Genian EDR

Release 2.0.134

GENIANS, INC.

Dec 17, 2024

GENIANS WHITE PAPER


DOWNLOAD PDF

CHAPTER

ONE

MACHINE LEARNING

[A new world is coming-A new change in malware detection using machine learning]

1.1 Introduction

In March 2016, the confrontation between Google's AlphaGo and Lee Sedol was enough to instill fear and possibility about artificial intelligence. A year and a half later, Google surprised the world again with the introduction of the new Alphago Zero. This is because they have won 100 of 100 matches against AlphaGo. What is even more surprising is the learning method of AlphaGoZero. This is because, while AlphaGo in the past repeatedly learned human notation, AlphaGoZero learned by itself based on the rules of Go. Through Reinforcement Learning without human supervision, I realized the basic knowledge of Go, such as understanding the 'axis', and reached a level that greatly exceeded my existing skills. Now, AlphaGo's scalability is drawing attention. This is because it has fully demonstrated the possibility that artificial intelligence and machine learning can be applied to various fields through general-purpose learning, not Go. What if it is applied to the field of information security? Based on this potential, many security companies are already introducing technologies and solutions that apply artificial intelligence and machine learning or are making large investments.

Machine learning is playing a big role in information security. A typical example is the use of malware detection technology to detect and block malicious codes such as APT and ransomware, as well as to prevent threats by detecting anomaly through network and user behavior monitoring.

This document introduces machine learning used by Genian Insights E (Insights) to detect malware. In addition, it aims to increase understanding of new technologies and products such as deep learning.

1.2 Understanding Machine Learning

To understand machine learning, it is first necessary to understand the relationship between artificial intelligence, machine learning, and deep learning. The figure below shows the relationship between them.

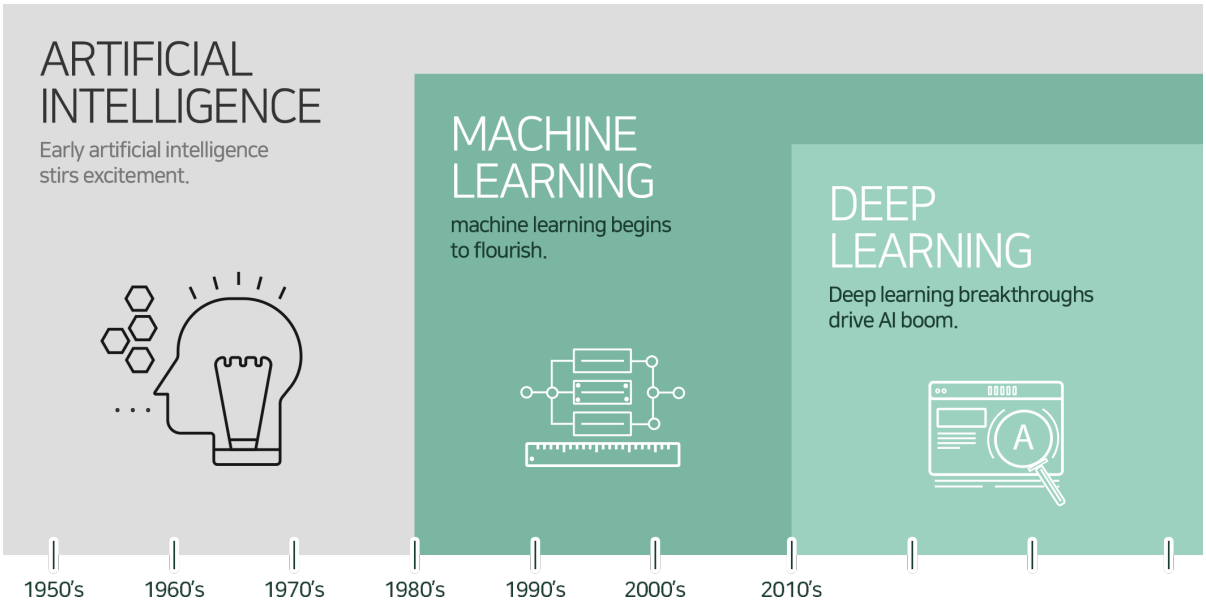


Fig. 1: [The relationship between artificial intelligence, machine learning, and deep learning – Nvidia]

1.2.1 Understanding Machine Learning

Artificial intelligence is a concept that emerged a long time ago. At the time, I dreamed of a computer with characteristics similar to human intelligence. In other words, we aimed to develop a general AI that has human thinking ability and thinks like a human. However, facing many difficulties, general AI has not been realized. The current level is a level that can handle certain tasks, such as classifying images or recognizing faces, at a level above humans. It can be said to be a category of Narrow AI.

1.2.2 Machine Learning: Narrow But Concise Artificial Intelligence

Machine learning is a concrete approach to implementing artificial intelligence. Machine learning analyzes data using algorithms, learns through analysis, and makes decisions or predictions based on what has been learned. In other words, it is a method of learning through a large amount of data and algorithms, rather than coding specific directions or guidelines.

1.2.3 Deep Learning: Deep Learning, the best machine learning to date

Deep learning is a branch of machine learning based on artificial neural networks (ANNs). Artificial neural networks also fluctuate, but achieve tremendous development by overcoming technological limitations, development of hardware such as General-Purpose computing on Graphics Processing Units (GPGPU), and mingling with Big Data. After that, it showed overwhelming performance in various machine learning competitions and stood out. Recently, research on deep learning has been actively conducted in the field of image processing and voice recognition.

1.3 Learning and application of machine learning

In the past, the learning method of artificial intelligence was a top-down approach that stores human knowledge and infers it. However, we are more often accumulating some knowledge as a learning process through various experiences and data. Machine learning is a bottom-up approach to developing algorithms and techniques that (machines can learn) improve on their own from data based on interactions with the environment as a way to implement learning capabilities through machines.

Machine learning can be divided into ① supervised learning, ② unsupervised learning, and ③ reinforcement learning according to the learning method.

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

Fig. 2: [Comparison of machine learning learning methods]

In the field of information security, research and application of machine learning is being actively carried out. Spam filtering can be said to be the most representative case where supervised learning is applied. In addition, depending on the learning method and characteristics, user behavior analysis (User Behavior Analytics), abnormal behavior detection

(Anomaly Detection), malware detection (Malware Detection), authentication (personal identification through behavior analysis), security control, forensic, etc. Research and application are ongoing in a wide range of cybersecurity fields.

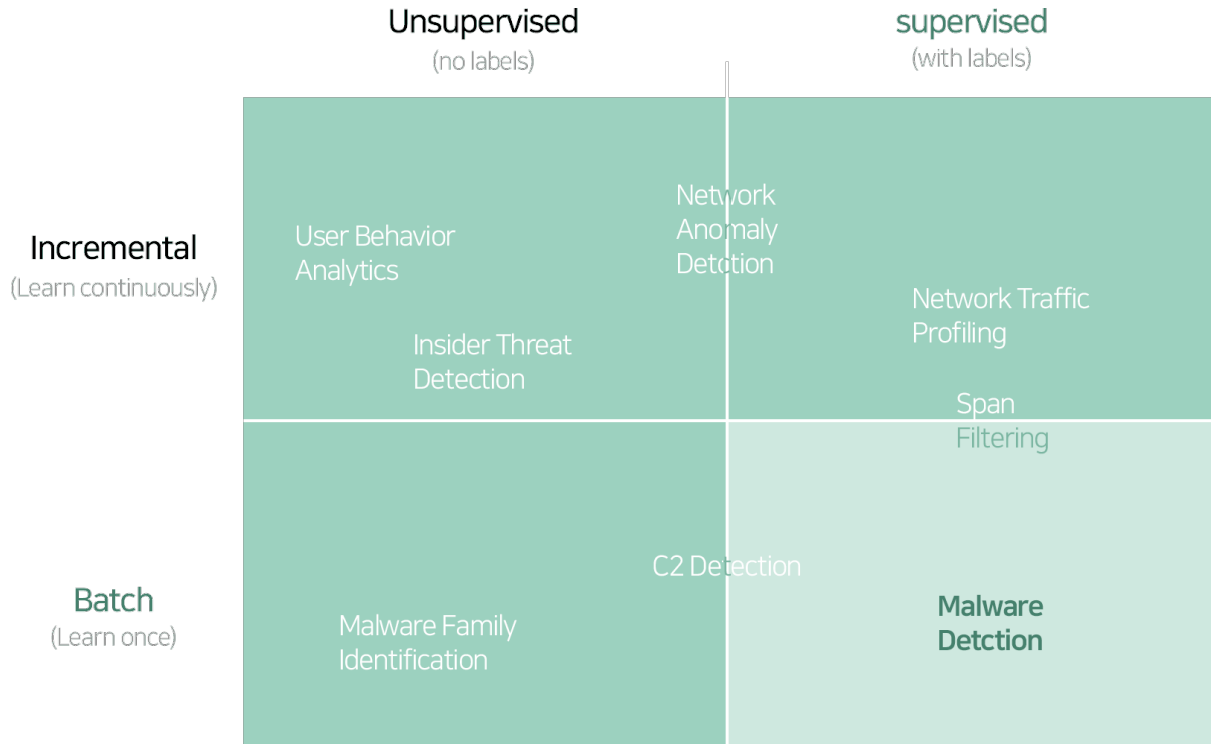


Fig. 3: [Utilization of Machine Learning in Information Security Field]

1.4 Machine Learning and the Rise of New Players

The use and development of deep learning in the field of malware detection is close to a revolution. Recently, as the number of advanced threats such as APT (Advanced Targeted Attack) and Ransomware has increased exponentially, the Threat Detection & Response capability of the Anti-Virus product line based on the signature is reaching its limit. . With these changes, the introduction of machine learning by traditional security companies such as Symantec is accelerating, and new areas of device security such as Next Generation Endpoint Security (NGES) or Next Generation Anti-Virus (NGAV). Along with that, players are getting attention.

They use machine learning to detect malware and remove threats by detecting abnormal behaviors such as system exploits. In addition, it can analyze network traffic and packets and learn the flow to detect anomaly and prevent threats. It expands the scope of response and enables precise response by analyzing the root cause of detected threats and the correlation between files, processes, and networks. It provides various visualization techniques such as chain events and attack timelines to ensure visibility into threats and timeliness of response.

It is evaluated that it greatly exceeds the functions and utility provided by existing vaccines and device security products. The market evaluation is also positive. The investment and valuation of the company proves this. Although Cylance was founded in 2012, it is valued at a whopping 1 trillion won.

How did these changes become possible in just a few years? Machine learning is at the center of change. In particular, among machine learning, deep learning (deep learning) greatly reduces the effort of programming compared to other machine learning learning methods. In the past, the biggest obstacle to using machine learning was feature engineering. This refers to a series of operations in which an analyst or data scientist extracts features from specific data and reprocesses them. Deep learning is a learning method that automatically extracts and learns these features. Therefore, if a lot of data and computing power are provided, sufficiently reliable results can be expected. In summary, it can be said that the following factors accelerated the emergence of new players along with the development of deep learning.

1.4.1 Reduce data costs

Along with the big data issue, the quantity and quality of data have greatly improved. In the past, only handwritten data (eg, MNIST) was everything, but now you can use tens of millions of high-resolution images (eg, ImageNet), YouTube, and SNS. In particular, in the case of malware such as ransomware, sharing and collaboration are becoming more important with the development of Cyber Threat Intelligence (CTI). As collaboration platforms such as analysis and evaluation of malicious codes such as VirusTotal, malwares.com, and Malc0de expand, the cost of acquiring and reprocessing very high-quality labeled data has increased. decreased, and development became possible based on this.

1.4.2 evolution of hardware

The learning process of machine learning requires enormous computational power. However, the CPU of a general-purpose computer has a limited number of physical cores and is specialized for sequential operations. In comparison, GPUs can have dozens or more cores, and processing them in parallel is very useful for multi-operation, especially for numbers or algorithms. In addition, as a language structure (eg, CuDA) that can use it efficiently was developed and the price became cheaper, deep learning was able to reduce the computing time to several tens. In the past, the 'Google Brain' project, which Google attempted to connect 1,000 general-purpose servers in parallel, can now be processed with three GPU-accelerated servers, and the hardware is developing rapidly.

1.4.3 The evolution of open platforms

Global IT companies such as Google and Microsoft and academic research groups are releasing machine learning-related platforms (frameworks and libraries, etc.) for free. These platforms dramatically lower the technical barriers to entry for users, allowing them to focus on applications and values. In particular, TensorFlow, released by Google, is most commonly used for spam filtering of image mail and image search, and is used in various fields such as malicious code detection and credit card misuse detection using it.

1.5 How does deep learning work?

Recently, deep learning has been receiving a lot of attention. A few years ago, machine learning began to attract the general public, and now, deep learning, a type of machine learning, is being talked about as representing machine learning. Companies are risking their lives to secure relevant manpower. Google acquired DeepMind, Facebook appointed Professor Yann LeCun, a master of deep learning, as the head of its AI center, and Baidu, also known as China's Google, also hired Professor Andrew Ng. It looks close to .

So, how does deep learning work?

Let's assume that we are making deep learning that can distinguish polygons and understand how it works conceptually. Which of these is the blue shape on the left?

A person can immediately recognize that the blue object on the left is a square. This is because a person has the knowledge of a concretely abstracted square. So you can immediately determine that the object on the left is a polygon and among them is a square. On the other hand, what about machines, i.e. machines? Unfortunately, it is impossible to store human knowledge and make decisions (judgments) based on it. In the end, it takes the method of recognizing each feature one by one and combining them to make a decision. As a result, the following steps are required.

These features are transferred to deep learning as input data. Deep learning refers to a neural network made up of several layers. A layer is in turn made up of several nodes. In the node, the actual operation takes place, and this operation process is designed to mimic the process that occurs in the neurons that make up the human neural network.

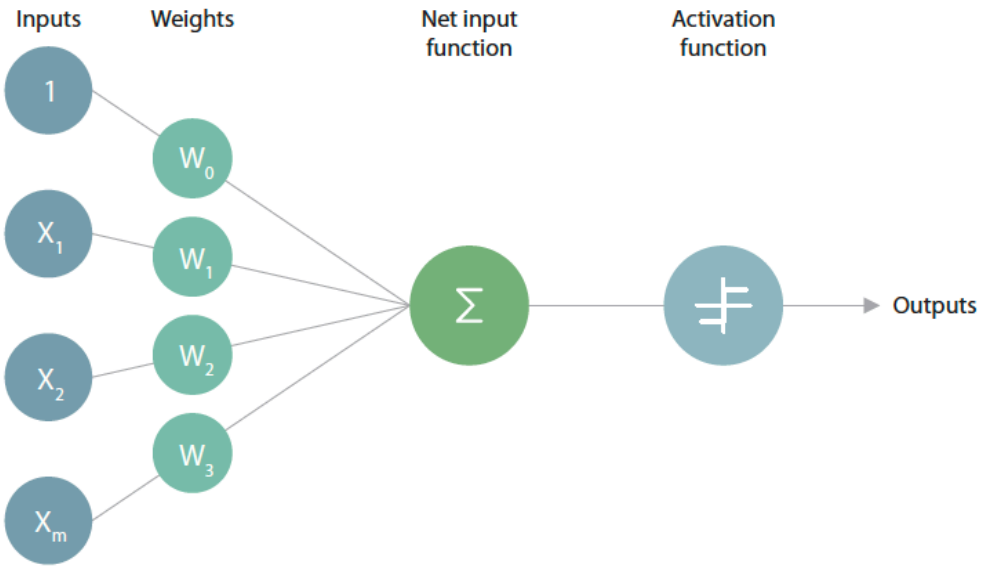


Fig. 4: [Operation of nodes – whether active is determined through input data and weights]

When a node receives a stimulus of a certain size or more, it responds, and the magnitude of the response is proportional to the product of the input value and the node's coefficients (or weights). In general, a node takes multiple inputs and has as many coefficients as there are inputs. So, by adjusting this coefficient, you can give different weights to different inputs. Finally, all the multiplied values are added and the sum is input to the Activation Function.

The features mentioned above are the input data of the first layer (Layer 1), and the output (result) of each layer after that becomes the input of the next layer (Layer 2). The more layers the more complex and abstract learning. Weights are fine-tuned during the training process and, as a result, determine which input each node considers important. Ultimately, learning can be said to be the process of optimizing and updating these coefficients so that an optimized result can be derived.

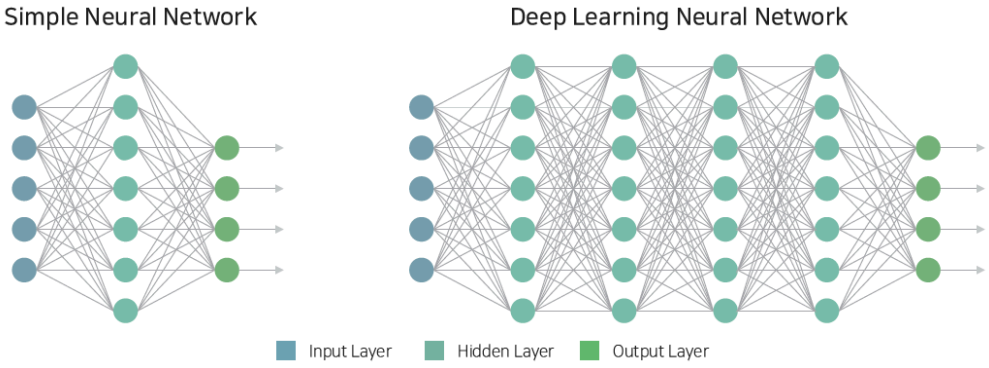


Fig. 5: [Simple Neural Network and Deep Neural Network]

After that, it is possible to determine what type of polygon it is by combining all the results. It looks like a decision tree. However, there may be two or more input variables from the previous stage to the next stage, which is a characteristic of the neural network, which is the basis of deep learning.

Deep learning is based on an artificial neural network (ANN), which is a deep neural network (DNN) having a hierarchical

structure of an input layer, an output layer, and a plurality of hidden layers. It is a branch of machine learning that is used as a primary method of learning. The actual operation of deep learning can be said to be a repetition of Linear Fitting and Nonlinear Transformation. In other words, it can be said that it is a hierarchical learning method that learns sequentially while building up a simple learning structure.

The biggest feature of deep learning is that extraction and learning of these features for an optimized decision are made together. This greatly reduces the effort of feature engineering described above. Therefore, if a large amount of labeled data is provided, a sufficiently reliable training model can be obtained.

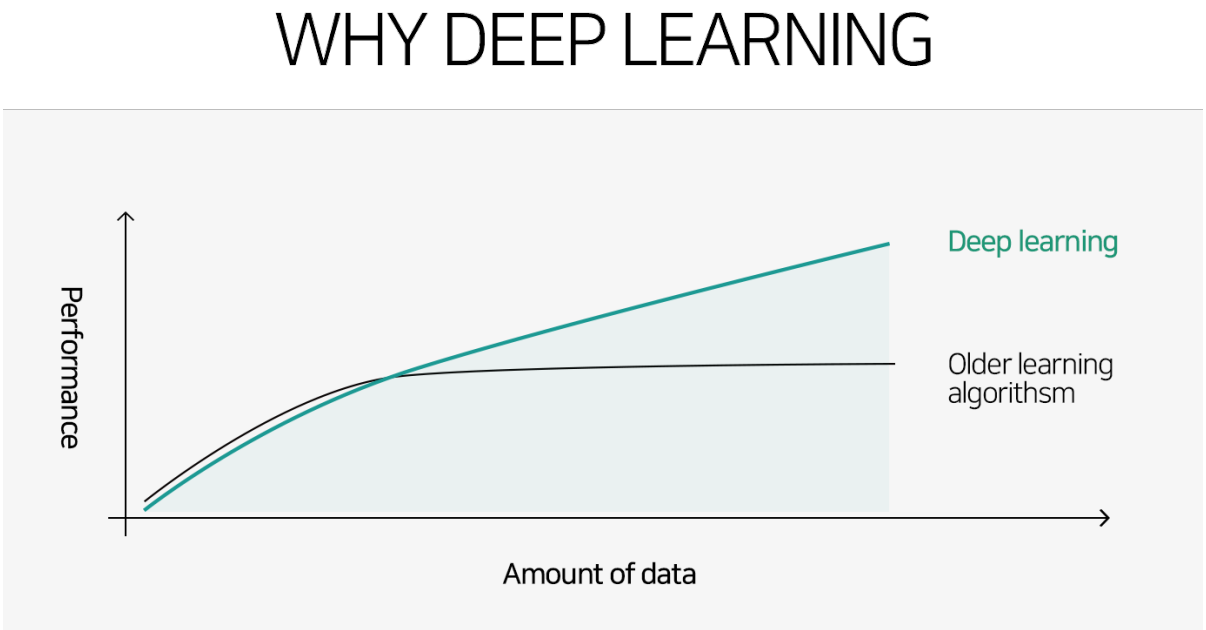


Fig. 6: [Why Deep Learning? _ Andrew Ng]

The figure above shows the relationship between the increase in data and the performance of deep learning. This can be said to be the reason why deep learning has received the most attention recently.

1.6 Machine Learning and Malware Detection

Recently, ransomware has become a big issue. Ransomware, a type of malware, is used by attackers for financial gain. According to Symantec's Internet Threats Trend Report (ISTR), the number of malicious codes generated in 2015 was about 430 million. The number of malicious codes generated in 2009 was about 2.36 million. In 2015, about 1.18 million malicious codes were generated per day. It can be said that it has increased by 30 times every year.

Variants are among the causes of the rapid increase in malicious code. Most malicious code creators create and distribute variant codes to avoid vaccines. According to German security firm G-Data, In the first quarter of this year, the number of new and variant malware detected reached 1.85 million. New malware appears every 4 seconds, and more than 60% of them are ransomware. Ransomware is spreading rapidly because anyone can easily obtain it and create variants and earn money without being tracked with the advent of virtual currency. The reasons why machine learning is receiving attention in relation to the detection of malicious codes in this environment can be summarized as follows.

