# Transcript

## Section A

00:00:00 Interviewer

Next, we are going to conduct an interview with TPR4.

00:00:06 Interviewer

OK.

00:00:07 Interviewer

Alright, then let's start with Section A, because the first question is about you being a private network security provider. The second question is about the company you work for, which is called?

00:00:19 TPR4

The company is called [a private company].

00:00:25 Interviewer

And then, for the third question, how long have you been working in this unit?

00:00:30 TPR4

It's been exactly 4 years.

00:00:31 Interviewer

Exactly 4 years, OK.

00:00:33 Interviewer

So, is it all within the same department?

00:00:37 TPR4

Yes.

00:00:38 Interviewer

And may I ask, what is your current position?

00:00:45 TPR4

My job title is Threat Intelligence Researcher.

00:00:49 Interviewer

Threat Intelligence Researcher.

00:00:52 Interviewer

Alright, and the final question is, what are your main responsibilities?

00:00:57 TPR4

Oh, our main responsibilities are researching malicious programs and tracking ATP groups.

00:01:06 Interviewer

Okay, great.

00:01:10 Interviewer

OK, then I'll just move on to the next section.

00:01:16 Interviewer

And I want to mention that because I study criminology, and criminology uses a more social science and sociology approach to study this, so I actually don't understand some of the specific terms in network security, so if you mention them, I may sometimes ask you to explain.

00:01:34 TPR4

OK, OK.

## Section E

00:01:38 Interviewer

Okay, let's move on to Part E, and the first question. I wanted to ask, based on your understanding, what are some of the main internet attacks that Taiwan is facing right now? And what are the methods of attack?

00:01:51 TPR4

Oh, here is mainly focused on internet attacks against companies. Generally speaking, internet attacks can be divided into those targeting individuals and those targeting companies. So, for companies, the main attacks we face are what's known as ATP attacks.

00:02:15 TPR4

ATP stands for advanced persistent threat, which is an advanced, ongoing attack.

00:02:19 Interviewer

OK.

00:02:20 TPR4

It's carried out by government-supported hacker groups who engage in activities such as network espionage. Its main goal is to obtain confidential information.

00:02:41 Interviewer

You said it's supported by the government?

00:02:45 TPR4

Yes, because we believe that the goal of these attacks is not money, so there must be other reasons for supporting these hacker groups.

00:02:56 Interviewer

OK, so most of these attacks supported by the government are from which government? Can you expose that?

00:03:06 TPR4

Ah, I don’t mean that. It's just that every country has its own interests, so yes, that's right. And of course, the biggest threat Taiwan faces is the internet attacks coming from China.

00:03:20 Interviewer

Alright, then let's move on to the second question.

00:03:25 Interviewer

The second question is, what are the main targets of the cyber attacks that Taiwan is currently facing, and what are the reasons behind them?

00:03:37 TPR4

Well, we have seen that Taiwan's targets of attack include government agencies, as well as some high-tech companies such as semiconductor manufacturers, and some industries such as gaming and finance. In addition, there are also ongoing attacks targeting transportation and what we call critical infrastructure.

00:04:07 TPR4

Of course, the main purpose of attacking government agencies is to steal sensitive information. As for the semiconductor industry, Taiwan has a strong technology sector with unique technologies, which is why these attacks are carried out to steal such information.

00:04:23 Interviewer

I see, so critical infrastructure is also targeted?

00:04:30 TPR4

Yes. I think these kinds of attacks can affect our daily lives, such as the recent event with CPC Corporation which could clearly affect our normal facilities in Taiwan. These impacts can cause a lot of disturbance.

00:04:56 Interviewer

Alright, so let's move on to the third question. What do you think are the factors that affect Taiwan's cybersecurity, and could you provide examples?

00:05:08 TPR4

What do you mean by this? I'm not quite clear on this question.

00:05:11 Interviewer

So basically, this question is quite general. For example, when it comes to factors related to internet security, I might personally think that politics could be a factor when it comes to our relationship with China. Another possibility is that the general public might not have a high awareness of internet security, for instance.

