20230325 지란지교 김원팀장님 미팅

(J : Jiranjigyo, T : Teiren)

current situation

The corporation is scheduled to be established in April.

Office Keeper is still under discussion because there are only view tables.

Ideas about certificate replacement issues

ex) The SSL certificate was originally on a three-year basis, but now it's on a one-year basis.
There are about 50 controlled servers that require certificate replacement each year. But the dates are all different, so it's hard to manage them all.
In general, there are all corporate websites, and there are many sites for Jiranjigyo, so if we try to change them all, the size becomes too large.
Even in the case of small companies, there are all corporate websites, and certificates must be replaced every year. It would be convenient to say that the entire process itself can be automated, such as having to do a corporate entity test to get a certificate reissued, paying for it, and replacing it with a file received.
I don't know how much demand it is because I didn't do an accurate market research on this issue, but in the case of Jiranjigyo, there are about 50 servers to replace certificates every year, so there is a demand.

T) Is it inconvenient enough to use it in Jiranjigyo when we develop it?

J) I don't know exactly about that. It's just that I need to replace all the certificates before they expire, make payments and change them, and I hope this will be automated.
Also, there is a foreign solution to this problem, but there is no solution in Korea.
Additionally, it's cheap in terms of cost. So it would be a little difficult to create the market itself with this solution.

About Teiren SIEM

J) What are the protection targets?

T) Corporate infrastructure. I heard that when an attack occurs, it is very difficult to figure out where the attack came through and what flow the attack took place.
If you correlate with asset management solutions such as BAS and CASM (Attack Surface Management Solution), you will be able to analyze how attacks come in and how to prevent them in detail within the company. Previously, it was a method of blocking all IPs in the event of an accident, but we think we can respond more precisely. Therefore, our product is more focused on post-mortem analysis.

J) The approach itself is not bad. From the point of view of the information protection manager, after identifying protected assets, priorities are set for control targets or control methods, and the infrastructure itself is not so high in priority.
It is important to understand where there is a need for control of the protected object.

Identification of accidents is also important, and there is a process for subsequent response when an accident occurs. If you think about what's more in the market, the approach to the attack surface is good, but it's actually isms-p. If sales are more than 10 billion won, it is a certification that must be obtained, so there is more need for it.
The certification required by the company itself will be different, and considering whether it can be introduced accordingly, **the important thing is what protection should be made and what role Teiren siem can play here.**

T) If you look at isms-p only, it depends on the size of the company, so I know it is one of the certificates that Korean SMB does not have to comply with.

J) In the case of isms-p, I said it because the needs are too clear.There is a need for isms-p because the Personal Information Protection law has been improved in Korea and criminal responsibility has been taken.
It is necessary to think about what parts of SMB have in relation to legal responsibility. SMB have no need for integrate in one place, that is, visibility.
For example, companies that do not use utm and do not manage authority well will not have a need for Teiren siem. **I think it's a product that should be based on the premise of 'sensing various products'. That's why it doesn't seem to fit well with SMB.**
Products are introduced in the order of vpn, WAF, utm based on the company corporation and the office. If you want to see it as one after introducing and sensing various products, you will then introduce Teiren siem. In this way, it seems more inappropriate to target SMB.

T) Through the compliance certification report, we tried to solve the most difficult part of the security personnel of small and medium-sized companies, that is, the part that takes a lot of time unnecessarily.

J) Isn't it fragmentary?

T) I will attach it to the siem function and provide it. Not the main feature. It is a function that can be used by companies that need to receive certification every year or multiple certification per year.

J) The domain involved in certification in Jiran is very wide, including security, assets, supply chains, infringement incidents, networks, data protection, system security, security requirements, development environment, and privacy management.
You need to see which domain is being certified and which is compliant.
In the case of preparing confidential (financial, etc.) information guidelines, a guideline document is required, but it is not available because it is confidential. So there's a need for this. There will be a need if there is a solution that can be automated for the company.