1.6.1 Limitations of detection methods

The most basic detection method of Anti-Virus products is comparison with Signature. In 2016 alone, about 1 million new cases of malware were discovered every day. Hundreds of these can be applied to antivirus products. Ultimately, we come to the conclusion that it is impossible to system all malicious codes as signatures.

1.6.2 Limitations of the way it works

Frequent updates are essential to keep signatures up-to-date. Updates over the network are unfortunately not available on closed networks. This is also a big stumbling block for how the cloud works. The recent hacking incident of the Ministry of National Defense can be said to be a representative example of how great results can be caused by an attempt to solve the limitation of such a closed network in a wrong way.

1.6.3 Bypassing security software such as antivirus

An attacker can use the method to detect malicious code in reverse. You can test your own malicious code using VirusTotal or Cuckoo Sandbox, or apply technical methods to bypass it.

For this reason, machine learning is being evaluated as a practical alternative for the detection of an increasing number of malicious codes. Machine learning is a signature It is a technology that detects malicious codes based on non-features. Therefore, there is no relationship between the quantity of malicious code and the detection rate, and it is advantageous for detection of similar variants. So how can machine learning detect malware? It is easy to understand if we think of the deep learning model that recognizes the polygons mentioned earlier. In order to recognize polygons, we talked about three features called 'straight line, connectedness, and angle' and some weights accordingly. The detection of malware is similar. What is important is which feature to use to determine as malicious code and which algorithm to use for learning.

What features can distinguish the executable program from harmful (malware) and normal (normal code)? There are many features available. These include file names and hash values (not useful), header information, calling functions, registry keys, DLLs, and more. Unfortunately, however, there is no single characteristic that can accurately distinguish malware from non-malware. For example, there is a field called SizeOfInitializedData in the header of the executable program. This means the total of the area in which the variables used in the program are initialized. Analysis of the distribution of the features for a number of malicious codes and normal codes is as follows.

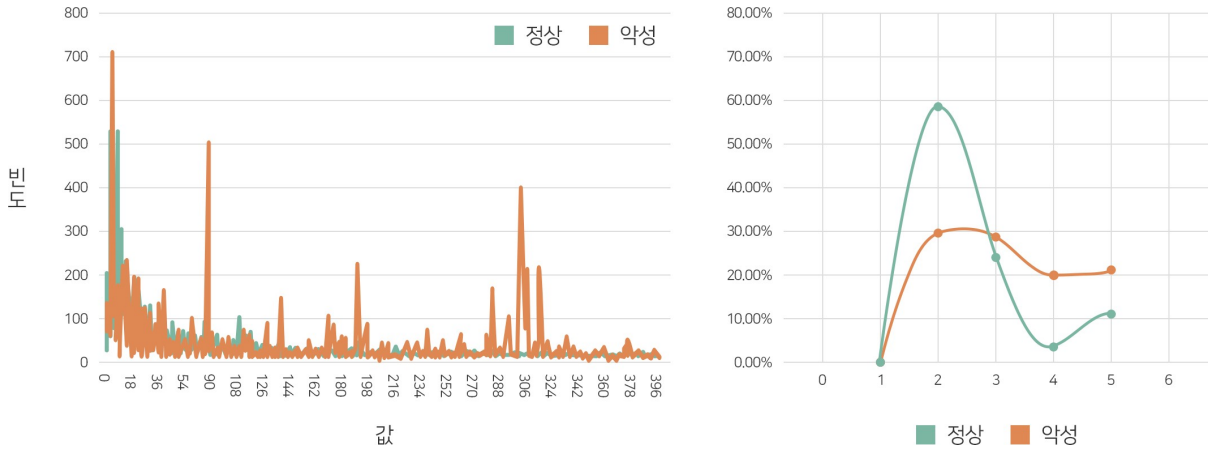


Fig. 7: [Distribution of SizeOfInitializedData value according to file size]

A phenomenon in which the distribution is reversed based on '3 sections' occurs. Unfortunately, this feature doesn't seem to be useful. These characteristics are the same and appear repeatedly in most malicious codes and normal codes.

Therefore, 'hundreds to thousands' of features and weights are combined and used for actual malware detection. That's why we need machine learning.

In the end, the detection performance depends on which algorithm and how it was trained using which features were extracted/used for malicious programs and normal programs. It is also the reason why various vendors using machine learning can appear. Currently, not only static features but also dynamic features are extracted and used, and various algorithms or ensemble methods that increase prediction performance by using various data together are being used.

1.7 Insights E and Machine Learning

Insights E (Insights E, hereafter) of Genius Co., Ltd. is an EDR (Endpoint Detection & Response) solution developed for the first time in Korea as a 'terminal-based intelligent Threats Threat Detection & Response solution'. You can detect advanced threats such as APTs and ransomware and gain visibility into attacks. Through close collaboration with NAC, it is possible to detect and respond to threats at an early stage and minimize the risk caused by threats, which is attracting attention in environments where NAC is already used.

Insights supports multi-step detection methods, including machine learning, to detect advanced threats.

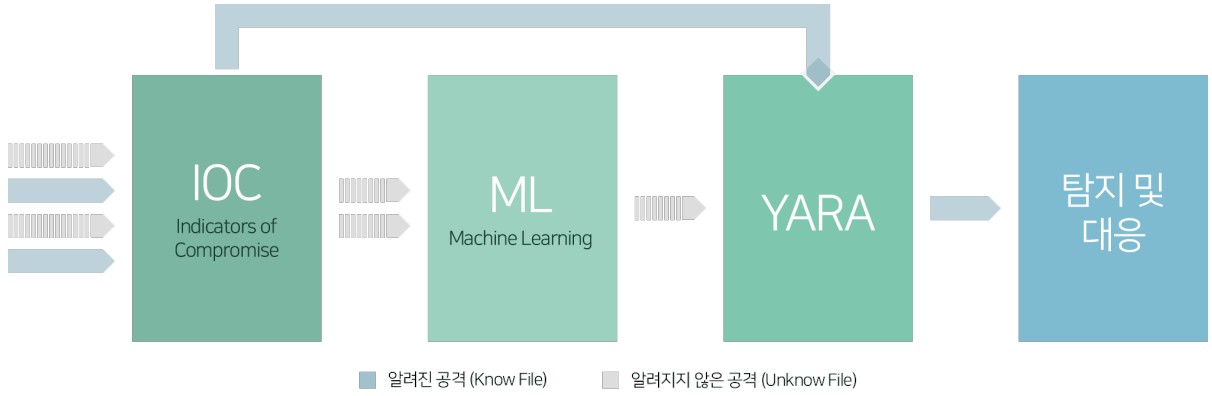


Fig. 8: [Insights' Threats Detection Stage]

1.7.1 IOC (Indicators of Compromise)

Malicious code is detected based on related information such as hash, classification, risk, and IP of known malicious code. It is similar to the signature of antivirus products, and many malicious codes are detected in advance at this stage.

1.7.2 Machine Learning (ML)

For executables that are not detected by the IOC, further exploration is done by machine learning. It takes less than a second to extract more than 1,000 features and apply a sophisticatedly trained model. The detection accuracy is more than 99%.

1.7.3 YARA (Yara)

In addition, it detects traces (String) of malicious code inside the executable file based on the rule. It can detect known or unknown pseudo-malware.

Insights uses more than 1,500 features to distinguish between malicious code and normal code, and is researching various learning methods based on deep learning. Among them, based on 4 learning models (Model A, B, C, D), the results of three tests on about 100,000 files are as follows. (The results below are internal measurement results and are derived by validating about 100,000 test sets after training with the training set.)

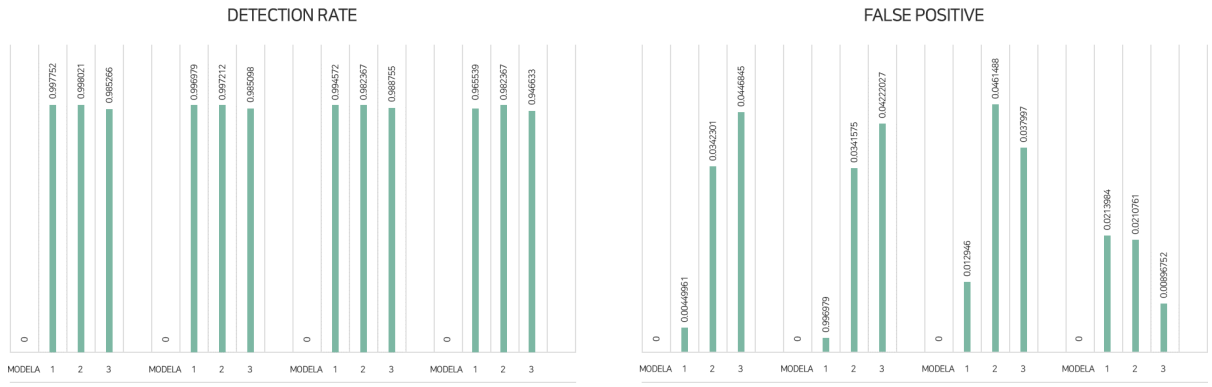
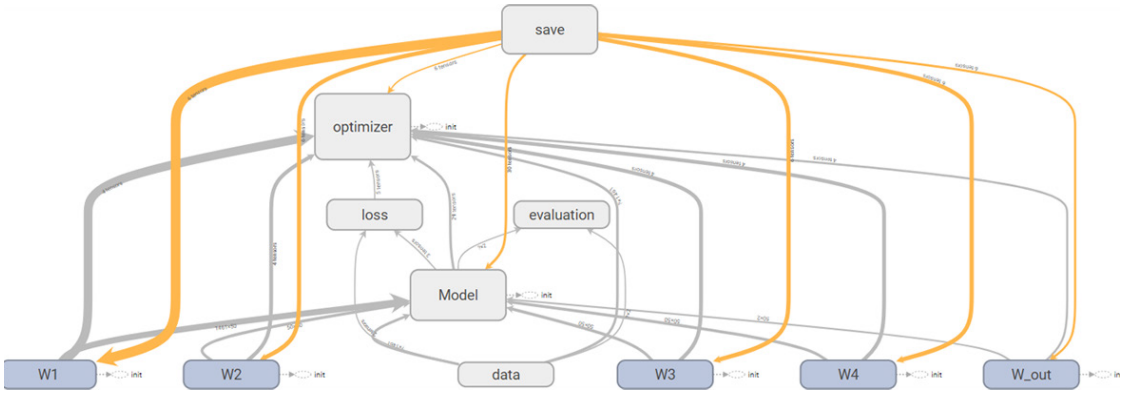


Fig. 9: [Result of detection rate (correction, false positive) measured using the test set]

In terms of malware detection rate, the average detection rate of the four models was 98.61%, and Model A, which showed the best result, was 99.36%. In the ratio of detecting normal files as malicious code (False Positive, Type I Error), the average of the four models was 2.6%, and the best Model D was confirmed to be 1.7%. In conclusion, it was confirmed that Model A is the best model in terms of detection rate of malware and Model D is the best model in terms of false positive rate for actual application.



Machine learning applied to real insights is much more complex and sophisticatedly optimized learning models are loaded. As in the previous example, different models are trained and used at the same time, or various methods are applied, such as re-learning judgment results. These efforts are expected to play an epochal role in eliminating security threats caused by actual malicious codes, leading to the advancement of detection rates and reduction of false positives.

Fig. 10: [Learning of Neural Network – An optimal model that can distinguish between malicious code and normal code is completed by repeatedly updating the input values and weights of numerous features.]

1.8 Is machine learning really all-purpose?

Many companies talk about machine learning. It seems that it is quickly taking its place as an alternative to the increase in malware, particularly the emergence of ransomware and variants. You can even see ransomware being 100% detectable and competing for detection rates. However, in the practical application of machine learning, the following limitations exist. Accurately understanding these characteristics and using them correctly is very important for machine learning applications.

1.8.1 Interpretation of detection results

When a malicious code is detected by machine learning, the result is expressed as a probability (%). That is, the detection result is the same as 'The file called foo.exe is judged to be malicious with a 90% probability'. Specifically, it is not possible to confirm (interpret) whether it was judged as malicious code for any reason. Additional models such as decision tree and linear regression can be used for this interpretation, but this is also close to estimation.

1.8.2 False Positive

More important than the 'high detection rate' is the 'low false positive rate'. In particular, the system of errors (False Positive, Type I Error) that judges normal files as malicious files is very important. A 5% false positive rate seems low in numbers. However, that equates to being able to delete 50 (5%) files when 1,000 files are scanned. Such errors can cause serious damage in practical applications.

1.8.3 Relationship between detection result and response

What action would you take if the file 'abc.dll' was detected as malicious code with a 55% probability? Should I just leave it alone? Or should I delete it? If the system does not boot normally or an application fails after deletion, who is responsible? No matter how excellent machine learning is, it is difficult to link the results to an immediate response. It can be said to be a challenge to a solution consisting of only a single machine learning.

1.8.4 Update

Machine learning also needs an update. The cycle can range from months to years. Threat Detection & Response can be difficult when completely different types of malware appear. Additional learning is required to keep up with the changes in the malware. Therefore, an Eco System that can continuously collect, analyze, and update new malicious codes is required.

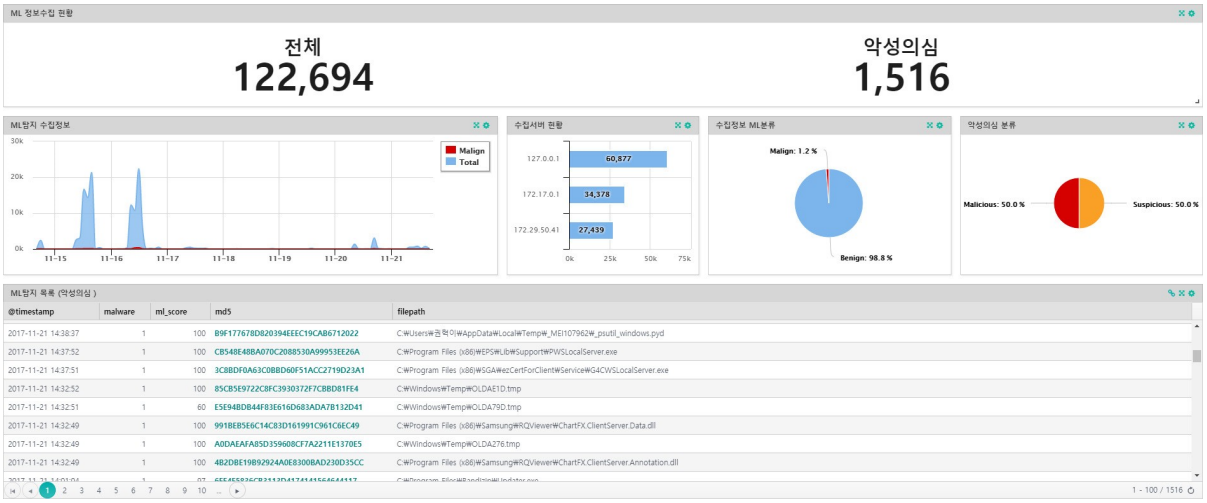


Fig. 11: [Requires a continuous system for detection rate and false positive rate]

1.9 Conclusion

Deep Learning has been studied for a long time. Although there have been ups and downs for a long time, the algorithm has been improved repeatedly as continuous research continues, and it is being evaluated as a machine learning method with the best performance in conjunction with the development of hardware and big data. It is rising with hope.

In particular, the advancement of deep learning in the field of malware detection is phenomenal. However, from the point of view of actual usage, it seems that the dichotomous evaluation of 'fantasy' or 'disappointment' still dominates. Why? This is because there was no accurate understanding and application of the new technology. I think it's because they evaluated the technology simply with distorted and fragmentary metrics such as high detection rates.

A new world is coming. The world has become a world where traditional powerhouses have collapsed in an instant, and new technologies and start-ups can present a new paradigm. Now, an environment where the system and the user are converge and there is no distinction between the network and the endpoints is coming. Information security is also being disrupted by new technologies such as machine learning. But no need to worry. After all, only technology and change for people will survive and expand.

CHAPTER

TWO

ANOMALY DETECTION ENGINE XBA

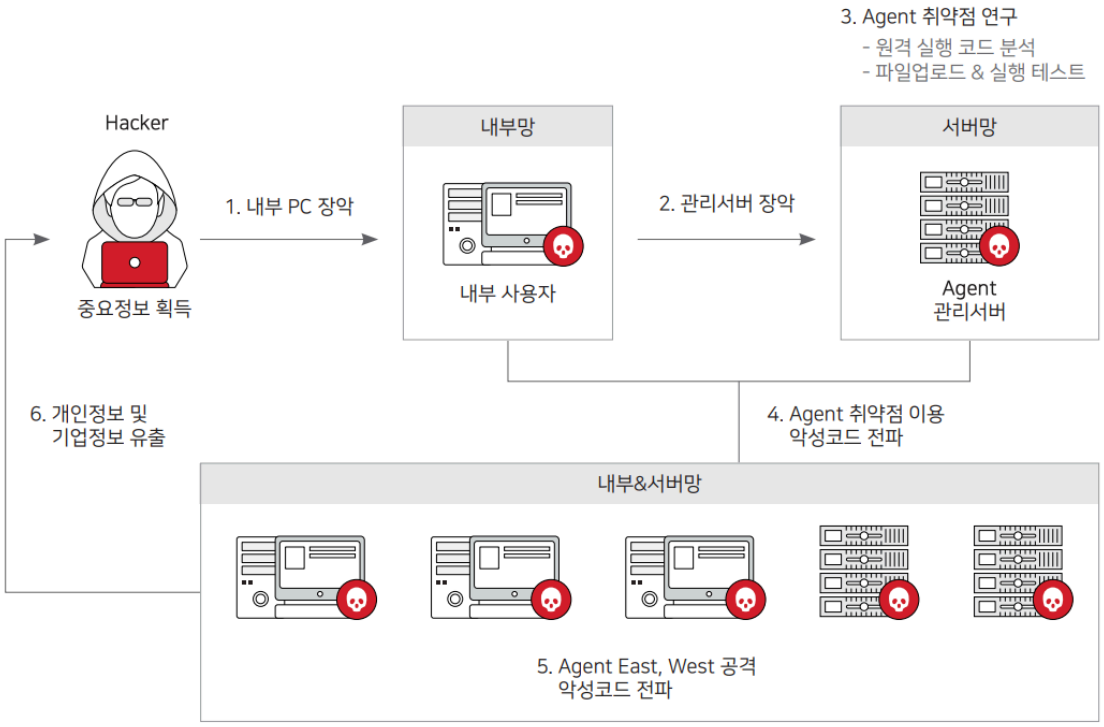
2.1 Introduction

Until now, the main response to cyber threats has been prevention. We were able to analyze Threats after damage or danger occurred, and created a solution or a process to defend against it. When internal resources (PC, etc.) are connected to external networks, new threats have arisen, and We developed a firewall for this purpose. Anti-Virus was developed when malicious code caused danger to the System.

However, these countermeasures are only effective for certain Threats. Complex, such as Advanced Persistent Threats Detection and response are impossible when threats occur. Antivirus can only respond to file-based known malware. It is not possible to respond to new or variant malicious codes. Also, malware that works without files (Fileless Malware) is also difficult to detect. A firewall can investigate and control traffic from the outside to the inside or from the inside to the outside, but it cannot respond to an attack that has already entered the inside.

According to SK infosec's '2019 Security Threats Prospect Report', the target of security threats in 2019 has been expanded, and various attacks have been combined. It is expected to develop in the form Ransomware attacks are combined with other types of malware to form an APT attack. It is expected to transform, and as IoT devices diversify, malware attacks are also expected to expand.

To counter these attacks, we need to analyze every point of threat and find a way to respond, but unfortunately, we cannot predict all the points of threat that may arise in advance, and attackers are constantly creating new types of attack methods.



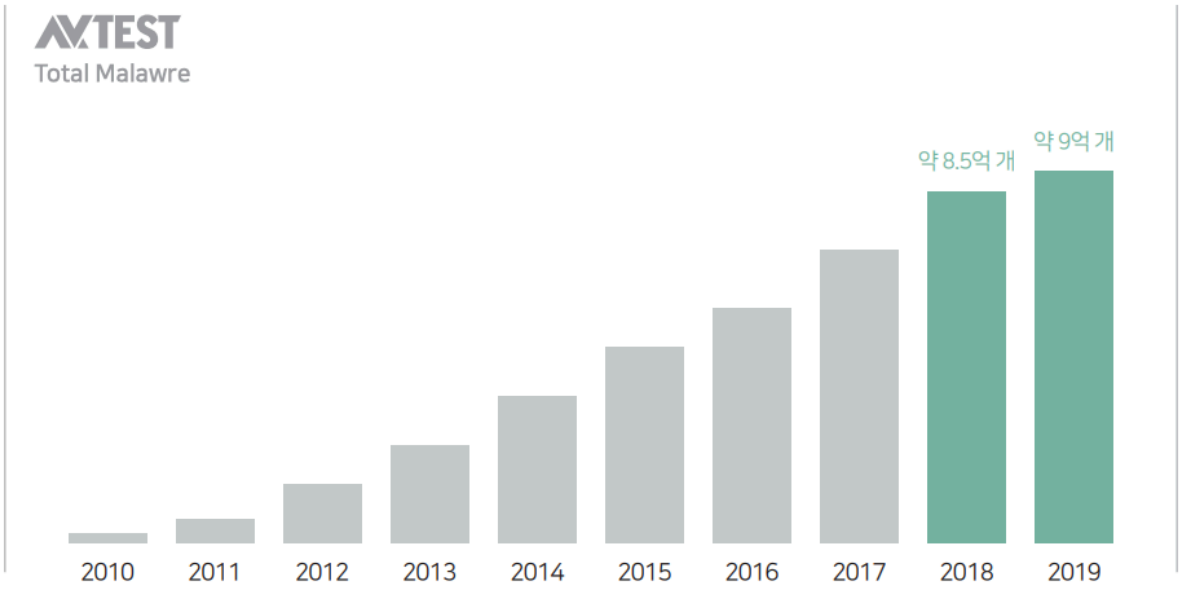
[그림1. 에이전트 취약점 기반 이스트-웨스트 공격, EQST 2019 보고서]

2.2 Rise of Malware and Threats

With the explosion of malware, security users and security companies are facing serious problems. That is, despite processing thousands to tens of thousands of malicious codes every hour, more and more new types of malware are being created. It is no longer possible to respond to all malicious codes with just a series of tasks that collect, analyze, and include malicious codes in the engine. According to AV-test.org, which is testing antivirus products, in 2018 alone, 350,000 pieces of malware were collected every day.