00:05:42 TPR4

OK.

00:05:43 Interviewer

But I would like to hear your answer.

00:05:45 TPR4

Sure. So I think the first factor for Taiwan's internet security is the ongoing attacks from China. We need to strengthen our defense against them. The second factor is that in Taiwan, the industry used to focus more on OEM (original equipment manufacturing) and did not pay much attention to soft power or internet security. Therefore, I think talent cultivation is still immature in this area. Many companies may only have IT personnel without a dedicated Chief Information Security Officer (CISO). Consequently, their protection measures may not be as robust, leading to the occurrence of numerous cyber incidents.

00:06:36 Interviewer

Okay, then let me ask you again, what do you think is the biggest difference between IT personnel and Chief Information Security Officers (CISOs)? For example, with IT, as you mentioned earlier, many companies only have IT personnel but may lack a dedicated CISO. If they ask IT personnel to take on the role of CISO, do you think they might face difficulties in bridging the gap?

00:07:05 TPR4

No, I believe there's a difference in talent cultivation between the two. IT personnel mainly focus on hardware and equipment facilities, but they may not have a comprehensive understanding of cybersecurity. To effectively defend against cyber threats, one needs to think like an attacker, which is why I think cybersecurity and IT talents should be distinguished. Although IT personnel should possess basic cybersecurity knowledge, cybersecurity itself requires a separate department to provide assistance and expertise.

00:07:41 Interviewer

OK, got it.

00:07:45 Interviewer

So I think in Taiwan, companies like yours are rare and hard to find.

00:07:54 TPR4

Yes, because we are what is called the service provider.

00:07:59 Interviewer

I think Taiwan needs more services like yours.

## Section F

00:08:06 Interviewer

Alright, so let's move on to the F section. My first question is, what are your company's current offerings in terms of network security technologies and services provided to customers?

00:08:22 TPR4

Well, currently we mainly have two products. The first one is a kind of endpoint product, EDR, which is similar to antivirus software that is directly installed on the customer's computer to perform monitoring or inspection. The second product mainly provides threat intelligence reports, which allows customers to understand the dynamics of network threats and possible changes in ATP methods through our reports.

00:08:45 Interviewer

OK.

00:09:06 Interviewer

You just mentioned endpoint software, which you called ED?

00:09:08 TPR4

EDR.

00:09:11 Interviewer

EDR.

00:09:14 TPR4

Its full name should be endpoint defense and resolution, as far as I can remember.

00:09:19 Interviewer

Ah, OK, got it. Let's move on to the second question. What are your main sources of customers?

00:09:32 TPR4

Currently, our customers mainly come from the United States, Japan, and Taiwan, and the industries we serve are primarily government agencies, fintech, telecommunications, and information security services.

00:09:35 Interviewer

OK, got it.

00:09:44 Interviewer

So, the third question is, what are the main reasons why these customers seek your services?

00:09:52 TPR4

Actually, most of the time, they have already experienced some abnormalities on the internet, and then they come to us to investigate the incidents. After the incident, we may continue to help them with monitoring.

00:10:09 Interviewer

So usually, they only want to strengthen their security after experiencing a cyber attack, and they don't usually do anything before that happens?

00:10:20 TPR4

Typically, in financial institutions, there is often a more significant budget allocated, and their regulations tend to be more stringent. However, currently, Taiwan's relevant laws and regulations in the cybersecurity domain are not yet fully mature. As a result, most organizations only seek to improve their cybersecurity measures after becoming victims of cyber incidents.

00:10:39 Interviewer

Okay, got it.

00:10:42 Interviewer

I want to ask, usually after they seek your services, do they start buying things like endpoint software from you?

00:10:52 TPR4

Yes, but sometimes not every company has the budget to achieve continuous monitoring, so sometimes it's a case-by-case basis rather than continuous prevention.

00:11:09 Interviewer

OK.

