TEIREN CLOUD SIEM

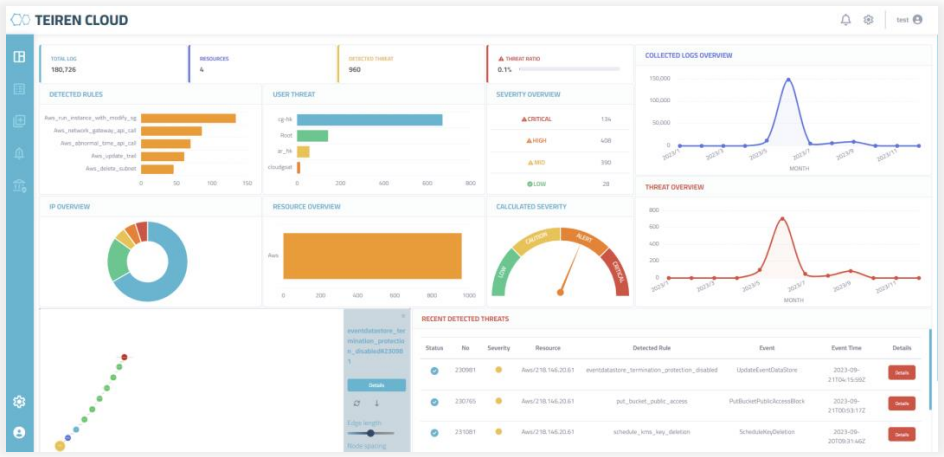
Visualize the Invisible

01
About SIEM

SIEM Introduction

About SIEM

What Is SIEM?



SIEM stands for Security Information & Event Management, a sophisticated solution designed to aggregate and integrate logs from all aspects of enterprise assets. This powerful tool enables the detection of threats across a broad spectrum, including cloud resources, applications, and external threat factors.

SIEM systems are engineered to identify threats, vulnerabilities, attacks, or suspicious activities as they occur, facilitating immediate response through detailed reporting. Essentially, SIEM provides an integrated security framework by consolidating and analyzing log data across various domains.

In recent developments, SIEM solutions have evolved to encompass security management, extending beyond mere log collection and integration. Today's SIEM solutions offer a comprehensive approach to security, covering both management and operational aspects. This ensures that businesses are not only aware of potential security incidents but are also equipped to manage and mitigate risks effectively.

Why Businesses Choose SIEM for Enhanced Security and Compliance

The adoption of Security Information & Event Management (SIEM) technology has become essential for businesses, driven by the need for operational efficiency in security management and compliance with legal requirements.

Enhanced Efficiency for Security Teams

For security professionals tasked with the oversight of corporate systems and various security devices, manually managing data and analyzing threats is time-consuming and inefficient. SIEM consolidates logs across all systems, offering an integrated approach to security management.

This not only boosts the efficiency of security personnel but also provides convenience, enabling them to focus on critical security tasks with improved effectiveness.

Compliance with Legal Requirements

Laws such as the Personal Information Protection Measures, the Information and Communication Network Act, and the GDPR mandate regular log reviews to ensure the stability of systems and to detect any external breaches. These regulations highlight the importance of maintaining a vigilant and proactive security posture.

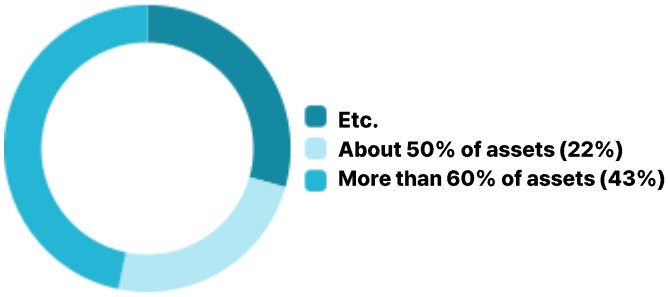
For businesses expanding into Europe, GDPR applies regardless of company size, necessitating the use of SIEM for both large corporations and SMEs to conduct log reviews and detect external attacks effectively.