Another problem is that the spread of malware is shrinking. According to a report by security company Symantec, 75% of the malware used in APT attacks was found on computers under the age of 50. If the spread of the malicious code is small, it is difficult to collect the malicious code. It can be interpreted as meaning that it is difficult to be reflected in the antivirus engine.

These characteristics are also appearing in ransomware. In the past, attackers preferred the method of distributing ransomware to unspecified masses. However, in recent years, the number of targeted ransomware targeting specific companies rather than the unspecified majority is increasing rapidly. World's largest aluminum in early 2019 A typical example is a ransomware attack targeting my investment, Norsk Hydro. Businesses need to recover critical information and maintain productivity. Attack patterns are changing in this way because they often execute huge recovery costs or have to pay ransom money, and attackers have a high success rate and high profit.



[그림 2. 악성코드 수집 추이]

Copyright(c) AV-TEST GmbH, www.av-test.org

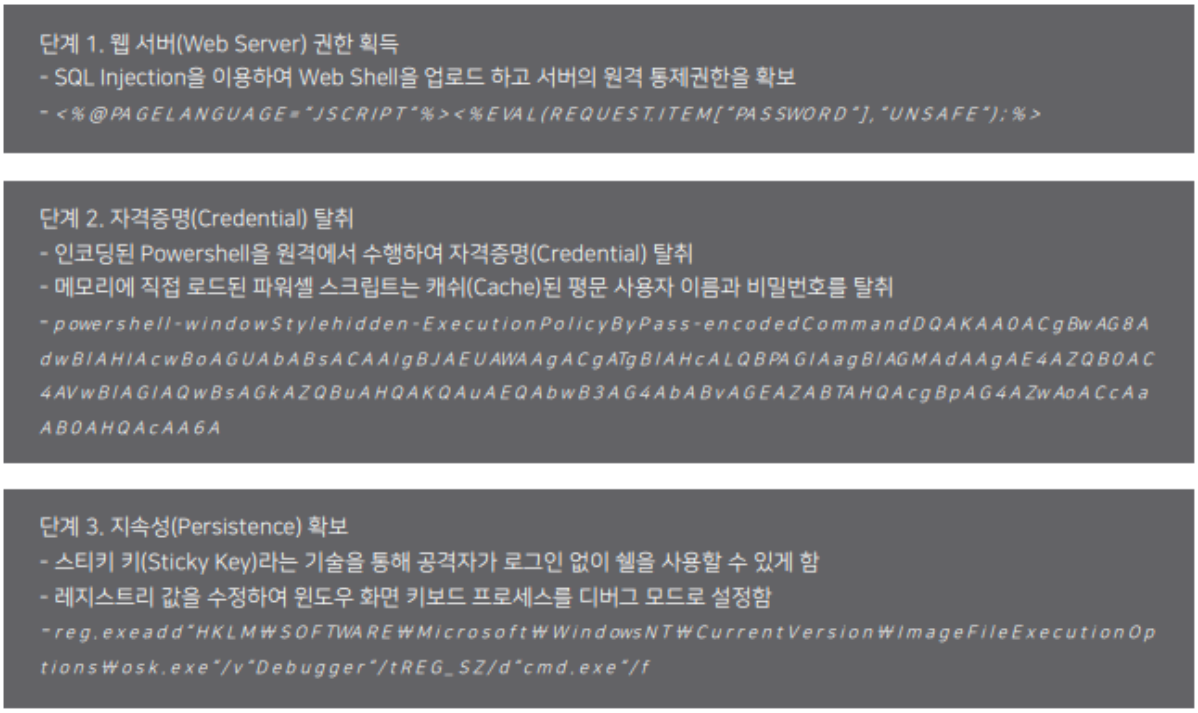
2.3 Increase in Threats Without Malware (Fileless, Non-Malware)

In addition to malware, there are new threats to watch out for. This is a fileless attack. This is where normal malware is downloaded (stored) and executed to perform malicious actions, whereas it is directly loaded (loaded) into memory to perform malicious actions. Therefore, the stored files A typical anti-virus that detects it is very difficult to find the attack. Whitelist based security solutions can also be bypassed. This is because you are using an application that has already been approved. Attacks using browser vulnerabilities or using Microsoft Word macros or PowerShell utilities are typical. In 2018, CrowdStrike reported that 8 out of 10 successful attacks were due to fileless attacks, and examples of actual fileless attacks are introduced as follows.

These fileless attacks are increasing and becoming more sophisticated. Carbon Black found that 52% of breaches in 2017 were caused by fileless attacks. “Fileless malware attacks are becoming much more common,” said Aviva Litan of Gartner Security Analysis. It bypasses Endpoints protection and detection tools.” These fileless attacks are also closely related to Lateral Movement, which will be described later.

2.4 Increase in Threats Without Malware (Fileless, Non-Malware)

For this reason, many experts are saying that the battlefield should move from the network to the endpoint. by malicious code In addition to responding to threats, it is also necessary to respond to threats without malicious code by collecting and analyzing all behaviors of the device. Analyze the collected information to find the inherent threats (Threat Hunting) or trace the behavior to check the timeline of anomalies or track the source (Root Cause Analysis) should also be possible. It is a concept similar to monitoring everything with CCTV in physical security and checking back to the time when an issue occurs. In order to detect abnormal behavior, all behavior information that occurs in the terminal must first be collected. Abnormal behavior can be detected only when normal (normal) behavior can be confirmed. The information collected varies widely. From information about credentials (authentication, etc.) to files, folders, and applications, as well as USB, network It is necessary to collect all object information such as communication, action information, and even information



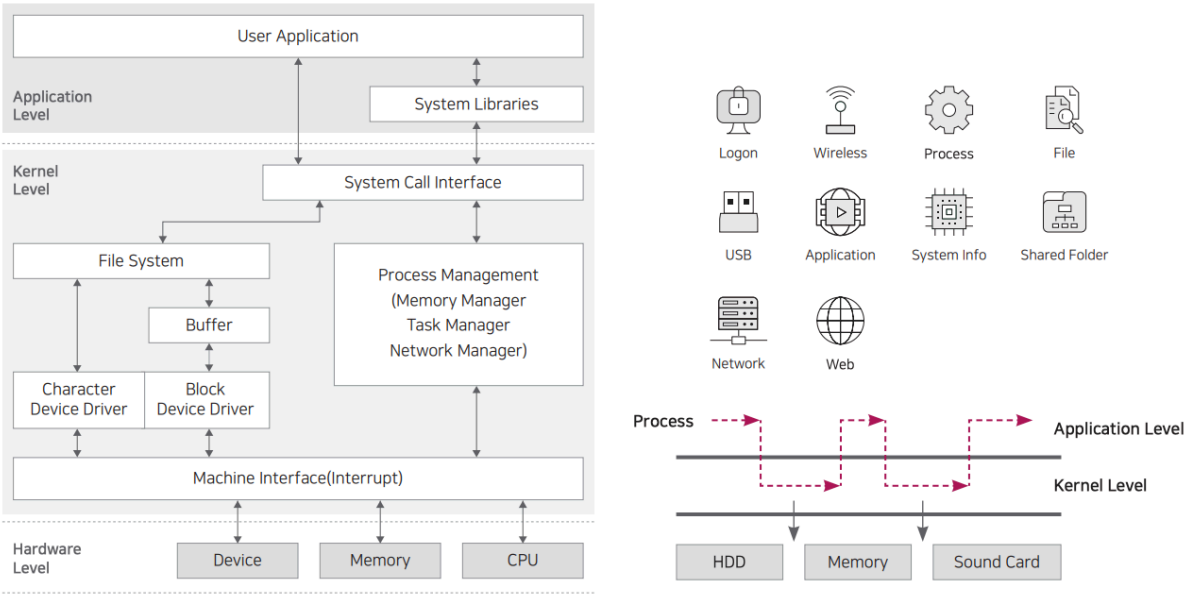
about dependencies. There are two ways to monitor the behavior of these devices. The first is a method of monitoring user level behavior, and the second is a method of monitoring at the kernel level. When a file or process is executed, it repeatedly enters and exits the user level and kernel level until it is terminated. Therefore, it is necessary to monitor both the user level and the kernel level including the system call to obtain complete information.

Also, in the case of rootkits, there are cases where they have a function to hide themselves at the user level, so if the kernel level cannot be monitored, it is impossible to detect them. Monitoring the behavior of Endpoints at the user level and the kernel level is essential to secure overall visibility of the entire terminal behavior. I need it. Monitoring at the user level is a useful method for products for general functions such as software for systems, but there are limitations in security software because it is a structure that cannot provide full visibility. However, monitoring at the kernel level is There are concerns about conflicts with other products and their impact on the performance of your PC. Therefore, there is a need for a structure that can effectively collect all behavioral events that occur in Endpoints while minimizing the possibility of conflict with other security solutions.

2.5 Terminal abnormal behavior detection, X Behavior Analysis (XBA)

XBA is a behavior-based threat detection engine applied to Genian Insights E (EDR). XBA detects anomalies and responds to malware-free threats Portfolio to respond. XBA can be used to detect the following typical abnormal behaviors.

- After reading the infected document file, something is downloaded and executed by the document tool
- The act of downloading a file or executing a downloaded file without the user's knowledge in the background through security vulnerabilities such as JavaScript and Flash by accessing a hacked web page (Drive by Download)
- Illegal access to external networks and file transfers using PowerShell
- Searching for shared folders through network scan and copying specific files and actions



[그림 3. 사용자레벨과 커널레벨의 관계]

The figure below shows a typical example of a fileless attack using PowerShell. PowerShell is a command interpreter featuring a CLI shell and scripting language developed by Microsoft. It is a script language that makes the system of application programs easy. is installed with . The outline of the process of file leakage using PowerShell is as follows.

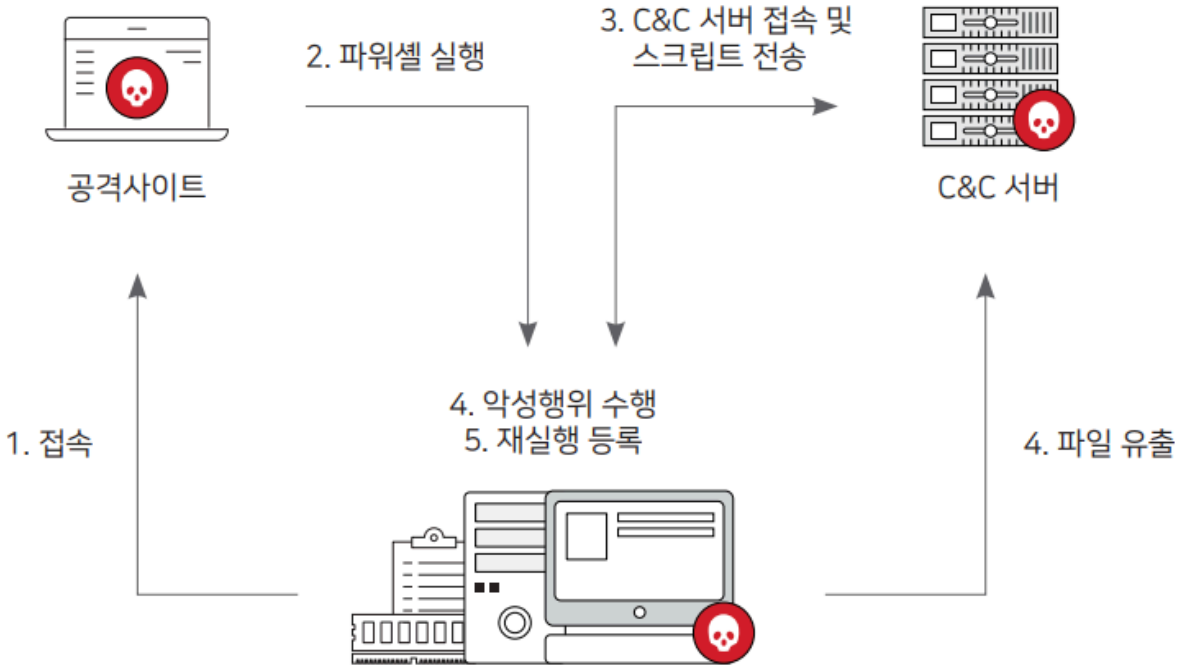
Explanation

1. A user visits a specific site using a web browser
2. Run PowerShell on the terminal by exploiting the vulnerability of the user's web browser, etc.
3. Connects to the attacker's control and command (C&C) server, mounts (loads) a malicious PowerShell script, and executes it

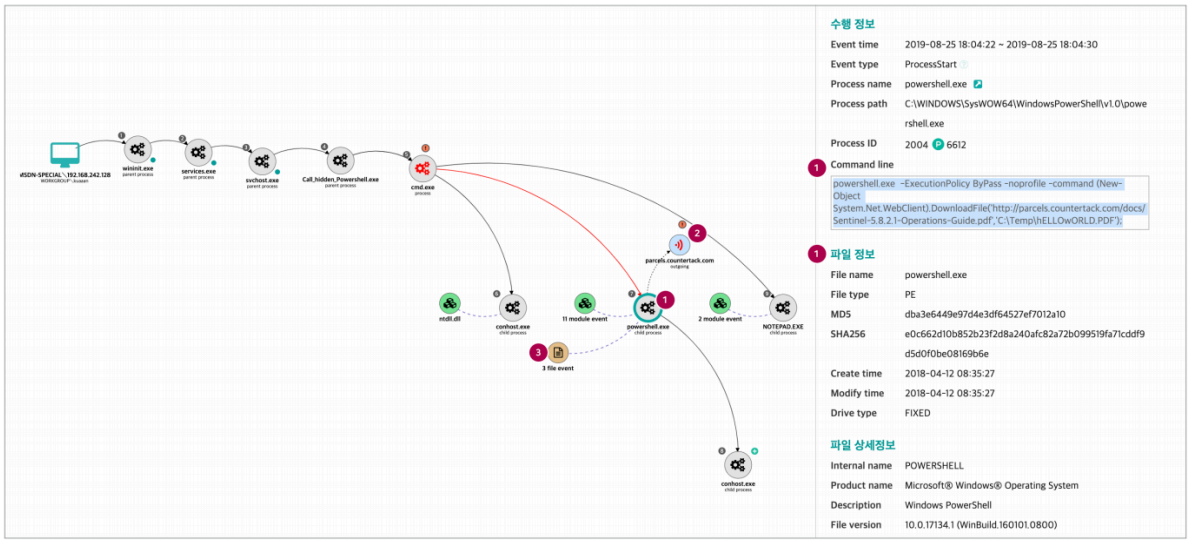
   (At this time, the script is transmitted in an encrypted state, making it difficult to detect by traffic analysis, and methods such as reflective DLL injection, memory exploits, and WMI persistence are performed simultaneously)
4. The script finds specific information in the terminal and sends it to the attacker's server
5. If re-execution is necessary, register information in related startup programs, registry, etc.

PowerShell is mainly used as a downloader or dropper for malware delivery. Also, the issue of execute permission is causing powershell You often run PowerShell inside another file rather than running alone. JavaScript (JavaScript, JS) and office files (doc, pptx) etc.), and in addition to that, Windows script files (Windows Script File, WSF) or shortcuts can be used. In the end, information leakage occurred, but the problem is that no trace of file-based malicious code can be found anywhere on the terminal. [Figure 5] shows how XBA's anomaly detection technology can be utilized in such a situation. PowerShell is not malware, it is a normal Windows file. However, while monitoring the behavior of PowerShell, ① When PowerShell is executed as a file or script, ② Connecting to the network When a related action occurs, such as accessing or attempting to access a document, ③ accessing a document file, or ④ sending a document to the outside through the network, it is detected as an abnormal behavior. In addition, XBA provides additional information for users' quick judgment, analysis, and response, and visualizes it. This provides an overall view.

In addition to PowerShell, XBA can detect typical abnormal behaviors occurring in the terminal as shown below. Number of each item under 9 large items ~ It has dozens of individual detection rules and can provide more accurate anomaly detection results through time series analysis and correlation analysis between each event.



[그림 4. 일반적인 파일리스(Fileless) 공격 흐름]



[그림 5. 파일리스(Fileless) 악성코드 탐지 예]

detection behavior	Representative Description
Policy / Permission Bypass	Arbitrary manipulation of system setting files and accounts, etc.
Suspicious process behavior	Execution of processes via unhealthy files, process names or paths, etc.
Misuse of system commands	Abnormal use of system commands for management purposes such as PowerShell, WMI, etc.
Known Threat Detection	Actions such as files, processes, registries, values, and connections known to be used for specific attacks such as backdoors, etc.
Stealing or Misuse of Privileges	Obtaining illegal rights by bypassing User Account Control (UAC), etc.
self-deletion	Change or deletion of abnormal behavior subjects (files, processes, etc.) and logs, etc.
Auto Rerun	Registering abnormal values in the Windows startup folder or registry, etc.
Lateral Movement	Attempts to spread infection to other systems through port scanning, etc.
Suspicious Office Behavior	Execution of macros, scripts, etc. by office applications such as Word

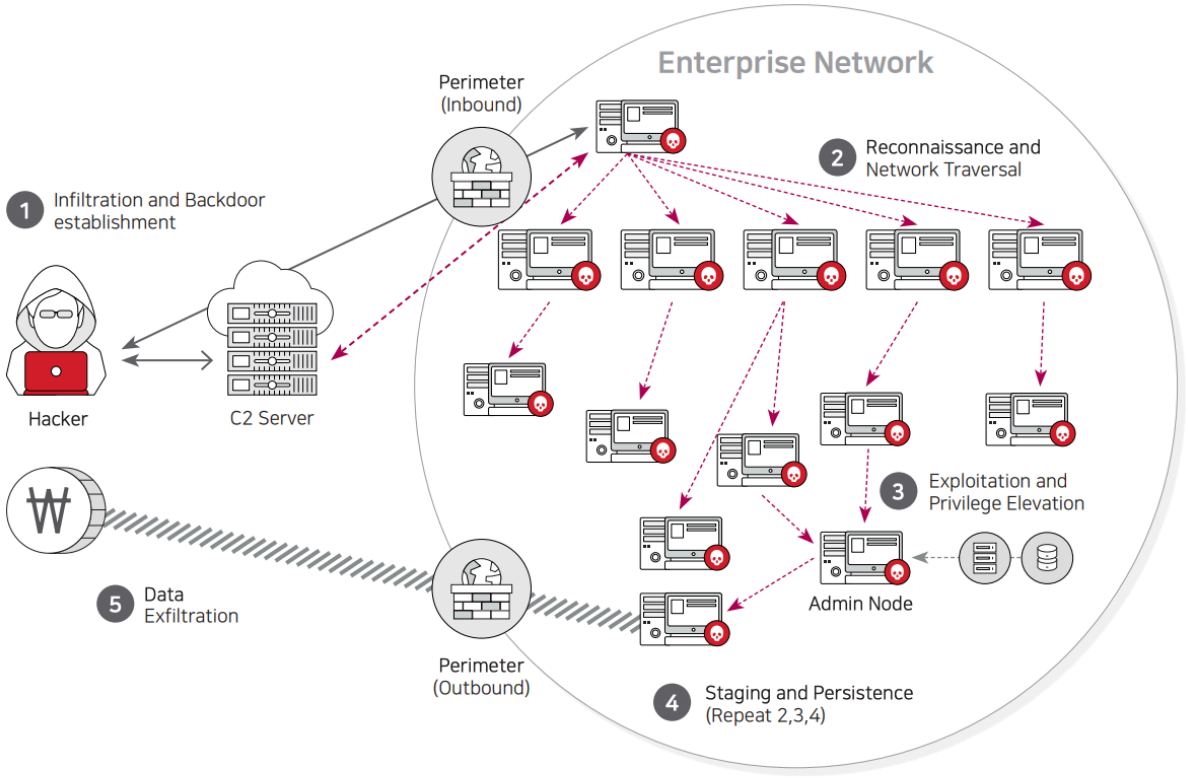
2.6 XBA and Lateral Movement

XBA can be used to detect lateral diffusion behavior. Lateral spread refers to the phenomenon in which an attacker spreads damage by crossing (moving) the internal system. The attacker succeeds in hacking the first internal terminal. Afterwards, it targets adjacent systems until the goal such as information leakage or system infection is achieved. (1) scan (reconnaissance) (2) attack (3) take control (4) hold (backdoor, command channel, etc.) repeatedly performing a series of actions, which causes damage to spread rapidly.

According to security firm SMOKESCREEN, attackers spend 80% of their attack time on lateral spread. In particular, in the case of an APT attack for the purpose of information leakage, it searches for a terminal (Users terminal, etc.) that has access to the information (specific DB, etc.) It can be said that a large amount of lateral diffusion attempts for a long time in order to compromise is an essential step. Therefore, early detection and response of lateral spread is very important in preventing the spread and damage of threats.