00:11:11 Interviewer

So assuming that they don't want to buy anything from you after the incident investigation, what kind of advice do you usually give them?

00:11:19 TPR4

When we investigate the incident, we will provide a root cause, which helps to identify where the possible weak points are. We will also provide a report on protective measures that they can take, so that they can improve their infrastructure or update their software to protect themselves.

00:11:43 Interviewer

OK, so it's kind of like consulting? You provide recommendations?

00:11:48 TPR4

Yes, our reports do provide such recommendations.

00:11:54 Interviewer

Alright, let's move on to the fourth question. So, in terms of internet security, which areas do you think are relatively insufficient for most customers in terms of their knowledge?

00:12:08 TPR4

Actually, we don't really understand this part very well.

00:12:10 Interviewer

That's okay, just based on your understanding.

00:12:13 TPR4

Are you saying that you think they lack certain equipment or knowledge?

00:12:19 Interviewer

Yes, either equipment or knowledge would work.

00:12:22 TPR4

Understood, yes, in Taiwan, most companies often have budget constraints, which also lead to a shortage of cybersecurity talent. As a result, they may lack the understanding of threat intelligence and how to utilize it effectively. Therefore, many organizations in Taiwan tend to focus on implementing defensive measures through equipment and hardware rather than investing in talent development or establishing robust cybersecurity management systems based on knowledge and expertise.

00:13:05 Interviewer

OK.

00:13:06 Interviewer

So, in general, there is a bit of….

00:13:12 TPR4

Yes, they hope to see immediate results, so I think they need to strengthen their knowledge and systems management at the grassroots level.

00:13:27 Interviewer

So, let's move on to the fifth question. The fifth question is, uh, what are some of the network attack forms that you have encountered in your current situation?

00:13:39 TPR4

Oh, this is what we just talked about. Because we mainly focus on government and enterprise, we mainly receive what is called ATP attacks.

00:13:49 TPR4

So, uh, they mainly want to steal confidential information, and they may use methods like sending phishing documents or directly exploiting vulnerabilities on websites to penetrate into these enterprises' internal systems.

00:14:08 Interviewer

Besides that, have you also dealt with threats such as when they steal data and then go and threaten them, like with ransomware?

00:14:14 TPR4

Oh, we have encountered incidents with ransomware.

00:14:22 Interviewer

Okay, but they are relatively rare? Like most of them happen beforehand?

00:14:25 TPR4

Yes, most threats are not so direct. Because cyber espionage is part of spying, they hope to remain hidden as long as possible. So in such attack forms, it is less common to have immediate and direct impact after they have penetrated. Most of the time, there may be some abnormal connections, and then they discover that everything has already been compromised, so there is no obvious action that alerts the victim when they are first attacked.

00:15:02 Interviewer

Okay.

00:15:04 Interviewer

And then the next question is, because I later realized that I might not have asked this question very well, so you may answer it however you can.

00:15:18 Interviewer

Yes, like the sixth question, because I, for the sixth question, what I mean is to ask…

00:15:24 Interviewer

Let me take a look.

00:15:26 Interviewer

Because, based on my understanding, when reading some literature or something, whether it's software or services, they may do a good job in terms of prevention, but they don't have, for example, even if you have good prevention, you still need to think about how to reduce the damage and handle crises if your defense line is breached one day. So, I want to ask, how do you deal with this aspect?

00:16:01 TPR4

Understood. So, I would like to point out that the current positioning of our product might have some differences from the real-time prevention aspect. Our product was originally designed for post-incident investigation and digital forensics, rather than real-time prevention. Therefore, our response to this question would be more appropriate if we focus on leveraging our services to conduct incident investigations and identify how attackers managed to breach our defenses.

00:16:45 TPR4

Yes, so I think our main mechanism is to have follow-up services and investigation.

00:16:51 Interviewer

OK, so after investigation, it means looking back to see where the vulnerabilities are? Alright, then I want to move on to the seventh question.

00:16:58 TPR4

Yes, sure.

