정보와 함께 PID(Process Identification Number) 및 PPID(Parent Process Identification Number) 정보, 에이전트 동작 시간 정보를 수집합니다.

공격 히스토리 라인 페이지에서는 에이전트가 동작하는 시간동안 위협으로 탐지된 프로세스의 PID, PPID, Device-id, EventTime 정보를 조합하여 위협 프로세스를 기준으로 해당 프로세스의 부모 프로세스, 위협 프로세스가 실행한 module 정보, 자식 프로세스 정보 및 위협 프로세스의 connection 정보를 표시합니다.

동일한 파일이 여러 엔드포인트에서 탐지된 경우, 최종 탐지(최신)된 엔드포인트를 대상으로 한 연결 정보를 제공합니다.

CHAPTER

SIX

PHASE 6 - 위협 처리

6.1 위협 처리

6.1.1 위협 처리

위협 분석 상세 페이지에서 위협관리를 활용하면 관리자가 확인 후 대응하거나, 오탐의 경우 다음에 탐지 되지 않도록 예외처리할 수 있는 기능을 제공 합니다.

위협 분석을 진행하고 난 뒤, 위협에 대한 처리를 진행하려면 다음과 같이 진행 합니다. 위협을 분석하는 방법은 이것을 참조 하세요. *Phase 5 - 위협 분석*

1. 상단 메뉴바에서 분석 > 위협 을 클릭합니다.
2. 위협 모니터링 화면에서 최근 위협 현황 내 처리하고자 하는 현황을 클릭합니다.
3. 위협 관리 화면에서 처리하고자 하는 위협의 우측 액션의 위협 분석을 클릭합니다.
4. 위협 분석 화면에서 우측 상단에 **위협 관리(신규)** 를 클릭합니다.
5. 내가 담당하기를 클릭하여 위협 판정을 진행합니다. 위협 판정은 아래 **위협판정** 내용을 참고하세요.
6. 설정완료를 클릭 합니다.

6.1.2 위협 판정

위협이 악성행위로 판정된 경우 **악성** 을 선택하고 대응정책을 설정할 수 있습니다.

항목	설명
대응정책-기본정책	해당 파일이 다시 탐지되면 정책에 설정된 규칙에 따라 처리합니다.
대응설정-알람	해당 파일이 다시 탐지되면 엔드포인트에 알람 발생 이벤트를 즉시 수행합니다.
대응설정-프로세스 강제종료	해당 프로세스가 탐지되면 엔드포인트에 프로세스 강제 종료 이벤트를 즉시 수행합니다.
대응설정-파일삭제	해당 파일이 다시 탐지되면 엔드포인트에 파일 삭제 이벤트를 즉시 전달 합니다.
대응설정-네트워크 격리	해당 파일이 다시 탐지되면 엔드포인트에 네트워크 격리 이벤트를 즉시 전달 합니다. Insights E 서버와는 기본 통신 됩니다.
자동해결	추후 동일한 위협이 다시 탐지되면 분석 메뉴에 표시되지 않고 처리 상태를 해결됨 으로 자동 변경합니다.
메모	탐지된 위협에 대해 관리자 메모를 작성할 수 있습니다.

위협이 오탐으로 판정된 경우 **안전** 을 선택하고 설정할 수 있습니다.

항목	설명
메모	탐지된 위협에 대해 관리자 메모를 작성할 수 있습니다.
오탐보고	정상적인 파일이지만 오탐된 경우, 오탐보고를 통해 Genian Cloud에 오탐을 보고하게 됩니다.

위협의 악성 여부를 판단할 수 없거나 정보가 부족할 경우 **보류** 를 선택하고 설정할 수 있습니다.

항목	설명
자동해결	추후 동일한 위협이 다시 탐지되면 분석 메뉴에 표시되지 않고 처리 상태를 해결됨 으로 자동 변경합니다.
메모	탐지된 위협에 대해 관리자 메모를 작성할 수 있습니다.

6.2 위협 이벤트 알림 설정

Genian Insights E는 관리자 계정에 설정된 메일로 위협 알림 및 리포트를 메일링 서비스를 제공하며, 엔드포인트 단말에 팝업 알림 기능을 제공합니다.

6.2.1 이메일 알림

Genian Insights E는 관리자 계정에 설정된 메일로 위협 알림 및 리포트를 메일링 서비스를 제공합니다.

메일서버 설정

1. **관리 > 설정 > 환경설정 > 시스템** 페이지로 이동하여 메일 서버를 먼저 설정합니다. 서버 설정 시 모든 정보를 빠짐없이 작성해야 하며, 설정 테스트를 통해 정상 동작 여부를 확인할 수 있습니다.

항목	내용
연결보안방식	**SMTP (25), SMTPS (465), MSA/STARTTLS (587)** 을 지원합니다.
서버포트	연결보안방식과 동일한 포트를 입력합니다.

사용자 계정 설정

1. **관리 > 설정 > 관리자** 에서 관리자 계정으로 이동하여 리포트를 전송받을 계정을 클릭합니다.
2. 사용자 수정 화면에서 **이메일 알림** 에 제공 받을 정보를 선택하고, **추가 정보** 에 리포트를 전송받을 메일 주소를 입력 후 수정 버튼을 클릭합니다.

항목	설명
위협알람	1시간 이내에 발생한 위협 정보를 메일로 전송합니다. (**매 시간마다 제공**)
디스크 사용률 알람	Insights E 장비의 디스크 사용률이 기본값 (**70%**) 초과 시 관리자 이메일로 사용률 초과에 대한 내용을 전송합니다.
일간 위협 리포트	24시간 동안 발생한 위협 정보를 종합하여 해당 리포트를 메일로 전송합니다. (**1일 1회, 01:00**)

관리자별 위협 알림을 받을 수 있습니다.

6.2.2 엔드포인트 알림

Note: **정책 > 그룹 정책 관리 > 에이전트** 중 알림 메시지 표시가 사용 으로 설정돼 있어야 합니다.

엔드포인트 알림은 에이전트가 설치된 단말에서 위협 탐지시 팝업 알림 기능 을 의미합니다.

관리자 알림 설정

1. **관리 > 설정 > 관리자**의 **에이전트 알림 > 위협 알람 설정** 을 클릭합니다.
2. 알림창을 표시할 관리자 PC의 `Device ID` 를 입력합니다.

`Device ID` 는 **분석 > 엔드포인트 목록** 단말의 기본 정보 탭에서 확인할 수 있습니다.

엔드포인트 알림 설정

정책 > 그룹 정책 관리 > 대응 에서 정책별 엔드포인트 알림 설정을 할 수 있습니다. XBA 탐지 알림 설정은 개별 XBA 룰에 대해 알림 설정이 필요합니다.

항목	설정	설명
알려진 악성코드 대응-에이전트 팝업표시	사용안함 / Low / Medium / High	**YARA, IOC DB에 등록된 위험 프로세스를 탐지할 경우** 에이전트 팝업을 통해 사용자에게 알려줄 지 여부를 선택합니다.
알려지지 않은 악성코드 대응-에이전트 알림 메시지	사용안함 / ML.Medium / ML.High	**머신러닝에 의한 탐지 시** 에이전트 팝업을 통해 사용자에게 표시할 최소 위험도를 설정합니다.
악성IP 대응-에이전트 팝업표시	사용안함 / 사용함	**IOC DB에 등록된 악성 IP로 접속을 탐지할 경우** 에이전트 팝업을 통해 사용자에게 알려줄 지 여부를 선택합니다.

정책 설정 후, **분석 > 엔드포인트** 그룹 설정 페이지의 정책 설정 또는 개별 엔드포인트 상세 화면에서 정책명을 통해 설정 가능합니다.

CHAPTER

SEVEN

PHASE 7 - 운영 및 유지관리

7.1 백업 및 보관

Genian Insights E 3.0 에서는 DB와 LOG의 백업 기능을 지원하고 있습니다. 데이터를 백업하여 서비스 장애 시 데이터 복원을 목적으로 제공드리고 있습니다.

7.1.1 백업 설정

특정 시간 백업

1. 관리 > 설정 > 환경설정 > 백업 항목으로 이동합니다.
2. **백업수행여부** 옵션을 On으로 설정합니다. (Default : On)
3. 백업수행시각을 지정합니다. (Default : 04:00)
4. 좌측 상단에 체크 표시를 클릭하여 저장합니다.

Note: 본 기능 이용 시 DB(Mysq), Log(Elasticsearch) 백업이 모두 수행됩니다. 실행 > 백업시작 버튼을 클릭할 경우 백업수행시각과 무관하게 지금 즉시 백업을 수행합니다.

7.1.2 정책DB 백업관리

저장장치

DB 백업파일 을 특정 저장장치로 지정하여 보관해야 할 경우 저장장치 옵션을 사용할 수 있습니다.

1. 관리 > 설정 > 환경설정 > 백업 항목으로 이동합니다.
2. 정책DB 백업관리 > 저장장치에서 원하는 저장장치 타입을 선택합니다.(지원되는 저장장치 유형은 아래 표를 참고하십시오.)
3. 저장장치 접근 및 백업을 위한 표출되는 하위 정보를 기입합니다.
4. 좌측 상단에 체크 표시를 클릭하여 저장합니다.

저장장치 유형

저장장치 유형	설명 및 설정값
로컬디스크	정책서버 디스크에 백업을 수행합니다.(별도 설정 필요없음)
외부저장장치	정책서버에 USB Type 드응로 연결된 외장 디스크에 백업을 수행합니다.
CIFS저장장치	윈도우 공유 기능을 이용하여 CIFS 사용 백업을 수행합니다.
NFS저장장치	Unix나 Linux file system의 디렉토리를 mount하여 백업을 수행합니다.
FTP SERVER	FTP(File Transfer Protocol)을 통해 백업파일을 전송합니다.
SFTP SERVER	SFTP(Secure File Transfer protocol)을 통해 백업 파일을 전송합니다.

Note: 백업파일에 저장장치를 로컬디스크 가 아닌 다른 타입 으로 지정할 경우 백업파일 보존여부 설정을 ON으로 설정 시 백업파일 유실에 대응할 수 있습니다.

백업파일 다운로드

1. 관리 > 설정 > 환경설정 > 백업 항목으로 이동합니다.
2. 정책DB 백업관리 항목 하단에 **백업파일 다운로드** 에서 다운로드 버튼을 클릭 합니다.
3. 백업 파일 리스트를 확인하고 원하는 일자의 파일을 클릭하여 다운로드 받습니다.

7.2 서버/에이전트 상태 모니터링

관리 > 시스템 > 서버 관리 > 서버 클릭 > 모듈 상태에서 주요 모듈의 상태를 직관적으로 모니터링 할 수 있습니다.

모듈의 상태 값은 **정상, 비정상** 상태로 나뉘어 표기되며 비정상이 표출되었을 경우 점검이 필요합니다.

각 모듈 별 해당되는 데몬은 아래와 같습니다.

모듈명	데몬
MessageServer	Kafka 모듈의 상태를 의미합니다.
Data Processing Engine	LogStash 모듈의 상태를 의미합니다.
ThreatDetector	ThreatDetector 모듈의 상태를 의미합니다.
LogServer	Elasticsearch 모듈의 상태를 의미합니다.
ManagementServer	Web관련데몬(httpd, tomcat) 모듈의 상태를 의미합니다.
Event Pipeline	kafka -> logstash -> elasticsearch / kafka -> threatdetector 각 2개의 pipeline 상태를 의미합니다.

Note: 상태 확인 시각은 모듈 상태를 확인한 시각을 의미합니다.

7.3 SIEM 연동 방법

7.3.1 SYSLOG 전송 설정

Insights E 서버에서 발생하는 로그는 인덱스 별로 SYSLOG 전송 기능을 제공합니다.

1. 관리 > 설정 > 환경설정 > 외부연동 메뉴로 이동, +추가 버튼을 클릭 합니다. 각 항목의 세부 설명은 아래 내용 을 참고 하세요
2. 필요한 인덱스와 필드 선택 시 아래와 같이 사용할 수 있는 모든 필드값이 자동으로 입력됩니다. 인덱스 별 설명은 다음을 참고하십시오. 수집 인덱스 구조 및 설명
3. 저장 버튼 클릭 후 좌측 상단 체크 버튼 까지 클릭 하여 적용 합니다.

각 항목의 설명은 아래와 같습니다.

이름	내용
서버IP	SYSLOG 를 전송할 서버 IP 주소를 입력합니다.
프로토콜	SYSLOG 전송 포트를 설정합니다. UDP,TCP,TCP(TLS) 지원하며 GMODULE의 경우 TCP(TLS) 만 지원합니다.
전송포트	기본포트는 UDP:514, TCP:1470, TCP(TLS):6514 이며, 그 외 별도 정의 된 포트가 존재한다면 포트를 입력합니다.
인덱스 선택	Insights E에 현재 저장되어 있는 인덱스 중 필요한 인덱스를 선택합니다.
중계서버 IP	다수의 Insights E 서버가 있을 경우 중계IP를 설정하여 SYSLOG 를 전송합니다.
인덱스 선택	SYSLOG를 전송할 인덱스를 선택합니다.
타임존	서버가 위치해 있는 지역을 선택합니다.
형식	SYSLOG 포맷을 설정합니다. RFC3164와 RFC5424를 지원합니다 (기본값:RFC3164)
필터 설정	특정 필드의 Key와 Value 조건으로 필터링하여 전송이 필요할 때 설정합니다.
SYSLOG 메시지	인덱스 타입 선택 시 사용할 수 있는 모든 필드값이 자동으로 입력됩니다.
존재하지 않는 필드명 대체 문자열	필드가 존재하지 않을 경우 공간을 채우기 위해 설정합니다.
필드 변환 사용	특정 필드에 저장되는 값을 다른 문자열로 변환이 필요할 때 설정합니다.

필드 변환

- **필드** : 치환 대상 필드를 입력합니다.
- **치환할 문자열** : 필드 내 지환이 필요한 문자열을 지정합니다.
- **치환될 문자열** : 치환할 문자열을 대체할 문자열을 지정합니다.

7.4 3rd Party 연동 사례

Genian Insights E 3.0은 기본으로 제공하는 위협정보 이외에 외부 서버에서 위협정보 데이터를 수집, 위협탐지에 활용할 수 있습니다.

외부 연동을 지원하는 제품을 보유한 고객에 한해 사용이 가능하며, 아래 제품에 대한 연동을 지원합니다.

2.0.11 버전부터 제품 설치 시 아래 플러그인은 자동으로 서버에 설치되며, 연동에 필요한 기본적인 정보 입력이 필요합니다.

7.4.1 서버 플러그인 업데이트

플러그인 추가

1. **관리 > 시스템 > 소프트웨어 관리 > 서버 플러그인 관리** 로 이동, 추가 버튼을 클릭하여 외부 연동 플러그인(확장자 gpp) 파일을 업로드 합니다.
2. 파일 목록 사용여부 필드에서 사용여부를 먼저 체크한 후, 화면 오른쪽에 있는 즉시실행 버튼을 클릭합니다.
3. 정상적으로 동작하는 경우 **상태 필드**에 파란색 아이콘이 표시됩니다.

