TEIREN CLOUD SIEM

Cloud Threat Detection Solution
through correlation analysis

Teiren

Contents

01
About Teiren

TEIREN 소개

Teiren

Combination of **Tera Byte + Siren**,
It is meant to analyze security threats in the Tera Byte unit and remind users of security like Siren.

Teiren works together to create innovative solutions that are faster and more comfortable to manage data and detect threats, with the entire team participating in development and compliance analysis.

Teiren Members

All of the team members are from the Best of the Best, a next-generation security talent training program organized by the Ministry of Science and ICT. We gathered to improve the country's cybersecurity.

CEO
김성연
Kim SungYeon

BS in Security Information
Bob 11th Consulting
CEO / Front-end

Developer
성유원
Sung YuWon

BS in Computer Science
Bob 11th Development
Back-end / ML

Researcher
이현경
Lee HyunKyung

BS in Security Information
Bob 11th Consulting
Rule Modeling / ML

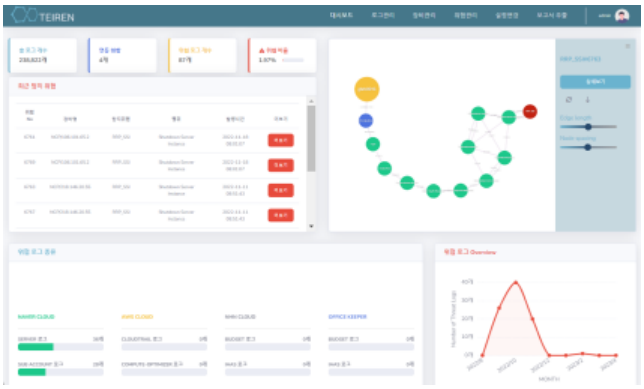
Researcher
조소망
Cho SoMang

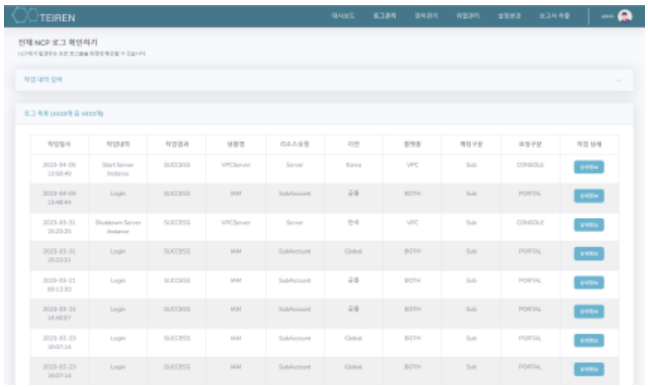
BS in Industrial Security
Bob 11th Consulting
Visualization / Web

02
About SIEM

About SIEM

What is SIEM?





SIEM stands for **Security Information & Event Management**, a solution that collects and integrates all *logs about corporate assets.

Threats can be detected in a variety of areas, including cloud resources, applications, and external threats. SIEM reports of threats, vulnerabilities, attacks, or suspicious behavior to enable immediate response. In other words, SIEM provides an integrated security framework by integrating and analyzing log data in various areas.

Recently, many products have been introduced to perform security management. The overall solution for security management as well as log collection and integration is called **SIEM**.

*log : all records of what and when the system was used

Why Enterprises Use SIEM

The use of SIEM is a requirement, not an option, because of the compliance with legal requirements and efficiency of security mangers

Security Manager's Work Efficiency

From the perspective of security managers who use SIEM, managing data from on-premises systems and various security equipment on a daily basis and analyzing threats against it is time consuming and inefficient.

SIEM, which integrates logs across the entire system and provides security management, can improve the efficiency and convenience of security managers.

Compliance with Legal Requirements

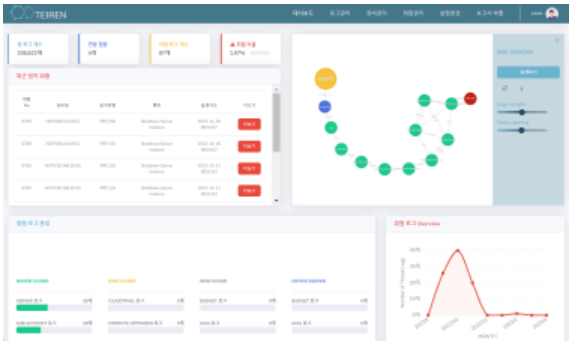
Laws such as Privacy Measures, Information and Communication Network Act, and the GDPR require regular log checks to maintain stable system status and identify external attacks.