The attacker steals account information (dump) for lateral spread and performs tasks such as remote access and remote execution. At this time, Mimikatz or Tools such as PsExec, PowerShell, RDP are used. However, in recent lateral diffusion, programs included in the operating system are used as they are. cases are increasing. Dubbed Living Off the Land Binaries (LOLBINS), these methods will allow you to bypass traditional antivirus or whitelist based security products. Such lateral diffusion is very difficult to detect and analyze because there is not enough information such as logs. First, secure trust (authorization) This is because the attack is done in one state and logs etc are intentionally deleted by some attackers. Therefore, it is essential to record the actions of the terminal and to collect and store detailed action logs.

XBA can detect these lateral diffusion attempts by analyzing the behavior of the terminal. From attempting to escalate privileges by bypassing UAC (User Account Control), to generating a large number of SMB (Server Message Block) packets, to WMI (Windows Management) requesting remote command execution Instrumentation) It detects the case of detection of related network packets or the execution of WMI-related commands of a specific pattern that can be used for lateral spread, such as Wmic.exe, and detects signs of lateral spread at an early stage through correlation analysis. can.



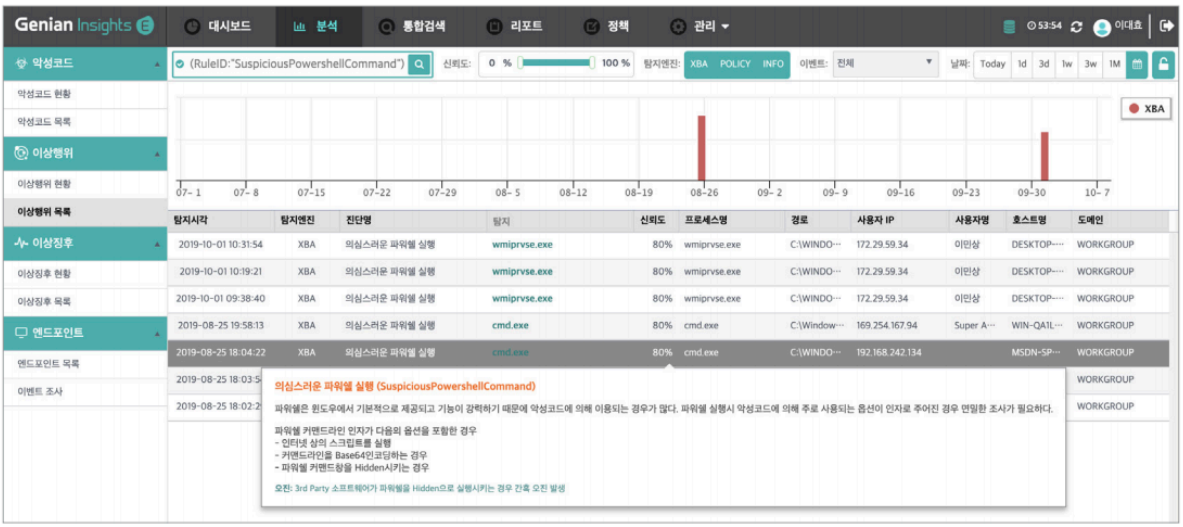
[그림 6, 대표적인 횡적확산의 사례]

2.7 Security Users' Concerns About Anomaly Detection

Perhaps a concern with anomaly detection technology is the occurrence of too many detection alarms (over-detection). In particular, security solutions targeting devices and malicious codes have many similarities in their operation methods. Therefore, if an abnormal behavior is detected by simply considering the operation method of the malicious code, over-detection is bound to be an expected tragedy. There is not.

Genians understands the domestic terminal environment well. XBA is designed to minimize the impact of overexploitation caused by terminal security security solutions. System functions such as exception handling for in-house dedicated software are included. In addition, detailed information about detected anomalies is provided. do. Many anomaly detection solutions do not provide a cause or reason for a detected outcome. Many solutions inform that they have detected an abnormal behavior, but do not tell us why this behavior is an abnormal behavior or where there is a possibility of misdiagnosis, so users can quickly judge the situation and respond There were many times when it was difficult. XBA provides a detailed explanation of why the detected anomaly was judged as an anomaly.

Anomaly detection is an essential function for users that can detect many threats to the internal network that existing security solutions cannot provide. On the other hand, if it is used incorrectly, the side effect of increasing only the work of security users may occur. Understanding the domestic IT environment and optimized detection function It is essential to provide a function that minimizes the burden on users by enabling quick setting of exceptions while providing In addition, proper operation is possible only if the function is provided so that users can determine information about abnormal behavior as quickly as possible and control the situation.



[그림 7. XBA 탐지 엔진 설명 화면]

2.8 Conclusion

The scope and target of Endpoints System is increasing due to changes in the IT environment and the occurrence of various security issues. At the same time, the system and work load are increasing due to the introduction of multiple individual security solutions. Nevertheless, malware continues to increase, and numerous companies are using advanced persistent threats (APTs), ransomware, and CoinMy You are exposed to threats like you. Even worse, many companies are unaware that they have been attacked. Network security solutions such as traditional firewalls and anti-virus are no longer sufficient. We are unable to respond to current security threats. It's time for Battlefield to turn into Endpoints. It is necessary to comprehensively recognize and respond to various threats as well as malware threats. By monitoring behavior information in real time Just as physical security monitors, detects, and defends CCTV, in information security, real-time behavioral information must be monitored and stored to secure visibility of the entire system, and to detect and respond to abnormal behavior.

CHAPTER

THREE

UNDERSTANDING GENIAN INSIGHTS E

3.1 What is EDR

According to Gartner, Endpoint Detection & Response (EDR) solutions are
Records and stores endpoint-level behavior, detects suspicious System behavior, provides contextual information, blocks malicious activity, and provides improvement suggestions to restore affected systems
It is defined as **solutions using various data analysis technologies**.

3.2 The problems EDR solves

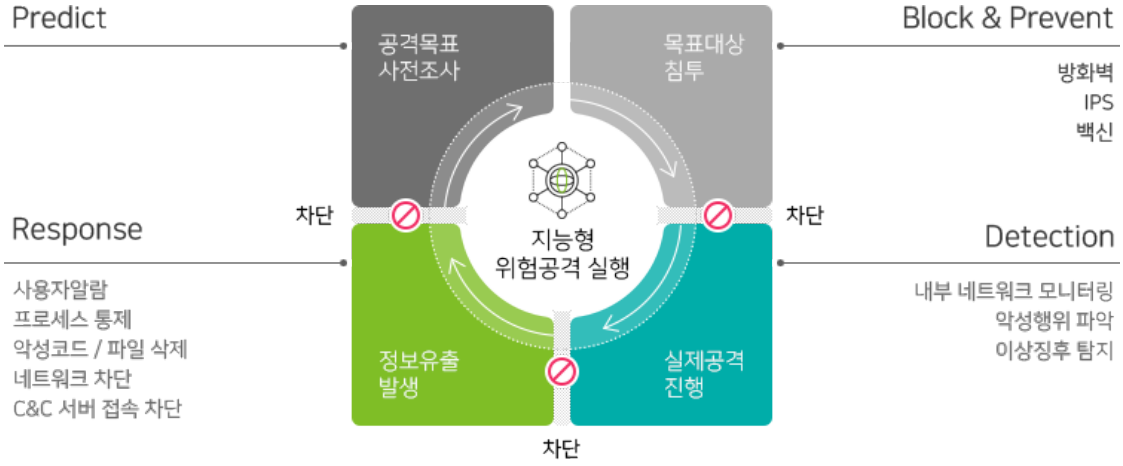
In Korea, the time when security users became aware of an incident caused by an advanced threat attack (APT) was from 2 to 8 months, after most of the internal information had already been leaked.
The reality is that it is very difficult to detect and respond to security threats, such as APT and ransomware, which are becoming more intelligent with only the traditional security solutions introduced.

Gartner announced one of its strategic technologies is an Adaptive Security Architecture that can be quickly adapted to a changing environment.

In order to system and control risks, it would be ideal to cover the entire cycle from
Predict-Prevention-Detect-Response suggested by the adaptive security architecture.
It's hard to expect all the features from just a single solution.

The EDR solution can satisfy the detection and response areas of the adaptive security architecture.

Genian Insights E can work with Genian NAC to efficiently respond to threats.



Prevention

Authentication/identification of terminals and users is carried out through Genian NAC, and the status of required S/W installation and security patch application is continuously monitored to isolate unpatched terminals from the network.

Investigation / Analysis(Detection)

By installing an agent and log interlocking with Genian NAC, the main actions occurring in the terminal are monitored, stored in real time, and then analyzed.

It detects threats step by step using IOC (Infringement Indicator), machine learning, and YARA, and provides the highest level of reconnaissance (malicious file + normal file detection).

It detects various types of malicious behaviors including file less through XBA (behavioral engine). Simultaneously with the detection of threats, it is possible to know exactly who the target of action is, 'user, department, ID', etc.

You can check the details of the detected threats through external intelligence (CTI) inquiry.

Proliferation/Recurrence Prevention (Response)

When a threat is detected in the terminal, the terminal and the network respond simultaneously in consideration of the 'severity, spread, and risk' of the threat.

Based on Policy (Policy), it acts immediately without user intervention, enabling initial response such as prevention of spread.

By interworking with Genian NAC, you can control network access of Threats devices, isolate Threats files, collect Threats files, and terminate processes.

3.3 Features of Genian Insights E

Genian Insights E (Genian Insights E) is a terminal-based intelligent Threats Threat Detection & Response (EDR: Endpoint Detection & Response) that can quickly detect, respond, and analyze various types of malicious codes and abnormal behaviors occurring in the terminal. Response) solution.

Rapid Threat Detection & Response is possible through the latest indicators of compromise (IOC: Indicators of Compromise) in the execution stage of security attacks such as APT and ransomware, which cannot be fundamentally defended by identifying malicious behaviors on internal networks and devices and detecting abnormal signs do.

Utilization of the latest IOC suitable for the domestic environment

- Response to the latest threats and incidents with periodic IOC updates
- Provides information on the level of risk, reliability and type of detected threats
- IOC DB System considering the domestic environment (minimize false positives and false positives)
- Addition of Custom Malware Hashes/IP, Good Hash/IP and System function

Various detection modules provided

- IOC (Indicator Of Compromise) violation indicator
- ML (Machine Learning) Machine Learning: Response to unknown similar variants
- **UEBA (User & Entity Behavior Analytics) User Behavior Analysis**
  - YARA Rule

Ecosystem linkage

- Share false positives and latest Threat Analysis results (reputation service) through the Ecosystem
- Process and redistribute collected Threats and Exceptional data

Analysis information visualization

- Provides 16 types of flexible widgets that enable data visualization in addition to basic information required by security users (Users can be added)
- System/infected terminal/risk-abnormal terminal/process/access information/newly created file monitoring possible
- Various Dashboard Settings such as System status / NAC sensor status / Genian product status are available (Import and Export supported)
- Threats list and Analysis screen provided

Light Agent

- Agent information collection design to minimize terminal load (using about 25MB resources)
- Data analysis is performed on Genian Insights E server

Easy to apply and expand

- Install NAC plug-in based extension module
- Design that can be quickly applied throughout the company when additional function modules are introduced

CHAPTER

FOUR

BUILD GENIAN INSIGHTS E

Genian Insights E requires various components to work. This chapter describes the role of each component and where to install it.

4.1 Understanding the components

Genian Insights E requires various components to work. This chapter describes the role and installation of each component.

4.1.1 policy server

The Policy Server is a central management system that stores all data and settings for Genian Insights E. Typically, the Policy Server is installed in an organization's datacenter.

Another role of the Policy Server is to provide an administrative console for administrators. Other components can be configured and managed through a web-based management console. You can view the collected information and establish your organization's security policy.

If you have a Genian NAC server, you can easily deploy the agent by adding a plugin.

It also acts as an agent management server, but since the Genian NAC server collects detailed asset information (IP, H/W, S/W, OS, Patch, etc.) of the endpoint, it is linked with Genian Insights E.

Continuous internal monitoring is possible.

For Genian Insights E exclusive version You can download the agent file from the policy server and distribute it through the distribution server, or you can install the agent by running the executable file directly.

4.1.2 agent

Agents are software installed on your PC. Collects all events that occur on the PC and sends them to the Policy Server.

Agents provide their own security features such as termination protection and deletion protection.

Table 1: Supported Operating Systems

Windows OS
Windows 7 (32/64bit)
Windows 10 (32/64bit)

CHAPTER

FIVE

INSTALL GENIAN INSIGHTS E

This chapter guides you through installing Genian Insights E on your System and users accessing the web console and CLI console.

5.1 Install the Policy Server

5.1.1 Choose the type of installation

The policy server physically operates the policy, IOC database, and log server on one or more systems.

Policy Server only A system can act alone as a Policy Server. However, in a large network environment, the Policy Server and Log Server can be separated for performance and stability. Separate server configuration requires separate guidance.

5.1.2 Hardware Preparation

You can install the Policy Server on a physical machine.

Hardware Specifications You can use a low-end general server for testing, but the hardware specifications commonly used are as follows.

Minimum Hardware Requirements

Table 1: Insights Policy Server

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 initial configuration

Genian Insights E provides two installation modes via CLI, and explains how to install using the Interactive Wizard.

Installation using the Interactive Wizard

1. On the CLI Initial Configuration Tool screen, enter 1 for installation type.

```
Genian Insights Initial Configuration Tool

1. Interactive Wizard
2. Manual Configuration

Select installation type :
```

2. Enter 1 for server type.

```
1. Single Server -Stand Alone

Select Server Type:
```

3. Enter 2 for System Language.

```
1. English
2. Korean

Select System Language :
```

4. Create a CLI login account.

```
Enter Console Username :
```

5. Create a CLI login password.

```
# Password must contain at least one alphabet, number, and special character
Enter Console Password :
```

6. Enter the password created in step 5 once more.

```
Try Again:
```

7. Select System timezone settings.

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

[Timezone] Select Continental :
```

8. Select System timezone settings.

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

9. If an NTP server exists, enter the server Domain information.

```
Enter NTP server:
```

10. Enter the IP information to be used as the server IP.

```
Enter IP Address:
```

11. Set the Netmask of the server IP.

```
Enter Netmask:
```

12. Set the server's Gateway.

```
Enter Default Gateway:
```

13. Enter the DNS server IP information.

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

14. When input is complete, confirm the information you entered and enter y. The database server password change process is additionally performed.

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

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

15. Genian Insights+E module requires additional settings to configure and detect IOC DB. If you are not using the E module, skip 15 and proceed to 17. When setting the ioc-updater enable command, it communicates with an external server to update more than 100 million IOC DBs. Since data update takes a lot of time over several days, you must INSERT the initial data through manual commands and then set ioc-updater enable. Please request separately for the initial DB INSERT method using the manual command.

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

16. After checking the settings through the show config command, reboot the device.

17. Connect to "https://policy server IP:8443/mc" in the web browser.

5.2 Install IOC Database

IOC DB is designed to download and insert data from an external IOC DB server during update settings.

However, in the initial configuration, it takes a lot of time to insert data, so the time can be reduced by downloading and inserting the compressed IOC DB.

5.2.1 Initialize IOC DB

1. After accessing the CLI, execute the update script as shown below. In this case, for the last date of the command, input the last date of the previous month. (For external server files, data files are created once a month on the last day of each month.) Typically, enter the last day of the previous month based on the date Insights was first installed.

Example) If this month is June 2021, the command is 20210531 , if it is May, enter 20210430 — initiocdb.sh all 20210531

2. After data update, execute the ioc-updater enable command in CLI Mode. The latest data was updated up to May 31, 2021 through the script performed in 1, and the latest data from June 1 to today's date is If you execute the ioc-updater enable command, updates are performed sequentially.

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

5.3 System console

Genian Insights E offers two types of System consoles. There is a command line interface (CLI) console that provides System Settings such as basic services and network configuration, and a web console that provides all other System and Policy Settings.

5.3.1 Web Console

The web console can be accessed by entering the server IP.

1. Open **web browser** and go to the following link.
2. Copy the link below and enter it into the address bar in your browser.
3. Replace **Policy Server IP Address** with your actual IP address.

```
https://"Policy Server IP Address":8443/mc/ (eg https://192.168.50.10:8443/mc/)
```

5.3.2 CLI Console

The CLI (Command Line Interface) console can be accessed via SSH.