플러그인 삭제

1. 삭제할 플러그인 목록을 선택하고, 삭제 버튼을 클릭합니다.
2. 플러그인 삭제 확인 팝업창이 발생하고, 확인을 클릭하면 플러그인이 삭제됩니다.

7.4.2 로그프레소 연동

로그프레소 마에스트로 및 소나 제품과의 연동기능을 제공합니다.
로그프레소 마에스트로는 보안 오케스트레이션 및 자동화 솔루션으로서 Genian Insights E에서 수집된 다양한 정보를 연동하여 자동화된 위협 분석과 대응을 수행을 사용자에게 제공합니다.

로그프레소와 연동을 위해서는 로그프레소 플랫폼에 **Genian Insights E** app 설치가 선행되어야 합니다.

로그프레소 Genian Insights E APP 다운로드

Step1. Genian Insights E 설정

Genian Insights E에서 수집된 로그를 로그프레소로 전송하는 설정을 합니다.

1. Web콘솔 접속 > 관리 > 설정 클릭
2. **외부연동** 클릭
3. SYSLOG 서버설정 > 추가 버튼 클릭
4. SYSLOG 서버 설정을 수행합니다.

항목	설명
사용	ON/OFF 설정
서버 IP	로그프레소 제품 IP 설정
프로토콜	SYSLOG 전송시 사용할 프로토콜 선택
전송포트	SYSLOG 전송시 사용할 포트번호 설정
중계 서버 IP	Genian Insights E SYSLOG를 중계 전송할 서버가 있다면 작성
인덱스 선택	SYSLOG로 전송할 Genian Insights E 인덱스 선택
타임존	SYSLOG 전송 시 메시지의 시간을 설정할 타임존

continues on next page

Table 1 – continued from previous page

항목	설명
필터 설정	필드의 Key와 Value의 조건으로 필터링하여 SYSLOG를 전송하는 설정
SYSLOG 메세지	전송할 SYSLOG의 내용
존재하지 않는 필드 대체 문자열	필드가 존재하지 않을 경우 대체할 문자열 설정
필드 변환 사용	필드 변환 기능 사용 설정

5. 아래 제공하는 SYSLOG 메시지를 복사하여 4개의 SYSLOG 설정을 추가합니다.

threat2 인덱스

```
THREAT:`%{[AlertDecision]}`%{[Assignee]}`%{[AssigneeName]}`%
↪{[AuthDeptCode]}`%{[AuthDeptName]}`%{[AuthID]}`%{[AuthName]}`%
↪{[AutoResolve]}`%{[AVName]}`%{[Category]}`%{[Catgry]}`%
↪{[Classification]}`%{[CmdLine]}`%{[CodeSign][Issuer]}`%
↪{[CodeSign][IssuerThumbPrint]}`%{[CodeSign][SignatureVerification]}`%
↪{[CodeSign][Signed]}`%{[CodeSign][SigningDate]}`%{[CodeSign][Subject]}`%
↪{[CodeSign][SubjectThumbPrint]}`%{[CodeSign][Type]}`%{[CollectServerID]}
↪`%{[CollectTime]}`%{[Confidence]}`%{[CreateTime]}`%{[DeptCodePath]}`%
↪{[DeptNamePath]}`%{[Details]}`%{[DetectID]}`%{[DetectKeyString]}`%
↪{[DetectMessage]}`%{[DetectSubType]}`%{[DetectTime]}`%{[DetectType]}`%
↪{[DeviceID]}`%{[Direction]}`%{[DNSName]}`%{[Domain]}`%{[EventSeq]}`%
↪{[EventSubType]}`%{[EventTime]}`%{[EventType]}`%{[Feed]}`%{[FileName]}`%
↪{[FileName2]}`%{[FilePath]}`%{[FilePath2]}`%{[FileSize]}`%{[FileType]}`%
↪{[FirstTime]}`%{[FollowLink]}`%{[HostName]}`%{[Information][CategoryID]}
↪`%{[Information][CategoryName]}`%{[Information][PathInfo]}`%
↪{[Information][ProductName]}`%{[Information][SourceName]}`%
↪{[Information][ThreatInfo]}`%{[Information][ThreatName]}`%{[IP]}`%
↪{[IsKnown]}`%{[Level]}`%{[LocalIP]}`%{[LocalPort]}`%{[LogonID]}`%{[MAC]}
↪`%{[MalwareKind]}`%{[MD5]}`%{[Memo]}`%{[MLLevel]}`%{[MLScore]}`%
↪{[ModifyTime]}`%{[Occurred]}`%{[PathInfo]}`%{[PathInfo2]}`%{[PathKey]}`%
↪{[PID]}`%{[Platform]}`%{[ProcGuid]}`%{[ProcName]}`%{[ProcPath]}`%
↪{[ProcPathKey]}`%{[Protocol]}`%{[RemoteIP]}`%{[RemotePort]}`%
↪{[Response]}`%{[ResponseInfo]}`%{[ResponseRule]}`%{[Result]}`%{[Rule]}`%
↪{[RuleID]}`%{[Score]}`%{[SessionID]}`%{[SHA256]}`%{[SSDEEP]}`%{[State]}
```

endpoint2 인덱스

```
ENDPOINT:`%{[Access]}`%{[AuthDeptCode]}`%{[AuthDeptName]}`%{[AuthID]}`%
↪{[AuthName]}`%{[BusType]}`%{[BytesRecved]}`%{[BytesSent]}`%{[Catgry]}`%
↪{[CheckFlag]}`%{[ChildPID]}`%{[ChildProcGuid]}`%{[CmdLine]}`%{[ConnCnt]}
↪`%{[CreateTime]}`%{[CustomTag]}`%{[DetectKey]}`%{[DetectType]}`%
↪{[DeviceID]}`%{[Direction]}`%{[DisconnCnt]}`%{[DisconnectFlag]}`%
↪{[DNSName]}`%{[DNSRequest]}`%{[DNSResponse]}`%{[Domain]}`%{[DriveType]}`
↪%{[DriveType2]}`%{[EventSeq]}`%{[EventSubType]}`%{[EventTime]}`%
↪{[EventType]}`%{[ExitFlag]}`%{[ExitTime]}`%{[Ext]}`%{[Ext2]}`%
↪{[FileAttr]}`%{[FileName]}`%{[FileName2]}`%{[FilePath]}`%{[FilePath2]}`%
↪{[FileSize]}`%{[FileType]}`%{[FinalName]}`%{[HasDump]}`%{[HostName]}`%
↪{[Important]}`%{[InflowSeq]}`%{[Info]}`%{[InfoTitle]}`%{[InjectionType]}
↪`%{[IntegrityLevel]}`%{[InteractiveFlag]}`%{[IP]}`%{[IsSystem]}`%
↪{[JsonInfo][DecodedCmdLine]}`%{[JsonInfo][WebTitle]}`%
↪{[JsonInfo][WebURL]}`%{[JsonInfo][WindowText]}`%{[LastDisconnTime]}`%
↪{[LocalIP]}`%{[LocalPort]}`%{[LogonID]}`%{[MD5]}`%{[ModifyTime]}`%
↪{[offline]}`%{[ParentProcEventSeq]}`%{[ParentProcGuid]}`%
↪{[ParentProcName]}`%{[PID]}`%{[PPID]}`%{[ProcGuid]}`%{[ProcName]}`%
↪{[ProcPath]}`%{[ProcUserID]}`%{[Protocol]}`%{[RegDataSize]}`%
↪{[RegDataType]}`%{[RegKeyPath]}`%{[RegNewKeyPath]}`%{[RegValue]}`%
```

(continues on next page)

(continued from previous page)

```
↪{[RegValueName]}`%{[RelatedEventSeq]}`%{[RelatedPID]}`%
↪{[RelatedProcGuid]}`%{[RelatedProcName]}`%{[RelatedProcPath]}`%
↪{[RemoteIP]}`%{[RemotePort]}`%{[ReqEventSeq]}`%{[ReqGuid]}`%{[ReqName]}`
↪%{[ReqPID]}`%{[Result]}`%{[RuleID]}`%{[SerialNumber]}`%{[SessionID]}`%
↪{[SHA256]}`%{[Tactic]}`%{[Tag]}`%{[TargetPID]}`%{[TargetProcGuid]}`%
↪{[TargetProcName]}`%{[TargetProcPath]}`%{[Technique]}`%{[TrunkID]}`%
↪{[Uncertain]}`%{[VolumeGuid]}`%{[VolumeType]}`%{[WindowClassName]}`%
↪{[WindowText]}
```

alert2 인덱스

```
ALERT:`%{[AuthDeptCode]}`%{[AuthDeptName]}`%{[AuthID]}`%{[AuthName]}`%
↪{[AVName]}`%{[Catgry]}`%{[Classification]}`%{[CmdLine]}`%
↪{[CodeSign][Issuer]}`%{[CodeSign][IssuerThumbPrint]}`%
↪{[CodeSign][SignatureVerification]}`%{[CodeSign][Signed]}`%
↪{[CodeSign][SigningDate]}`%{[CodeSign][Subject]}`%
↪{[CodeSign][SubjectThumbPrint]}`%{[CodeSign][Type]}`%{[Confidence]}`%
↪{[CreateTime]}`%{[DeptCodePath]}`%{[DeptNamePath]}`%{[Details]}`%
↪{[DetectID]}`%{[DetectKeyString]}`%{[DetectMessage]}`%{[DetectSubType]}`
↪%{[DetectTime]}`%{[DetectType]}`%{[DeviceID]}`%{[Direction]}`%
↪{[DNSName]}`%{[Domain]}`%{[EventSeq]}`%{[EventSubType]}`%{[EventTime]}`%
↪{[EventType]}`%{[Feed]}`%{[FileName]}`%{[FileName2]}`%{[FilePath]}`%
↪{[FilePath2]}`%{[FileSize]}`%{[FileType]}`%{[FollowLink]}`%{[HostName]}`
↪%{[Information][CategoryID]}`%{[Information][CategoryName]}`%
↪{[Information][PathInfo]}`%{[Information][ProductName]}`%
↪{[Information][SourceName]}`%{[Information][ThreatInfo]}`%
↪{[Information][ThreatName]}`%{[IP]}`%{[IsKnown]}`%{[Level]}`%{[LocalIP]}
↪`%{[LocalPort]}`%{[LogonID]}`%{[MAC]}`%{[MalwareKind]}`%{[MD5]}`%
↪{[MLLevel]}`%{[MLScore]}`%{[ModifyTime]}`%{[PathInfo]}`%{[PathInfo2]}`%
↪{[PathKey]}`%{[PID]}`%{[Platform]}`%{[ProcGuid]}`%{[ProcName]}`%
↪{[ProcPath]}`%{[ProcPathKey]}`%{[Protocol]}`%{[RemoteIP]}`%
↪{[RemotePort]}`%{[Response]}`%{[ResponseInfo]}`%{[ResponseRule]}`%
↪{[Result]}`%{[RuleID]}`%{[Score]}`%{[SessionID]}`%{[SHA256]}`%{[SSDEEP]}
↪`%{[SuspiciousInfo][Confidence]}`%{[SuspiciousInfo][FileName]}`%
↪{[SuspiciousInfo][FilePath]}`%{[SuspiciousInfo][FileSize]}`%
↪{[SuspiciousInfo][FileType]}`%{[SuspiciousInfo][MD5]}`%
↪{[SuspiciousInfo][MLLevel]}`%{[SuspiciousInfo][MLScore]}`%
↪{[SuspiciousInfo][SHA256]}`%{[SuspiciousInfo][SSDEEP]}`%
↪{[SuspiciousInfo2][Confidence]}`%{[SuspiciousInfo2][FileName]}`%
↪{[SuspiciousInfo2][FilePath]}`%{[SuspiciousInfo2][FileSize]}`%
↪{[SuspiciousInfo2][FileType]}`%{[SuspiciousInfo2][MD5]}`%
↪{[SuspiciousInfo2][MLLevel]}`%{[SuspiciousInfo2][MLScore]}`%
↪{[SuspiciousInfo2][SHA256]}`%{[SuspiciousInfo2][SSDEEP]}`%
↪{[SuspiciousInfo3][Confidence]}`%{[SuspiciousInfo3][FileName]}`%
↪{[SuspiciousInfo3][FilePath]}`%{[SuspiciousInfo3][FileSize]}`%
↪{[SuspiciousInfo3][FileType]}`%{[SuspiciousInfo3][MD5]}`%
↪{[SuspiciousInfo3][MLLevel]}`%{[SuspiciousInfo3][MLScore]}`%
↪{[SuspiciousInfo3][SHA256]}`%{[SuspiciousInfo3][SSDEEP]}`%{[ThreatID]}`%
↪{[YaraRuleID]}`%{[YaraRuleName]}
```

sequoia 인덱스

```
AUDIT:`%{[@timestamp]}`%{[actionStatusCode]}`%{[logAlertId]}`%
↪{[logDetail]}`%{[logDeviceId]}`%{[logId]}`%{[logIdStr]}`%{[logIp]}`%
↪{[logLinkID]}`%{[logLinkType]}`%{[logMac]}`%{[logMsg]}`%{[logThreatId]}`
↪%{[logType]}`%{[logTypeStr]}`%{[logUserId]}`%{[logUserName]}
```

Step2. 로그프레소 수집기 설정

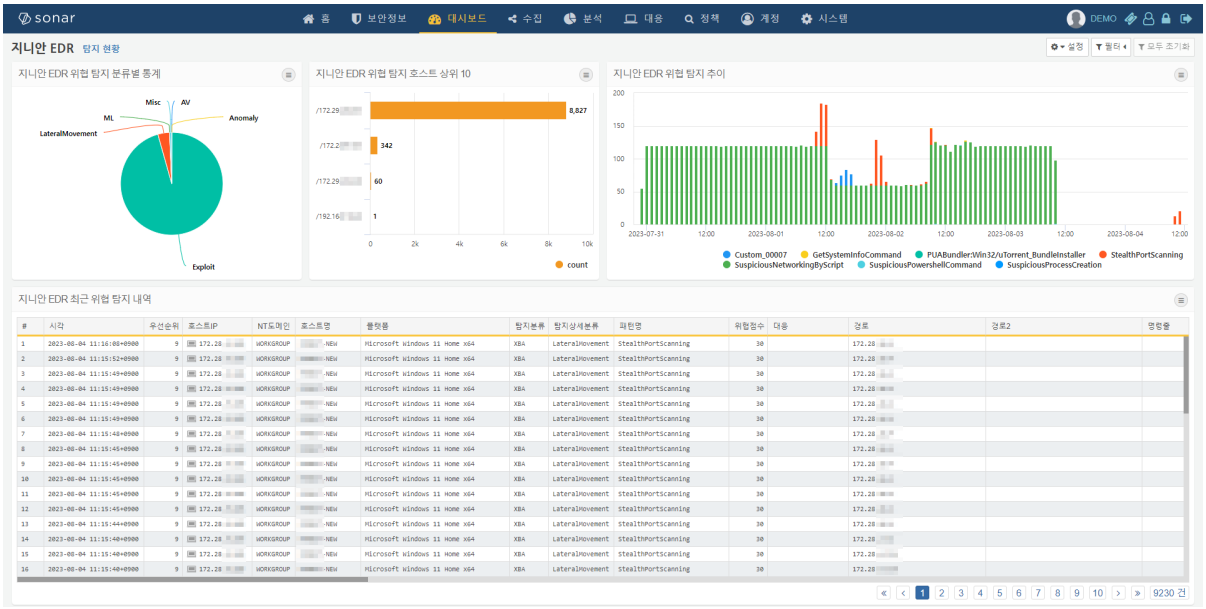
로그프레소에서 Genian Insights E 수집기를 추가하고 활성화합니다.