00:17:04 Interviewer

Yes, so the seventh question I want to ask is it's a bit like, for example, as you just mentioned, you provide endpoint services and software. So, the concept is a bit like… you need electricity when operating a company, and if the electricity suddenly goes out, there may be some backup power sources to keep the company running so that the whole thing doesn't shut down. So, going back to the network, is there something like this concept, like real-time backup conditions or software and equipment functions to reduce the damage in case the network is paralyzed?

00:17:54 TPR4

I want to ask, is this for our company itself, or are we providing this kind of service for others?

00:18:00 Interviewer

It can be both. You can answer however you like.

00:18:06 TPR4

I'm not quite sure about this part, because if it's for other companies, we offer restoration protection as part of our services. So if our clients are affected by ransomware or something similar, we can activate our restoration mechanism once we detect it. That's how it works.

00:18:33 Interviewer

OK, so you have this kind of mechanism.

00:18:39 TPR4

Yes, but it's not really focused on the network. I think you might need to use services to ensure that the entire system can quickly return to normal.

00:18:51 Interviewer

Right, that's what I wanted to ask.

00:18:53 TPR4

That should not be a problem.

00:18:55 Interviewer

OK, so how would you evaluate the restoration service that you currently provide?

00:19:04 Interviewer

Right, because I'm not trying to criticize your company's services. I want to know if there are areas where you can continue to improve, even if your services are already good.

00:19:22 TPR4

I, I think to say, the current restoration mechanism is still manual, so it cannot be done in real-time. So, why do we do it this way? It's actually because we are worried about the possibility of misjudgments. If the alert today is not a real threat and we proceed with automatic restoration, it may cause downtime for the services during the restoration process. So, we won't do it that way. Therefore, it's probably in the manual alert judgment part where I think we may need to strengthen our clients' knowledge. We also need to enhance this service on our end, hoping to achieve a quicker response, yes.

00:20:13 Interviewer

OK, got it.

00:20:14 Interviewer

So let's move on to the eighth question, which is about the overall integration of the technologies or services you are currently providing. In which aspect do you think you are lacking or want to improve? I think questions eight and nine can be answered together. Which services do you want to improve in the future from your perspective to make them better?

00:20:44 TPR4

Okay, so my response here would be that, in fact, ATP attacks are often targeted towards specific groups, meaning they focus on specific actors. Each different group targets different industries or entities. Therefore, we need to broaden our horizons and gain knowledge in new industries, especially those that are emerging and crossing boundaries. Currently, we might lack understanding or familiarity with attacks on these industries. This could be a challenge for our marketing efforts, as it may be difficult to easily penetrate more private or niche sectors.

00:21:31 TPR4

There are many ways to improve, such as reading more reports provided by other vendors. In terms of endpoint products, there may be some environments that we are not familiar with and cannot execute smoothly. So we need to invest more manpower and testing environment to improve the entire service.

00:22:04 Interviewer

Okay, for the tenth question, I want to ask if you, from your perspective, do you know whether your company wants to expand or improve in a certain direction in the future?

00:22:22 TPR4

Um, for this part, I think what we want here is for the victims or the manufacturers in Taiwan to have sufficient knowledge and ability to use our endpoint products and threat intelligence reports simultaneously. So we will integrate our endpoint products and threat intelligence reports to help them better understand the event when it occurs, instead of just seeing an alert and coming to us. They can also use our platform more effectively to do more comprehensive protection. So in our own planning, we hope to integrate the endpoint products and threat intelligence as a more complete service.

00:23:10 TPR4

At the same time, when an event is discovered, they can understand the whole context, who is attacking them, and what kind of actions may be taken afterwards.

00:23:23 Interviewer

So it's about integrating technology services to make it more comprehensive?

00:23:25 TPR4

Yes, because there is not a particularly high degree of integration between our two products right now, so I hope to achieve a more comprehensive service.

00:23:37 Interviewer

OK, got it.

00:23:39 Interviewer

And because you just mentioned that you may not want customers to immediately come to you when they encounter problems, so you also hope that your service can help them improve their knowledge in this area?