```
# ssh "Policy Server IP address"
```

Genian Insights E does not allow SSH access to the System by default until Users add an accessible IP address.

To allow access, refer to "Allow remote access via SSH" in /system/default-settings-appliance.

5.4 Agent installation

Agent collects all events that occur on an endpoint and takes control upon threat detection. The agent can download the installation package from the Genian Insights E server and install it on Windows OS.

5.4.1 Install Windows Agent

Genian Insights E **Standalone Version Agent** Describes the installed version by default. You can check the NAC+IE (plug-in) agent installation in Genian NAC Integration.

Download and install the agent

After uploading the agent package in **System > System > Agent Package Management**, download the installation file (.exe) according to the Windows version (x64, x84). You can install the agent on Windows 7 or Windows 10 through the downloaded agent executable file (.exe).

After installation, you can check the terminal where the agent is installed in **Analysis > Management**.

Agent Package Management

1. When uploading a package (.gpf) file, it provides the ability to system the agent package, such as version information and upload time.
2. Uploaded packages can be used by selecting the distribution version in Agent Update.

Update Agent

The Agent Self Update Settings in System > Settings > System must be set to 'ON'.

Agent Update

Insights E provides the continuous distribution system function through its own distribution system after the initial installation of the agent through PMS, etc. You can set the distribution system in **System > System > Agent Update**.

1. Select the group to deploy the agent to.
2. **Tasks > {Select | All} Instantly deploy through the Instantly perform agent update** button.
3. Distributed deployment is possible via automatic update or distributed update in **Deployment Settings**.
4. Agent version, automatic update time, and distributed update settings are available in Deployment Settings.

Verify Windows Agent installation

1. When agent distribution is completed, ✓ is displayed on the status of the completed terminal.
2. You can check the installation and update logs of the deployed Agent through the audit log.

5.4.2 delete agent

Delete Agent provides a delete function in the Genian Insights E Web System console.

Request to delete the agent

1. In **Analysis > Management**, select the terminal you want to delete.
2. After selecting a device, click the **Tasks > Agent Tasks > Delete Agent** button.
3. After checking account Possword Policies for self-authentication in the web system console, a delete command is sent to the agent of the terminal.

Confirm agent deletion

You can check the agent deletion request information in the Endpoints Details > **Log** tab that requested deletion.

Changes on agent deletion

1. **Analysis > Overview** > Change the number of 'UP' and 'DOWN' terminals in **Entpoint Status**
2. **Analysis > Management** Create a delete icon in the deleted terminal status in the list

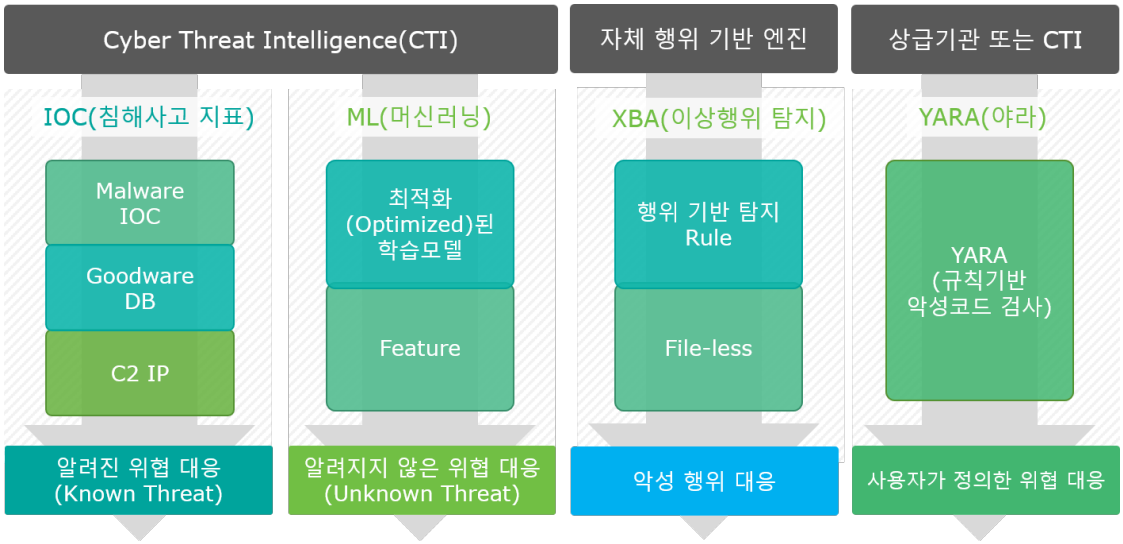
CHAPTER

SIX

THREAT DETECTION TECHNOLOGY

Genian Insights E detects and responds to Threats using various detection modules according to **Threats type**.

File-based Threats are largely classified into **Malware**, and malicious code can be subdivided into **Known Threats** and **Unknown Threats**.
File-less-based Threats are classified as **Anomaly** and are detected by the behavior-based anomaly detection engine.



This chapter describes various Threats detection techniques.

6.1 Malware detection

IOC (Indicator of Compromise) collects traces of infringement incidents that occur and are recorded around the world and systems this information into a separate DB,
The Insights Policy server periodically communicates with the external IOC DB server to update the latest threat information.
In a closed network environment, you can directly update the IOC DB on a monthly basis in the policy server.

When an event for a file or process occurs in Endpoints, the Threat Detector engine of the Policy Server checks whether the hash value of the file is registered in the IOC DB.

If file information is registered, the file is classified as **Known Threats**, and you can check the reliability, risk, and malware type information registered in the IOC.

If the file information is not registered in the IOC DB, check the machine learning information.

6.1.1 How to handle data not registered in IOC

Genian Insights E enables Threat Detection & Response to known threats using IOC (Indicators of Compromise) Database. The IOC Database is updated regularly, but provides the **Custom IOC Management** function, which allows users to register and detect unknown malicious programs or malicious IPs. The malicious program can be detected by registering the MD5 Hash value.

Through Genian Insights E Settings, you can check the MD5 HASH value for the program from the information collected during agent installation.

How to check MD5 Hash value

1. Go to **Discovery > Endpoint** menu, the process information collected by the agent is displayed, and double-click the list of files to register.
2. Among the selectable field items, you can check MD5 Hash information.

You can check how to register a hash value with the verified information by moving to the corresponding list below.

Malware Hash

1. Go to **Policy > Custom IOC Management > Malware Hashes** menu, and click the Add button at the top.
2. Enter the hash value as required and click the Save button after entering other necessary information.

Item	Description
Response-Detection Only	When Malware Hashes is detected, only relevant information tags are displayed in the Analysis tab corresponding column of the Users page, and no special action is performed on the user's PC.
Response-Detection and Response	When Malware Hashes is detected, related information, tags, and Actions (Users custom tag) set in Genian NAC are performed in the Analysis tab corresponding column of the Users page. Response settings follow the Threat Detector plugin settings.
Response-Prevention	If the agent has data registered as Malware Hashes and a file with the same hash is executed, it is immediately blocked and a blocking notification message is displayed on the user PC.

Fix Malware Hashes

1. Go to **Policy > Custom IOC Management > Malware Hashes** and click the value of the hash list to modify.
2. You can edit any information except hash value.
3. If you click the external link button on the hash edit page, you can inquire information about the hash value from the pre-registered search site.

Delete Malware Hashes

1. Go to **Policy > Custom IOC Management > Malware Hashes** menu and select the checkbox of the hash list to delete. Click the button when it becomes active.
2. A confirmation pop-up window appears, click the OK button.

Malicious IP

Add Malicious IP

1. Go to **Policy > Custom IOC Management > Malicious IP** menu and click the Add button at the top.
2. Separation allows you to select single, subnet, or address range. Enter the IP as required and click the Save button after entering other necessary information.

Item	Description
Response-detection Only	When Malicious IP is detected, only relevant information is displayed in the corresponding column of the Analysis tab of the Users page, and no special action is performed on the user's PC.
Response-Detection and Response	When Malicious IP is detected, related information, tags, and Actions (Users custom tag) are executed in the corresponding column of the Analysis tab of the Users page. Response settings follow the Threat Detector plugin settings.

Malicious IP fix

1. Go to **Policy > Custom IOC Management > Malicious IP** menu and click the IP list to be modified.
2. You can edit any information except IP.

Delete Malicious IP

1. Go to **Policy > Custom IOC Management > Malicious IP** menu and select the checkbox of the IP list to be deleted. Click the button when it becomes active.
2. A confirmation pop-up window appears, click the OK button.

Goodware Hash

If it is registered and detected in IOC (Indicator of Compromise), but it is judged to be a normal file, but a false positive occurs because the IOC Database is not updated. Users can directly register related information to handle exceptions.

Add Goodware Hashes

1. Go to **Policy > Custom IOC Management > Goodware Hashes** menu and click the Add button at the top.
2. Enter the hash(MD5) value as required and click the Save button after entering other necessary information.

Fix Goodware Hashes

1. Go to **Policy > Custom IOC Management > Goodware Hashes** menu and click the MD5 hash list to edit.
2. Information except hash(MD5) value can be modified.
3. If you click the external link button on the Goodware Hashes edit page, you can inquire information about the corresponding MD5 hash value from the pre-registered search site.

Delete Goodware Hashes

1. Go to **Policy > Custom IOC Management > Goodware Hashes** menu and select the checkbox of the MD5 hash list to delete. Click the button when it becomes active.
2. A confirmation pop-up window appears, click the OK button.

Good IP

Add Good IPs

1. Go to **Policy > Custom IOC Management > Good IPs** menu and click the 'Add' button at the top.
2. In Classification, you can set Single, Subnet, and Address Range. Single button click. Enter the IP as required and click the Save button after entering other necessary information.
3. Also, in case of Network Event, you can add Good IPs by clicking the custom 'Register as Good IPs' button in Analysis > Management > Attack Storyline**.

Fix Good IPs

1. Go to **Policy > Custom IOC Management > Good IPs** menu and click the IP list to be modified.
2. You can edit any information except IP.

Delete Good IPs

1. Go to **Policy > Custom IOC Management > Good IPs** menu and select the checkbox of the IP list to be deleted. Click the button when it becomes active.
2. A confirmation pop-up window appears, click the OK button.

6.2 machine learning detection

If the type of file among the information collected by Endpoints is an executable file (PE), the feature of the file is extracted.
This feature information is used for malware detection by machine learning.

If the file is viewed, it is classified as **Known Threats**, and if there is no information, it is classified as **Unknown Threats**.

Known Threats and Unknown Threats are alarms, process kills, and file deletions on the agent according to the policy (action method) set in advance by the user.

If it is not detected even by machine learning, it performs the procedure of once again checking whether the file is registered in an external intelligence (CTI: Cyber Threat Intelligence Service) such as Reversing Labs or VirusTotal.

6.3 Abnormal behavior detection

File-less-based threats are classified as **abnormal behavior** and are detected by the anomaly detection (XBA:X Behavior Analysis) engine.
The behavior-based anomaly detection engine has a predefined anomaly policy, and when anomaly is detected in Endpoints, Threat Detection & Response is possible immediately.
MITER ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge - a knowledge base that provides tactics, techniques, and procedures from an attacker's perspective as a framework) provides attack technique detection and related information.

6.3.1 How to set the anomaly detection policy

All Endpoints apply Default registered in XBA Rule Sets. If it is necessary to apply a separate anomaly rule to a specific endpoint, you can add a ruleset and set it to apply the separately created ruleset to the group policy to which the endpoints belong.

Abnormal behavior detection Settings

Default

Item	Description
Category	Insights E Rule and MITER ATT&CK Rule are supported.
Name	Predefined diagnostic name.
OS	It is an OS that can diagnose abnormal behavior, and currently only Windows is supported.
Enable	Use of anomaly diagnosis rule is an option. (Default: on)
Event Type	When diagnosing abnormal behavior, the diagnosis policy is different depending on the event type (file, module, network, process, registry).
Reliability	Internally defined reliability.
Threats Type	Threats types are divided into 8 categories: Anomaly, Autorun, Exploit, Fake, LateralMovement, Ransomware, Rootkit, UacBypass.
MITER ATT&CK Technique	Miter ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge - a knowledge base that provides a framework for tactics, techniques, and procedures from an attacker's perspective) If there is MITER ATT&CK Technique information, click it to go to the relevant information site.
Auto Response Rules	Sets the method (notification, forced process termination, no response) to automatically respond when abnormal behavior is detected by the abnormal behavior rule.
Exception Rules	abnormal behavior rule is set to diagnose by default, but you can set the exception rule not to use the abnormal behavior rule. In **Policy > XBA Rule Management > Exception Rules**, you can create an exception rule and select a rule to reflect exception handling, or set the exception handling rule directly on the Abnormal Behavior Rule System Details screen.
Description	Enter Users memo for the anomalous rule.

Add ruleset

If there are rules to be applied or excluded only for specific Endpoints other than Default, you can add rulesets to which exceptions are applied.

1. Click the Add button, select the ruleset to be copied, and click the Create button.
2. After modifying the ruleset to be applied differently, click Save and the 'Apply Policy Immediately' button at the top.
3. On the detailed screen of the created policy in the **Policy > Group Policy Management > Group Policies** menu, select the XBA Rule Sets created in step 1, and then save and apply the policy immediately.

Response when abnormal behavior is detected

When detection by anomaly policy, false positives and frequent alarms may occur, so the basic response is to be recognized only by users in the Web Console. When a notification is required on the terminal (PC) or the process of abnormal behavior needs to be terminated, you can respond to threats through the automatic response settings.

1. Click the name of the anomalous behavior rule you want to set the response settings to, and select 'automatic response' in the detailed settings.
2. When selecting automatic response, you must click the Save button in the upper left for the changes to be reflected, and after saving is complete, click the 'Apply Policy Immediately' button in the upper right to deliver the policy to the agent.
3. If an abnormal behavior set in the automatic response settings is detected, you can check the automatic response policy item in the summary information of the corresponding threat in the **Analysis > Management** menu.

Abnormal behavior detection exception Settings

Anomaly engine detects anomaly rules predefined in the Web Console.

To reduce false positives, you can set the exception policy before detection or handle exceptions through Management after false positives.

Exception Rules before detection

Create Exception Rules

1. Go to **Policy > XBA Rule Management > Exception Rules** menu and click the 'Add' button at the top.
2. After setting the rule name, operation mode and exception rule, click the 'Save' button.

-	Item	Description
Exception application Type	All	Apply the Diagnostic Exception Policy to all Endpoints.
Exception application Type	Setting The Target Not applied	Set the target not to apply exception handling.
Exception application Type	Setting The Target applied	Set the target to apply exception handling.

The target of policy application can be set by entering IP or department information. After setting the policy exception handling target, enter the rest of the detailed information and click the Save button. 3. You can check the exception settings registered by the user in the list, and click the 'Apply Policy Immediately' button next to the top right menu 4. The policy application pop-up window will be displayed, and if you click the 'OK' button, it will be applied to Endpoints immediately.

Modify Exception Rules

1. Go to **Policy > XBA Rule Management > Abnormal Behavior Rule System > Exception Rules** menu and click the name of the rule to be modified.
2. After modifying the rules, click the `Save` button.
3. Click the `Apply Now` button next to the top right menu.
4. The policy application pop-up window will be displayed, and if you click the 'OK' button, it will be applied to Endpoints immediately.

Delete Exception Rules

1. Go to **Policy > XBA Rule Management > Abnormal Behavior Rule System > Exception Rules** menu and select the checkbox of the list to be deleted. Click the 'Delete' button when it becomes active.

Exception Rules Excel Export

1. Go to **Policy > XBA Rule Management > Abnormal Behavior Rule System > Diagnostic Exception Settings**, click the Save button in the upper left corner, and click the Export menu.
2. If no list is selected in step 1, the entire currently registered list is exported, and only the selected item can be exported when selecting the list.

Exception Rules Import Excel

1. Go to **Policy > XBA Rule Management > Abnormal Behavior Rule System > Diagnosis Exception Settings** menu, click the 'Save' button in the upper left corner, and click the Import menu.
2. After overwriting the Excel list on the list registered on the Users page or deleting the registered list, only the list registered in the Excel file can be registered.
3. **Retain Existing Data** When data A exists on the server and data A exists in the same Excel file, if you select Keep Existing Data and upload the file Existing data retention counts are displayed.

Exception Rules after detection

Anomalies diagnosed as false positives can be handled by users directly in the Web Console.

1. Go to the **Analysis > Threats > Management** menu.
2. Click the `Details` button on the right screen of the anomaly detection list to be treated as an exception among the threats detected list.
3. The detailed information screen for the detected threats is displayed. Click the `Management(new)` button in the upper right corner.
4. The Management Details screen is displayed, and click the `Assign to me` button.
5. If you select the `Safe` radio button in the Threats verdict, the blue button `Setting Detection Exception - Add to Exception` is activated Click the `Add to Exception` button.
6. A pop-up window for adding a diagnostic exception rule with the process name or file path or suspicious file path automatically created as a false positive appears. After entering the rule name freely, click the `Save` button.

7. Click the `Save` button under the Add Diagnostic Exception Rule button to complete the exception settings.
8. The `Apply Now` button is blinking in the upper right corner, and click to apply the exception policy to the agent immediately.
9. If the same behavior as in Exception Settings occurs next time, it is treated as an exception in diagnosis as an abnormal behavior.
10. Details of exception handling on the Management screen can be checked in the list by going to **Policy > XBA Rule Management > Exception Rules** menu.

6.4 Yara Rules detection

YARA is a tool that allows you to search and classify malicious code based on a string or binary pattern (Hex string).
In addition to finding the signature of a file using only string and binary patterns, specify a specific Entry Point value, or suggest File Offset and Virtual Memory Address.
Efficient pattern matching is possible using regular expressions.

Genian Insights E allows users to quickly and efficiently detect Threats from Endpoints through Yara Rules written by users.

6.4.1 How to register for Yara Rules

YARA is a tool used for the purpose of identifying and classifying malicious code types using malicious code signatures. The signature of the malicious code is a text string or binary pattern included in a file, process, and Genian Insights enables Threat Detection & Response to the pattern included in the malicious code sample using YARA. YARA works by creating Yara Rules containing pattern information that users want to check directly in a file or process, and executing Yara Rules check commands on individual endpoints.

How to register Yara Rules and execute the inspection command is as follows.

Add Yara Rules

1. Go to **Policy > Yara Rule Management > Yara Rules** menu and click the `Add` button at the top.
2. Fill in the name and rule as required and click the Save button.

Item	Description
Name	Enter a name for the Yara Rules Policy. You can enter up to 128 characters.
Rule	Create Yara Rules containing the pattern information you want to check in a file or process. You can enter up to 12000 characters.

The minimum required form of Yara Rules is as follows.