1. 수집 > 수집설정 > 수집기를 추가합니다.

항목	설명
수집 모델	Genian Insights E
테이블	Insights E_GENIAN(테이블명 변경 시 데이터셋의 테이블 이름도 변경 필요)
원격지 IP	Genian Insights E 서버의 IP를 입력합니다.

Step3. 로그프레소 대시보드 모니터링

설정을 완료하고 로그프레소 대시보드 메뉴로 이동하여 탐지 현황 대시보드를 확인 할수 있으며 화면에 표시되는 다양한 정보를 활용하여 위협 탐지 내역을 분석할 수 있습니다.



7.4.3 KISA C-TAS 연동

KISA 에서 제공하는 사이버위협정보 분석-공유 시스템(C-TAS)과 연동 기능을 제공합니다. C-TAS에 가입되어 연동을 위한 KEY를 제공받은 고객에 한해 사용가능하며, Genian Insights E 서버에서는 IOC DB Framework 버전 v2 로 변경이 필요합니다.

항목	설명
Export Key	KISA로부터 고객에게 발급된 Export Key(exp key) 정보를 입력합니다.
기관코드	KISA로부터 할당받은 기관(고객)코드(OrgKey)정보를 입력합니다.
동기화 주기	C-TAS로부터 받은 데이터를 몇분 간격으로 IOC Database에 등록할 지 설정합니다.(기본값:30분)

continues on next page

Table 3 – continued from previous page

항목	설명
IP 주소 보관기간	연동 설정으로 수집한 IP주소의 보관기간을 설정합니다.(기본값:10일)

1. 2.0.11 버전부터 제품 설치 시 C-TAS 플러그인이 함께 설치됩니다. 정상적으로 설치가 된 경우, **관리 > 설정 > 환경설정 > 탐지 및 대응** 메뉴에 KISA C-TAS 연동 설정을 확인할 수 있습니다.
2. 연동여부를 **사용** 으로 변경하고, KISA로부터 제공받은 연동 정보 및 부가 정보를 입력합니다.
3. 정보 입력 후 왼쪽 상단의 체크 버튼을 클릭하여 설정한 정보를 저장합니다.
4. **관리 > 시스템 > 소프트웨어 관리 > 서버 플러그인 관리** 메뉴로 이동, 플러그인 목록에서 CTAS를 확인한 후, 오른쪽에서 즉시실행 버튼을 클릭하여 연동을 수행합니다.
5. 2에서 설정한 주기마다 C-TAS로부터 데이터를 수신받아 IOC Database에 업데이트 합니다.
6. C-TAS 에 등록된 정보로 위협 탐지 시 Threat2 인덱스의 Feed 정보에 CTAS로 표시 됩니다.

7.4.4 ReversingLabs A1000 연동

ReversingLabs A1000을 이용한 악성코드 분석 기능을 제공합니다.(ReversingLabs A1000 보유 고객에 해당) Threat2 인덱스에 존재하는 파일 정보를 ReversingLabs A1000로 전달하여 악성코드 여부를 분석 요청하고, 결과를 Genian Insights E 서버에서 확인할 수 있습니다.

항목	설명
제품 URL	ReversingLabs A1000 제품 IP 또는 URL 정보를 설정합니다.
USER-NAME	ReversingLabs A1000 제품 연동을 위한 USERNAME 정보입니다.
PASS-WORD	ReversingLabs A1000 제품 연동을 위한 PASSWORD 정보입니다.
연동 결과	ReversingLabs A1000 제품과의 연동 상태를 표시합니다. 정상적으로 통신이 되는 경우 '연동됨'으로 표시됩니다.

1. 2.0.11 버전부터 제품 설치 시 ReversingLabs A1000 플러그인이 함께 설치됩니다. **관리 > 설정 > 환경설정 > 악성코드 분석** 메뉴로 이동, **ReversingLabs A1000 연동** 설정을 ON 으로 변경하고, URL 및 계정 정보 입력 후 왼쪽 상단의 체크 버튼을 클릭하여 설정한 정보를 저장합니다. 2. 위협분석이 끝나면 **분석 > 위협 관리** 메뉴 목록 중 화면 왼쪽의 위협 분석 버튼을 클릭하면 위협 상세 화면으로 이동하여 왼쪽 상단의 위협 분석 결과 버튼을 클릭합니다. 3. 연동 플러그인 별로 위협 분석 리포트를 확인할 수 있습니다.

7.4.5 Check Point SandBlast TE1000X 연동

Check Point SandBlast TE1000X를 이용한 악성코드 분석 기능을 제공합니다.(Check Point SandBlast TE1000X 보유 고객에 해당) Threat2 인덱스에 존재하는 파일 정보를 Check Point SandBlast TE1000X로 전달하여 악성코드 여부를 분석 요청하고, 결과를 Genian Insights E 서버에서 확인할 수 있습니다.

항목	설명
제품 URL	Check Point SandBlast TE1000X 제품 IP 또는 URL을 입력합니다.
제품 버전	Check Point SandBlast TE1000X 제품 버전을 입력합니다.(입력 예:v1)

continues on next page

Table 5 – continued from previous page

항목	설명
연동 API Key	Check Point SandBlast TE1000X 제품에서 제공하는 API key 정보를 설정합니다.
연동 결과	Check Point SandBlast TE1000X 제품과의 연동 상태를 표시합니다. 정상적으로 통신이 되는 경우 '연동됨'으로 표시됩니다.

1. 2.0.11 버전부터 제품 설치 시 Check Point SandBlast TE1000X 플러그인이 함께 설치됩니다. **관리 > 설정 > 환경설정 > 악성코드 분석** 메뉴로 이동, **Check Point SandBlast TE1000X 연동** 설정을 ON 으로 변경합니다. 2. URL및 제품 버전, 연동 API Key 입력 후 왼쪽 상단의 체크 버튼을 클릭하여 설정한 정보를 저장합니다. 3. 위협분석이 끝나면 **분석 > 위협 관리** 메뉴 목록 중 화면 왼쪽의 위협 분석 버튼을 클릭하면 위협 상세 화면으로 이동하여 왼쪽 상단의 위협 분석 결과 버튼을 클릭합니다. 4. 연동 플러그인 별로 위협 분석 리포트를 확인할 수 있습니다.

7.4.6 Seculayer eyeCloudXOAR 연동

Genian Insights E 제품과 Seculayer eyeCloudXOAR 를 연동하여 위협 대응 프로세스 자동화를 수행 할 수 있습니다.

eyeCloudXOAR에서 생성된 Malware Hash 및 Malicious IP를 Genian Insights E 정책에 등록/삭제/조회를 연동하여 자동화된 위협 대응을 수행합니다.

Step1. eyeCloudXOAR 설정

1. **보안장비 연계관리 화면에서 장비 정보 세팅**
   Genian Insights E에서 제공하는 Rest API를 각 컴포넌트에 등록합니다.

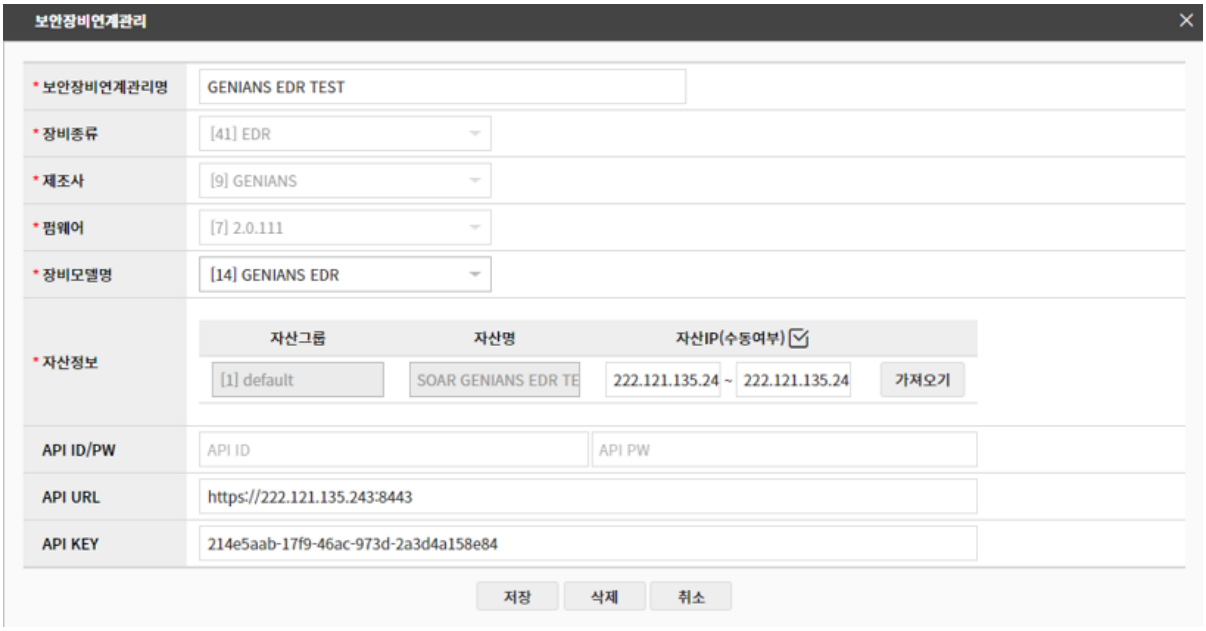


Fig. 1: 컴포넌트 설정 화면

2. 플레이북 관리에서 각 컴포넌트를 세팅

Fig. 2: Genian Insights E REST API

Step2. 수동 테스트

Genian Insights E 컴포넌트를 전부 배치 후 수동으로 테스트 차단/조회/해제 테스트 후 Genian Insights E Web 콘솔에 정상 반영되는지 확인합니다.

7.4.7 TrendMicro DDA 연동

TrendMicro DDA를 이용한 악성코드 분석 기능을 제공합니다.(TrendMicro DDA 보유 고객에 해당하며 연동이 가능한 버전은 Deep Discovery Analyzer 6.1 입니다.) Threat2 인덱스에 존재하는 파일 정보를 TrendMicro DDA로 전달하여 악성코드 여부를 분석 요청하고, 결과를 Genian Insights E 서버에서 확인할 수 있습니다.

항목	설명
연동 API Key	TRENDMICRO DDA 제품에서 제공하는 API key 정보를 설정합니다. API key는 DDA 제품의 Help 메뉴의 About 화면에서 제공됩니다.
제품 URL	TRENDMICRO DDA 제품 IP 또는 URL을 입력합니다.
제품 타임존	TRENDMICRO DDA 제품에서 사용하는 타임존을 설정합니다.
연동 결과	TRENDMICRO DDA 제품과의 연동 상태를 표시합니다. 정상적으로 통신이 되는 경우 '연동됨'으로 표시됩니다.

1. 2.0.11 버전부터 제품 설치 시 TrendMicro DDA 플러그인이 함께 설치됩니다. **관리 > 설정 > 환경설정 > 악성코드 분석** 메뉴로 이동, **TrendMicro DDA 연동** 설정을 ON 으로 변경하고, 연동 API Key, URL 및 타임존 정보 입력 후 왼쪽 상단의 체크 버튼을 클릭하여 설정한 정보를 저장합니다. 2. 위협분석이 끝나면 **분석 > 위협관리** 메뉴 목록 중 화면 왼쪽의 위협 분석 버튼을 클릭하면 위협 상세 화면으로 이동하여 왼쪽 상단의 위협 분석 결과 버튼을 클릭합니다. 3. 연동 플러그인 별로 위협 분석 리포트를 확인할 수 있습니다.

7.4.8 FireeyeAX 연동

Fireeye AX을 이용한 악성코드 분석 기능을 제공합니다.(Fireeye AX SandBox 보유 고객에 해당) Threat2 인덱스에 존재하는 파일 정보를 Fireeye AX로 전달하여 악성코드 여부를 분석 요청하고, 결과를 Genian Insights E 서버에서 확인할 수 있습니다.