00:23:52 TPR4

Yes, we can provide them with more knowledge, and they can use our threat intelligence platform to understand the possible causes of the event. This will also enable them to recover faster on their own.

00:24:08 Interviewer

That's great, because it responds to the fact that generally, some enterprises or the general public lack sufficient knowledge in this area.

00:24:17 TPR4

Yes, that's right.

00:24:19 Interviewer

OK, got it.

## Section G

00:24:20 Interviewer

So, now we're moving on to section G.

00:24:23 Interviewer

Regarding section G, I want to ask about the cooperation between the public and private sectors.

00:24:27 Interviewer

Okay, the first question I want to ask is your opinion on whether you think that if public agencies cooperate with companies like yours in the field of complete network security, it will really help the development of network security?

00:24:42 TPR4

Uh, I would like to first talk about the cooperation with the public sector. Our current mode of cooperation is mostly that they come to purchase our products, and then we will periodically help them with a check.

00:24:58 TPR4

In terms of other forms of cooperation, we may also have regular so-called educational training. If they do not have a plan to cultivate cybersecurity talents, then we can provide corresponding courses to train them. I believe that in this way, we can help them cultivate their own talents, and they can help us with research. I think it is a very good cooperation.

00:25:20 Interviewer

OK.

00:25:22 Interviewer

So, it's really helpful for development?

00:25:23 TPR4

Yes, it is.

00:25:25 Interviewer

So, in response to the second question, I was wondering if your company have any experience with public-private sector collaborations or do you know any this kind of collaborations in Taiwan? Are there any examples you can share?

00:25:42 TPR4

Understood. In most cases, if we discover malicious programs connecting to Taiwan IPs, we do not have the authority to access the IP records. Therefore, when encountering such situations, we may seek cooperation with law enforcement agencies. That's the first point. The second point is as I mentioned earlier, if government agencies face network threats, they may approach us for investigation or seek our collaboration in providing education and training.

00:26:24 Interviewer

Okay, let's move on to the third question. What do you think of the current collaboration model and mechanism?

00:26:32 TPR4

I think it's good overall, with positive feedback. After all, sometimes we can meet their needs, and they can also meet our needs.

00:26:42

Hmm, I see.

00:26:43 TPR4

So, our current collaboration is quite pleasant.

00:26:48 TPR4

The more common issue we encounter is the timeline, as there are often sensitive procedures and protocols within government agencies that may cause delays. Due to the nature of their work, the approval and confirmation process can be time-consuming, which could be an area for improvement in our collaboration mechanism.

00:27:17 Interviewer

OK, they are usually slower because they have many procedures to go through, OK.

00:27:21 TPR4

Yes, yes, yes.

00:27:24 Interviewer

So that's the main difficulty, but are there any other difficulties in collaboration?

00:27:29 TPR4

Any other difficulties?

00:27:34 TPR4

If we talk about their needs, I believe the overall budget allocation for the government is still insufficient.

00:27:48 Interviewer

OK, insufficient budget. So, where do you think more can be done? To improve? Or in what direction do you think the future collaboration models can be improved to better assist in the development of network security?

00:28:07 TPR4

I think one thing that could be helpful for security firms like ours is the possibility of receiving additional incentives, such as tax deductions, from the government. This kind of encouragement through tax incentives would promote the establishment of more cybersecurity companies like ours, leading to better development in the field. So, I believe there should be more policy measures to encourage and support cybersecurity firms to provide their assistance.

00:28:46 Interviewer

I very much agree with this point because of the insufficient budget.

00:28:49 TPR4

This is my opinion, so there needs to be some mutual benefit.

00:28:54 Interviewer

Yes, there needs to be mutual benefit so that companies are willing to collaborate with the government.

00:28:57 TPR4

Yes, yes, yes.

00:28:58 Interviewer

Okay, besides the mutual benefits, do you think there are other ways to cooperate?