02
Teiren SIEM

About Teiren SIEM

Problem

Current Challenges in Corporate Security

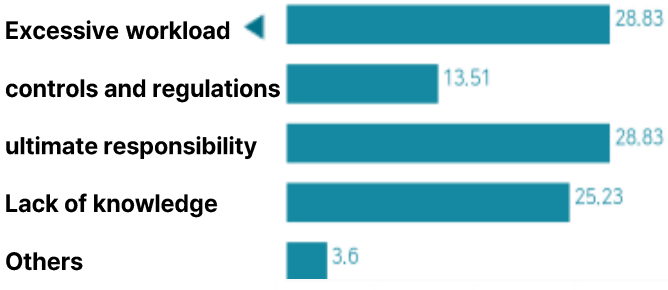


Cloud-based Assets

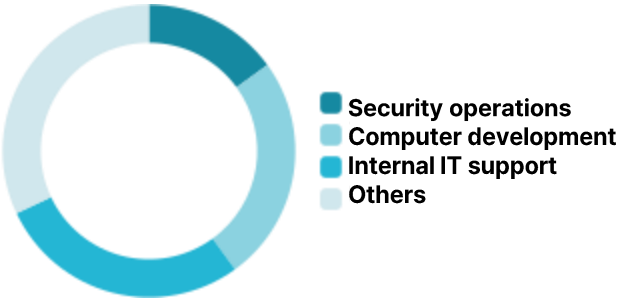
Experiencing Attacks on Unmanaged Assets

A significant portion of corporate assets remains unmanaged, making them vulnerable to cyberattacks. This issue has become increasingly prevalent with the adoption of cloud technology. More than 40% of businesses that have embraced cloud computing report having the majority of their assets hosted in the cloud. This transition has led to an increase in the number of events occurring within these environments, subsequently raising the proportion of cyberattacks targeting unmanaged assets. [Source: 2021 MIT Technology Review Insights Survey]

The shift to cloud-based asset management has introduced complexities in tracking the origin, method, and progression of cyberattacks. The expanded scope of security targets due to cloud adoption complicates the response to security incidents. In essence, the broadening of assets into the cloud has made it more challenging to identify and respond to cyber threats effectively.



Growing Workload of Security Team



Areas Impacted by Security Workload

Security officers are facing significant challenges in managing their responsibilities due to various factors. A notable portion of these challenges stems from the diversion of resources to other IT support tasks, leading to neglect in security operations and management. This has been highlighted by responses indicating that security personnel feel overwhelmed by their workload, exacerbated by a lack of manpower and budgetary constraints. [Source: 2022 National Intelligence Service National Cybersecurity White Paper]

Furthermore, security staff in small and medium-sized enterprises (SMEs) acknowledge the critical importance of security management within their roles. However, they report that attention to security operations and management is compromised due to the allocation of resources to other IT support requirements, indicating a prevalent issue of inadequate security measures within SMEs. [Source: JiranjiGyo SME Information Security Survey]

Solution

Threat Detection and Analysis

Teiren has revolutionized the way businesses handle the complexity of tracing attack paths through innovative changes in their database systems. By initiating from the point of attack, it becomes possible to trace the emergence of logs and their progression. This includes the creation of the initial log via the firewall, followed by actions such as logging into the cloud to alter company policies - all part of the attacker's modus operandi. These activities are visualized, making it significantly easier for security personnel, even those with limited expertise, to understand the root of the attack.

Moreover, leveraging graph databases has demonstrated a remarkable increase in speed, showing performance enhancements of up to 180 times, 1135 times, and beyond, especially as relationships within the data expand, compared to traditional databases.