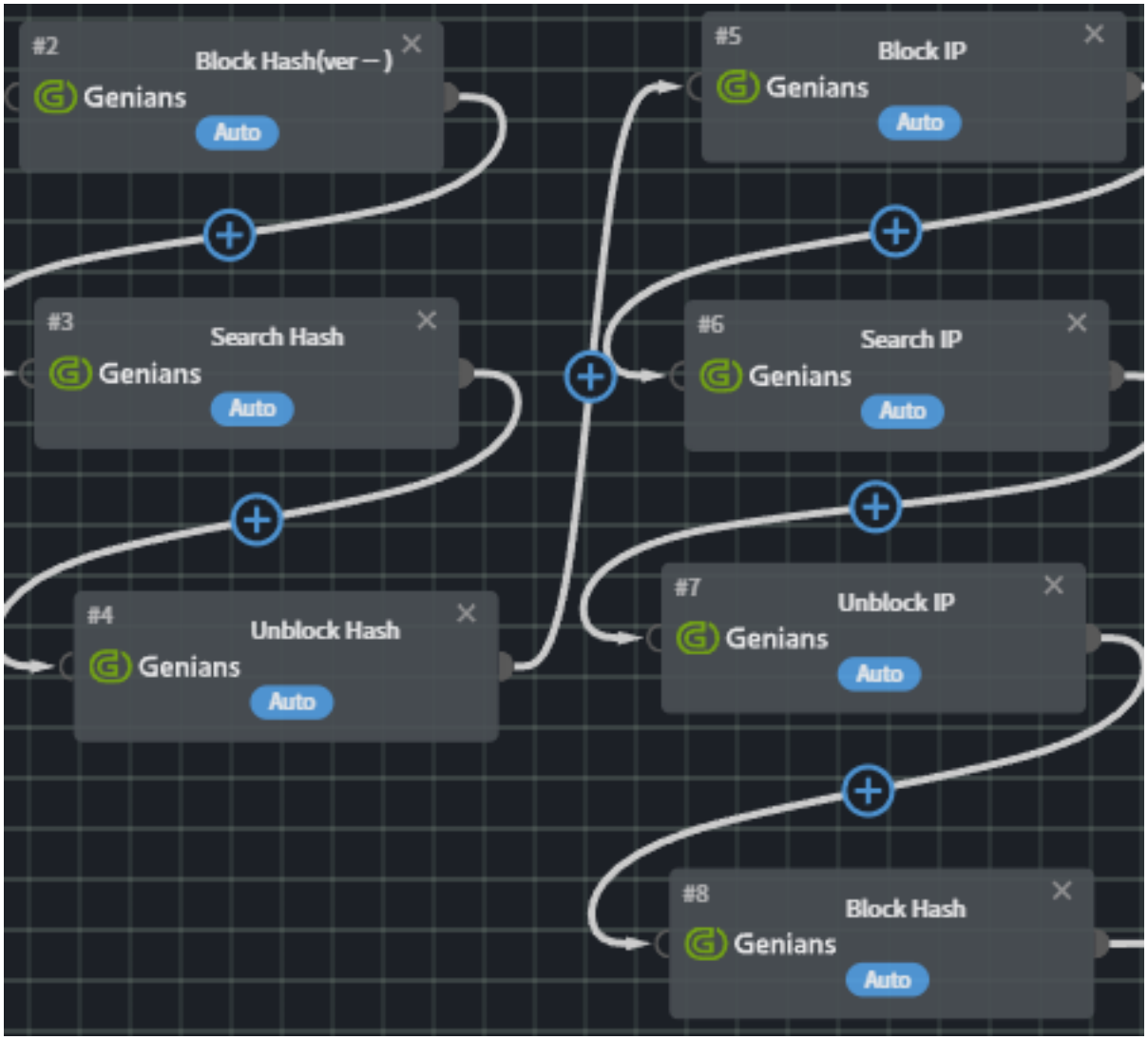


Fig. 3: 컴포넌트 세팅 화면

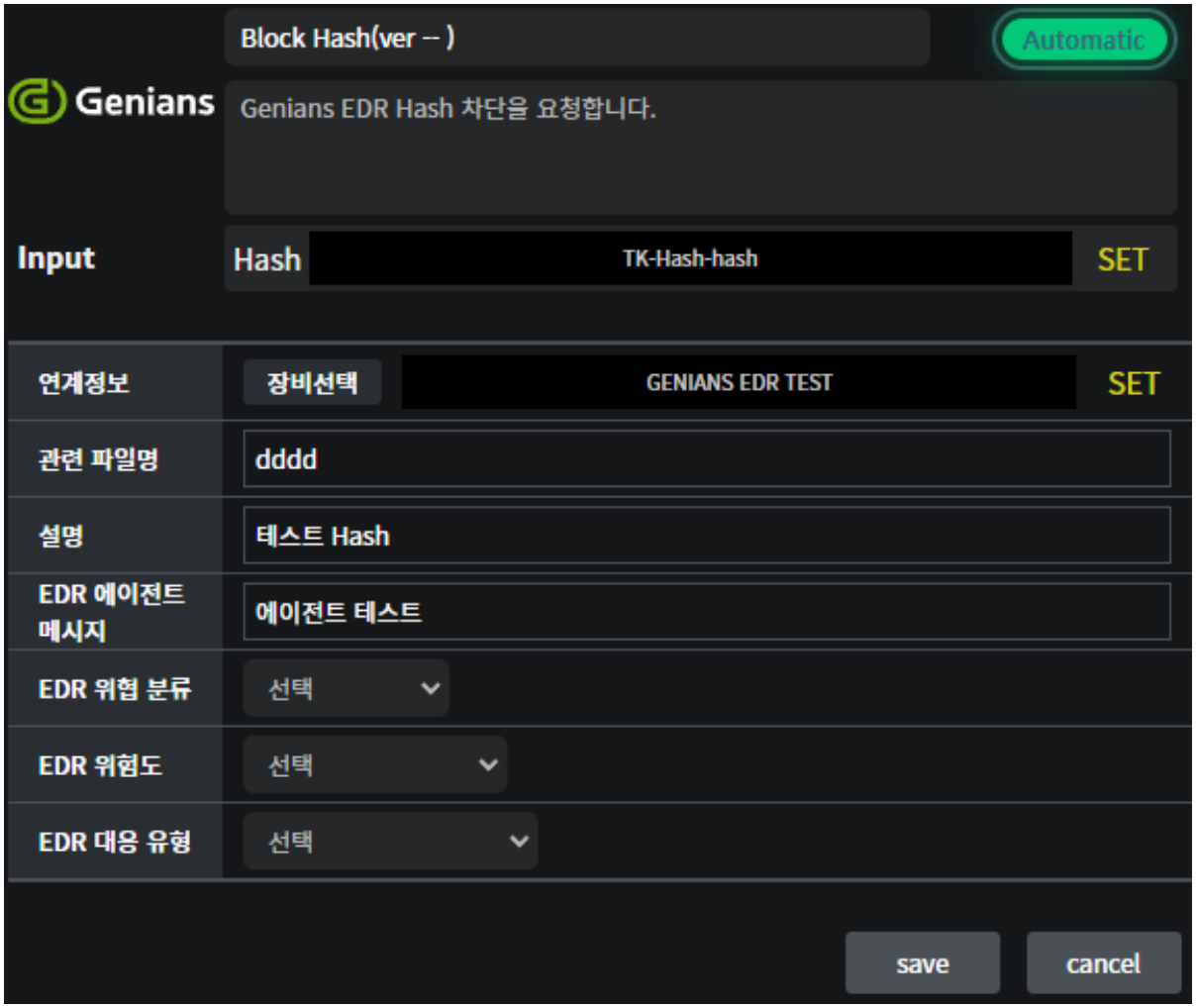


Fig. 4: 컴포넌트 세부 설정 화면

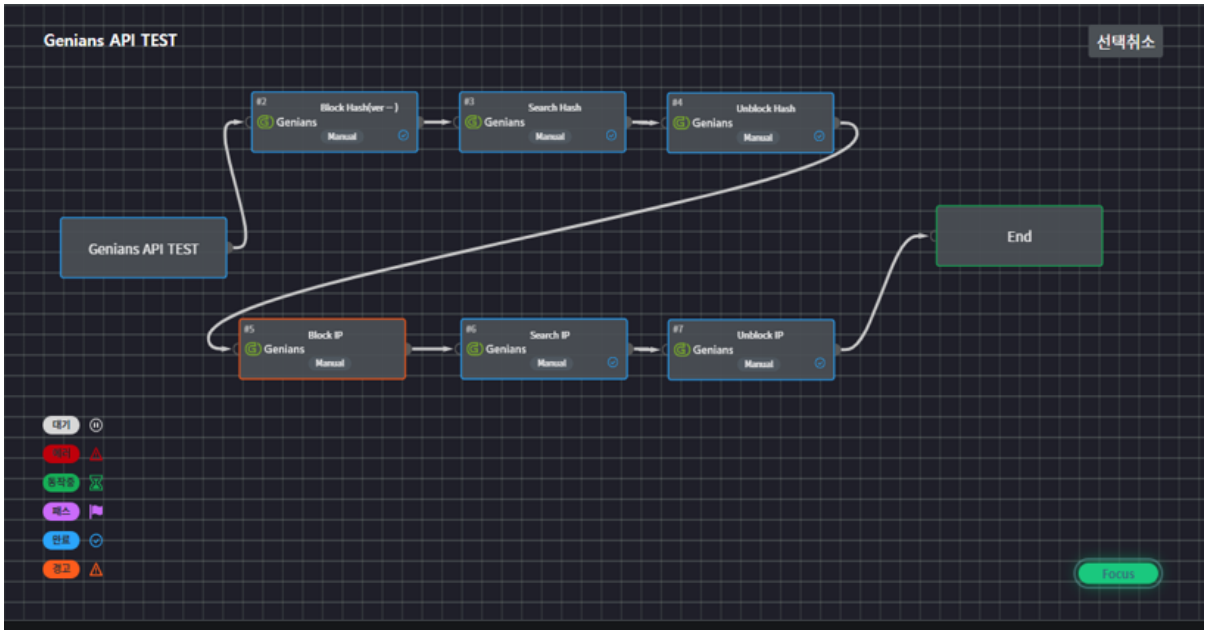


Fig. 5: 플레이북 세팅 후 테스트 화면

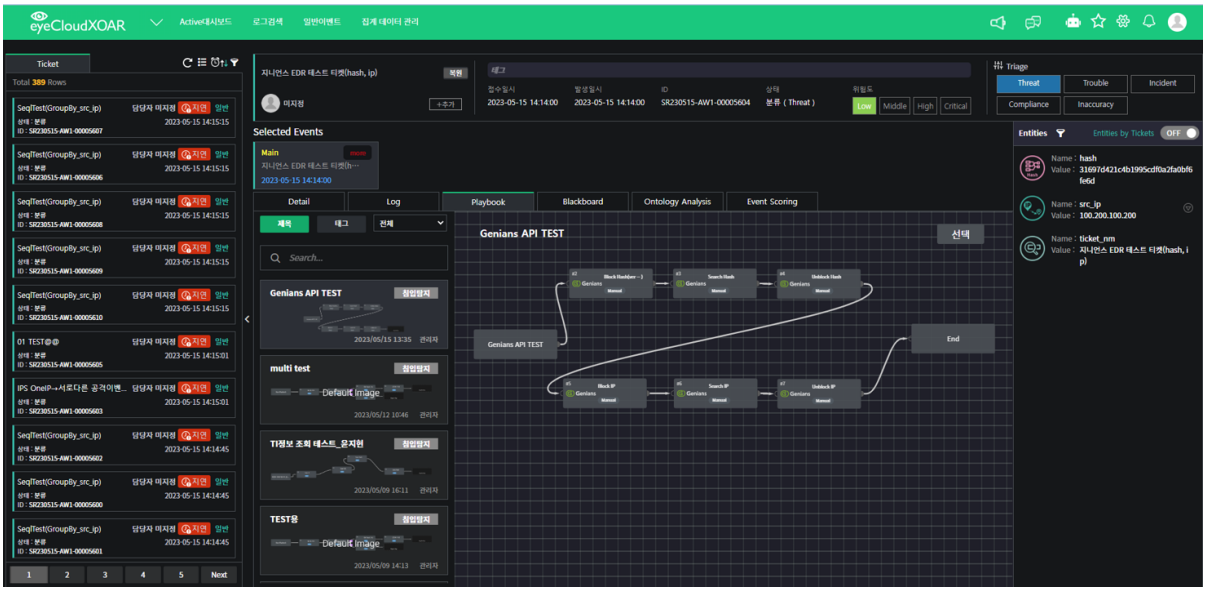


Fig. 6: 플레이북 테스트 결과 화면

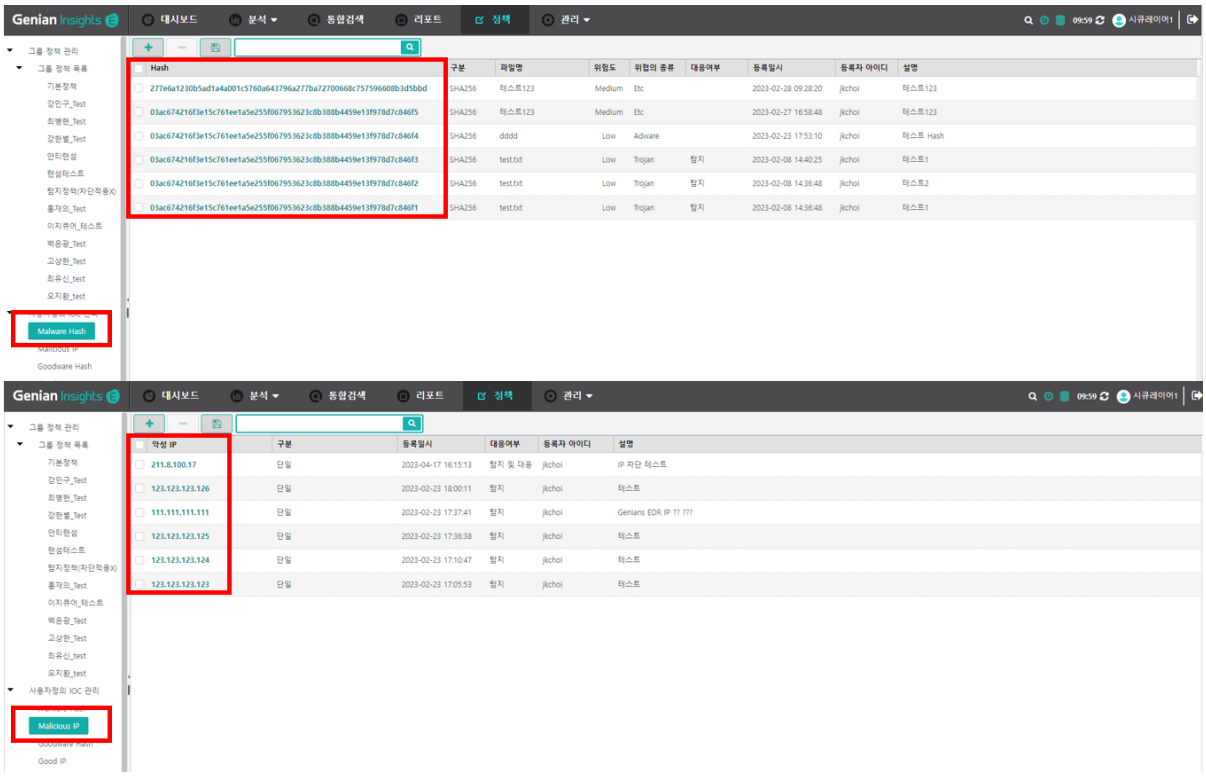


Fig. 7: Genian Insights E 자동 설정된 화면

CHAPTER

EIGHT

안티바이러스 (AV)

Genian AV는 엔드포인트에서 발생하는 악성코드 위협을 정밀하게 탐지하고 신속하게 대응합니다.

악성코드 탐지 결과뿐 아니라, 프로세스 실행 흐름과 유입 경로 등 위협의 맥락 정보를 함께 제공하여 보다 정확한 분석과 신속한 대응을 가능하게 합니다.

이 장에서는 Genian AV의 전반적인 내용을 소개합니다.

8.1 에이전트 설치 및 구성

Genian AV 에이전트는 엔드포인트에 설치되어 백그라운드에서 실시간 보호 기능을 수행합니다.

8.1.1 에이전트 다운로드 및 설치

1. **관리 > 시스템 > 에이전트 패키지** 에서 에이전트 패키지를 업로드 합니다.
2. Windows 버전(x64, x84)에 맞게 설치 파일(.exe)을 다운로드 합니다. 이 때, **다운로드 받은 실행 파일의 이름은 변경하지 않도록 합니다.**
3. 다운로드한 실행 파일을 직접 더블클릭하여 설치하거나, PMS 등을 통해 설치합니다.

8.1.2 에이전트 동작 상태 및 패턴 버전 확인

1. **관리 > 분석 > 엔드포인트 목록** 에서 Genian AV 동작 상태 및 DB 버전 확인 가능합니다.

Note: 동작 상태 및 DB 버전 정보는 **PluginStatus** , **DBVersionAM** 컬럼 추가가 필요합니다.