For companies entering Europe, the GDPR law applies regardless of the size of the company, so SMEs may also need SIEM to check logs and identify external attacks.

03
Teiren SIEM

TEIREN SIEM

Teiren SIEM Dashboard

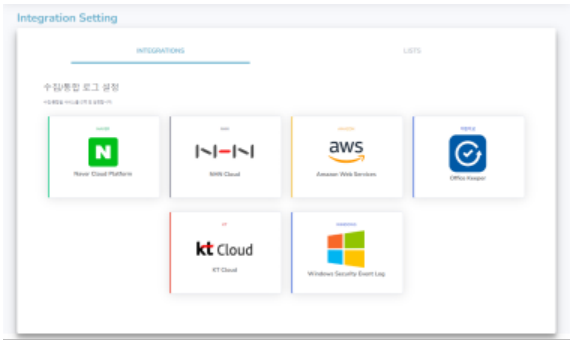


Dashboard Page

The Teiren SIEM dashboard allows users to monitor real-time threats by viewing the total number of logs and threat logs, threat rates, and recent detected threats.

It also provides real-time graphs of CPU, Memory, Network usage when using SIEM.

System Integration

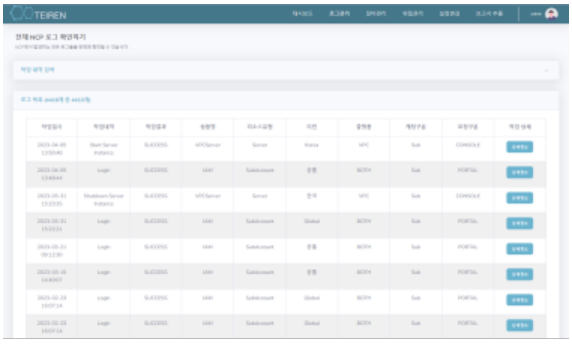


Integration Page

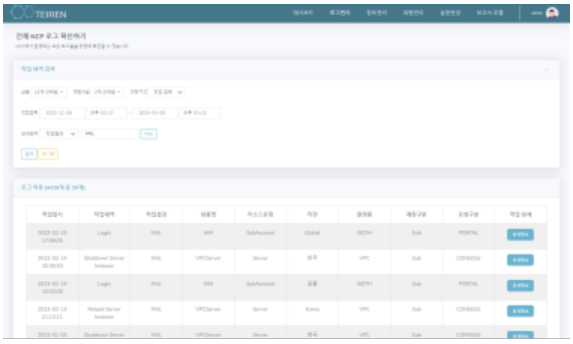
On the System Integration page, users can enter the API key to register various clouds and systems to be linked.

Currently, Teiren SIEM is integrating Naver, NHN, AWS Cloud, Windows Security Event Log, and Office Keeper (Jiran Security's DLP Solution).

Log Management



Log Output Page



Log Filtering

Log data is collected, integrated and provided as a table on the web. Users can view and understand the vast amount of log data collected from various clouds and systems at a glance. If the users want to see more details about the log data, they can also view it in JSON format, the original format of the log data.

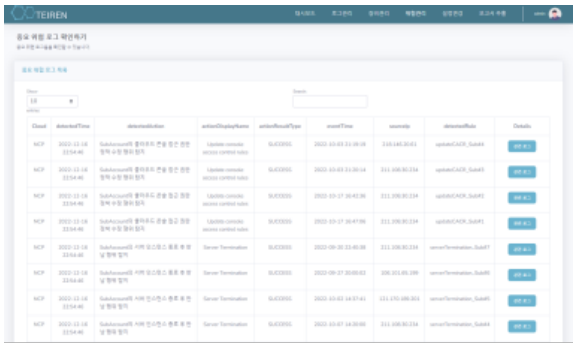
Users can filter and selectively view the logs among the large amount of log data collected. Log data can be classified according to selected values by selecting product names, accounts, and inquiry time respectively, and users can search in detail using regular expressions.