Customization

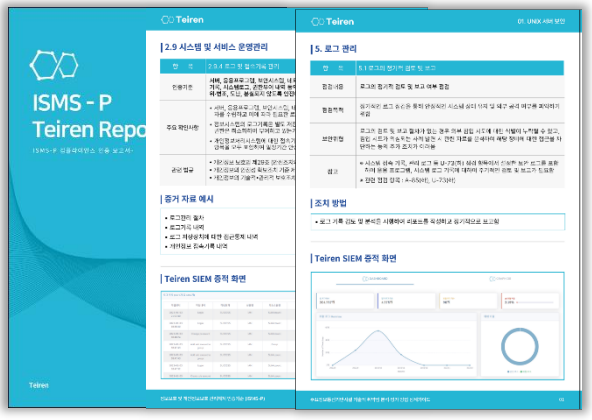
Traditional log management solutions or SIEM (Security Information and Event Management) systems often fall short of addressing customer needs fully. According to Teiren's own survey among users of log management solutions, common grievances include insufficient visualization, inadequate filtering capabilities, challenging customization, and poor performance. Many log management solutions hesitate to customize due to the risk of significant impacts on the overall solution for minor changes.

Teiren prioritizes resolving customer complaints, promptly incorporating feedback, and ultimately delivering a log management solution that ensures customer satisfaction through customization.

Enhanced Efficiency for Security Officers with Compliance Certification Reports

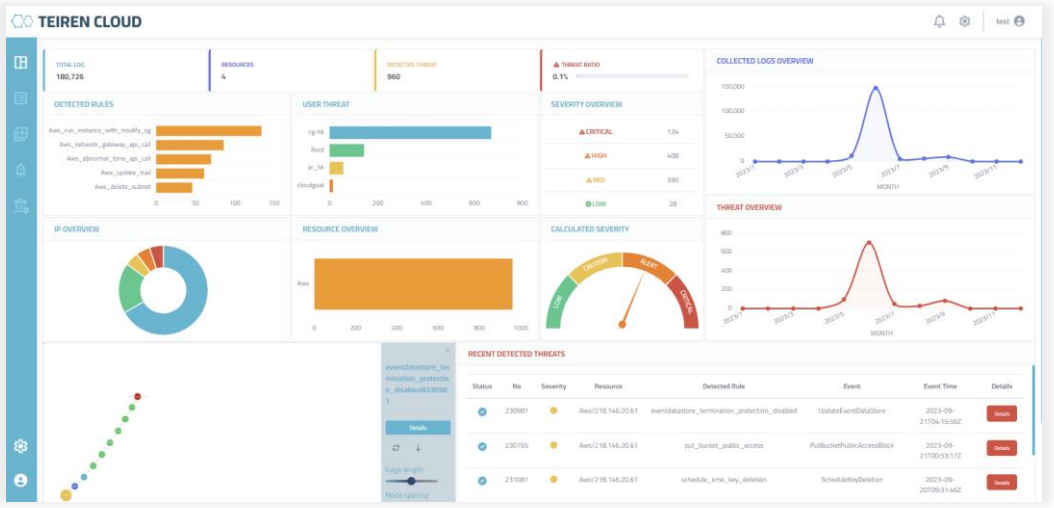
Teiren SIEM alleviates the workload on security personnel by providing compliance certification reports. Security officers spend upwards of two weeks on the tedious task of collecting evidence for security certification audits like ISMS-P. Utilizing the comprehensive security management capabilities of SIEM, it verifies compliance and generates evidence in the form of capture reports.

By merely reviewing these reports, security officers can significantly reduce the time spent on this task, thereby increasing operational efficiency.



TEIREN SIEM

Teiren SIEM Dashboard



Dashboard

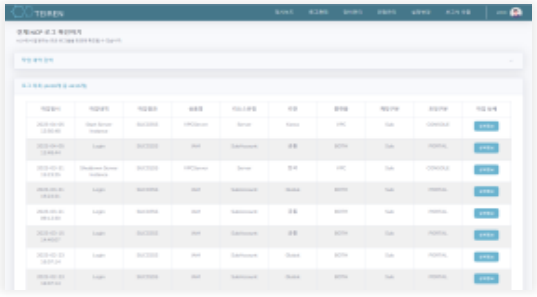
The Teiren SIEM Dashboard allows for real-time threat monitoring by providing an overview of the total number of logs, the number of threat logs, the threat ratio, and the most recently detected threats. Additionally, it offers real-time graphs showing the usage of CPU/Memory, aiding in the efficient utilization of the SIEM system.