8.1.3 에이전트 프로세스

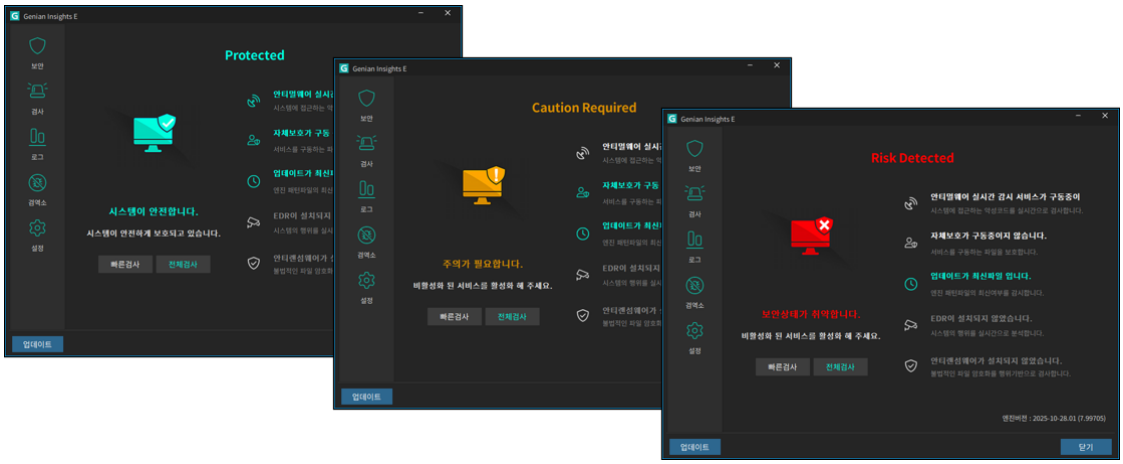
에이전트 설치 시 작업 관리자에서 아래의 4개 프로세스를 확인할 수 있으며, 각 프로세스의 역할은 다음과 같습니다.

프로세스명	용도	비고
GsAgent.exe	메인 프로세스	Insights E, AV 동일 프로세스 사용
GsProtect.exe	무결성 모니터링 모듈	단독 사용 가능
GsView.exe	에이전트 트레이 아이콘	트레이 아이콘 사용안함 설정 시 미동작
GsFlow.exe	보안센터	보안센터 실행 시 동작

8.1.4 에이전트 보안센터

보안센터 - 보안

에이전트 트레이 아이콘 > 우측 마우스 버튼 > 보안센터 클릭 > 보안 에서 서비스 및 기능 활성화 여부에 따른 상태 값 확인할 수 있습니다.



에이전트 상세 상태 값

구분	Protected	Caution Required	Risk Detected
AV 단독	아래 조건 모두 만족 • 실시간 감시 ON • 자체 보호 ON • 업데이트 ON • 안티랜섬 License(기능 OFF) 또는 안티랜섬 License 미포함	다음 중 1개 OFF • 실시간 감시 • 자체 보호 • 업데이트 또는 • 실시간 감시 ON • 자체 보호 ON • 업데이트 ON • 안티랜섬 License(기능 OFF)	다음 중 2개 이상 OFF • 실시간 감시 • 자체 보호 • 업데이트

보안센터 - 검사

에이전트 트레이 아이콘 > 우측 마우스 버튼 > 보안센터 클릭 > 검사 에서 검사 진행사항 및 검사 결과 확인할 수 있습니다.

보안센터 - 로그

에이전트 트레이 아이콘 > 우측 마우스 버튼 > 보안센터 클릭 > 로그 에서 탐지 위협 및 감사 로그 확인할 수 있습니다.

- **위협 탐지 로그 :** 탐지된 위협 로그
- **감사 로그 :** 에이전트 감사 로그

8.2 정책 관리

관리 > 정책 > 그룹 정책 목록 > 기본정책 > 안티멀웨어 에서 Genian AV 관련 정책을 설정할 수 있습니다.

8.2.1 실시간 검사

파일 I/O가 발생하면 실시간으로 악성코드를 검사합니다.

구분	설정값	설명
실시간 검사 사용	사용 / 사용안함	파일 I/O 발생에 따라 실시간 악성코드 검사
지연된 시작 설정	즉시시작 / 1분 후 / 3분 후 / 5분 후 / 10분 후 / 20분 후 / 30분 후 / 1시간 후	PC가 재부팅 될 경우 실시간 검사구동 지연
검사 파일 크기 제한	제한없음 / 100MB / 500MB / 1GB / 3GB / 5GB	검사 파일의 크기 설정, 크기가 초과된 파일은 검사하지 않음
대상파일	모든 파일 / 주요 감염 파일(실행파일)	실시간 검사 대상 파일
이동식 디스크 감지 및 검사	사용 / 사용안함	이동식 디스크가 감지되면 자동으로 검사 수행
CD 감지 및 검사	사용 / 사용안함	CD가 감지되면 자동으로 검사 수행
치료 설정 - 악성코드	그대로 두기 / 치료하기	악성코드가 발견되었을 경우 대응
치료 설정 - 유해가능	그대로 두기 / 치료하기	유해 가능 프로그램이 발견되었을 경우 대응

8.2.2 수동 검사

사용자가 필요하다고 판단할 때 직접 악성코드를 검사합니다.

구분		설정값	설명
검사 파일 크기 제한		제한없음 / 100MB / 500MB / 1GB / 3GB / 5GB	검사 파일의 크기 설정, 크기가 초과된 파일은 검사하지 않음
전체 검사 대상 설정	메모리	사용 / 사용안함	메모리에 대한 위협 검사
	부트영역	사용 / 사용안함	부트영역에 대한 위협 검사
	압축파일	사용 / 사용안함	압축파일에 대한 위협 검사
	대상파일	모든 파일 / 주요 감염 파일(실행파일)	전체 검사 대상 파일
빠른 검사 대상 설정	메모리	사용 / 사용안함	메모리에 대한 위협 검사
	부트영역	사용 / 사용안함	부트영역에 대한 위협 검사
	압축파일	사용 / 사용안함	압축파일에 대한 위협 검사
	대상파일	모든 파일 / 주요 감염 파일(실행파일)	빠른 검사 대상 파일

8.2.3 예약 검사

사용자가 설정한 특정 시간이나 주기에 맞춰 자동으로 검사를 수행합니다.

구분	항목	설정값	설명
예약 검사 목록 추가	이름	Text	예약 검사 이름 입력 예) 중식 시간 검사
	주기	매일 / 매주 (시간 별도 설정)	검사 주기 및 시간 설정
예약 검사 목록 추가	검사 위치	전체 디스크 빠른 검사 직접 추가 %SystemDrive% %WinDir% %SystemDir% %ProgramFiles% %UserDir% %Temp% %TempInternet% %GenianDir%	검사 대상 경로 설정

8.2.4 알림

실시간 검사에서 악성코드 진단, 업데이트, 시스템 등 알림을 설정합니다.

구분	설정값	설명
실시간 검사 진단 알림	사용 / 사용안함	실시간 검사에서 악성코드 진단 시 사용자 알림
업데이트 알림	사용 / 사용안함	진단 패턴의 업데이트 알림
시스템 알림	사용 / 사용안함	시스템 운영에 필요한 알림

8.2.5 업데이트

패턴 업데이트를 자동으로 수행합니다.

구분	설정값	설명
자동 업데이트 사용 여부	사용 / 사용안함	패턴 업데이트 자동 수행
업데이트 주기	4시간 / 8시간 / 12시간	자동 업데이트 주기 설정
부팅 시 업데이트 진행	사용 / 사용안함	부팅 시 업데이트 자동 수행
업데이트 완료 후 검사	사용 / 사용안함	업데이트 완료 후 검사 수행

8.2.6 진단 예외 패턴

위협 진단 대상에서 예외 처리할 파일, 폴더 경로, 해시, 위협명을 설정합니다.

파일 정보

구분	설정값	설명
이름	정책 이름	
파일 및 폴더 경로	파일 및 폴더 경로	UI 내 각 OS별 입력 방법 참조
파일의 SHA256 해시	파일의 SHA256 해시	
설명	설명 문구	

위협 정보

구분	설정값	설명
이름	정책 이름	
위협명	탐지명, 위협 이름(유사도지표), 위협명	
설명	설명 문구	

8.3 시스템 요구사항

8.3.1 하드웨어 요구사항

구분	시스템 요구사항
CPU	Intel Core i3 이상
메모리	4GB 이상
디스크	2GB 이상의 여유 공간
지원 언어	한국어, 영어

8.3.2 소프트웨어 요구사항

제품명	운영 체제
Genian AV	Microsoft Windows OS (32bit/64bit) • Windows 7 SP1 (KB4490628 및 KB4474419 설치) • Windows 8 / 8.1 / 10 / 11 • Windows Server 2012 / 2016 / 2019 / 2022 / 2025

CHAPTER

NINE

매체제어

매체제어 기능은 엔드포인트 기기에 연결되는 다양한 외부 인터페이스 및 저장 매체를 실시간으로 제어하여, 인가되지 않은 데이터 유출을 방지하여 기업의 데이터 자산을 안전하게 보호합니다.

관리자는 필요에 따라 각 기능별 On/Off 하여 운영할 수 있습니다.

9.1 1. 매체 제어 기능

- **이동식 저장 매체 관리**: USB, 외장 디스크, CD/DVD 등 다양한 이동식 저장 매체에 대한 사용, 차단, 읽기, 쓰기 권한을 개별적으로 설정하여 제어합니다.

9.2 2. 장치 제어 기능

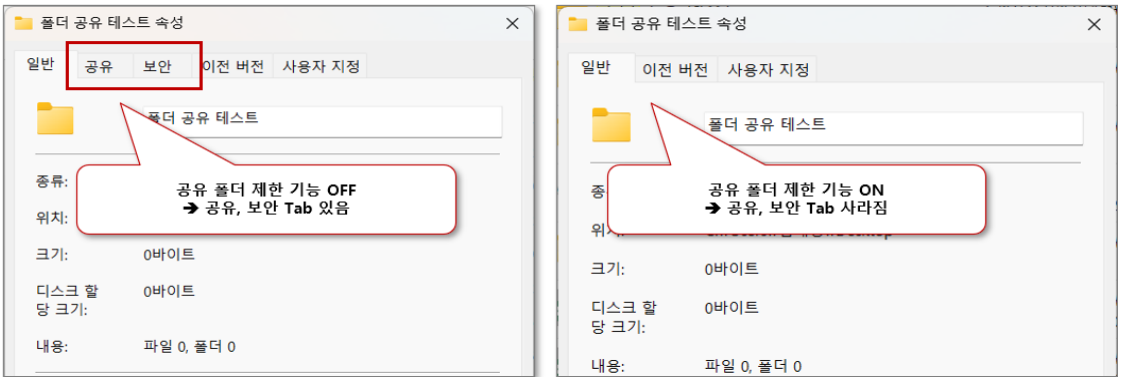
- **주변 장치 연결 제한**: 저장 매체 외의 다양한 하드웨어 장치에 대한 사용을 제한하여 내부 정보 유출을 방지합니다.
- **지원 대상**: 스마트폰, 테더링, 웹캠, 모뎀, 외장 랜카드 등 폭넓은 장치 제어를 지원합니다.

9.3 3. 무선 네트워크 제어

- **비인가 무선랜 접속 차단**: 사내 보안 정책에 어긋나는 비인가 무선 액세스 포인트(AP)로의 접속을 차단합니다.
  - **모니터링**: 주변의 무선 네트워크 환경을 실시간으로 감시하여 정책에 위배되는 비인가 AP 연결 시도를 탐지하고 기록합니다.
  - **차단**: 허가되지 않은 AP나 보안이 취약한 외부 와이파이로의 연결을 즉각 차단하여 네트워크 보안 공백을 방지합니다.
- **허용 AP 목록 관리**: 사내에서 인가된 무선 액세스 포인트(AP) 목록을 구성하여 관리합니다.
  - **접속 권한 통제**: 목록에 등록된 허용 AP 외에 스마트폰 테더링(핫스팟)이나 인근 외부 와이파이 등 비인가 네트워크로의 접속을 제한합니다.
  - **우회 경로 차단**: 인가되지 않은 외부 네트워크 접속을 원천 차단함으로써 내부 데이터가 보안 네트워크 외부로 유출되는 경로를 방지합니다.

9.4 4. 공유 폴더 제어

- **폴더 공유 통제**: 네트워크상의 공유 폴더에 대한 접근 및 생성 권한을 관리하여 불필요한 데이터 노출을 줄입니다.
  - **Everyone 권한 제거**: 보안에 취약한 'Everyone' 공유 권한을 일괄 제거하여 인가된 사용자만 접근할 수 있도록 통제합니다.
  - **공유 해제**: 불필요하게 설정된 공유 설정을 해제하여 잠재적인 데이터 유출 경로를 원천 차단합니다.
- **폴더 공유 UI 숨기기**: 탐색기 등에서 폴더 공유와 관련된 메뉴나 인터페이스를 비활성화하여, 사용자가 임의로 폴더를 공유하는 행위를 사전에 방지합니다.
- **보안 탭 숨기기**: 파일 및 폴더의 속성 창에서 '보안' 탭을 숨겨, 권한 설정을 임의로 변경하거나 확인하려는 시도를 차단합니다.



9.5 5. 안전모드 진입 차단

- **안전모드 진입 차단**: 보안 에이전트의 감시를 회피하기 위해 사용자가 Windows 안전모드로 부팅하는 것을 원천 차단합니다.

Note: 안전모드로 진입이 필요할 경우 설정된 패스워드를 통해 안전모드 사용이 가능하도록 구현했습니다.

CHAPTER

TEN

API 가이드

Genian Insights E는 정책서버로 부터 원하는 정보를 얻거나 보안정책 및 각종 객체들을 설정하기 위한 REST API를 제공합니다. 외부에서 정책서버로 API를 호출하기 위해서는 API Key가 필요합니다. API Key는 각 관리자별로 생성되며 관리자에 부여된 권한에 따라 정보에 접근하거나 설정할 수 있게 됩니다.

관리자 API Key를 생성하거나 확인하기 위해서는 다음과 같이 합니다.

1. 상단 패널에서 관리 > 계정 관리 > 관리자 로 이동
2. API Key를 생성할 관리자명 클릭
3. 관리설정 > API 키 항목에서 API KEY 생성 버튼 클릭
4. 수정 클릭

Warning: API Key 유출 시, 시스템의 정보가 노출될 수 있으니 주의하시기 바랍니다. 또한 보안을 위해 주기적으로 변경하는 것을 권장드립니다.

위 과정을 통해 설정된 API KEY는 다음과 같이 Request URL의 파라메터로 전달되어야 합니다.

```
curl -X GET "https://{Policy Server Management IP}/mc/api/apiKey={API Key}"
```

좀 더 자세한 사용법은 REST API 활용 가이드 를 참고하시기 바랍니다.

Genian Insights E 3.0에서 제공되는 API 목록은 아래에서 확인할 수 있습니다.

- **https://[정책서버IP]:8443/mc/swagger** (관리자는 정책 서버에 로그인되어야 합니다.)