TEIREN SIEM

Threat Detection

Teiren SIEM enables advanced threat detection with improved performance with Graph DB.

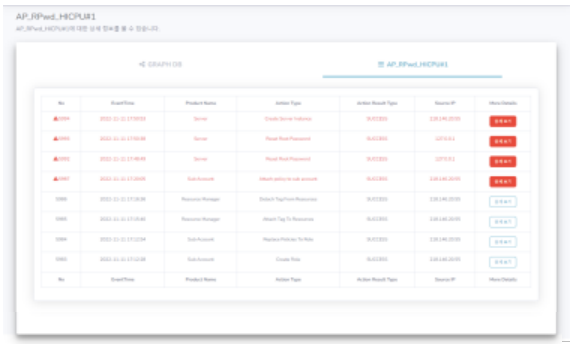
Security Rule Setting Page



Threat Alert

Users can set security rules for threat detection. By default, Teiren provides approximately 150 security rules, and the default rules alone enable simple threat deteciton. Users can control the default rules through on/off button, and can add rules directly by setting details to suit their environment. Threats detected in these rules can be found on the Threat Alert page.

Threat Flow Detection



Threat Detection

In addition, users can set the flow of multiple rules to detect threats based on the flow of behavior, not just one anomaly. This also allows users to add rules directly through flow specification.

Teiren SIEM visualizes and shows the flow of user behavior to the threat in a graph format so that it can be seen at a glance when detecting the threat. Moreover, detected threats are presented in a table format, along with related actions.

Graph Database

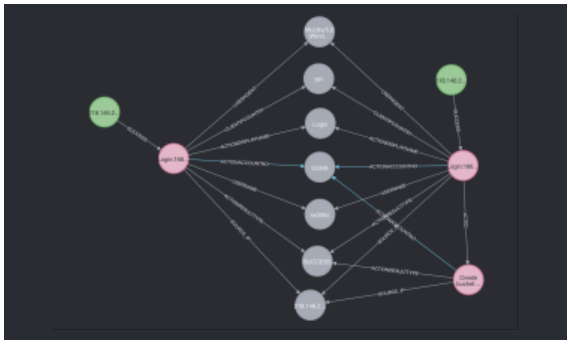
Graph Database is a graph theory-based NoSQL database that makes it easier to analyze vast amounts of data based on relationships between data.

It is possible to store the data in the form of a graph, with points and lines to represent the relationship between the data. In the event of a threat, you can easily search for associated nodes without an index, and you can visualize the graph to make the DB configuration easier to see at a glance.

TEIREN SIEM

Attack Path Visualization / Machine Learning

Threat Analysis Visualization



UEBA

Teiren SIEM visualizes flows from user nodes to detected security policies. Users can see what flow the detected threat is through and how it relates to the other actions of the user caused the threat, which enables to analyze correlation between them.

Furthermore, machine learning is performed based on the user's behavior pattern. It measures the similarity between each user behavior log and sends security notifications if an unusual pattern of behavior occurs.

Report

월간 보고서 요약(2023/02)

근 5개월 위협

날짜	2022/8	2022/9	2022/10	2022/11	2022/12	근 5개월 합계
위협개수	0	0	1	0	0	1

이번달 요약

내용	총 로그 수(개)	총 위협 로그 수 (개)	연동 제품 수(개)	총 위협 비율(%)
결과	238822	87	3	1.97

최근 탐지 위협 top 5

No	장비명/IP	탐지 위협	명위	
1	NCP/218.146.20.55	serverTermination_S	Server Termination	202
2	NCP/106.101.66.81	attachPolicyAccount	Attach policy to sub	202
3	NCP/106.101.65.2	serverTermination_S	Server Termination	202
4	NCP/106.101.65.2	RRP_SSH#1	Shutdown Server	202
5	NCP/106.101.65.2	RRP_SSH#2	Shutdown Server	202