```
rule RuleName
{
condition:
Boolean VALUE
}
```

Edit Yara Rules

1. Go to the **Policy > Yara Rule Management > Yara Rules** menu and click the Yara Rules you want to edit.
2. After modifying the Rule, click the `Save` button.

Delete Yara Rules

1. Go to the **Policy > Yara Rule Management > Yara Rules** menu and select the checkbox of the Yara Rules list to be deleted. Click the button when it becomes active.

Whether to use Yara Rules

1. Go to the **Policy > Yara Rule Management > Yara Rules** menu and select the checkbox in the Yara Rules list to modify whether to use or not. Choose whether to enable or disable it in Select Actions. Changes are reflected immediately when selecting whether to use or not.

Apply Yara Rules Policy

After creating Yara Rules, you need to run the check command on individual Endpoints.

1. Go to the **Analysis > Endpoints > Management** menu and click the list to run the scan command.
2. On the Endpoints detailed list screen, click Tasks, 'Check Yara Rules'. Click either the entire Rule or the selected Rule from the list. The example below describes how to apply the selected Rule.
3. When you click the selected Rule, a list of policies created in **Policy > Yara Rule Management** whose use is enabled is displayed.
4. As to whether Yara Rules is checked or not, in the **Analysis > Endpoints > Management** menu, the gear icon is activated in blue as shown in the picture.
5. In **Analysis > Endpoints > Management**, click 'IP' to go to the Log tab, you can check the results of the agent's threat detection and processing and Yara Rules related logs.
6. Click ‘Yara Rules detection list’ in **Analysis > Management** to check which files were detected on the detailed screen. Detailed information can be accessed by clicking the Threats Analysis button to the right of the list to go to the details screen.
7. If you want to register a Yara Rules detected file as a quarantine or threat file, select 'Response Method' in Management on the right.

CHAPTER

SEVEN

POLICY AND GROUP

Genian Insights E uses IP/MAC/department information to set Endpoints as a group, and supports event collection, threat detection and response policies differently for each group.

Group: Groups Endpoints based on IP, MAC, department code, and department name.
Policy : Detailed settings for event selection collection, threat detection level, and response method

After server installation and agent deployment, it is necessary to set fine-grained policies according to the target of policy application in the Web Console.

7.1 Group Policy Management

Genian Insights E provides group-specific event collection, detection, response and agent policy settings. To add a new policy, you can create a new policy group through the Add Policy button in **Policy > Group Policy Management**.

7.1.1 Default

All Endpoints connecting to Genian Insights E servers are initially subject to **DefaultPolicy**. Policy consists of Policy for Collection, Detection, Response, Agent Settings, and Advanced Settings. The policy group applied by the agent can be changed through **Policy Settings** in **Management, Groups**.

7.1.2 collect

Events to be collected

Item	collection event
Basic	Collect important events such as process execution, execution/document/compressed file creation, etc.
Designation	Collection of selected items among file, module, network, and registry events
All	Collect all collectable events

file collection list

Policy	Description
Collect the list of executables	Collect a list of executable files. The list of collected files can be checked in the FileList index.
Index specified file list	The file information defined in the 'designated extension' is indexed and stored on the PC.
file crawling	Collect file information when PC is idle **Document/Compressed File:** Collects document/compressed file information by checking the signature of all files. **Specified file:** Collects file information defined in 'specified extension'. **Quick Collection:** Aggressive use of System resources to gather information quickly. **Executable File:** Collects the list of executables by checking the signatures of all files. **Collect lock screen:** Crawl while on lock screen. **Time to wait for action:** Starts crawling if there is no user input during Settings time. **Crawling Run cycle:** Sets the cycle to rerun after crawling is completed. **Exception Path Setting:** Sets the file crawl exception path.

Collect Windows Events (ETW)

Windows Event provides various shutdown events that are important for security. Insights E provides a function that allows users to collect and search for window events when they register a desired window event.

Policy	Settings
windowsEvent Collection List	Collection of event information recorded in Windows Event Viewer, XBA linkage Settings
Collect description	Collect event data in natural language form
Collect eventdata	Collect event data in json format

The set window event is saved in the winevt index and can be searched in **integrated search**.

7.1.3 Detect

Detection engine

Engine	Description
Indicators of Compromise (IOC)	When detecting known threats such as the minimum confidence level of 10%, IOC, YARA, etc., the Settings function is provided to detect only when the confidence level is higher than the set confidence level.
Machine Learning (ML)	It applies machine learning detection to files sent by the agent and provides detection information in the Discovery and Endpoints detailed menus when detecting threats.
Abnormal behavior (XBA)	**XBA Rule Sets** Settings feature.

7.1.4 Response

If the agent distribution method is single version, NAC linkage is not supported.

The corresponding settings are as follows.

Policy	Settings
Response to known malware	Response when detecting dangerous processes registered in YARA and IOC DB Settings
NAC Interworking	Tags to be assigned to the node when the agent detects Threats Settings
Response to unknown malware	Response Settings in case of detection by machine learning
Malicious IP	Response when a connection is detected with a malicious IP registered in the IOC DB Settings

You can set the corresponding policy settings according to the policy, such as displaying agent notifications, forcibly ending processes, and deleting files.

7.1.5 Agent

Default Settings

Policy	Settings
Connection Server IP	In case of multi-server configuration, enter the server IP or domain from which the agent will connect and download the policy for server load balancing.
User notification pop-up	Whether or not to display a notification pop-up on Endpoints when Management responds to **Force process termination** or **File deletion** after malware detection Settings
Display tray icon	show agent tray icon (Disabled for NAC and agent icon integration)
Display Notification message	Write an alarm message text that occurs in Endpoints when network isolation and release Quarantine Message: The text in the pop-up window displayed in Endpoints when the user performs the Network Quarantine command to Endpoints in the Web Console. Release Message: The text of the popup displayed in Endpoints when the user performs the command to disable Network Quarantine on Endpoints from the Web Console.
Allowed IPs	IP settings to allow for network isolation (Genian NAC and Genian Insights E server IP can communicate without separate settings)

Block network access

Policy	Description
Network Block IP and Port	Enter the **IP and Port** to block access regardless of the network isolation policy. (TCP port) Servers associated with Genian Insights E server operations are not blocked.

Backup

Policy	Description
Windows VSS Backup	Backup all hard disk files using Windows VSS in preparation for ransomware attack. To prevent snapshots from being deleted by ransomware when using the VSS function, you need to **Policy > XBA Rule Management > XBA Rule Sets > Default** screen and set the 'Auto Response' setting of the "Document Extension Rename Threshold Exceeded" and "delete ShadowCopy" Rules.

Etc

Policy	Description
Using API Hooking	Hooking the API to monitor various events. Conflict with other software may occur, so it needs to be applied after stability test, and PC reboot is required when Settings `ON/OFF`.

7.2 Groups

Genian Insights E allows you to set Endpoints as a group with specific conditions, and set Threats Threat Detection & Response Policy according to the group. If you do not create a group, all Endpoints are included in the default group in the **Analysis > Endpoints > Groups** menu.

One Endpoints can be included in multiple groups depending on the condition, but according to the policy creation order, the 'high list group policy' among the order corresponding to the group condition is applied.

7.2.1 Create group

1. Go to **Analysis > Endpoints > Groups** menu and click the 'Add' button in the upper left corner to create a new group.
2. A pop-up window for adding a new group appears. After setting the group name, basic operation, and group selection to copy, click the 'Create' button.

Item	Description
Group Name	Enter a group name.
Basic Operation	`AND` - When using more than one condition, all conditions must be satisfied to be included in the group. `OR` - When using more than one condition, it is included in the group even if only one of the many conditions is satisfied.
Select group to copy	Select a group to copy the condition from among the already created groups.

7.2.2 Group Condition Settings

1. After creating a group, click the group name to move to the group condition Settings screen and set the conditions to be included in the group.
2. Click the Add button to set the conditions. After setting the condition, click the check button to save the condition setting.
3. After saving, click the 'Apply group condition immediately' button so that the server knows which Endpoints meet the group condition.
4. When you click the Apply group condition immediately button, you are automatically moved to the list screen containing the Endpoints set in step 3.

7.2.3 Modify group condition

1. To edit or delete group conditions, click the ‘Group Condition Settings’ button on the group condition detail screen.
2. After adding or deleting the detailed condition settings screen, click the 'Apply Now' button to be reflected in the server immediately.

7.2.4 Policy Settings

In **Policy > Group Policies**, you can set the policy for event collection, detection, and response.

After setting the Endpoints group, you can set the policy in the ‘Policy Settings’ list for that group.

1. First, set the policy for event collection, detection, and response in **Policy > Group Policies** according to the manual.
2. From the list of policies created in step 1, select the policy to be applied to the Endpoints group and click the ‘Apply immediately’ button.
3. When the policy application confirmation pop-up window appears, click the OK button.
4. Policy changes are reflected in the server, and to deliver the changed policy to Endpoints, click the ‘Apply Now’ button in the upper right corner.

CHAPTER

EIGHT

EVENT COLLECTION

Genian Insights E can collect all events that occur in Endpoints, not just Threats events.

Events collected from Endpoints can be indexed in **System > System > index**.

In addition, if the amount of events is large and the events are frequently generated by security programs, you can selectively set event collection exception settings.

8.1 event collection

Event Bypass Management and Exception Settings can be set in **Policy > Event Bypass Management**.

8.1.1 Collect Endpoints Events

When the agent installation on the device is completed, the event generated by Endpoints is sent to the Insights E server. According to Genian Insights E server Settings, it collects events that it considers important (process execution, execution/documentation/compressed file creation), and more necessary information can be changed in Server Settings.

Events collected by Endpoints can be viewed in **Discovery**. The default index is shown below.

- **Endpoint2:** Events (file, process, module, network, registry) that occur in Endpoints
- **Alert2:** Information on threats detected as threats by Threat Detector engine and alarms and threat information detected by XBA engine are displayed on an event-based basis.
- **Threat2:** Status-based display of information detected as Threats by Threat Detector engine and generated alarms and Threats detected by XBA engine
- **Inflow:** file inflow information
- **Volume:** External storage device mount information
- **FileMaster:** PE, Script file information
- **system-info:** PC resource information collected by Agent

Window Events (ETW)

In **Policy > Group Policy Management > Collection**, you can set the collection target window event.

Genian Insights E provides a function that allows users to collect and search for window events when they register desired window events. Relevant events are stored in the `winevt` index and can be searched in **Discovery**.

- **WindowEvent:** Windows Event information generated by Endpoints

8.1.2 Event Search

The **Analysis > Investigation > Event Search** page allows you to view and analyze events that occurred across all Endpoints, not specific Endpoints.

Event Search

- In the Event Search screen, you can search all fields related to a file at once with a single keyword. Fields that can be searched without entering a field name are marked with a blue star when clicking the search bar.
- When searching for data in the search bar of other menus, you must search in the same format as 'Field Name: Data', but you can search for keywords in the Event Search screen.
- If the kiwid to be searched contains spaces, surround the keyword with double quotation marks and search.
- The fields `AuthName`, `AuthDeptName`, and `HostName` must be entered in full text when searching for keywords. For example, if the AuthName is Hong Gil-dong, it will not be searched if only the word Hong-gil is entered in the search.

Event Investigation

The Event Investigation list allows you to check the event history of all Endpoints.

- The history of the set date (ex.Today,1d,3d, etc.) is displayed in a chart, and you can check detailed information by clicking and dragging the mouse within the chart to narrow the event date period.

When you click the event list, the **event detail information screen** appears.

- When you click the exception handling icon on the event detail screen, you can register not to collect the event.
- When you click the docking pop-up on the right screen, a separate pop-up window will appear. In the event details screen, the clicked item was initially executed by a certain process, and if connection information exists, even destination IP information can be identified.
- When the floating icon is clicked, Process, File, Module, Network, and Registry information related to the clicked item is displayed based on the first occurrence time. (Data not collected according to Collection Target Event Settings of Policy > Group Policy > Policy with Endpoints is not displayed.)
- For the event selected in the event details, view only events that are directly related from the Endpoints information to the selected event being executed, or Settings can be set to display all related events based on event type.

Event Investigation Column Settings

In the Event Search screen, you can display only the information that users want to check through the column Settings.

1. In **Analysis > Investigation > Event Search**, click the Settings icon in the upper right corner and select 'Edit column' to display the Column Settings screen.
2. Move the column item you want to display to the right and click the 'Save' button to display the column set by the user.

8.2 Event Bypass Management

Genian Insights E can collect all events that occur in Endpoints, not just Threats events. If the volume of events is large and the events are frequently triggered by security programs, you can selectively use **Event Bypass Rules**.

In addition, if events occur frequently due to security programs and business programs, you can selectively use Event Bypass Rules. Exception handling for known security programs is provided by default, and new **exception handling rules** can be added by copying group settings based on the default exception group.

8.2.1 Add Event Bypass Rules

1. Go to **Policy > Event Bypass Management > Event Bypass Rules** menu and click the 'Add' button at the top.
2. The Add Event Collection Exception Group pop-up window appears. After confirming the name, whether to use it, and whether to select an exception group to copy, click the 'Create' button. By checking the exception items of the program registered as default, you can conveniently set the collection exception when selecting the exception group to copy.
3. After adding an exception group, click 'Added group name' in the list.
4. Click the Add Event Collection Exception button. In the screen below, if you move your mouse over the business program exception, you can edit the name and add a description when you click the 'pencil icon'.
5. A pop-up window for adding event collection exception appears, select the event type (file, process, module, network, registry) and click the OK button.
6. When adding process exception handling as shown below, a pop-up window for inputting additional information is displayed.
7. After entering information about the process to be handled as an exception, click the Save button.
8. You can check the exception handling process information added earlier on the collection exception detail screen.
9. When setting exceptions, you must click the 'Apply Now' button in the upper right corner to send the policy to the agent immediately.

8.2.2 Delete Event Bypass Rules

1. After selecting the exception group to delete, the 'Delete' button will be activated, allowing you to delete the exception group.
2. When deleting exception settings, the policy is delivered to the agent immediately after clicking the 'Apply Now' button at the top right.

CHAPTER

NINE

THREATS RESPONSE

On the **Analysis > Threats > Management** page, you can check the various threat information detected by the Threat Detector plug-in of Genian Insights E.

Among them, the Threats notification, response policy, and processing corresponding to the Threats response are described.

9.1 Threats notifications

9.1.1 Email notifications

Insights E provides a mailing service for Threats notifications and reports to the mail set in the Users account.

Mail Server Settings

1. Go to **System > Settings > Perferences > System** page and set the mail server first. When setting the server, all information must be filled out, and through the Settings test, You can check whether it is operating normally.

Item	Content
Connection security method	Supports SMTP(25), SMTPS(465), MSA/STARTTLS(587).
Server Port	Enter the same port as the connection security method.

User Account Settings

1. In **System > Settings > Users**, go to the Users account and click the account to which the report will be sent.
2. In the user edit screen, select the information to be provided in the e-mail notification, enter the e-mail address to which the report will be sent in the additional information and click the edit button.

Item	Description
Threat Notifycation	Send threat information generated within 1 hour by e-mail. (available every hour)
Disk Usage Notification	Insights When the device's disk utilization exceeds the default value (70%), information about the excess utilization is sent to Users email.
Daily Threat Report	Aggregates the threat information generated over 24 hours and sends the report by e-mail. (Once a day, 01:00)

You can receive Threats notifications by user.

9.1.2 Endpoints notifications

In **Policy > Group Policy Management > Agent**, the notification message display must be set to 'Enable'.

Endpoints notification means 'pop-up notification function when a threat is detected' on the terminal where the agent is installed.

Users Notification Settings

1. In **System > Settings > Users**, check Agent Notifications > Threat alert.
2. Enter the 'Device ID' of the Users PC to display the notification window.

`Device ID` can be checked in the Basic Information tab of **Analysis > Management** terminal.

Endpoints Notification Settings

You can configure Endpoints notification settings for each policy in **Policy > Group Policy Management > Response**. XBA detection notification settings require notification settings for individual XBA rules.

Item	Settings	Description
Response to Known malware-Agent Notification Messages	Disable /Low/Medium/High	**YARA, Select whether to notify the user through the agent pop-up when a dangerous process registered in the IOC DB is detected**.
Response to Unknown malware response-Agent Notification Messages	Disabled/ML.Medium/ML.High	**When detected by machine learning** Sets the minimum risk to be displayed to the user through the agent pop-up.
Response to Malicious IP-Agent Notification Messages	Disable/Enable	**When a connection is detected with a malicious IP registered in the IOC DB** Select whether to notify the user through the agent pop-up.

After Policy Settings, settings can be made through 'Policy Settings' on the **Analysis > Endpoints** group settings page or 'Policy Name' on the individual Endpoints detailed screen.

9.2 Threats Response Policy

Analysis > Threats > Management provides policy settings for Maliware and XBA Threats.

Item	Description
Safe	Exclude selected Threats as Safe.
Malicious-Response Policy	Registers response settings for the selected Threats.
pending	Treats the Threats verdict for the selected Threats as Hold.
Reset	Resets the Threats verdict for the selected Threats to a new state.

9.2.1 Endpoints Threats Response Policy

In **Analysis > Threats > Management**, the Policy Settings function is activated when the list of detected risks is selected in Threats by Status.

Item	Description
Default-Policy	If the file is detected again, it is processed according to the rules set in GroupPolicy-Response.
Detect Only	When the file is detected again, only the detection is performed without raising any other events.
Notify	When the file is detected again, it immediately triggers an alarm event on Endpoints.
Kill Process	Initiate a Kill Process event to Endpoints when the corresponding process (file X) is detected.
File Delete	Promptly forwards a file deletion event to Endpoints when the file is detected again. The files are quarantined in the `c:\program files\geni\insights\Isolate` folder and deleted after a certain period of time has elapsed.

You can set the desired response policy among them. In addition, you can add a description of the policy through a note according to the Threats Response Policy.

9.2.2 Endpoints Individual Response Policy

When a threat file is detected based on the MD5 hash value, it is possible to immediately respond with the response policy set in Management, but it provides the setting function for the response policy for each endpoint. Selecting Endpoints from the list activates the Policy Settings feature.

- When you click the `Exception` button after selecting Endpoints, files detected by the Endpoints are set to be excluded from Threats detection.
- After selecting Endpoints, click the 'Threats Response Policy' button to select the response to be triggered only on the device.
- If you set the individual response policy, the set values (alarm/process forced termination, deletion) are saved in the individual response policy.
- If the file or process is running at the time the response policy is applied, 'Delete immediately' (moved to quarantine and deleted after a certain period of time has elapsed)/'Forced process termination' is performed.

If you want to initialize an individual response policy, select Endpoints and click the Reset button.

9.3 Handling Threats

Analysis > Threats > Management provides Threats handling settings for Maliware and XBA Threats.

Item	Description
Safe	Exclude selected Threats as Safe.
Malicious-Response	Registers response settings for the selected Threats.
Pending	Treats the Threats verdict for the selected Threats as Hold.
Reset	Resets the Threats verdict for the selected Threats to a new state.

9.3.1 Threats file response and exception handling

The agent can respond primarily to files detected as Threats, but In the Users UI, you can set 'React immediately' for files or perform 'React commands' for individual Endpoints. In addition, if a file with the same MD5 hash value is detected in the future, users can set whether to prevent separate confirmation or continue displaying threats through Management.

1. If you want to respond after checking basic information about a file, click the Threats Analysis button in the Threats list in Management.
2. You can handle immediate response, exception handling, and false positive report on the right Management screen of the detailed list.
3. On the ThreatsSystem screen, if you click I am responsible, users can directly handle malicious/safe/hold settings for currently detected files.
4. Depending on the Threats judgment selection value, detailed response and exception handling screens are displayed.

9.3.2 Malicious file/process response

Item	Settings	Description
ResponsePolicy	Default	If the file is detected again, it is processed according to the rules set in Group Policy-Response.
ResponsePolicy	Notify	If the file is detected again, it immediately triggers an notify event on Endpoints.
ResponsePolicy	Kill Process	When the corresponding process (file X) is detected, it immediately issues a process kill event to Endpoints.
Response Policy	Delete File	Promptly forward a file deletion event to Endpoints when the file is detected again. The file is quarantined in the `c:\program files\geni\insights\Isolate` folder, and the file is deleted after a certain period of time has elapsed.
Auto Resolve	-	When a file with the same MD5 hash value is detected again, the processing status is automatically changed to Resolved without displaying it in the Analysis menu.
Notes	-	Users can take notes about detected Threats.

1. In case of a malicious file, you can select a malicious item and set the response policy.
2. Click the Settings Complete button for the malicious file, and the set response policy will be executed immediately.
3. If you want to set the Threats Response Policy for a detected file without checking basic information, select the list displayed in the Threats list and the Threats Response Policy button is displayed at the top of the screen.

If automatic resolution is selected for malicious files, the next time the same file is detected again, it is treated as resolved rather than registered as a new file in the Analysis screen. Even if duplicates are detected, if it is determined that the user's confirmation is necessary, the automatic resolution option should be turned off.

Batch Threats response policy (notify, process termination, deletion) can be set in the list, not the Management screen, and the basic operation is the same as the response policy of 1.

9.3.3 Malicious file/process exception handling

If the detected file is a false positive, settings for exception handling are also performed in the Management menu.

Item	Description
Notes	Users can write notes about detected files.
Reporting false positives	Reports false positives to `Ecosystem` through false positive reporting in case of a normal file but false positives. File information reported as false detection will be registered in the Goodware DB later.

If it is detected as a Threats file, but users cannot determine whether it is malicious or there is insufficient information to be confirmed through external links, the response to the file can be withheld. The target of the hold can be primarily files detected by machine learning.

CHAPTER

TEN

FILE COLLECTION

Genian Insights E provides various functions such as automatic file collection, analysis, and download when a threat is detected.

10.1 Collect files

Upon detection of threats, you can collect Threats file samples or general files from the Web Console, download and delete files.

10.1.1 Collecting malware samples

1. In **Analysis > Threats > Management**, click the 'Details' button in the Threats list to go to the detailed screen, and the Sample Collection button is displayed as shown below. Click the 'Collect Sample' button.
2. An alarm window related to sample collection appears, click OK.
3. When sample collection is complete, the Download Samples button is displayed and you can download or delete files from the Acquisitions menu at the same time.

10.1.2 Download and delete files

Malicious file samples and normal file samples are classified as follows.

type	Explanation
It is a malicious code file detected as Threat	Threats, and an alarm window for entering a password occurs when the file is downloaded. Click the OK button to download the password-applied hash value and zip file. If you want to change the password set by default, you can set the sample download password on the **System > Settings > Perferences > Threat Detection & Response** page.
File	It is a general file collected by the sample collection command of Users and does not require a separate password input.
It is a general file collected by the Artifact collection command of Artifact	Users and does not require a separate password input.
Agentlog	Displayed when an agent log file was collected by a manual command from Users on the server.

1. You can download the file by clicking the sample download button generated during the malware sample collection process or clicking the download button in **Analysis > Investigation > Acquisitions**.

2. If you click the Delete button in the file list, the file is deleted from the server and also in the Acquisitions list.
3. If you are collecting large files via Live Response, you will see an upload icon in the Acquisitions list. When you click the list, the progress of file collection is displayed. The collection progress is updated with every click on the list.
4. When collecting artifacts, click on the Load Data button in the Acquisitions list. After loading the collected data, the 'G-Report' button is created.
5. When you click the 'G-Report' button, the G-Report window is created and you can check the artifact-collected data in Report format.

10.2 Collect artifacts

Insights E provides the **Automatic artifact collection function** for XBA diagnostics.

10.2.1 Artifact collection Settings

Artifact collection settings can be set in **Artifact Collection Target** in **System > Settings > Threat Detection & Response**.

The objects of collection are as follows.

Collected Objects	Description
system information	System information collection
Autorun	Collect autorun items
Browser History	Collecting browser browsing history
Registry	Collect registry hives
Window Events	Windows event log collection
Prefetch Files	Prefetch file collection
FileSystem Information	Suspicious file collection

Registry, File, and Process are artifacts automatically collected.

10.2.2 Collect artifact samples

Collect samples

1. In **Analysis > Threats > Management**, click the 'Details' button of Threats that can request artifact collection from the list of threats detected as anomalies. On the detail screen, click the Artifact 'Collect button'.
2. Select the desired terminal list in **Analysis > Endpoints > Endpoint List** and click the **Tasks > Collect Artifact** button.
3. After selecting the desired group list in **Analysis > Endpoints > Groups**, click the **Tasks > Collect Artifact** button.

Check Collected Artifacts

Collected artifacts can be viewed in **Analysis > Acquisitions**.

1. When collecting artifacts, click the 'Load Data' button in the Acquisitions list. After loading the collected data, the 'G-Report' button is created.
2. When you click the 'G-Report' button, the G-Report window is created and you can check the artifact-collected data in Report format.

CHAPTER

ELEVEN

THREATS ANALYSIS

Based on the events collected by Endpoints, when Threats are detected by the Threats detection engine, you can view Threats details in the Web Console.

The information you can check in **Analysis > Overview** is as follows.

Item	Description
Threats Status	New: Number of newly detected threats. In Process: The number of Threats the person in charge is reviewing by clicking the 'take me' button in Management. Resolved: The number of completion of Threats determination (Malicious/Safe/Hold) by the person in charge by clicking the 'I'm in charge' button in Management. The Resolved number is only displayed when **Include Resolved Threats** is selected.
Endpoints Status	UP: The number of endpoints in operation (UP) among endpoints where the agent is installed. DOWN: The number of endpoints that are in a down state among endpoints where the agent is installed. Deleted: Number of Endpoints for which the agent was deleted. Quarantined: Number of Endpoints that are in Network Blocked (Quarantine) status. Even if Endpoints are Blocked (Quarantine) status, they can communicate with Insights server.
New Threats	Displays the latest 5 Threats occurrence information (yellow background if within 1 hour)
Show Threats Settings	Include Resolved Threats: Set whether to display including threats that have been checked by Users when detecting threats. Search Date: Search Threats from at least today to up to 1 month. The date search range is as follows. ex) If the current time is 2021-06-06 13:00 Today:2021-06-06 00:00 ~2021-06-06 23:59 Yesterday:2021-06-05 00:00 ~2021-06-05 23:59 This week:2021-06-04 00:00 ~2021-06-10 23:59 Last week:2021-05-28 00:00 ~2021-06-03 23:59 Day 1 :2021-06-05 00:00 ~2021-06-06 23:59 1 week :2021-05-30 00:00 ~2021-06-06 23:59 1 month :2021-05-06 00:00 ~2021-06-06 23:59 Print : Prints the Overview screen. Auto Refresh: The Overview screen is refreshed every minute. Full Screen View: Displays the Overview screen in full screen.
Threats Statistics-Recent Threats Status	Total Threats: The number of detections for all items of file/process (IOC, machine learning, YARA), malicious IP, and batch detection. Infection: Threats The number of detections for files/processes (IOC, machine learning, YARA, batch detection). Malicious IP: The number of detected information registered as malicious IP. Abnormal behavior: The number of threats detected by the Abnormal behavior policy. Batch: The number of detected batches. Batch detection means that when the IOC DB is updated after the agent sends PC information, it is collected for a certain period of time (default: 3 days). It serves to check information and analyze whether there are newly updated threats. (Performed every day at 02:00, ends within 06:00) The number of detections varies depending on whether **resolved threats are included** or not.
Top 10 malware distributed across multiple endpoints	A list is displayed based on the MD5 of the malicious code, and the number box indicates the number of terminals where the malicious code occurred.
Top 10 Abnormal Behaviors accurring in multiple endpoints	A list is displayed based on the anomalous behavior policy, and the number box indicates the number of devices that have detected the aberrant behavior policy.
Top 10 endpoints with multiple threats	Displays the number of Threats (Malware + Abnormal Behavior) detected by authenticated user name/host name/IP/department name. When you click the Settings icon, you can select the display criteria. When detecting, the color of the background of the number changes depending on the number. (8 pieces or less - light color, more than 8 pieces - dark color)
Threats classifi-	If there is more than one detected threat type (IOC, CTI, ML, MaliciosIP, YARA, by anomaly classification), the Threats occurrence rate is displayed.

11.1 Threats detection information

On the Threats Analysis detail page, you can check detailed analysis information of Threats, process a threat response, collect samples, and check information required for analysis.

Item	Description
filename	Displays the process OR file name detected as Threats. Displays the final detection time, detection classification/detection detailed classification, and tag information.
Print Icon	Provides the ability to print the detailed information screen.
Management(new)	ThreatsSystem- Provides the ability for users to respond differently after checking when a threat is detected, or to handle an exception so that it is not detected next in case of a false positive.

11.2 Basic Information

The Basic Information page displays information about detected threats and file information, MD5 hash of malicious files, or external links that allow searching whether IP information is a known file.

Item	Description
Indicators	Displays the engine type that detected the Threats and Threats information.
Threats Information	**Processes performed:** Threats Displays detected process information. **Threats classification (displayed only in case of malicious code):** Displays the predefined types of malicious code through IOC DB or file reputation inquiry. Adware, Backdoor, Browser, Dialer, Downloader, Exploit, Hacktool, Infostealer, Keylogger, Malware, Network, PUA, Packed, Ransomware, Rogue, Rootkit, Spyware, Trojan, Virus, Worm **Threats name (displayed only in case of malicious code):** Displays the threat name. **Sample type (displayed only in case of malicious code):** Displays the sample type. **Events:** Threats displays the types of events detected. (file, process, network, module) **Summary:** Displays information about predefined malicious codes and abnormal behaviors. **MITER ATT&CK:** If there is predefined MITER ATT&CK information when detected by abnormal behavior, it is displayed, and when clicked, it connects to an external link where you can check related information.
Management information	**Threats verdict:** Information classified by users as malicious (malicious, safe, pending) in Management. **Response Policy:** This is the information that the user sets the response policy (alarm, process termination, file deletion) when a threat is detected in Management. **Processing Status:** Displays the Threats processing status (New, Processing, Resolved). **Person (ID):** Displays the User ID who changed the Threats status in Management.
detection time	**LOCAL:** The time the threat was detected in LOCAL **GLOBAL:** Visual information on which threats are detected in the reputation inquiry system if the ecosystem is linked when malicious code is detected
Malicious File Information	Threats Displays file name, file path, file type, file size, version registered in file attribute value, language, copyright, architecture, executable file type, MD5, SHA-256, and digital signature information for the detected file. (FileMaster index information)
External Links	Whether the MD5 hash or IP information of the malicious file is a known file can be searched through an external link. External links can be edited in **System > Settings > Properties > External Links**.

11.3 Detection information for each device

If the detected threats are detected by multiple devices, you can check the device list in the detection information for each device. Up to 10 endpoints are displayed, and if more endpoints are detected, click the Search All Device Events button to view a list of all endpoints with the corresponding threat.

Item	Description
status	Shows the operational status of Endpoints.
IP	Displays IP.
Username	If the threat detection terminal is a user authenticated by Genian NAC, the authenticated user name is displayed.
hostname	The host name of the Threats detection device is displayed.
Response Rule	If you need an immediate response or exception handling for a malicious file or malicious IP, you can set it on the ThreatsSystem screen.
Same Threats information by Device	If the same file is detected multiple times, the detection path, detection information, and response result are displayed.

11.4 Analysis Indicators

Analysis indicator displays related Threats indicator, related behavior indicator, similarity indicator, and AI Analysis indicator information.

Item	Description
Associated Threats Indicators	Displays the endpoints where Threats was last detected and all Threats detection information from those endpoints.
Associated Behavior Tags	If tag information exists in the event of all processes related to Threats, the corresponding tag is displayed as related behavior indicator information, Click to go to the Event Search list.
Similarity	When a suspicious malicious file is detected, whether it is a known malicious file variant is inquired through the Ecosystem, and similarity information is displayed. When the refresh icon is clicked, the latest information is inquired in Ecosystem once more.
AI Analysis	With the information detected by ML, it provides an index that predicts the threat classification and threat name of malicious code. Type: Analysis indicators for the types of malware threats (Adware, Trojan, Virus, etc.) Family: Analysis indicator for FamilyName of malware Analysis Perspective: The Perspective That Created AI Indicators

11.5 Attack Story Line

The agent is a process identification number (PID) and Collects PPID (Parent Process Identification Number) information and agent operation time information.

In the attack history line page, the PID, PPID, Device-id, and EventTime information of the process detected as Threats are combined during the time the agent is operating. Based on the Threats process, it displays the parent process of the corresponding process, module information executed by the Threats process, child process information, and connection information of the Threats process.

If the same file is detected on multiple Endpoints, it provides connection information for the last detected (latest) Endpoints.

CHAPTER

TWELVE

DISCOVERY

Events collected through Agent and Collector Settings can be viewed in the Discovery menu.

12.1 How to search logs

Logs are stored in different indexes depending on the type of event, and logs can be searched after selecting an index.

1. Go to the **Discovery** menu, select the index you want to search the log from in the tree on the left.
2. Enter a query to be searched directly in the search bar or click a value to search in the log detail view to automatically create a data chip in the query input device. When typing directly into the query input method, Genian Insights' log searches use Lucene grammar. (More detailed syntax can be found in the Lucene Documentation.)

   ex) If you want to search for a value with user ID 'admin' in Insights Logs

   After selecting **Discovery > Insights Logs**, enter logUserId:"admin" in the query input device and click the `Search` button. Only the values with the user ID of admin are searched and the query is highlighted.

Audit records generated by the Genian Insights E server are stored in the Insights Logs index, and details by log ID are as follows.

Log ID	Name	Content
100	Administrator Login	Login related to Administrators' login status
110	Group	Endpoints Group Creation, Modification, and Deletion Logs
118	Update	License update log
120	CLI	CLI connection related log
121	User Directory	User Directory Logs for Information, User, Department, etc.
130	Agent	Agent operation status, plug-in update related logs
132	System	Endpoints' System operation status (sleep, log on, log off. disk usage) related logs
140	Agent Action	Endpoints Threats Response Results, Process Dump Collection, File Collection, Yara Rule
150	System	Backup, index cleanup, deletion of inactive endpoints, Trendmicro linkage results, server se
160	Policy	Web Console's policy immediately applied, Endpoints Policy reception related log
200	Settings changed	Logs related to various settings change in Web Console
300	User	Logs related to user creation, deletion, Roles, and user information change in Web Console
400	Index	Index in Web ConsoleSystem Settings Related Logs
500	Collector	Logs related to Collector Settings in Web Console
600	Profile	Logs related to Collector Settings Profiles and Server Profiles in Web Console
700	Filter	Logs related to search filter
750	Threat	ThreatsSystem (Threats determination, person in charge Settings, etc..) status related logs
770	CTI	Audit log for deletion information when PE File is deleted
790	File	Logs related to file collection status in the CollectSystem menu

Table 1 – continued from previous page

Log ID	Name	Content
800	IOC DB	IOC DB update related log
810	Threat	Threats detection related logs
815	Device Tag	IOC Device Tag Settings Log
820	Notification	Display Notification Messages on Endpoints Log
825	Process Terminated	Terminating Process When Threats are Detected Log
826	Process Terminated (Manually)	Users Directly Terminating Process Log
830	File Quarantined	Delete File when Threats are detected Log
831	File Quarantined Manually	Log files directly deleted by users
835	Sample File Collected	Executable Sample Collection Log
836	Sample File Collected Manually	Logs of Manual Collection of Executable Samples
837	Collection	File Sample Collection Log
838	Collection Manually	File Sample Manual Collection Log
841	Network isolate(Manually)	Logged Network Quarantine Command Directly by Users
850	Anomaly Detection	Anomaly Detection Log
870	Anomaly	Abnormal behavior rule system and exception Policy Settings related log
900	Dashboard	Logs related to Dashboard in Web Console
912	Report	Logs related to changes in the Report menu of the Web Console
999	Miscellaneous	GenianNac log creation and deletion related logs

12.2 Save search history and favorites

1. Discovery screen After entering and searching data in the search window, click the `Favorites` button to display the Add Favorites screen with the search conditions displayed on the screen automatically entered.
2. When you click `Search Filter` after saving your favorites, you can check the list of added favorites and your recent search history (up to 50 each). Your recent browsing history is also cleared when your browser cache is cleared.

CHAPTER

THIRTEEN

DASHBOARD

13.1 Share Dashboard

If you have difficulty creating a dashboard, you can import multiple dashboards registered in Genian Ecosystem, or share dashboards among users.

13.1.1 Add ECO Sharing Dashboard

We are collecting a lot of information from Endpoints, but we are having a hard time generating the information that users need into Dashboard. If Genian Insights E server communicates with Ecosystem, you can add Dashboard created and shared in Ecosystem.

To use the ECO Sharing Dashboard, Network Connection with eco.genians.net is required, and Ecosystem link must be on in the basic settings of **System > Settings > Perferences > System**.

1. After logging in to the Web Console, go to the Dashboard menu, click **Add Shared Dashboard** in the **Options** menu in the upper right corner.
2. The Add Shared Dashboard pop-up window will appear, click the ECO Service Dashboard tab. Click the 'Add Dashboard' button.
3. You can check the Dashboard added in 2.

13.1.2 Add Users Shared Dashboard

Dashboards can be shared among users.

1. A Users are registered in the user sharing dashboard by going to the Dashboard menu after logging in to the Web Console, selecting the dashboard they want to share, and clicking Share Dashboard in the options.
2. Dashboard sharing confirmation pop-up window appears, click the OK button. A shared dashboard displays a share icon in the tab name.
3. B Users can add a dashboard shared by A Users by clicking Add Shared Dashboard in Options, in the User Shared Dashboard tab.

CHAPTER

FOURTEEN

AUTHENTICATION INTEGRATION

The Authentication Integration utilizes a user ID and password to identify a user in Endpoints.

Insights provides the Authentication Integration feature in a number of ways.

Authentication Integration can be done using Genian NAC interworking, Syslog authentication replacement, Active Directory and user information interworking of external systems.

14.1 Authentication Integration method

Authentication Integration can be done using Genian NAC interworking, Syslog authentication replacement, Active Directory and user information interworking of external systems.

14.1.1 Authentication Integration using Genian NAC

If you are operating Genian NAC and are using the Authentication Integration Policy, you can use NAC's authentication information for Insights Endpoints authentication.

How to handle authentication

1. To use NAC authentication information, agent deployment method must be set to **NAC plugin** or **Standalone + NAC link** mode in Insights Web Console Settings.
2. After authentication integration in the NAC agent, when GsAgent is activated, the authentication information value recorded in the registry is checked and the authentication information is transmitted to the Genian Insights E server together.
3. Authenticated user information can be checked in the AuthName and Department Name columns of **Analysis > Endpoints > Management** after logging into the Insights Web Console.

14.1.2 Authentication Integration using external system interworking

If there is an external system with user ID, department information, IP, and MAC information, information from the external system can be imported to Genian Insights E server and used for Endpoints authentication.

User Data Synchronization

1. First, go through the synchronization settings that bring the user ID and department information of the external system to the Genian Insights E server. **Go to the System > Settings > Employees > Data Synchronization** menu, and click the 'Add' button at the top left.
2. Set the synchronization execution cycle and execution options in the Basic Settings item.
3. Find DB type menu in Detailed Settings. Select the database type from which data is to be read and input external system information.
4. Find user information, department information, and job position information in Detailed Settings and add the necessary information. (If using CSV, leave it blank). Enter the authentication processing IP or authentication processing MAC column information as well.
5. After checking the entered information, click the 'Save' button in the upper left corner.
6. Select the item you want to synchronize from the Data Synchronization list and click 'Auth Sync Immediate Action'. "Are you sure you want to request Auth Sync Immediate Action for the selected item?" A pop-up window will appear, click 'OK'. After that, data synchronization is performed according to the synchronization execution cycle set in step 2.
7. After synchronization is complete, you can check the audit log like **"Data Synchronization Completed.ID=XXXXX", "User Synchronization Completed. ID=XXXXXX"** in **Discovery > Insights Logs**.

Syslog authentication replacement

1. Perform user data synchronization first.
2. Go to the **System > Settings > Employees > Authentication Integration** menu and change Syslog Authentication Alternate Settings to On.
3. After setting the Prefix, Endpoints search method, and whether to disable Release authentication, click the 'Save' button in the upper left corner.
4. When data is received in the format set in 3 through Syslog, the Genian Insights E server performs authentication processing for Endpoints.
5. Authenticated user information can be checked in the AuthName and Department Name columns of **Analysis > Endpoints > Management**.

Active Directory Authentication

1. Perform user data synchronization first.
2. Go to the **System > Settings > Employees > Authentication Integration** menu and change Active Directory Settings to On.
3. Enter the domain information to be authenticated. If the domains match, authentication is processed. If there are multiple domains, enter them separated by commas and click the 'Save' button at the top left.
4. If user data synchronization is processed after Endpoints authentication, click the 'User Information Update' button to perform authentication processing again on the server.
5. Authenticated user information can be checked in the AuthName and Department Name columns of **Analysis > Endpoints > Management**.

CHAPTER

FIFTEEN

SECURITY CHECK

It provides a Live Response (security check) function that allows you to access Endpoints in real time from the Web Console to perform various commands and check the results.

15.1 Command Settings

The security check function can only be used by users who have been assigned the security check function authority, and only specific commands can be used by authority. After adding the commands to be used for security check first, set the available commands according to Roles.

15.1.1 Add command

1. If you need to register a command, go to the **System > Settings > Properties > LiveResponse commands** menu and click the 'Add' button to add a command.

number	name	Description
1	command	Enter the command to be used in the security check console.
2	Permission Control	Choose whether to control permissions for commands. If it is **Disabled**, users with security check permission in Roles can freely use the command. If it is **Enabled**, only Users who have permission to use the command in Roles can use the command.
3	Help Message	Enter a description to provide as command help.

15.1.2 delete command

In addition to the default commands, commands added by users can be deleted.

1. Select the added command from the command list and click the 'Delete' button to delete the command. If a command to be deleted is assigned to Roles, when the command is deleted, the command assigned to Roles is also deleted.

15.1.3 How to assign commands by authority

If the security check command has permission control settings, it is necessary to assign usable commands.

1. Go to **System > Settings > User Management > Roles** menu, and click the role ID to assign a command to. The role modification screen is displayed, and among the items, change the Live Response permission to on.
2. In the available commands, select and save the commands to be used among the **commands with permission control settings** in LiveResponse commands.
3. After checking the assigned command, click the 'Update' button.
4. When connecting the security check to Endpoints, items with unchecked permission control (cls,help,exit) and commands assigned with available commands in 3 are displayed.

15.2 Connect to Endpoints

The security check function can only be used by users who have been assigned the security check function right. LiveResponse commands and usage rights assignment can be set in *Command assignment method by authority*.

1. Click **Analysis > Endpoints > Management**. Click the IP you want to connect to. Live Response (security check) can only connect to running Endpoints.
2. Click the Live Response icon in the upper right corner.
3. The Possword Policies confirmation window appears, and input the Possword Policies of the currently logged in users.
4. After checking the Possword Policies, a security check pop-up window appears, and when the connection is successful, the check pop-up window says "Agent connection was successful." A message is displayed, and the default path links to the agent installation path.
5. When the inspection window is closed or the exit command is sent, the security inspection connection is terminated.

15.3 security check command

Supports Endpoints' process list check, specified extension search, and file collection. Detailed commands are as follows.

15.3.1 Basic commands

command	Description
sendnow	Events that have not yet been sent, logs are sent to the server immediately.
help	Provides help for commands.
dir	Lists files and subdirectories in a directory.
cd	Shows or changes the current directory name.
cls	Clear the screen.
exit	End Live Response.
quicksearch	Retrieves a list of executables or files with the specified extension from the indexed DB.

You can check the directory name by using the Tab key on the Live Response screen.

When you press the Tab key with only the cursor, commands that can be checked with help are displayed, and when you enter only a specific alphabet and press the Tab key, commands that can be executed with that alphabet are displayed.

15.3.2 Search for a specified extension

1. In order to search for an extension, you must enable indexing of the specified file list in the detailed Policy Settings of **Policy > Group Policy Management**, and the extension to be searched must be defined in the specified extension.
2. Search is possible only for extensions that change from the time the policy is applied to the agent.
3. If a search is required for all files that do not change, set File Crawling to Enabled in Policy Detailed Settings in **Policy > Group Policy Management** and turn on Executable Files, Documents/Compressed Files, and Specified Files Settings should be changed to

When using file crawling, it takes a lot of time to gather the entire list of files.

quicksearch command: Search the indexed DB for a list of executable files or files with a specified extension.

Supported file extensions: |.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|

Additional options can be found through the command help (quicksearch /?)

command	Description	Usage Examples
quicksearch	Retrieves a list of files in the current path.	*quicksearch doc_test.docx* Search for the doc_test.docx file in the current path.
quicksearch file path file name	Retrieves a list of specific files in a specific path.	*quicksearch c:\Temp\doc_test.docx* Search for the doc_test.docx file in the c:\Temp\ path.
quicksearch /s file path file name	Retrieves a list of specific files from a specific path and its subpaths.	*quicksearch /s doc_test.docx* Search for the doc_test.docx file in the subpath that contains the current path.
quicksearch /a filename	Retrieves a list of specific files from the full path.	*quicksearch /a doc_test.docx* Search for the doc_test.docx file in the full path.
quicksearch /c file path file name	Retrieves the number of specific file listings in a specific path.	*quicksearch /vc:\Temp\doc_test.docx* Search the c:\Temp\doc_test.docx file to display the details.
quicksearch /v file path file name	Retrieves a detailed list of specific files in a specific path.	quicksearch /v /sc:\Temp Retrieve a detailed list of files in the subdirectory containing c:\Temp.
quicksearch /p process name	Retrieves a list of files created by a specific process in the current path.	*quicksearch /p winword.exe* Retrieves a list of files created by the winword.exe process in the current path.

15.3.3 Check Process

tasklist command: Lists all currently running tasks (including services).

Additional options can be found through the command help (tasklist /?)

command	Description
tasklist	Displays a list of processes (image name, PID, session name, session, memory usage)
tasklist /v	Displays detailed job information. (Image Name,PID, Session Name, Session, Memory Usage, State, Username, CPU Time, Window Title)
tasklist /m module name	List all jobs using that exe/dll name. Lists all loaded tasks if no module name is specified. (If no pattern name is entered, image name, PID, and module information are displayed)
tasklist /svc	Displays the services hosted by each process. (image name, PID, service)

CHAPTER

SIXTEEN

SYSTEM

System can make environment settings necessary for maintaining and operating Genian Insights E System.

16.1 System shutdown and reboot

Warning: To avoid damaging the System, do not manually power off the device before removing power to the device or properly shutting down service.

16.1.1 Power Control via Command Line Interface (CLI)

See: *CLI(Command Line Interface)*

1. Connect to the Policy Server through the Command Line Interface (CLI).
2. Go to Global Configuration mode.
3. work:
    - Reboot: Enter the command **restart system** or **reboot**
    - Shutdown: Enter command **shutdown** or **halt**

Note: After performing the shutdown command, the device will remain powered on, but it is safe to power off manually.

16.2 CLI(Command Line Interface)

For Command Line Interface (CLI) access to the Genian Insights E System, you must use an SSH client.

If you are unable to connect this way, you will need to log in to the web console and set an IP address accessible to the System. See "Allow remote access via SSH" in /system/default-settings-appliance.

16.2.1 Connect to CLI(Command Line Interface)

Attention: SSH access is only allowed from authorized IPs. See /system/default-settings-appliance to add accessible IPs.

The policy server can be connected through a dedicated SSH client or a utility that supports SSH.

1. Set up an SSH connection to the Policy Server IP address using standard procedures for the utility of your choice.
2. Log in with your Genian Insights E Users name and password.

16.2.2 CLI command

When accessing CLI (Command Line Interface), you can check the basic system status and supported commands in console mode. This article explains how to use the commands in console mode.

Basic commands

Command	Description
enable	Activate Global Configuration mode
exit	CLI service shutdown
help	command help
history	Display command usage history
quit	Terminate the console mode connection
configure terminal	Immediately apply commands set in Global mode
configure batch	Apply after rebooting the command set in Global mode
clear arp	Initialize system arp table information
clear screen	Initialize the console display
clock set	System Time Manual Settings
do backup	Perform System Backup
do cdbackup	Backup the most recent backup data to CDR
do cdrestore	Recover with Backup data stored on CD
do initdisk	Perform external disk initialization
do restore	Recover with backup data
geniup	If Genians Update Server is set up, perform an upgrade with the latest files on the server.
halt	System power down mode
kill pid	Terminate process based on pid
kill pname	Terminate process based on name
ping	Test ICMP request for IP of remote device
reboot	Perform system reboot
restart system	System service restart
shutdown service	System service shutdown
traceroute	Show routing path to IP
show	Display items that can be viewed with the show command

view command

Command	Description
show arp	ARP table information display
show backup	Display a list of backed up databases
show configuration	Display the current settings of the system
Show cpu	display cpu information
show filesystem	Display filesystem information
show hosts	List hosts file
show interface	Display system's network interface information
show logging	Display the most recent log among logs registered as GENIAN equipment with log ID
show memory	Display memory information
show processes	Display of running process information
show route	Display routing table information
show time	Current System time display
show uptime	System operation time information display
show version	System software version information display

16.3 Network configuration

You can change the interface IP address through the command line interface (CLI).

16.3.1 Change interface IP address

You can change the IP address of any interface through the CLI Console.

Step 1. Change the interface IP address

1. After logging in to the CLI Console, go to Config mode.
2. Enter "interface eth0 address [IP address] [subnet mask]" as shown below.

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

Step 2. Confirm the interface IP address change

1. Enter "show configuration | grep interface eth0" as shown below.