10.1 REST API 활용 가이드

10.1.1 가이드 개요

Genian Insights E 3.0 은 타 장비 또는 타 시스템 등과의 연동을 위해 이벤트 정보의 제공, 사용자 정의 IOC 생성/수정/삭제, 설정변경, 수집 정보 조회 등이 가능하도록 REST API를 제공합니다.

본 가이드는 **Genian Insights E 3.0** 의 REST API를 활용하기 위한 사전 준비사항, 주요 API 등에 대한 안내를 목적으로 합니다.

10.1.2 사전 준비사항

외부 장비에서 Genian Insights E 3.0으로 REST API를 호출하기 위해서 인증이 필요하며, 인증을 위해서는 `API KEY` 값 생성이 필요합니다.

API KEY

- API KEY방식은 연동을 위한 계정의 API KEY를 생성하여 Genian Insights E 3.0 API를 호출할 때마다 API KEY를 첨부하여 활용하는 방식 입니다.
- 각 관리자 계정 별로 별도로 생성하여 활용이 가능합니다. 호출의 권한은 해당 계정의 권한에 종속됩니다.
- API KEY생성 방안은 다음을 참고하시기 바랍니다. *API 가이드*

10.1.3 주요 API

Genian Insights E 3.0과 연동을 위한 주요 API 항목은 **Managements**, **Endpoint**, **Indicator**, **Events**, **Acquisitions** 등이 있고, 각각 상세 내용은 아래와 같습니다.

Managements API

Genian Insights E 3.0 에서는 업무 역할에 따라 권한을 제어하여 사용할 수 있도록 관리역할을 생성할 수 있으며, 생성된 관리역할을 할당하여 관리자 계정을 생성하여 시스템을 관리할 수 있습니다.

Managements API를 활용하시면 관리자 계정, 관리역할에 대한 관리를 수행할 수 있습니다.

관리자 계정 관련한 주요 API는 다음과 같습니다.

Description	Type	API Path	주요 목적
등록된 관리자 계정 검색	GET	/managements/users	사용자 아이디, 사용자명, 접근허용IP 등 등록되어 있는 모든 관리자 계정 관련 정보를 조회하기 위한 목적으로 사용됩니다.
특정 관리자 계정 검색	GET	/managements/users/{user_id}	USER_ID 기준으로 특정 관리자 계정 정보만을 조회하기 위한 목적으로 사용됩니다.
관리자 계정 생성	POST	/managements/users	신규로 관리자 계정을 생성하기 위한 목적으로 사용됩니다.
관리자 계정 수정	PUT	/managements/users/{user_id}	이미 등록되어 있는 관리자 계정 정보를 수정하기 위한 목적으로 사용됩니다.
관리자 계정 삭제	DELETE	/managements/users/{user_id}	이미 등록되어 있는 관리자 계정 정보를 삭제하기 위한 목적으로 사용됩니다.
관리자 API 키 생성	POST	/managements/users/{user_id}/apikey	특정 관리자 계정의 API KEY를 생성하여 API연동, NAC연동을 위한 목적으로 사용됩니다.
관리자 API 키 삭제	DELETE	/managements/users/{user_id}/apikey	특정 관리자 계정의 API KEY를 삭제하기 위한 목적으로 사용됩니다.

관리역할 관련한 주요 API는 다음과 같습니다.

Description	Type	API Path	주요 목적
관리역할 검색	GET	/managements/roles	현재 등록되어 있는 관리역할을 조회하는 목적으로 사용됩니다.
관리역할 조회	GET	/managements/roles/{role_id}	role_id 기준으로 특정 관리역할을 조회하는 목적으로 사용됩니다.
관리역할 생성	POST	/managements/roles	기 정의 된 관리역할 외 신규 관리역할을 생성하는 목적으로 사용됩니다.
관리역할 수정	PUT	/managements/roles/{role_id}	role_id 기준으로 특정 관리역할의 권한 등을 수정하는 목적으로 사용됩니다.

Endpoint API

Genian Insights E 3.0에서는 에이전트가 설치 된 단말은 Endpoint로 명칭하고, 개별 Endpoint에 대해 관리자가 명령을 수행 할 수 있습니다.

Endpoints API를 활용하시면 Endpoint에 네트워크 격리, 아티팩트 수집 등 특정 명령을 수행할 수 있습니다.

Endpoint와 관련한 주요 API는 다음과 같습니다.

Description	Type	API Path	주요 목적
네트워크 격리/해제	POST	/endpoints/command	특정 Endpoint가 감염 된 것으로 추정되어 네트워크 격리가 필요한 경우, 혹은 위협 분석 결과 안전으로 판명될 경우 해제의 목적으로 사용됩니다. command에 isolate_network를 입력하면 됩니다.
아티팩트 수집	POST	/endpoints/command	특정 Endpoint에 대한 상세 분석이 필요한 경우 아티팩트 수집의 목적으로 사용됩니다. command에 collect_artifact를 입력하면 됩니다.
파일 수집	POST	/endpoints/command	특정 Endpoint에 존재하는 파일 수집의 목적으로 사용됩니다. command에 collect_file를 입력하면 됩니다.

Indicator API

Genians Insights E 3.0에서는 MalwareHash(악성HASH), SuspiciousIP(악성IP), GoodwareHash(안전HASH), GoodIP(안전IP) 와 같이 분류하여 위협 정보를 관리하고 있습니다.

Indicator API를 활용하시면 사용자정의 IOC를 조회/추가/삭제를 수행할 수 있습니다.

Indicator와 관련한 주요 API는 다음과 같습니다.

Description	Type	API Path	주요 목적
MalwareHash 조회	GET	/indicators/custom/malwarehashes	등록되어 있는 사용자정의 MalwareHash 정보를 조회하기 위한 목적으로 사용됩니다.
MalwareHash 생성	POST	/indicators/custom/malwarehashes	파라미터에 입력된 정보를 기반으로 사용자정의 MalwareHash 정보를 다중 생성할 목적으로 사용됩니다.
MalwareHash 수정	PUT	/indicators/custom/malwarehashes	등록되어 있는 사용자의 MalwareHash 정보를 수정하기 위한 목적으로 사용됩니다.
MalwareHash 삭제	DELETE	/indicators/custom/malwarehashes	등록되어 있는 사용자의 MalwareHash 정보를 삭제하기 위한 목적으로 사용됩니다.
GoodWareHash 조회	GET	/indicators/custom/goodwarehashes	등록되어 있는 사용자의 GoodwareHash 정보를 조회하기 위한 목적으로 사용됩니다.
GoodWareHash 생성	POST	/indicators/custom/goodwarehashes	파라미터에 입력된 정보를 기반으로 사용자정의 GoodwareHash 정보를 생성할 목적으로 사용됩니다.
GoodWareHash 수정	PUT	/indicators/custom/goodwarehashes	등록되어 있는 사용자의 GoodwareHash 정보를 수정하기 위한 목적으로 사용됩니다.
GoodWareHash 삭제	DELETE	/indicators/custom/goodwarehashes	등록되어 있는 사용자의 GoodwareHash 정보를 삭제하기 위한 목적으로 사용됩니다.
Suspiciousip 조회	GET	/indicators/custom/Suspiciousips	등록되어 있는 사용자의 Suspiciousip 정보를 조회하기 위한 목적으로 사용됩니다.
Suspiciousip 생성	POST	/indicators/custom/Suspiciousips	파라미터에 입력된 정보를 기반으로 사용자정의 Suspiciousip 정보를 생성할 목적으로 사용됩니다.
Suspiciousip 수정	PUT	/indicators/custom/Suspiciousips	등록되어 있는 사용자의 Suspiciousip 정보를 수정하기 위한 목적으로 사용됩니다.
Suspiciousip 삭제	DELETE	/indicators/custom/Suspiciousips	등록되어 있는 사용자의 Suspiciousip 정보를 삭제하기 위한 목적으로 사용됩니다.
Goodip 조회	GET	/indicators/custom/goodips	등록되어 있는 사용자의 goodip 정보를 조회하기 위한 목적으로 사용됩니다.
Goodip 생성	POST	/indicators/custom/goodips	파라미터에 입력된 정보를 기반으로 사용자정의 goodip를 생성할 목적으로 사용됩니다.
Goodip 수정	PUT	/indicators/custom/goodips	등록되어 있는 사용자의 goodip 정보를 수정하기 위한 목적으로 사용됩니다.
Goodip 삭제	DELETE	/indicators/custom/goodips	등록되어 있는 사용자의 goodip 정보를 삭제하기 위한 목적으로 사용됩니다.

Events API

Genian Insights E 3.0에서는 Endpoint 이벤트 수집, 위협 이벤트 탐지, 소프트웨어 정보 수집, 저장매체 정보 수집 등 다양한 정보를 수집하여 저장하고 있습니다.

Events API를 활용하시면 수집 이벤트, 위협 이벤트, 소프트웨어 정보, 외부매체 정보 등 Insights E에 적재된 이벤트를 조회 할 수 있습니다.

Description	Type	API Path	주요 목적
이벤트 조회 및 집계	GET	/events/endpoints	수집된 이벤트를 조회 및 집계하는 목적으로 사용됩니다.(단, 검색범위는 24H 초과불가, 반환 건수는 최대 1000건, API KEY 별 1초내 연속 요청 제한)
위협 이벤트 조회 및 집계	GET	/events/alerts	위협 이벤트를 조회 및 집계하는 목적으로 사용됩니다. (단, 검색범위는 일주일 초과불가, 반환 건수는 최대 1000건, API KEY 별 1초내 연속 요청 제한)
소프트웨어 정보 조회 및 집계	GET	/events/softwares	엔드포인트에 설치되어 있는 소프트웨어 정보를 조회하는 목적으로 사용됩니다. (단, 반환 건수는 최대 1000건, API KEY 별 1초내 연속 요청 제한)
파일 정보 조회 및 집계	GET	/events/filemasters	엔드포인트에서 수집한 파일에 대한 해시, 속성, 전자서명 등 정보를 조회하는 목적으로 사용됩니다. (단, 반환 건수는 최대 1000건, API KEY 별 1초내 연속 요청 제한)
시스템 정보 조회 및 집계	GET	/events/systems	엔드포인트 시스템 소프트웨어 정보(cpu,mem,list 등)를 조회하는 목적으로 사용됩니다. (단, 반환 건수는 최대 1000건, API KEY 별 1초내 연속 요청 제한)
실행파일 유입경로 정보 조회 및 집계	GET	/events/inflows	실행파일의 유입 경로에 대한 정보를 조회하는 목적으로 사용됩니다. (단, 검색범위는 일주일 초과불가, 반환 건수는 최대 1000건, API KEY 별 1초내 연속 요청 제한)
외부매체 정보 조회 및 집계	GET	/events/volumes	외부매체(이동식 디스크, 외장 HDD 등) 정보를 조회하는 목적으로 사용됩니다. (단, 검색범위는 일주일 초과불가, 반환 건수는 최대 1000건, API KEY 별 1초내 연속 요청 제한)

Acquisitions API

Genian Insights E 3.0에서는 에이전트 로그 수집, Endpoint 파일 수집, 악성 샘플파일 수집 등 다양한 파일을 수집할 수 있습니다.

Acquisitions API를 활용하시면 에이전트 로그 수집, 파일 수집 기능, 아티팩트 수집, 악성 샘플파일 수집 등 다양한 파일을 수집할 수 있습니다.

Description	Type	API Path	주요 목적
수집된 파일 검색	GET	/acquisitions	수집관리 메뉴 내 수집된 파일을 검색하는 목적으로 사용됩니다. (단, 검색범위는 30일 초과불가, 반환 건수는 최대 1000건, API KEY 별 1초내 연속 요청 제한)
수집된 파일 다운로드	GET	/acquisitions/download	수집관리 메뉴 내 수집된 파일을 다운로드 하는 목적으로 사용됩니다. (단, API KEY 별 1초내 연속 요청 제한)

10.1.4 RESPONSE CODE

아래 표는 REST API에서 사용하는 HTTP Status Codes를 나타냅니다.

Code	Name	Detailed Descriptions
200	OK	요청이 성공적으로 되었습니다.
201	Created	요청이 성공적이었으며 그 결과로 새로운 리소스가 생성되었습니다.
400	Bad Request	잘못된 구문으로 인해 서버가 요청을 이해할 수 없습니다.
401	Unauthorized	요청한 응답을 받기 위해서는 사용자 인증이 필요합니다.
403	Forbidden	콘텐츠에 접근할 권리를 가지고 있지 않습니다.
404	Not Found	서버는 요청받은 리소스를 찾을 수 없습니다.
406	Not Acceptable	요청한 페이지가 요청한 콘텐츠 특성으로 응답할 수 없습니다.
500	Internal Server Error	서버에 예기치 않은 오류가 발생했습니다.
503	Service Unavailable	서버가 요청을 처리할 준비가 되지 않았습니다.

10.1.5 참고 - API활용도구 제공:Swagger

Genian Insights E 3.0를 활용하는데 도움을 드리고자, Swagger 페이지를 제공하고 있습니다. Swagger는 웹페이지를 통해서 REST API 정보와 테스트 도구를 제공합니다.

1단계. Swagger 접속

1. Genian Insights E 3.0 의 관리자 계정으로 WEB 콘솔 1차 접속
2. 로그인이 된 상태에서 주소창에 https://{정책서버IP}:8443/mc/swagger 를 입력하여 2차 접속
3. Swagger 접속 확인

2단계. Swagger를 이용한 테스트

1. 활용하고자 하는 API를 선택한 후, 해당 API의 우측에 Try It out 버튼 클릭
2. Parameters 항목에서 Description 값 입력
3. 아래의 Execute 버튼 클릭
4. Responses 항목에서 curl 및 Request URL 값 확인 (Server response 항목에서 Code값이 200 일 때 정상동작합니다.)

Note: Content Type은 JSON을 사용하며 'application/json;charset=UTF-8'을 표준으로 합니다. (포맷이 다른 경우, 폰트가 손상되어 보일 수 있습니다.)

CHAPTER

ELEVEN

FAQ

제품 출시 주기는 언제입니까?

- Genian Insights E는 1개월마다 새로운 버전을 출시합니다.

소프트웨어 버전을 다운 그레이드 할 수 있습니까?

- 아니요, 다운 그레이드는 지원되지 않습니다. 다운 그레이드의 경우 업그레이드하기 전에 백업을 만든 다음 소프트웨어를 다시 설치하고 백업 데이터를 복원해야합니다.

구성 요소 간의 통신이 암호화되어 있습니까?

- 각 구성 요소 간의 통신은 TLS를 통해 암호화됩니다.

Genian Insights E가 백신을 대체 할 수 있나요?

- **Insights E 3.0** 에서 기존 Insights E 기능에 자체 개발한 차세대 백신(AV) 엔진을 통합하여, 알려진 위협과 알려지지 않은 위협 모두 수행할 수 있습니다.

에이전트 리소스 및 로그량은 어떻게 되나요?