Product Integration

Product Integration

Through the product integration page, users can register various cloud services and systems by entering an API key. Teiren supports integration with AWS Cloud, Windows Security Event Logs, and Jiran Ji Gyo's security solution, Office Keeper, enhancing the system's capabilities and support.

Log Output and Filtering



Log Management

Users can easily view and understand the vast amount of log data collected from AWS at a glance. For more detailed insights, a detailed view button provides access to more information and the original JSON format of the log data.

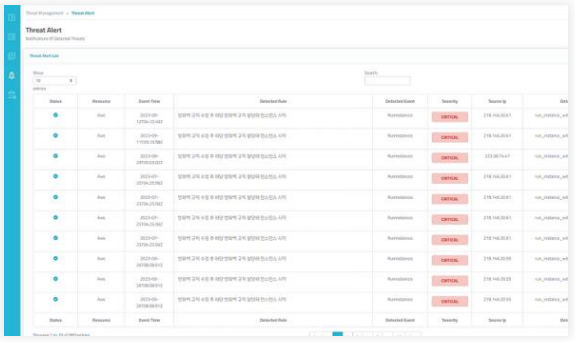
Users can categorize log data by selecting specific product names, accounts, and query periods. Furthermore, for detailed searches, users can utilize regular expressions to conduct precise searches.

TEIREN SIEM

Threat Detection

Teiren SIEM enables advanced and sophisticated threat detection through the use of Graph DB for enhanced performance.

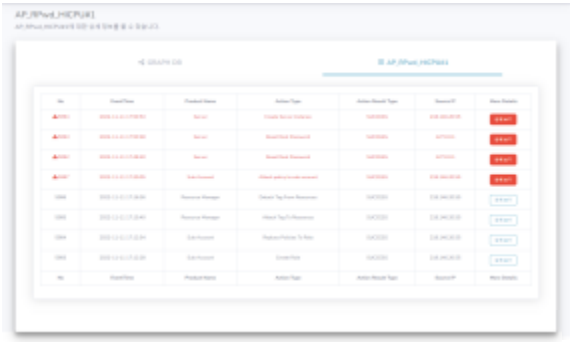
▲ Security Policy Configuration Screen



▲ Threat Notifications

Users can set security policies for threat detection. Teiren provides approximately 150 predefined security policies, which can facilitate basic threat detection. Users have the flexibility to turn these basic policies on or off and can add custom policies or specify policy flows to suit their corporate environment. Detected threats under these policies can be viewed on the threat notification page.

▲ Flow-based Threat Detection Screen



▲ Threat Detection Screen

Moreover, Teiren allows for the identification of threats based on the flow of actions, rather than isolated incidents, by enabling the specification of multiple policy flows. Users can directly add policies through flow specification. The path leading to a detected threat is visualized in a graph format for easy comprehension, and detected threats are displayed alongside related actions in a table format for quick reference.

Graph Database

Graph Database is a NoSQL database founded on graph theory, facilitating the analysis of vast amounts of data through the relationships between data points.

It stores data in the form of graphs, consisting of nodes (points) and edges (lines), making it possible to represent the relationships between data as direct connections between objects. In the event of a threat, related nodes can be swiftly searched without the need for indexes, enhancing the efficiency of threat detection and analysis. Furthermore, graph visualization enables a clear and comprehensive view of the database configuration, simplifying database management and oversight.

TEIREN SIEM

Threat Path Visualization and Machine Learning

Threat Analysis Visualization

Machine Learning based on User Behavior Patterns

Teiren SIEM offers a comprehensive visualization feature that maps the journey from user nodes to detected security policies, allowing for an immediate and clear understanding of the flow through which threats are generated. It enables quick identification of the relationships between a given threat and other activities of the user responsible, facilitating the detection of correlations between various threats.

Moreover, Teiren SIEM advances its capabilities by employing machine learning based on user behavior patterns. It measures the similarity between logs of user activities to identify deviations from normal patterns. Any abnormal behavior is considered a potential threat, triggering a security alert.

Report Generation

Monthly Threat Report.xlsx

Compliance Certification Report

Teiren SIEM provides basic threat reports in an Excel format. These reports include a summary, logs of detected threats, and the status of integrations.