```
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
```

16.4 Backup and Restore System

It can be set to backup at a scheduled time, and can be restored using the backup file in case of a system failure.

16.4.1 Backup settings

You can set to back up at a scheduled time, and set to keep the backup file in the storage device.

Schedule backups at specified times

1. Go to **Admin > Settings** in the top panel.
2. Go to **Backup** in the left preferences panel.
3. Set whether to perform backup to **On** for backup scheduling.
4. To repeat the backup, specify the **Daily at**.
5. Specifies the **Space Threshold** to ensure the minimum space required for the backup.
6. Click the **Update** button.

Configure storage type

1. Go to **Admin > Settings** in the top panel.
2. Go to **Backup** in the left preferences panel.
3. Locate Storage and select the appropriate **Repository Type** from the drop-down.
4. Click the **Update** button.

storage type	Description and settings
local disk	Perform a backup to the policy server disk.
external storage	Backup to an external disk connected to the policy server by USB type.
CIFS storage device	Perform CIFS backup using the Windows sharing function.
NFS storage	Perform backup by mounting the directory of Unix or Linux file system.
FTP SERVER	Transfer the backup file through FTP (File Transfer Protocol). (For security reasons, it is not recommended because the password is transmitted in plain text)
SFTP SERVER	Transfer the backup file through SFTP (Secure File Transfer Protocol). (For security, it is recommended to perform encryption/decryption based on SSH)

16.4.2 Restoring from an existing backup file

In case of system failure, backup data can be restored. You must have CLI access to perform this restore process.

Find and restore backup files

1. After logging into the Web Console, click **System > System** on the top menu.
2. Go to **Preferences > Backup** in the left menu.
3. Click the **Download** button.
4. After copying the backup file to be restored from the list, close the connection.
5. Access the Policy Server console through CLI.
6. Enter **enable** and **Users Possword Policies** to go to **Global Mode**.
7. "restore<filename> all" to restore the backup data.

16.5 External Send Email Server Settings

This feature allows receiving Settings from the Users profile, and supports Threats Report notifications and disk utilization alarms by email.

16.5.1 Email Account Settings

1. Go to **System > Settings** in the top menu.
2. Go to the **Preferences > System** panel on the left, go to the **Email Server** section.

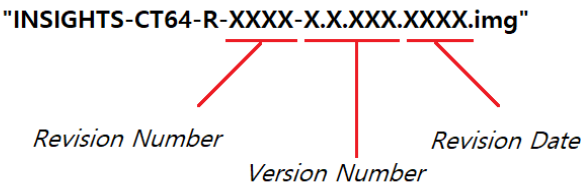
Mail Server Settings

1. **Server Address:** Server Address (*Example: smtp.gmail.com*)
2. **Server Port :** Enter the port number. (*Example: SSL = 465, TLS / STARTTLS = 587*)
3. **Sender address:** Sender's address field (E-mail address to be displayed in **)
4. **Sender Name:** Enter the sender name (the name you want to display in **)
5. **SSL Connection** (On when using *SSL port*)
6. Enter your user name in **Authenticated User**.
7. For **AuthenticationPossword Policies**, enter Possword Policies and re-enter.
8. Click the **Update** button.
9. Click **Send** to send the e-mail by entering the sending address, subject, and content of the e-mail.

16.6 System Software

System software (Policy server and agent) can be System. A software package is divided into four parts: name, revision number, product version, and revision date.

- **INSIGHTS-CT64** Policy Server Software
- **NAC-ThreatDetector2** agent software
- **GenianInsights_ServerIP.exe** Single version agent software



16.6.1 Policy Server Update

You can update the policy server through the web console.

Manually update the policy server

Download the Genian Insights E software, save it locally on your computer, and then upload it to the server to perform the update.

Prepare System file to upload:

1. Prepare an .img file that starts with **INSIGHTS-CT64** .
2. After logging into the Web Console, go to **System > System > Software > System OS**.
3. Click the **Product Upload** button to display the file selection button. Click the **Select File** button to upload the prepared file.
4. When the file upload is complete, click **Start Upgrade**.

After system upgrade, it automatically reboots, and when normal service starts, it switches to the Users login page of the system console.

Update via Command Line Interface (CLI)

Using command: **geniup**

For more information, please refer to *CLI(Command Line Interface)*.

16.6.2 Agent update

You can update the agent by uploading the updated gpf file through the web console.

Agent update

1. Connect and log in to the agent system server.
2. Go to **System** in the top panel.
3. In the left System panel, go to **Update > Software > Plugins**.
4. Select the **Tasks > Upload Plugin** menu and click the Select File button to upload the latest gpf file starting with NAC-ThreatDetector2_*.
5. Click **Upload**.

Note: Agent updates are sequential according to the node policy update cycle of the agent system server (Genian NAC server).

16.7 Environment Settings in the System console

You can configure the web console screen with the settings you want.

16.7.1 web console

1. Go to **System > Settings** in the top panel.
2. Go to the **Preferences > Web Console** tab in the left panel.

In Basic Settings, you can set the session time, number of columns to be printed per page, web browser title text, logo file, and date time format.

- When setting **Session Timeout** and Session Timeout, the user account is automatically logged out after a certain period of time, and the timeout time is renewed when moving between pages (up to 10 minutes)
- **The number of output columns per page** , The number of columns to be output in the table list is set to 30 by default.
- **Browser Tab Name** , you can set the title of the web browser, and the default value is Genian Insights.
- **Company Logo Image** , Changes the logo image in the upper left corner when users log in and the Genian Insights logo image in the login page. The recommended size is 328 horizontal and 50 vertical pixels.
- **Date Time Format** , You can set the default date and time format to be printed on the web console.

Login screen Settings allows you to customize login-related information.

After logging in, set whether to display user information, change the text and header image of the login screen, and select whether to activate the ID save function.

- **Displaying User Information** , Sets whether to display information of logged-in users in the upper right corner.
- **HTML Message for Login** , Users can set the text to be displayed on the login page.
- **Header for Login Page** , Select whether to use the login page screen header. You can change the color or change the background image. If only header image is used, the maximum size is 380 horizontal and 270 vertical pixels.

- **Displaying 'Save Username'** , Users can select whether to use the Save ID checkbox on the login page screen.

In Dashboard Settings, you can set the number of columns that determine the horizontal size of the Dashboard or the spacing between widgets.

- **Number of Columns** , Set the default number of columns that compose the grid in Dashboard. Default: 24
- **Widget Margins** , Set the widget spacing that composes the grid in Dashboard.
- **Immediate Saving Widget Layout Changes** , Set whether to save immediately when changing the position and size of the Dashboard widget. Default: On
- **Number Rows Limit in Excel Export** , When exporting data to Excel from the Discovery menu, the maximum row value is set. Default: 10000

CHAPTER

SEVENTEEN

SERVER PLUGIN INTEGRATION

Genian Insights E can collect threat information data from external servers in addition to the basic threat information and utilize it for threat detection.

It can be used only for customers who have products that support external linkage, and linkage for the following products is supported.

- KISA C-TAS
- ReversingLabs A1000
- TrendMicro DDA
- SandBlast TE1000X

17.1 Server plugin linkage Settings

From version 2.0.11, the following plug-ins are automatically installed on the server when the product is installed, and basic information required for linkage is required.

- KISA C-TAS
- ReversingLabs A1000
- TrendMicro DDA
- Check Point SandBlast TE1000X

17.1.1 KISA C-TAS interworking

It provides an interworking function with the Cyber Threats information analysis-sharing system (C-TAS) provided by KISA. It can be used only for customers who have signed up for C-TAS and have been provided with a key for interworking, and Genian Insights E server requires a change to IOC DB Framework version v2.

Item	Description
Export Key	Enter the Export Key information assigned by KISA.
Code(orgKey)	Enter the organization code (OrgKey) information assigned by KISA.
Sync interval	Sets how many minutes the data received from C-TAS is registered in the IOC Database (default: 30 minutes)
IP address expiration date	Sets the retention period of the IP addresses collected by Link Settings. (Default: 10 days)

1. From version 2.0.11, the C-TAS plug-in is installed together when installing the product. If installed normally, you can check the KISA C-TAS linkage settings in the **System > Settings > Perferences > Threat Detection & Response** menu.
2. Change the linkage status to **Use** and enter the linkage information and additional information provided by KISA.
3. After entering information, click the check button in the upper left corner to save the settings information.
4. Go to **System > System > Software > Server Plugin Management** menu, check CTAS in the plug-in list, and click the 'Immediate execution' button on the right to perform the linkage.
5. Receives data from C-TAS every cycle set in 2 and updates it in the IOC Database.
6. When a threat is detected with information registered in C-TAS, it is displayed as CTAS in the Feed information of the Threat2 index.

17.1.2 Integration with ReversingLabs A1000

Threat Analysis using ReversingLabs A1000 is provided. (Applicable to ReversingLabs A1000 customers) By sending the file information present in the Threat2 index to ReversingLabs A1000, you can request analysis for malicious code and check the result on the Genian Insights E server.

Item	Description
URL	Settings for ReversingLabs A1000 product IP or URL information.
USER-NAME	USERNAME information for ReversingLabs A1000 product linkage.
PASS-WORD	PASSWORD information for reversingLabs A1000 product linkage.
Link result	Displays the status of interworking with ReversingLabs A1000 products. If communication is successful, 'Linked' is displayed.

1. Starting with version 2.0.11, ReversingLabs A1000 plug-in is installed when installing the product. **Go to the System > Settings > Perferences > Threat Analysis** menu, change the **ReversingLabs A1000** Settings to ON, enter the URL and account information, and click the 'Check' button at the top left to view the settings Save.
2. After ThreatsAnalysis, click the Threats Analysis button on the left side of the **Analysis > Management** menu list to go to the Threats detail screen and click the 'Threats Analysis Results' button on the upper left.
3. You can check the Threats Analysis Report for each integration plug-in.

17.1.3 TrendMicro DDA integration

Threat Analysis using TrendMicro DDA is provided. (Applicable to customers who have TrendMicro DDA, and the compatible version is Deep Discovery Analyzer 6.1.) By sending the file information that exists in the Threat2 index to TrendMicro DDA, you can request analysis of whether it is malicious code, and check the result on the Genian Insights E server.

Item	Description
API Key	Sets the API key information provided by the TRENDMICRO DDA product. The API key is provided on the About screen of the Help menu of the DDA product.
URL	Enter the TRENDMICRO DDA product IP or URL.
Time Zone	Sets the time zone used by the TRENDMICRO DDA product.
Link result	Displays the linkage status with TRENDMICRO DDA products. If communication is successful, 'Linked' is displayed.

1. From version 2.0.11, TrendMicro DDA plug-in is installed together with product installation. **Go to the System > Settings > Perferences > Threat Analysis** menu, change the **TrendMicro DDA** Settings to ON, enter the integration API Key, URL and time zone information, and click the 'Check' button at the top left to save the settings information.
2. After ThreatsAnalysis, click the Threats Analysis button on the left side of the **Analysis > Management** menu list to go to the Threats detail screen and click the 'Threats Analysis Results' button on the upper left.
3. You can check the Threats Analysis Report for each integration plug-in.

17.1.4 Check Point SandBlast TE1000X interlock

Threat Analysis using Check Point SandBlast TE1000X is provided. (Applicable to customers with Check Point SandBlast TE1000X) By sending the file information that exists in the Threat2 index to Check Point SandBlast TE1000X, you can request whether it is malicious code or not, and check the result on the Genian Insights E server.

Item	Description
URL	Enter the Check Point SandBlast TE1000X product IP or URL.
Version	Enter the Check Point SandBlast TE1000X product version (Example: v1)
API Key	Check Point Sets API key information provided by SandBlast TE1000X product.
Link result	Check Point SandBlast TE1000X Displays the linkage status. If communication is successful, 'Linked' is displayed.

1. From version 2.0.11, Check Point SandBlast TE1000X plug-in is installed together when installing the product. Go to the **System > Settings > Perferences > Threat Analysis** menu, and change the **Check Point SandBlast TE1000X** Settings to ON
2. After entering the URL, product version, and linked API Key, click the 'Check' button at the top left to save the settings information.
3. After ThreatsAnalysis, click the Threats Analysis button on the left side of the **Analysis > Management** menu list to go to the Threats detail screen and click the 'Threats Analysis Results' button on the upper left.
4. You can check the Threats Analysis Report for each integration plug-in.

17.1.5 Update Server Plugin

Add plugin

1. Go to **System > System > Software > Server Plugin Management** and click the 'Add' button to upload the external linkage plug-in (extension gpp) file.
2. After checking whether to use the file list in the field whether to use it first, click the 'Immediate' button on the right side of the screen.
3. A blue icon is displayed in the **Status field** if it is operating normally.

Delete plugin

1. Select the plug-in list to be deleted and click the ‘Delete’ button.
2. A pop-up window to confirm deletion of the plug-in appears, and if you click OK, the plug-in is deleted.

CHAPTER

EIGHTEEN

GENIAN NAC INTERWORKING

If Genian NAC is being operated, NAC audit logs and various asset information and network information collected by agents can be monitored by linking with Genian Insights E server.

In addition, GsAgent can be easily deployed as a plug-in to the NAC agent.

18.1 Agent installation

Agent collects all events that occur on an endpoint and takes control upon threat detection. The agent can be installed on Windows OS through the agent installation page of Genian NAC.

18.1.1 Windows Agent installation

Agents in Genian Insights E can install **agents** on Windows devices via the Captive Web Portal (CWP) of the Genian NAC Policy Server.

Windows agent installation

- *Download and install via agent download page*
- *Verify Windows Agent installation*
- *Where to find agent logs on Windows devices*

Download and install via agent download page

1. Download Agent
   - https://(*IP or FQDN*)/agent
2. Select agent: Do not rename the file to avoid name conflicts.
   - Windows installation Users version: **GnUpdate_** (*IP or FQDN*) .exe

---

Note: The installer cannot be run if the user does not have permission to install the file, so when installing the file, you must run it as Users.

Verify Windows Agent installation

1. Log in to the Web Console and select **Analysis > Management**.
2. If the agent is installed and running on the node, a blue icon is displayed along with the node information.

Genian agent menu

1. Go to **Systray** on your Windows device.
2. Locate the **Genian Agent icon** and right-click on it.
3. You can use the listed options to:
    - **View Announcements:** Shows current announcements from Users.
    - **View Notification Messages:** Displays current messages from Users.
    - **Check my status :** Go to the **Captive Web Portal (CWP)** page.
    - **Genian Insights-Detected Threats :** You can check the processing results (notification, quarantine, process termination) and view detailed information for files detected as Threats.
    - **Authentication Integration (L):** Allows users to log in and displays the CWP page upon successful login.
    - **Disable Authentication Integration with (O):** Allows user to logout.
    - **Authentication Integration Information:** User can view account information upon successful login.
    - **Network Connection Information:** Allows users to view active network connection devices.
    - **USB Device Information:** Allows the user to view the USB information of the device.
    - **Remote Agent Delete:** (*Users cannot delete installed agents, Users must do this.*)
    - **Program Information:** The user can view the latest information about the installed Agent.

Where to find agent logs on Windows devices

1. Open **File Explorer** on your Windows device.
2. Navigate to the folder **C:\Program Files\Geni\Insights\Logs**.

18.2 NAC Collection Settings

Genian Insights E can collect audit log information in real time through linking with Genian NAC server and monitor the status of the NAC system in real time.
In addition, you can install an agent on Endpoints, collect asset information on Endpoints, monitor major actions occurring in Endpoints, and save and analyze in real time.

It is broadly classified into event collection by interworking between servers and agent installation, and several preliminary preparations are required to collect various information.

18.2.1 Environment Settings for Information Collection

Agent Actions:

1. Prepare a .gpf file that starts with **NAC-ThreatDetector2** .
2. From **System > Update**, go to the Plugins menu.
3. Double-click the gpf file prepared by clicking **Tasks-Upload Plugin** and clicking the **Choose File** button.
4. When the file name is displayed on the screen, click the **Upload** button to upload the file.
5. Go to **Policy > NodePolicy > NodeAction**.
6. Click the **Tasks -Create** menu, enter an action name, and then select the **Plug-in-Threat Detector2** item in the Settings section to enter basic information and click the **Create** button.

Server Actions:

1. Log in to the NAC web console, and click Policy Server IP in the **System > SystemSystem** column.
2. In the **Environment Settings** tab, change the **Use or not in the **SNMP Agent Settings** section to On**, enter the **username** and click the **Edit** button.
3. Access the NAC CLI and set the IP that allows external access to the database.

> **Warning:** The MySQL service on the NAC server will be restarted when IP settings are approved

4. On the Roles screen, check **insightsConnector** and save it.

Note: insightsConnector can only be set in NAC Server version 4.0.1X,5.0.

---

5. You can see that the insightsConnector account has been created in **Settings > User Authentication > Roles**.
6. In the **System > Users** column, click **Tasks -> User Registration**.
7. Set the System role to **insightsConnector** and create a user.
8. In the **UsersSettings** tab, click the Create New Key button of the API Key item to create and save a new API.
9. Create a **nodegroup** to select the nodes on which to install the plugin.
10. Create a **Node Policy** to assign the node group created above.
11. Assign and save the Threat Detector2 action.
12. Click **Apply ChangePolicy** in the upper right corner.

18.2.2 NAC audit log collection

Environment Settings for information collection Once completed, Settings to get NAC audit logs from Insights E server are required.

1. Log in to the Genian Insights E web console and click **GENIAN NAC** in the drop-down menu of the **Configurator** located in **System > Collector Settings > Collector Sets**.
2. On the Add Collector Automation screen, enter information and click the Save button.

- **Collector Sets name:** Collector Sets name and Collector Sets description are the values displayed in the Collector Sets field.

- **Server hostname:** The server string that will appear in the log. - **Center Address:** Enter the Genian NAC Policy Server IP and the Genian NAC DB Server IP in the DB Server Address. - **DB user name and PASSWORD:** Enter the user name and PASSWORD of the NAC DB server.
- Select **Audit Log** from the information to be collected and save it.

3. Click the **Start** button of the added Collector Sets in the Collector Sets field. If the NAC log collection (syslog) in the collector starts normally, you can see that the **Genian Insights** filter is created in **Log > Search Filter** in the Genian NAC web console. At this time, Insights<-> NAC-to-NAC communication CHARSET must be 'UTF-8'.

Note: In version 4.0.X, the following 4 steps are separately required for NAC server event processing after automatic search filter creation.

---

4. Click on the generated Genian insights filter name as shown below.

5. Click the **Edit** button at the bottom left. The insights filter detail screen is displayed on the right. If you click the **Edit** button once more, syslog transmission starts from that point.

6. Whenever an audit record is generated from the NAC server, data is sent to the Insights E server through syslog, and the log can be viewed in the Insights E web console **Discovery > NAC logs** menu.

18.2.3 NAC asset information collection

When the environment settings for information collection are completed, you can access the NAC server database from the Insights E server and collect various asset information of Endpoints.

1. Log in to the Genian Insights E web console and click **GENIAN NAC** in the drop-down menu of the **Configurator** located in **System > Collector Settings > Collector Sets**.
2. On the Add Collector Automation screen, enter information and click the Save button.

- **Collector Sets name:** Collector Sets name and Collector Sets description are the values displayed in the Collector Sets field.
- **Server hostname:** The server string that will appear in the log. - **Center Address:** Enter the Genian NAC Policy Server IP and the Genian NAC DB Server IP in the DB Server Address. - **DB user name and PASSWORD:** Enter the user name and PASSWORD of the NAC DB server.
- Select the asset information to be collected from the collection target information and save it.

3. Click the **Start** button of the added Collector Sets in the Collector Sets field.
4. Asset information is collected according to the collection cycle set by default, and the log can be checked in the Insights E web console **Discovery > NAC Assets** menu.

CHAPTER

NINETEEN

FAQ

19.1 When is the product release cycle?

Genian Insights E releases a new version every month.

19.2 Can I downgrade the software version?

No, downgrade is not supported. In case of downgrade, you need to create a Backup before upgrading, then reinstall the software and restore the Backup data.

19.3 Is communication between each component encrypted?

Yes, communication between each component is encrypted via TLS.

CHAPTER

TWENTY

TROUBLESHOOTING

20.1 Debug Collection and Symptom Analysis

20.1.1 Memory dump analysis when BSoD occurs

When BSoD occurs in Endpoints, you can guess the cause by following the procedure below.

If the Insights-related driver file name is checked on the BSoD screen

1. Collect %windir%memory.dmp and agent full log and make an analysis request.
2. Conversely, if another product driver name is displayed on the BSoD screen, a cause analysis request is made to the corresponding product developer.

If the driver file name is not confirmed on the BSoD screen

Install the necessary Analysis program to determine which driver files are causing the problem.

1. **windbg installation:** windbg is the `windows sdk<https://docs.microsoft.com/en-us/windows-hardware/drivers/debugger/debugger-download-tools> You can install it via `_ . (When installing windows sdk, select only "Debugging Tools for Windows" among the elements to be installed and uncheck the rest)
2. **Open dump file:** After installing windbg on a PC with internet access, try to open %windir%memory.dmp in windbg. (After setting read permission in memory.dmp, drag it to the windbg window.)
3. **Symbol path Settings:** When the dump is opened, execute the following command.