- 리소스 : CPU : 1% 미만, MEM은 40MB 미만이며, 임계치 제한 기능도 제공하고 있습니다.
- 로그량 : 1일 1PC 당 20MB 기준이며, 이벤트는 암호화/압축 전송으로 1.3 kbps/PC 트래빅이 발생합니다.

문서의 복사, 이동, 업/다운로드가 보이는데 DLP와의 차이점이 무엇인가요?

- DLP는 데이터 유출을 실시간으로 감시하고 차단하는 '사전 예방'에 집중하는 반면, Insights E는 모든 행위 로그를 기록하고 분석하여 유출 경로를 추적하는 '리스크 관리'에 특화되어 있습니다.

XDR, SOAR 연동은 가능한가요?

- SYSLOG, SNMP, REST API 등을 통해 SIEM/SOAR 연동이 가능합니다.

침해대응 및 악성코드 분석 필요 시 제조사 지원이 되나요?

- Insights E를 운영 중인 고객사에서 보안 사고가 발생할 경우, 1차적으로 ES기술부가 신속하게 지원하며, 심층 분석이 필요한 2차 단계에서는 **GSC** 가 투입되어 정밀한 위협 분석 서비스를 제공합니다.

Note: GSC(Genians Security Center)는 2023년도에 설립되었으며, 악성파일 위협 분석가들로 구성된 조직입니다.

CHAPTER

TWELVE

TROUBLESHOOTING

12.1 디버그 수집과 증상 분석

12.1.1 BSoD 발생 시 메모리덤프 분석

엔드포인트에서 BSoD 발생 시 아래 절차를 통해 발생 원인을 추측할 수 있습니다.

BSoD 화면에서 Insights E 관련 드라이버 파일명이 확인되는 경우

1. %windir%memory.dmp 와 에이전트 Full 로그를 수집하여 분석요청을 합니다.
2. 반대로 BSoD 화면상에 다른 제품 드라이버 명이 출력되는 경우, 해당 제품 개발사에 원인 분석요청을 합니다.

BSoD 화면에서 드라이버 파일명이 확인되지 않는 경우

문제가 발생하는 드라이버 파일을 확인하기 위해 필요한 분석 프로그램을 설치합니다.

1. **windbg 설치:** windbg는 windows sdk 를 통해 설치할 수 있습니다. (windows sdk를 설치하면서 설치할 요소 중 "Debugging Tools for Windows" 만 선택하고 나머지는 선택 해제)
2. **덤프파일 열기:** 인터넷이 가능한 PC에서 windbg를 설치한 후 windbg에서 %windir%memory.dmp 를 열어봅니다. (memory.dmp에 읽기 권한 설정 후 windbg 창에 drag 합니다.)
3. **심볼경로 설정:** 덤프가 열리면 다음의 명령 실행합니다.

```
.symfix+
.reload
```

4. **자동분석 실행:** !analyze -v를 실행한 후 출력되는 분석 보고서를 면밀하게 읽어봅니다.

분석 결과 중에 아래와 같은 부분(MODULE_NAME)이 있으면 이 드라이버가 문제일 가능성이 높습니다. 문제 드라이버가 확인된 경우 해당 드라이버 개발사에 원인 분석을 요청합니다.

```
6: kd> !analyze -v
*******************************************************************************
*                                                                             *
*                        Bugcheck Analysis                                    *
*                                                                             *
*******************************************************************************

DPC_WATCHDOG_VIOLATION (133)
```

(continues on next page)

(continued from previous page)

```
The DPC watchdog detected a prolonged run time at an IRQL of DISPATCH_LEVEL
or above.
Arguments:
Arg1: 0000000000000001, The system cumulatively spent an extended period of time at
        DISPATCH_LEVEL or above. The offending component can usually be
        identified with a stack trace.
...
MODULE_NAME: check64   <<< 이 부분!!
IMAGE_NAME:  check64.sys
...
```

의심스러운 드라이버 이름이 확인되었지만, 이 드라이버에 대한 정확한 정보를 파악할 수 없다면 해당 PC 에서 드라이버 파일을 찾아 정보를 확인해야 합니다. 예를 들어, 확인된 드라이버 이름이 f_ih.sys 인 경우 lmvm 명령으로 해당 드라이버 위치(Image path)를 확인할 수 있습니다. 드라이버 파일을 찾아서 등록정보 등을 확인해보면 개발사를 유추할 수 있습니다.

```
6: kd> lmvm f_ih
Browse full module list
start             end                 module name
fffff805`37030000 fffff805`3703a000   f_ih       (deferred)
  Image path: \??\C:\windows\SYSTEM32\DRIVERS\f_ih.sys
  Image name: f_ih.sys
  Browse all global symbols  functions  data
  Timestamp:        Tue Oct 18 09:43:46 2016 (58057042)

  CheckSum:         0001256B
  ImageSize:        0000A000
  Translations:     0000.04b0 0000.04e4 0409.04b0 0409.04e4
  Information from resource tables:
```

6. !analyze -v 결과 중에 의심 드라이버가 특정되지 않은 경우, CallStack 부분을 주의깊게 살펴봅니다.

```
STACK_TEXT:
ffff9881`99fe5b08  : nt!KeBugCheckEx
ffff9881`99fe5b10  : nt!KeAccumulateTicks+0x181641
ffff9881`99fe5b70  : nt!KeClockInterruptNotify+0x98c
ffff9881`99fe5f30  : hal!HalpTimerClockInterrupt+0xf7
ffff9881`99fe5f60  : nt!KiCallInterruptServiceRoutine+0xa5
ffff9881`99fe5fb0  : nt!KiInterruptSubDispatchNoLockNoEtw+0xfa
fffffbd05`dfd57660  : nt!KiInterruptDispatchNoLockNoEtw+0x37
fffffbd05`dfd577f0  : nt!KxWaitForSpinLockAndAcquire+0x30
fffffbd05`dfd57820  : nt!KeAcquireSpinLockRaiseToDpc+0x87
fffffbd05`dfd57850  : check64!test::Lock+0x30 [c:\test.cpp @ 205]
fffffbd05`dfd57880  : check64!test::EnumElement+0x65 [c:\test.cpp @ 277]
fffffbd05`dfd578d0  : check64!testanalyze::fileinfo+0x10f [c:\testanalyze.cpp @ 1786]
fffffbd05`dfd57950  : check64!testcheckInfo+0x100 [c:\testcheck.cpp @ 7214]
fffffbd05`dfd579f0  : check64!testcheckCallback+0x1ca [c:\testcheck.cpp @ 3189]
fffffbd05`dfd57a50  : check64!stest::memoryQueue+0x9e [c:\stest.cpp @ 118]
fffffbd05`dfd57a90  : check64!stest::checkFunc+0x9d [c:\stest.cpp @ 145]
fffffbd05`dfd57b10  : nt!PspSystemThreadStartup+0x55
fffffbd05`dfd57b60  : nt!KiStartSystemThread+0x28
```

Callstack의 각 항목은 다음과 같은 의미를 가집니다.

```
[주소/인자 등 16진수] : [모듈이름] ! [해당 모듈 내의 주소 / Offset]
```

예를 들어 아래와 같은 항목은 nt 커널의 KiStartSystemThread+0x28 메모리 주소를 의미합니다.

```
ffffbd05`dfd57b60  : nt!KiStartSystemThread+0x28
```

Callstack은 아래쪽이 먼저 호출된 함수, 윗쪽이 나중에 호출된 함수를 의미합니다. Callstack을 위에서부터 아래로 내려오면서 나중에 호출된 모듈부터 살펴봅니다. 이때, Windows의 구성요소가 아닌 모듈 중 가장 처음 나타나는 모듈이 문제를 일으켰을 가능성이 높습니다. 예를 들어, 위의 Callstack에서는 다음과 같은 순서로 모듈이 나타납니다.

```
nt >> hal >> nt >> check64 >> nt
```

이 중에서 nt, hal 는 windows의 구성요소이기 때문에 windows 구성요소가 아닌 모듈중에서 처음으로 나타난 check64가 문제를 일으킨 모듈입니다. 일반적으로 Callstack에 많이 등장하는 Windows 모듈명들은 다음과 같습니다.

Table 1: windows 모듈명

모듈명	역할
nt	윈도우즈커널
hal	H/W 관장
io	IO manager
netio	Network I/O Subsystem
fltmgr	Filter manager
ob	Object manager

의심스러운 모듈을 찾아냈다면 lmvm 명령으로 파일의 경로를 확인하고, 해당 파일의 등록정보나 전자서명 정보에서 제조사 등의 정보를 체크합니다. 확인된 의심 모듈이 Insights E 관련 모듈이거나 윈도우즈 관련 모듈인 경우, %windir%memory.dmp 및 에이전트 로그를 수집하여 원인 분석을 요청합니다.

CHAPTER

THIRTEEN

RELEASE NOTE

Genian Insights 업그레이드 시 주의사항과 Genian Insights V3.0 버전에서 새롭게 변경된 내용을 담고 있는 릴리즈 노트를 제공합니다.

릴리즈 노트의 내용은 Genian Insights를 사용하는 사용자를 위해서 작성되었으며, Genian Insights 사용자가 아닌 사람에게 배포하는 것은 허용되지 않습니다.
릴리즈 노트의 내용은 제품 개선에 따라 예고없이 변경될 수 있습니다.

13.1 업그레이드 가이드

13.1.1 주의사항

- 업그레이드를 하기 전 반드시 업그레이드 가이드와 릴리즈 노트를 충분히 읽어보신 뒤 문제되는 사항이 없는지를 확인하신 후 진행하시기 바랍니다.
- 제품 다운그레이드는 지원되지 않습니다. 제품을 다운그레이드 하는경우 상위버전에서 수행한 DB 테이블 변경으로 인해 오동작할 수 있습니다.부득이하게 다운그레이드를 해야하는 경우 다운그레이드 하는 버전에서 생성한 백업파일로 DB를 복구해서 사용해야 합니다.
- 정책서버 및 DB 업그레이드를 하는 경우 반드시 백업을 수행하는것을 권장합니다.
- 기존버전과 업그레이드 버전간의 버전차이가 큰 경우 다수의 DB테이블 구조변경으로 인한 Migration으로 인해서 업그레이드가 장시간 소요될 수 있습니다. 이때 CLI 콘솔에 접속하면 DB migration중임을 알리는 메시지가 표시되며, migration 중인 경우 절대로 서비스를 중지하거나 장비를 재부팅해서는 안됩니다.

13.1.2 정책서버 업그레이드 방법

Genian Insights E는 관리콘솔에서 업그레이드를 진행할 수 있습니다.

WEBUI를 이용한 진행

- .img 파일을 **관리> 업데이트 관리 에 시스템OS** 에서 제품 업로드 버튼을 클릭하여 제품을 업로드 한 후, 업그레이드 시작 버튼을 클릭합니다. 업그레이드 완료되면 로그인페이지로 이동 됩니다.

13.1.3 에이전트 업데이트 방법(Genian NAC 에서 수행)

정책서버 업그레이드 후 에이전트도 함께 업데이트 해야 합니다. 시스템 > 에이전트 > 플러그인 에 플러그인 업로드를 선택하여 Threat Detector2 플러그인을 업로드 합니다.

Genian NAC에 설정 된 시스템 정책 동작 주기에 따라 자동으로 플러그인 업데이트를 진행 합니다.

13.2 Release Notes

13.2.1 Current Versions

Genian Insights 3.0.7 (R) Release Notes (2026-05-08)

Last Updated: 2026-05-26

Security Vulnerability

Revision	Key	Components	Description	Affects Versions	CVSS Score
51750	GS-12461	GenianOS	Linux 커널 버전 업그레이드 6.6.89 -> 6.6.137		

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
50482	GS-11993	Frontend	위협 이벤트 상세정보 미제공 케이스 예외 처리 및 안내 메시지 문구 개선	
50478	GS-12094	Backend	엔드포인트 빠른 검색에 로그온ID(LogonID) 필드 추가	
50477	GS-12068	AgentWindows	CMSTPLUA COM 객체를 악용한 UAC 우회 탐지	
50662	GS-12005	ATT&CK	MITRE 내장 진단 룰 최신화	
50678	GS-11858	AgentWindows	Yara 최신 버전 적용	
50848	GS-11897	Backend	OpenSSL 3.5 버전 업그레이드	
50859	GS-10024	Frontend	관리자 정보에서 기존 API 키를 ClientSecret로 관리하도록 개선	
50875	GS-8840	Frontend	파일 상세 분석 화면에 기간 검색 필터 기능 추가	
50894	GS-12096	AgentWindows	자동실행 탐지경로에 RunOnce/RunOnceEx 추가	
50894	GS-11950	AgentLinux/AgentMacOS	gs-daemon, 단말-정책서버 간 이벤트 타임스탬프 동기화	
51020	GS-11825	Frontend	위젯 간 의존모드 사용 시 전달된 검색 조건을 초기화할 수 있는 기능 추가	
51007	GS-12152	AgentWindows	에이전트 OpenSSL Dual Version (3.0.19 / 3.5.5) 적용	
51760	GS-12409	Frontend	엑셀 가져오기/내보내기 버튼 동작 개선(내보내기 단일 기능 지원)	
51760	GS-12089	Backend	에이전트 트레이 메뉴에서 사용자 본인의 매체제어 예외 신청 현황을 확인 및 재신청할 수 있는 기능 추가	
51760	GS-12350	Frontend	매체 제어 예외 현황 화면 및 재신청 기능 개발	
51125	GS-10021	Backend	M2M 환경 보안 강화를 위한 OAuth 2.0 토큰 기반 연동 전환	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
50481	GS-6757	Frontend	파일 업로드 시 파일명이 정상적으로 표시되지 않는 문제	1.0.0
50484	GS-11978	Frontend	관리자 추가 팝업창에서 사용자 정보가 자동 완성되는 문제	1.0.0
50485	GS-12084	Frontend	루씬 쿼리 필드명 앞 느낌표(!), 대시(-) 포함 시 문법 검사 실패하는 문제	2.0.123
50675	GS-12049	Frontend	대시보드 빈 박스 위젯에서 이미지 업로드 후 이미지가 표시되지 않는 문제	2.0.101
50843	GS-12178	Frontend	추가 수집 확장자 Input Box에서 Enter를 입력하는 경우 서버에 즉시 전송할 이벤트 목록 팝업이 출력되는 현상	1.0.0
50854	GS-12046	Frontend	엔드포인트 그룹 상세화면의 정책명 Select Box 옵션 목록에 스크롤이 노출되지 않는 현상	3.0.3
51013	GS-12186	Frontend	가상 키보드 사용해 사용자 정보 수정 시 로그아웃되는 문제	3.0.1
51021	GS-12124	Frontend	대시보드 분석 탭에서 기간 비교 그리드의 데이터가 실제 결과와 일치하지 않는 문제	2.0.0
51381	GS-12343	Backend	위협관리에서 대응정책 수정시 에이전트가 변경된 대응정책 수신하지 못하는 문제	3.0.2
51707	GS-12389	Frontend	정책>고급>에이전트 운영제한 사용 시 하단 요일 체크박스가 정상 출력되지 않는 증상	2.0.101
51751	GS-11134	Frontend	위협 관리 화면에 탐지 지표 데이터가 보이지 않는 오류	2.0.132
51873	GS-12557	AgentEvent	위협 탐지 Rule에 매칭된 프로세스명(위협 탐지 근거)이 한글인 경우 깨지는 문제	2.0.129