탐지 로그 전체 리스트

정책명	행위 결과
Create Role	SUCCESS
Create Role	SUCCESS
Create Role	SUCCESS
Attach policy to sub account	SUCCESS
Attach policy to sub account	SUCCESS
Attach policy to sub account	SUCCESS
Attach policy to sub account	SUCCESS
Attach policy to sub account	SUCCESS
Attach policy to sub account	SUCCESS
Attach policy to sub account	SUCCESS

Monthly Threat Report.xlsx

Compliance Cerification Report

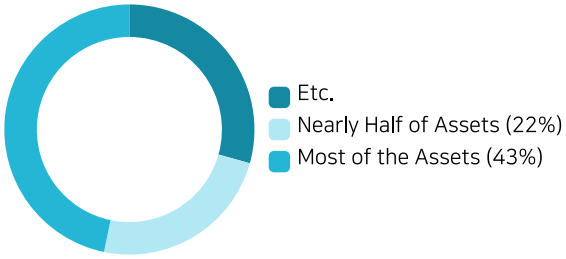
Teiren provides basic Excel threat reports. The report contains summary reports, logs detected by threats, and information about the status of the system integration.

Teiren SIEM provides compliance certification reports to ease the burden on security managers. Security managers spend at least two weeks on simple labor collecting evidence for security certification screening, such as ISMS-P. Taking advantage of SIEM's security management of the entire system, it identifies the compliance of the enterprise and provides a capture of the evidence.

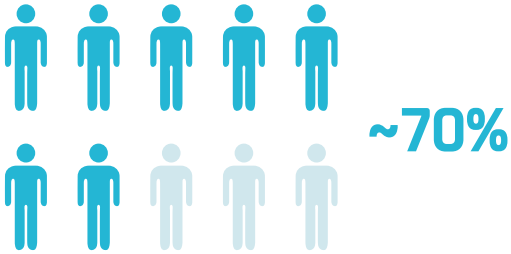
04
Teiren Business Plan

Problem

Problem of Existing Companies



Percentage of assets in the cloud

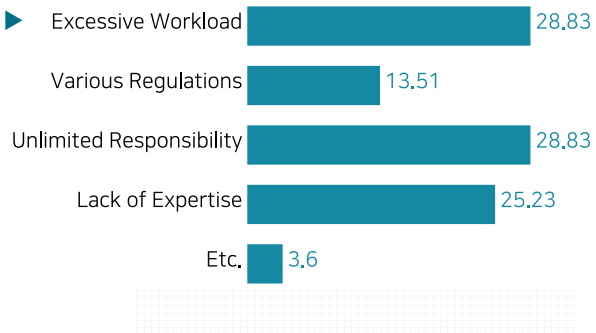


Experience attacks on unmanaged assets

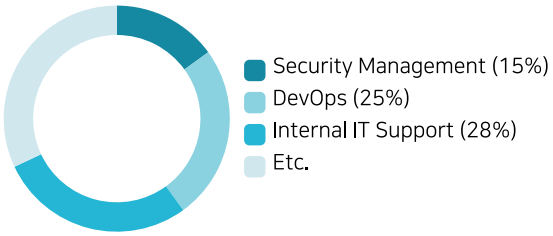
More than 40% of enterprises that adopt the cloud have the majority of their assets deployed in the cloud. This deployment of enterprise assets in the cloud has led to more events within the enterprise than ever before, and cyberattacks on assets that are not actually managed are also high.

[Source: 2021 MIT Technology Review Insight Survey]

This makes it even more difficult to understand where, which, and how this attack occurred when a cyberattack occurred, based on a different increase in corporate assets than ever before.
In other words, cloud adoption is increasing the challenge of responding to security.



Reasons of Security Manger's burden



Security Management is neglected due to other in-house IT support

Security managers responded that they felt a heavy burden on their security operations due to excessive workload. Furthermore, they had major difficulties due to lack of manpower and budget.

[Source: 2022 National Intelligence Service White Paper]

Additionally, small and medium-sized enterprise security managera say that security management is the most important aspect of their work, but other in-house IT support is making security operations and management is getting neglected. This indicates that small and medium-sized enterprises are also lacking in security management.

[Source: Jiran Security's Survey on Information Security of SMEs]

Solution

Graph DB, Detecting Attack Routes

With Graph DB, Teiren can solve the problem that was difficult to find an attack route.