T) I think there are quite a few items that can be kept with just one siem, so I made this function because I thought it would be convenient for us to capture and show it at once.

J) Not bad. It would be nice if the guide came out by turning the tool in preparation. It's comfortable, but is it necessary? I'm not sure.
Security measures come out in the process of certification, and you can only modify them for a fixed period of time and leave evidence for them, and in a way, **it is more important to see what the protection target is in the overall structure and how they can be protected.** Since there is no sensor, the idea of linking it with the existing solution comes out, and in fact, this will not be easy.
In most companies, such as drm and utm, pay attention to reports, but it is another matter whether they are integrated or not.
If you look at siem as a smb target, you'll really have very little needs.
There is definitely an effect of market share. There is a threshold itself. So, in terms of area, the product line is siem. **You have to clearly set the area.**

J) Make something that doesn't exist, or do something that existed. Either of them, which do you think is better to be invested in?

T) From the customer's point of view, I think I will definitely buy it if there are products that I can't use because I don't have. So I thought it would be better for sales to make something that doesn't exist.

J) **I think the existing product line is better.**

The process of creating a market for any product is necessary. It takes a lot of effort to create a market, but it will be harder to make a product without it. There is rarely a market for the product itself.

If you think you're getting invested in seriesA, you have to write a business plan. You need to analyze the market and plan it, but you need to have a market to get the target market share here, and you get the expected sales, so how do you analyze this here when there is no market in the first place?

If you look at how much money this will be, it will be too difficult to judge a product without a market.

Siem itself has a weak market.

T) I think selling the first product is the first crisis we face. I thought it would matter if it was really sold or not. It's not whether they'll sell a lot. I thought I could get an investment if I saw a possibility.

J) The approach itself must go to absorb the existing market.

ex) When I don't have a cell phone, I use an alarm clock, a notebook, etc., and as I get a cell phone, the coverage of this market becomes 100%. The market demand is 100%.

The fact that there is a market demand while making this product means that there is a demand for the existing market anyway, so there is a basis for judgment.

It is necessary to show what to make in a year, how much corporate value to make, how much intrinsic value to make, and the criteria for judging it.

You've never worked at a company before, so going to B2B must be difficult. **There is no company in our country that does well by making new things.** Is there a company in Korea that does something that doesn't exist before? None.

J) **It feels like there's no point.**

If any company wants to collaborate together, they look for a company that they don't have, but Teirensiem seems ambiguous about what its core function is.

I feel like the basic function itself is not materialized.

T) Siem itself manages logs and detects threats, so why do you think so?

J) Most siem-making companies start sensing first. Does not start with 'siem'. If they want to see all of our products as one after they finish sensing, then they make siem.

Just because there are some companies that are friendly to you, don't make functions based on them.

T) When purchasing a security product, do you buy it based on the recognition first?

J) Most of the time, I buy it after seeing the recognition first. Non-recognition cases, when we make a new product, introduce it to a company that has been on good terms. Making it a test bad by giving it cheap to the first company, and expanding customers by making references.

It's a win-win if the client company meets all the requirements while testing. That's why you can't make good money from the beginning.

J) Why is the target smb?

T) In the case of large companies, it is well done on its own, and in the case of Jiranjikyo, it is used by many users, and in our case, we thought it would be difficult for many people to use it from the beginning, and there would be a demand for many security solutions depending on legal problems. I thought the price was very high for a company that was already doing well. I just think that if a customer uses it to comply with the law, they won't need too advanced functionality while using too expensive products.
It's not a product that doesn't exist at all, and there are companies that are leading the way. I thought we could sell our product to smb initially with reasonable threat detection, reasonable price, etc.

J) To survive in a changing environment, **you need core technology.**
I think it would be better to think about items other than siem.
Also, I think it would be better to think about marketability. I don't think it's going to be clear with siem anyway.
Complex premises make it difficult to introduce a product. Siem can be introduced only when everything is done. I think it would be nice if there was something sensing.
Also, I want you to clarify the control items. What are you going to identify and what are you going to use to analyze scenarios to control them.