13.2.2 Previous Versions

Genian Insights 3.0.6 Release Notes (2026-04-02)

Last Updated: 2026-04-07

Security Vulnerability

Revision	Key	Components	Description	Affects Versions	CVSS Score
51238	GS-12047	Backend	Tomcat 버전 업그레이드 9.0.112 -> 9.0.117		9.1

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
51134	GS-9471	AgentWindows	악용 가능한 커널 드라이버 로딩 사전 차단 기능 구현	
51134	GS-11942	python	C-TAS 플러그인 ExportAPI Client v3.0 업그레이드	
51134	GS-11874	Frontend	에이전트 설치 페이지 내 에이전트 등록 방식에 대한 설명 툴팁 추가	
51134	GS-11823	Frontend	Node.js 16.17.0 -> 24.13.1, Webpack v4.44.1 -> v5.88.0 업그레이드	
51134	GS-11655	Backend, Frontend	라이선스 모듈별 장비수 제한 기능 추가	
51134	GS-10762	Frontend	기본 대시보드 템플릿 제공 및 관리자 선택 적용 기능 개발	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
51134	GS-11948	Frontend	위협 모니터링 화면에서 상태별 위협 탐지 현황 수치가 커질 경우 영역을 벗어나는 오류	2.0.11
51134	GS-11814	Frontend	이벤트 조사에서 Module 이벤트를 진단 규칙으로 추가 시 File.CmdLine 정보가 포함되는 문제	2.0.15
51134	GS-11737	AgentWindows	서비스 종료 시 Log 플러그인 종료 대기로 인한 에이전트 Hang 발생	2.0.132

Genian Insights 3.0.5 Release Notes (2026-03-05)

Last Updated: 2026-03-25

Security Vulnerability

Revision	Key	Components	Description	Affects Versions	CVSS Score
50408	GS-11818	Frontend	crypto-js 버전 업그레이드 (4.1.1 -> 4.2.0)		9.1

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
50805	GS-12202	Frontend	매체 제어 예외 신청 시 "대리 신청 모드" 일 때, 대리 신청자 정보를 저장하도록 개선	
50604	GS-11664	Frontend	매체 제어 예외 신청 및 관리 시스템 개발	
50408	GS-8985	Backend, Elasticsearch	Elasticsearch v8.19.7 업그레이드	
50408	GS-8878	Frontend	옵션에 따라 파일 평판 정보 업데이트와 유사도 지표 갱신 버튼이 보이도록 개선	
50408	GS-8274	Backend, Elasticsearch	Elasticsearch 노드 간 통신(Transport layer) 암호화 적용	
50408	GS-11643	Elasticsearch	구버전 Elasticsearch 인덱스를 현재 구동 중인 Elasticsearch 버전의 인덱스로 재색인 할 수 있도록 Background Reindex 기능 추가	
50408	GS-11582	Frontend	대시보드 자동 갱신 기능 추가	
50408	GS-11301	Database	MySQL 8.4.7 LTS 업그레이드 (CT64)	
50408	GS-10856	Frontend	이벤트 수집 관리에서 수집 예외 설정 시 수정된 항목이 없는 경우 표시되는 오류 메시지 개선	
50408	GS-10536	Frontend	대시보드 화면 다크 모드 지원	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
50839	GS-12040	Backend	사용자정의 MalwareHash 사전실행차단 설정 시 SHA256은 차단되지 않는 오류	2.0.14
50674	GS-12092	Frontend	매체 제어 예외 신청 및 관리 시스템 개발 관련 피드백 수정	3.0.5 (R)
50673	GS-12134	Frontend	관리콘솔 언어 설정이 영문인 경우, 위협 분석 화면의 "요약 내용" 이 표시되지 않는 문제	2.0.100
50408	GS-11722	Frontend	Add/Remove Component에서 실제 데이터에 일부 컬럼의 값이 없을 때 데이터 행이 표시되지 않는 문제	2.0.144, 3.0.1
50408	GS-11613	Frontend	매트릭스 그리드 위젯 설정 시 정상 동작 하지 않는 문제	1.5.100
50408	GS-11551	Frontend	위협 요약 화면에서 XBA위협 정보 중에 CmdLine 정보가 표시되지 않는 문제	3.0.1

Genian Insights 3.0.4 Release Notes (2026-02-04)

Last Updated: 2026-02-04

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
49768	GS-11563	Agent	NAC와 Insights E 에이전트(보안센터)의 트레이 메뉴 연동 개선	
49768	GS-11549	Agent	장치 제어(스마트폰, 테더링, 웹캠, 모뎀, 외장 랜 카드) 기능 구현	3.0.4 (R)
49768	GS-11543	Agent	AV 진단 패턴 최신 업데이트 만료기간 설정 기능 추가	
49768	GS-11445	Frontend	Insights E 일본어 추가	
49768	GS-11232	Agent	[안티랜섬] 서비스 지연 기능 추가	
49768	GS-11092	Frontend	악성코드에 대한 위협 인텔리전스 분석 정보 확대	
49768	GS-10174	Agent	FileUpload / FileAttach XBA 진단 시 첨부파일 수집 기능	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
49768	GS-11750	Frontend	엔드포인트 그룹관리 상세에서 컬럼 설정 버튼이 동작하지 않는 문제	3.0.4 (R)
49768	GS-11633	Frontend	관리자의 접근제어 IP 설정 시 잘못된 문자열 검증	2.0.101
49768	GS-11459	Frontend	위협 이벤트의 이벤트 상세보기 도킹 모드인 경우 그리드 전환 옵션이 활성화되어 있는 문제	2.0.13

Genian Insights 3.0.3 Release Notes (2026-01-08)

Last Updated: 2026-02-03

Security Vulnerability

Revision	Key	Components	Description	Affects Versions	CVSS Score
49244	GS-11298	Backend	Tomcat 버전 업그레이드 9.0.108 -> 9.0.112		7.5

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
49687	GS-11710	Agent	SQLite 모듈 업그레이드	2.0.106
49244	GS-9687	Backend	서버 관리 메뉴에 Kafka 인증서 갱신 기능 추가	
49244	GS-11513	GenianOS	batch configuration mode 사용 시 프롬프트가 genian(config-batch)으로 출력되도록 개선	
49244	GS-11461	Frontend	이벤트 조사의 이벤트 상세 분류가 RequestProcessCreate 인 경우 이벤트 요약을 보다 상세하게 출력	
49244	GS-11428	Agent	예약검사 경로에 대해 미리 정의한 항목을 선택할 수 있도록 기능 추가	3.0.3
49244	GS-11396	Frontend	서버 모듈 상태 표시 화면에 인증서 만료 경고 표시 추가	
49244	GS-11350	Frontend	관리 역할화면에서 기본 제공 권한의 권한 정보를 확인할 수 있도록 개선	
49244	GS-11013	Backend	관리역할 API 에 권한 설정 기능 제공	
49244	GS-10878	Backend	엔드포인트 정보 조회 API 추가	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
49722	GS-11756	Frontend	GMODULE에서 superAdmin 권한을 가진 계정에서 페이지 이동 시 세션 갱신이 되지 않는 문제	2.0.106
49715	GS-11833	Frontend	기간 검색의 간편 검색 최근 항목 선택 시 종료 시간이 고정되는 문제	2.0.133
49405	GS-11489	Frontend	위협 분석 화면에서 다른 페이지로 이동한 뒤, 화면 내 "뒤로 가기" 버튼으로 재이동 시 화면이 제대로 표시되지 않는 문제	2.0.0
49397	GS-11749	Frontend	엔드포인트 그룹 관리에서 즉시 적용 버튼이 동작하지 않는 오류	3.0.3
49295	GS-11659	Backend	진단예외규칙 추가 시 64자 길이 제한으로 인해, 부모프로세스 경로가 일부만 저장되는 문제	2.0.144, 3.0.1
49244	GS-9849	Frontend	대시보드의 분석모드 즐겨찾기 저장 시 시간 설정과 무관하게 절대적 설정으로 저장되는 문제	2.0.100
49244	GS-8951	Frontend	Elasticsearch 필드 컨버터 중 "링크 컨버터"의 타겟이 "팝업으로"인 경우 링크가 제대로 동작하지 않는 문제	2.0.102
49244	GS-11434	Frontend	실제 요청 프로세스가 최상위 프로세스인 경우 스토리 라인에 부모 프로세스가 그려지지 않는 문제	1.5.101
49244	GS-11334	Frontend	엔드포인트 목록의 조직 필터에서 하위 조직 토글 시 동일한 하위 조직이 중복으로 추가되는 문제	2.0.136
49244	GS-11276	ML	mldetector가 메모리를 과점유하는 문제	2.0.134

Genian Insights 3.0.2 Release Notes (2025-12-04)

Last Updated: 2026-01-06

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
48821	GS-9184	Backend, Frontend	"이벤트 수집 관리" 메뉴에 내보내기/가져오기 기능 추가	
48821	GS-11206	Frontend	압축 파일 내 내부 파일 정보를 위협 분석 상세화면에 표시하도록 개선	
48821	GS-11200	Backend	에이전트 Up/Down 상태 감사로그 기록 옵션 추가	
48821	GS-11071	Backend	관리자 생성, 수정 API에서 '비밀번호 변경 강제' 활성화 여부 기능 추가	
48821	GS-10998	Backend	업그레이드 시 새 에이전트 패키지가 등록된경우, 사용하지 않는 옛날 에이전트 파일 및 데이터 자동 삭제 처리	
48821	GS-10210	Backend	이상행위 룰 내보내기 시 진단규칙, 예외설정을 포함하도록 개선	
48821	GS-10014	Backend	Endpoint 정리 주기를 정책별로 설정할 수 있도록 개선	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
49117	GS-11609	Backend	정책에서 '안티멀웨어 플러그인 삭제' 옵션을 변경 후 저장할경우 406에러 발생하는 문제	2.0.144, 3.0.1
48821	GS-11450	Backend	이메일 2단계인증 시 인증번호가 맞아도 틀렸다고 나오는 문제	2.0.145, 3.0.2
48821	GS-11449	Frontend	2단계 인증 활성화 창에서 이메일 선택 시 인증 메일이 발송되지 않는 문제	2.0.145, 3.0.2
48821	GS-11398	Backend	XBA 룰 수정시 접속프로파일에 적용되지 않는 문제	2.0.145, 3.0.2
48821	GS-11309	Frontend	관리자별 관리 단말 제한기능 사용 시 관리자에 관리 그룹이 설정되지 않는 오류	2.0.145, 3.0.2
48821	GS-11210	Frontend	Runscript 다운로드 받을 경우 원본 스크립트와 상이한 문제	2.0.114
48821	GS-11199	Frontend	XBA 탐지 시 위협 이벤트와 이벤트 상세정보의 통신 방향과 상이한 문제	2.0.11
48821	GS-11051	Backend	로그인 시도 계정 사용중지 처리 기능이 동작하지 않는 오류	2.0.140

Genian Insights 3.0.1 Release Notes (2025-11-03)

Last Updated: 2025-12-01

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
48091	GS-9235	Frontend	조직관리 목록에 회사 필드 추가	
48091	GS-11170	Frontend	이상행위 룰 진단 규칙 및 이벤트 수집 설정(수집 예외, 수집 추가, 태크 추가) 시 입력값에 대한 유효성 검증 처리	
48091	GS-10999	Frontend	안티멀웨어 예약 검사 목록의 요일 필드를 보고 요일 정보를 쉽게 알아볼 수 있도록 개선	2.0.138
48091	GS-10968	Frontend	위협 분석 화면의 "단말별 탐지 정보"에서 단말별 관련 이벤트 조회 조건 개선	
48091	GS-10883	Backend	Insights E+안티멀웨어 라이선스 -> 단독AV 라이선스로 변경할 경우 사용모드 값이 초기화되도록 개선	
48091	GS-10882	Agent	AM 진단 예외 패턴 등록 시 "전자서명" 기반 예외 등록 기능 제거	
48091	GS-10881	Backend	안티멀웨어, CTI 순서로 위협탐지된 경우에 안티멀웨어 위협정보를 유지하도록 처리	
48091	GS-10759	Frontend	로그인 없이 에이전트를 다운 받을 수 있는 페이지 개발	
48091	GS-10734	Frontend	안티랜섬, 안티멀웨어 위협에서도 SSDEEP 유사도지표 제공	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
48487	GS-11269	Backend	에이전트 배포관리에서 업데이트 현황의 완료 위 숫자 클릭 시 목록이 조회되지 않는 문제	2.0.143
48471	GS-11404	Database	"아티팩트 수집" 메뉴가 나타나지 않는 문제	2.0.143, 3.0.1 (R)
48461	GS-10983	Backend	관리자 비밀번호 업데이트 시 발생하는 응답 지연 문제 수정	2.0.143
48449	GS-11371	Backend	이상행위 커스텀 룰의 위협 유형 수정 시 적용되지 않는 문제	2.0.130
48309	GS-10849	Frontend	OTP 인증키 초기화 후에도 여전히 "OTP 인증키 초기화" 버튼이 유지되는 문제	2.0.140
48236	GS-11314	Database	안티멀웨어 리눅스 에이전트에 정책이 잘못 배포되는 문제	2.0.132
48145	GS-11271	Frontend	배포 그룹 상세 화면에 업데이트 현황 카운트가 표시되지 않는 문제	2.0.121
48091	GS-11031	Backend	Auditor 권한으로 사용자정의IOC, 이벤트 수집관리 생성, 수정, 삭제 가능한 문제	2.0.111
48091	GS-10666	Frontend	로그인 화면 문구에 HTML 태그 기능이 동작하지 않는 문제	2.0.16
48060	GS-11268	Backend	두 대 이상 클러스터 환경에서 웹 관리 콘솔을 통한 업그레이드 시 서버 목록이 사라져 업그레이드가 진행되지 않는 문제	2.0.144 (R)
48025	GS-11484	Agent	이상행위 커스텀 룰 진단규칙에서 존재하지 않는 UNC 경로를 추가 시 PC멈춤 및 에이전트 재시작 오류 수정	1.5.100

CHAPTER

FOURTEEN

SECURITY ADVISORIES

Last Updated: 2026-02-12

14.1 Security Vulnerability

Fixed Versions	Key	Components	Description	Affects Versions	CVSS Score
3.0.5 (RC)	GS-11818	Frontend	crypto-js 버전 업그레이드 (4.1.1 -> 4.2.0)		9.1
3.0.4 (R)	GS-11846	Backend, Etc	OpenSSL 버전 업그레이드 (3.0.13 -> 3.0.19)		9.8
3.0.3 (RC)	GS-11298	Backend1	Tomcat 버전 업그레이드 (9.0.108 -> 9.0.112)		7.5