```
.symfix+
.reload
```

4. **Run Automatic Analysis:** Carefully read the Analysis report that is output after running !analyze -v.

If there is a part (MODULE_NAME) like the one below in the analysis result, it is most likely that this driver is the problem. If the problem driver is identified, request the cause analysis from the driver developer.

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

(continues on next page)

(continued from previous page)

```
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 <<< This part!!
IMAGE_NAME:  check64.sys
...
```

If you have identified a suspicious driver name, but cannot determine the exact information about this driver, you will need to find the driver file on your PC to verify the information. For example, if the resolved driver name is f_ih.sys, you can check the driver location (Image path) with the lmvm command. You can infer the developer by finding the driver file and checking the registration information.

```
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. If the !analyze -v result does not identify the suspect driver, look carefully at the CallStack section.

```
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]
ffffbd05`dfd57b10  : nt!PspSystemThreadStartup+0x55
ffffbd05`dfd57b60  : nt!KiStartSystemThread+0x28
```

Each entry in Callstack has the following meaning:

```
[Address/argument, etc. hexadecimal] : [Module name] ! [Address in the module /␣
↪Offset]
```

For example, the entry below means the KiStartSystemThread+0x28 memory address of the nt kernel.

```
ffffbd05dfd57b60  : nt!KiStartSystemThread+0x28
```

Callstack means the function called first at the bottom and the function called last at the top. We go through the callstack from top to bottom, starting with the module that was called later. In this case, it is most likely that the first module that appears among the non-components of Windows is causing the problem. For example, in the Callstack above, modules appear in the following order:

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

Among these, nt and hal are components of windows, so check64, which appeared first among non-windows modules, is the module that caused the problem. Windows module names that appear frequently in Callstack are as follows.

Table 1: windows module name

module name	role
nt	Windows Kernel
hal	H/W director
io	IO manager
netio	Network I/O Subsystem
fltmgr	Filter manager
ob	Object manager

If you find a suspicious module, check the path of the file with the lmvm command, and check the information such as Investigation in the file's properties or digital signature information. If the identified suspicious module is an Insights-related module or a Windows-related module, collect %windir%memory.dmp and agent logs to request cause analysis.

CHAPTER

TWENTYONE

RELEASE NOTE

It provides a release note containing notes on upgrading Genian Insights E and new changes from Genian Insights E V2.0 version.

The contents of the release notes are intended for users of Genian Insights E, and distribution to non-Genian Insights E users is not permitted.
The contents of the release notes are subject to change without notice due to product improvement.

21.1 Upgrade Guide

21.1.1 Precautions

- Before upgrading, be sure to read the upgrade guide and release notes thoroughly and check if there are any problems before proceeding.
- Product downgrade is not supported. In case of downgrading the product, it may malfunction due to DB table changes performed in the higher version. If downgrade is unavoidable, you must restore the DB with the backup file created in the downgrade version and use it.
- When upgrading the policy server and DB, it is recommended to perform a backup.
- If the version difference between the existing version and the upgraded version is large, the upgrade may take a long time due to migration caused by a large number of DB table structure changes. At this time, when accessing the CLI console, a message indicating that DB migration is in progress is displayed. In the case of migration, the service must never be stopped or the equipment must be rebooted.

21.1.2 How to upgrade policy server

Genian Insights E can be upgraded from the Web Console.

Progress using WEBUI

- After uploading the .img file to **System > System > Software > SystemOS** , and then click the Upgrade Start button. When the upgrade is complete, you will be directed to the login page.

21.1.3 How to update agents (performed by Genian NAC)

After upgrading the policy server, the agent must also be updated. Upload the Threat Detector2 plug-in by selecting System > Agents > Upload plug-in to plug-ins.

Plug-in updates are automatically performed according to the System Policy operation cycle set in Genian NAC.