To alleviate the workload on security personnel, Teiren SIEM also offers compliance certification reports. It automatically maps the compliance requirements that a business needs to adhere to and generates evidence in the form of screenshots, compiled into a PDF report.

By reviewing these reports, security officers can reduce their routine tasks, thereby decreasing their workload and enhancing efficiency.

03

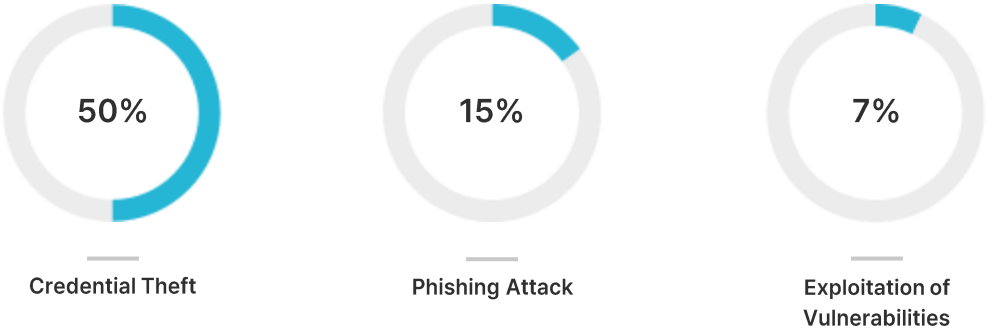
Teiren SIEM use-case

Teiren SIEM Usage Examples

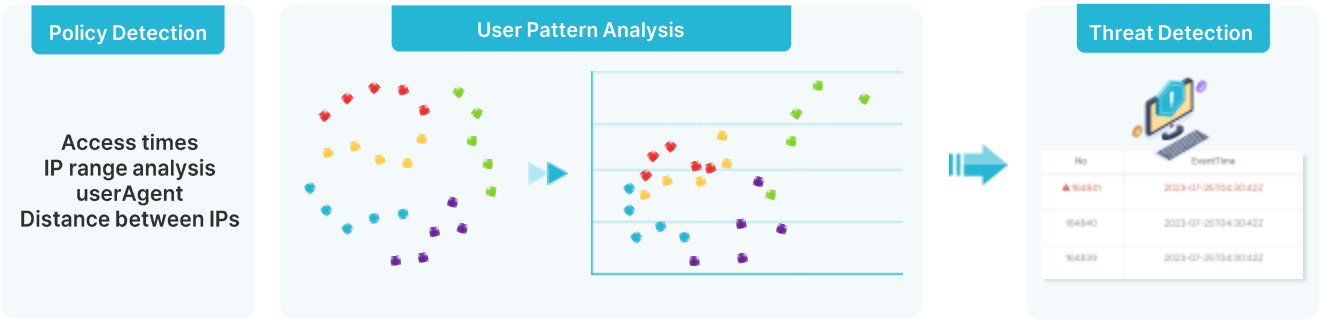
TEIREN SIEM Use Case 1

Detecting Compromised User Credentials (Account Takeover)

As cloud usage has surged and remote work has expanded due to COVID-19, the constraints on working environments have diminished. This shift has normalized access to cloud environments from diverse geographical locations, leading to an increase in malicious access exploiting vulnerabilities in cloud environment configurations. Identifying malicious behavior patterns within the cloud has become critical to prevent data breaches and security incidents. According to the Verizon 2023 Data Breach Investigations Report, credential theft is highlighted as one of the three primary methods of attack.



For users with administrative privileges over cloud environments, expanded asset access can lead to critical damage if an attacker commandeers a user's account for malicious activities. Moreover, because these activities utilize the permissions of trusted insiders, they can appear legitimate and may not be easily distinguished or identified as threats by security solutions. TEIREN SIEM addresses this challenge by analyzing user behavior patterns, including IP ranges used, cloud regions, and normal activity times, to identify deviations from normal behavior patterns. Furthermore, by employing artificial intelligence to measure the similarity between user behavior patterns, TEIREN SIEM can detect and analyze activities that deviate from the norm, even when such deviations cannot be detected by policy alone.