You can see what logs are generated from the point of the attack, and you can visualize the flow of an attacker's behavior, such as creating the first log through the firewall, then logging into the Cloud and changing corporate policies.

Visualizing and showing the flow makes it easy for even less experienced security mangers to identify the attack route.

Benefits of Using Graph DB

By specifying relationships between data, data can be analyzed on a relationship basis.
Moreover, users can experiece improved performance of handling massive amounts of events, faster search speeds and faster data read-write effects.

Additionally, when we compared the search speed of Graph DB and SQL DB, we found that as the relationship increased, the search speed of Graph DB over SQL DB increased by 180 times, 1135 times, and more.

Improving security Manager's Work Efficiency with Compliance Certification Reports

Teiren SIEM provides compliance certification reports to ease the burden on security mangers.

Security officers spend at least two weeks on simple labor collecting evidence to undergo security certification screening such as ISMS-P. Leveraging SIEM's security management of the entire infrastructure, it confirms compliance with the enterprise and provides a capture of the evidence.

Teiren SIEM allows security managers to only review reports, by reducing time and increasing work efficiency.

Price Plan

Security manager first consider whether they have the budget for security solution. Threfore, Teiren SIEM introduced basic, standard, and premium monthly licenses as a solution to high cost of existing SIEM solution's permanent licenses. Compared to the SIEMs in the existing market, we wanted to increase accessibility by making it more reasonable in terms of price.

Basic

Account 100

Features
- Logs Collection
- Logs Filtering
- Policies Customizing
- Flow-based threat detection
- Attack Path Visualiztion

300,000₩/month

Standard

- 3개월 무료 체험 가능 -

Account 100 (*Additional Cost)

Features
- Logs Collection
- Logs Filtering
- Policies Customizing
- Flow-based threat detection
- Attack Path Visualiztion
- Compliance Certification Report
- Machine Learning + UEBA

1,500,000₩/month

Premium

Account 100 (*Additional Cost)

Features
- Logs Collection
- Logs Filtering
- Policies Customizing
- Flow-based threat detection
- Attack Path Visualiztion
- Compliance Certification Report
- Machine Learning + UEBA
- Threat Detection Customizing

Contact Sales Team

Why Teiren SIEM?

Threat Detection

Using Graph DB, Teiren SIEM can analyze based on the relationship between logs for more advanced threat detection.

Interworking between systems enables integrated security management through correlation analysis of the entire system and assets.

Increase Work Efficiency

In addition to multi-cloud environments, security solutions, systems, and more can be linked to Teiren SIEM to manage multiple environments simultaneously with one solution.

You can also increase the efficiency of your security managers with compliance reports for security certification.

Applicable

Teiren SIEM supports domestic (Korean) cloud services that currently lack support.

Teiren SIEM can be applied to not just SMEs, but also to Major National Information and Communication Infrastructure.

Target Market

Target Customer (SME)

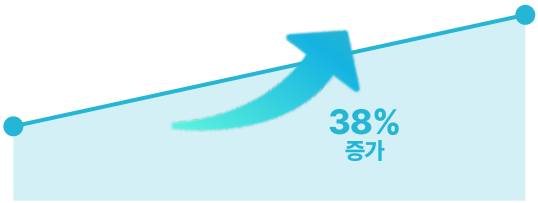
Due to the introduction of Covid-19 and **rapid increase in the online working environment**, **cyber attacks are intensively occurring against SMEs** that usually lack security infrastructure.

Security is becoming more serious as the damage spreads to the government/large enterprise, which has partership with SMEs. As a result, security laws targeting SME are also being strengthened.

Reason SMEs Should Use SIEM

According to Article 6 of the Privacy Measures Standard, **"In order to prevent illegal access and intrusion, proper operation and management of intrusion prevention and intrusion detection policies, prevention of log damage, etc. are required."**

Teiren wanted to contribute to improving the security of SMEs by providing them SIEM to comply with these laws and manage security.



Increasing the supply of security solutions for SME

ICT SME Information Protection Support Project

The strengthening of laws has increased the demand for security solutions from SMEs, and companies which provide security solutions for SMB, such as JiranSecurity and SecureLink, reported that there is a significant increase in solution supply. Accordingly, the government is also supporting SMEs to purchase security solutions.

