Good morning. I'm Joseph Cho, one of the co-founders of Teiren.

Before introducing our product, I would like to briefly introduce our team. We are constructed with members from BoB Best of the Best, which is the best cybersecurity training program in South Korea. I want to emphasize on our Active Chairman, MinPyo Hong. He is one of top 3 hackers in Korea and will be joining our team this year. We are looking forward for him to help us with sales department with the knowledge from his previous start up experience.

Problem

With this amazing team, Teiren is creating Teiren SIEM to detect and analyze attack in real-time.

When we interviewed security managers over the world including Singapore, Korea, Italy, US, they are still experiencing difficulties and shortcomings of using already existing security solutions including SIEM. These problems led to 3 big topics. 'identifying correlations of log is too difficult', 'there are too many security alerts for simple threats and false-positive threats', and 'following security regulation is too time-consuming'.

Problem & Solution

Security managers are experiencing at least 10 thousand of these unwanted alerts each day, which resulted in increase of workload stress analyzing each and every alert.

Most of the existing SIEM solution in the market look at one problem at a time. They would see three events and alert three notifications. However, Teiren SIEM would see multiple of events as one flow of event and alert one notification. In other words, Teiren SIEM will abate multiples of unwanted alerts so that security managers can focus on the important ones.

And also, if I were the security manager, I wouldn't want to spend my time analyzing the unwanted alerts especially if they are only in words. That is what other SIEM solutions are showing to the security managers now. Very boring right? Wouldn't it be better to analyze in a more convenient way? Teiren SIEM will automatically form a graph visualization of the threat with related logs so that the security managers don't have to go back and forth to look for logs related to certain threat. By visualizing the threat with a graph, like a mind map, we were able to show the correlations between logs that are related to the threat and reduce unwanted alerts, like what security managers wanted!

The database that is used for this solution is actually formed in a graph as well. With nodes and relationship edges, it was convenient to analyze the correlations between logs and the performance was outstanding compared to other databases.
When compared to SQL, searching for correlations with graph database was much faster. For example, if I want to find correlations in depth of 5? Graph database was more than 5,000 times faster than SQL database.

Another problem with existing solutions was dealing with security regulations. It might differ from countries to countries, but when we interviewed Korean and Italian companies, they had problems dealing with regulations such as GDPR.
Most of the security managers say that although it is simple repetitive tasks but takes too long to go over every asset. The average time for Korean companies to create evidence report takes about 2 weeks. However, with the reporting feature in Teiren SIEM, it reduces the time to approximately 2 hours. This feature was the 2nd most favorable feature, following the correlation feature, which means that there is a big need for automation of creating evidence reports to the security managers. And I believe that this feature will also satisfy the security managers.

COMPETITION

ManageEngine's Log360 is one of the existing SIEM solution that has similar features with Teiren SIEM. Comparing with the existing solution, although existing solutions was better in collecting various logs and detecting single and simple detection, Teiren SIEM had better flow detection where it detects multiple actions into one alert, had better correlation analysis and reporting feature.

When we calculated our pricing plan, we have focused on the difficulties that security managers or the companies are facing on brining SIEM into their company. The most concerns we have heard about existing security solutions is that it is too expensive. However, Teiren SIEM is much more cost effective compared to big SIEM companies like Splunk, Elasticsearch. It is at least half the price of existing solutions therefore has better accessibility to companies that are hesitating on buying SIEM solutions.

Product

Now we will show you a demo page of Teiren SIEM

After showing our demo page to security managers all around the world including US, Singapore, and Italy, we received various positive comments on our product. Most of them had great interest on our Dynamic/flow-based detection, correlation analysis, and compliance reporting features.

Especially an MSP from Korea and security manager from number 1 telecommunication company in Singapore Singtel are showing great interest in our product and are contacting with us frequently for product updates.

Market

The reason of SIEM market growth is the introduction of cloud to companies. After the introduction of cloud, there are too many data and alerts to deal with as we talked about in the previous slides. Therefore, security managers are looking for security solutions that are cost-effective and easy to use. Teiren SIEM is just the product that security managers are looking for.