For instance, TEIREN considers activities such as API calls from geographically improbable IP addresses or cloud access outside of regular working hours as potential threats. Users receive threat warnings, allowing them to review the warning content, corresponding logs, and the flow of activities. This enables a more systematic approach to cloud protection.

TEIREN SIEM Use Case 2

Abuse of Cloud Infrastructure Privileges

According to a study by CyberArk, on average, employees can access over 30 applications and accounts, with 52% of an organization's workforce capable of accessing critical corporate data. Moreover, 80% of organizations experienced misuse or abuse of access to business applications throughout 2022, underscoring the need for improved visibility into user sessions and activities.

Palo Alto Networks' Unit42 Cloud Threat Report indicates that misconfigurations are often at the heart of most known cloud security incidents, frequently due to poorly crafted IAM (Identity and Access Management) policies. It was found that 99% of cloud users, roles, services, and resources had been granted excessive privileges not used within 60 days, alongside common configuration errors like weak password policies or exposing cloud resources publicly.

The exploitation of these vulnerabilities in cloud infrastructure configurations is on the rise, necessitating more secure and thorough security management of infrastructure configurations. To minimize damage when attackers successfully access the cloud environment, appropriate configurations are essential to prevent such breaches.

TEIREN provides its own recommended configurations for cloud infrastructure and IAM. For instance, it offers information on potential risks associated with events like stopping event logging, easing IAM password policies, or making instances publicly available, along with a corrective guide that includes improvements and methods.

Risk information due to vulnerable configurations and a guide with corrective actions via the cloud console or CLI, enabling users to easily change configurations for a more secure infrastructure setup.

TEIREN SIEM Use Case 3

ISMS-P Compliance (Korean)

In an era where cyber incidents such as hacking, ransomware infections, and data breaches are increasingly frequent, and attack methodologies are becoming more sophisticated, the importance of robust information and personal data protection management has never been more critical. The advent of cloud technology has further escalated the frequency of corporate events, amplifying the impact of security breaches on businesses. This evolving landscape underscores the necessity for systematic certification systems in information protection, making the acquisition of ISMS-P (Information Security Management System - Personal Information Protection Management System) certification imperative for organizations.

The ISMS-P certification is a testament to an organization's compliance with a set of actions and activities established to ensure the stability of information and communication networks and the protection of personal information. It is based on three categories: management system establishment and operation, protection measures requirements, and requirements for each stage of personal information processing. This certification is awarded by accrediting bodies that evaluate whether these measures meet the certification standards.

ISMS-P Mandatory Certification Targets

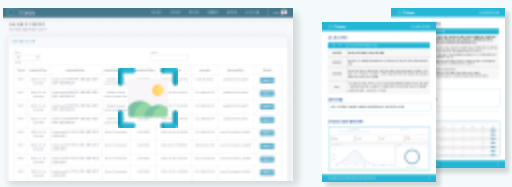
Enterprises with annual sales exceeding 150 Billion KRW	Medical sector (tertiary hospitals) Educational institutions (more than 10,000 students)
Information and Communication Service Companies	Companies with annual sales over 10 Billion KRW Companies with an average over 1 million users in a 3-month period

Although these are the mandatory targets, any organization that builds and operates an information protection management system or requires one can obtain ISMS-P certification. Achieving ISMS-P certification enables companies to implement more systematic and comprehensive protection measures, enhancing their information and personal data protection management levels. It also facilitates rapid response to security incidents and data breaches, minimizing damage and losses.

Teiren SIEM automates the mapping of items that can demonstrate compliance, collecting evidence automatically and generating reports as required by ISMS-P. This includes:

Item Mapping

Alerts and Correction Guides



Ideal for:

Financial institutions, public agencies, ISMS-P certified companies (companies with assets of 2 trillion won and a permanent staff of 300 at the end of the last business year), personal information processing companies, ICT companies, cloud service users (AWS, GCP, Azure, etc.), domestic cloud service users (NCP, NHN, KT Cloud, etc.), and other companies requiring log management.
Enhance your organization's compliance posture with Teiren SIEM, the comprehensive solution for meeting ISMS-P standards efficiently and effectively.