Teiren would like to create and provide SIEMs firstly for SMEs with reasonable prices and great convenience to insufficient security manpower.

Strategy

General SMB
Basic

Most SMEs use the product simply to comply with the law on regular log checks and external attacks.

Teiren can offer products by introducing a Basic license that enables basic SIEM functions to be used at an efficient price of 300,000 won per month.

ICT SME/SME Dealing Personal Information
Standard

ICT SMEs and SMEs dealing with personal information have more data to manage than other SMEs and need to put more effort into security management as the Personal Information Protection Act is strengthened.

Teiren can provide Standard license to SMEs with fewer security managers to perform security management more efficiently with compliance.

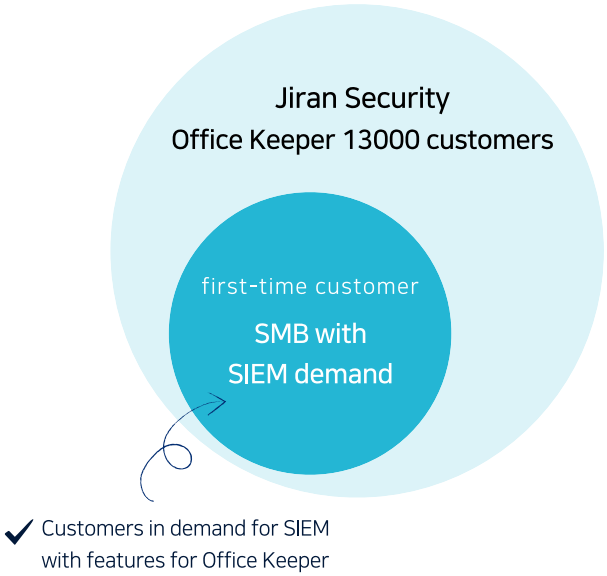
최초 고객 확보 전략

Jiran Security
Security software company founded in 2014

Teiren currently working with Jiran Security, and have received Office Keeper, a data leakage prevention solution, and have completed the integrating with SIEM.

Office Keeper
Office Keeper has ~13,000 customers in Korea. Teiren have confirmed that there is a demand for SIEMs with features for Office Keeper and is currently working on utilization plans for Office Keeper.

Most of Jiran Security's 13,000 customers are SMEs, which can be Teiren's target customers. Teiren wants to do a beta testing on them and get the first customer.



Channel Acquisition Status

Teiren have worked hard to secure various channels to attract customers. First, Teiren has secured a Jiran Security channel and is currently collaborating with them.

In addition, through meetings with various domestic and foreign companies such as Beyond Security, Coontec, and Megazone Cloud, Teiren will continue to identify customer needs and sell SIEM to related companies and their clients.

Future Plan

Scale-Up

After the stabilization stage for domestic SMEs, Teiren plans to enter B2G service for scale-up. According to KISA's guidelines for using major information and communication infrastructure as a cloud service, **"Infrastructure management organizations must establish cloud service facilities in Korea, process and store data in Korea, and use cloud services certified (ISMS) or equivalent."**

▲ Domestic and foreign SIEM
(sumologic, Datadog, splunk)

However, currently, domestic and foreign cloud SIEMs do not have the ability to support the major clouds in Korea. Therefore, there is an ironic situation that facilities using domestic clouds are perchasing separate security management for domestic clouds, even though they already are using SIEM.

To solve these problems, Teiren created a service that supports domestic clouds.

In order to provide B2G solutions, CSAP, a cloud security product certification, must be obtained, and Teiren will expand business to major national information and communication infrastructure after preparing for CSAP certification review from 2024.

Milestone

2023

- Startup Support Program
- Recruitment (Developer & Threat Detection Expert)
- Development complete
- Beta testing
- Gain first-time customer
- Generate revenue

2024

- Preparing for CSAP
- SMB Customer Expansion
- Particpation in ICT SME Security Support Project
- Sales of 1 billion Won

2025

- Enter Cloud Marketplace
- Expanding Customers to Larger Companies
- Sales of 5 billion Won

2026

- Obtain CSAP Ceritfication
- 8 billion Won in sales for larger companies

Teiren