00:29:08 TPR4

Currently, we have a mechanism in place, like a consortium, where we can share threat intelligence. Personally, I think this kind of collaboration is beneficial, but the actual efficiency of its operation is quite low. The reason is that within this consortium, there are competing firms, and most of the shared information comes from the public sector. So, I believe this mechanism might need some changes. Instead of the ideal scenario of sharing everything in one group, it might be more effective to adopt a one-to-one sharing approach rather than a one-to-many approach.

00:29:58 TPR4

This is my personal view on the current situation regarding sharing intelligence information. There may be some concerns in this area, because we still have a competitive relationship with other cybersecurity companies.

00:30:09 Interviewer

Would it be better if it were anonymous?

00:30:13 TPR4

Actually, not necessarily, because we may still hope that these public agencies can use a more normal way of cooperation to work with us, rather than just exchanging information, because currently, I think that the amount of data exchanged is unequal.

00:30:23 Interviewer

I see.

00:30:31 TPR4

Yes, that's right.

00:30:33 Interviewer

You mentioned the consortium just now, what is it called?

00:30:36 TPR4

Um, I don't think I can disclose.

00:30:39 Interviewer

Oh, you can't disclose, it’s okay.

00:30:41 TPR4

Right.

00:30:41 Interviewer

Is this something that the general public doesn't really know about?

00:30:44 TPR4

There should be relevant information available, but I cannot say that we are a part of the consortium.

00:30:47 Interviewer

Okay, I understand. So there's a consortium where you can share some intelligence information?

00:30:54 TPR4

Yes, that's correct. We have such a mechanism in place, which is a collaboration between the public and private sectors. The purpose of this mechanism is to encourage sharing of information between us and the government agencies, and vice versa. However, it's important to note that there might be some competition dynamics within this setup.

00:31:12 Interviewer

Okay, I think that's all for the questions. Thank you.

00:31:25 Interviewer

Okay, because I just want to ask, because you mentioned earlier that, um, what are the things that the public and private sectors in Taiwan are currently cooperating on? And then, what are the models for cooperation between your company and government agencies? And what are the differences? For example, what areas do you think are the most common for cooperation between your company and public agencies in Taiwan?

00:31:54 TPR4

Are you asking which units we cooperate with the most or...?

00:31:57 Interviewer

Just in what ways?

00:32:00 TPR4

The main forms of cooperation are as I mentioned earlier, where they may purchase some products or acquire threat intelligence from us. Another common collaboration is when they request us to provide educational training. These are the most basic forms of cooperation. The second type of cooperation involves conducting investigations in Taiwan, where we may seek assistance from judicial authorities for conducting the investigation.

00:32:27 Interviewer

Earlier, you mentioned that there are areas where we can improve. It seems that you hope for policies that offer mutual incentives. As for the consortium, you prefer a one-on-one sharing mechanism, rather than a one-to-many approach, right?

00:32:40 TPR4

Yes, that's right. This part of the consortium is more focused on the whole of Taiwan, not just our company.

00:32:46 Interviewer

Ah, okay.

00:32:48 TPR4

Yes, because I wanted to bring it up separately. We also have another collaboration that is more like a partnership. The previous one sounded more like a normal client relationship, which is what other companies do as well. But we have a more special collaboration with the government.

00:33:08 Interviewer

OK, so you were talking about Taiwan earlier. Regarding your company, which aspect do you think could be improved in the collaboration with public agencies? How can you further develop this aspect?

00:33:33 TPR4

We hope that they can promptly report any incidents or events related to our products to us, so that we can be more involved. In some sensitive units, they purchase our products as tools and do not subscribe to our services. When they use these tools to discover events, they do not necessarily report them back to us. We wish they would inform us of these events, so we can continue our research and improve our tools. This is an essential point because what we sell is not…it’s just a service, and they are not obligated to report such incidents to us. It's regrettable that we currently lack a comprehensive view or perspective to effectively collect the information and intelligence from the tools we provide to these government units in Taiwan.

00:34:38 Interviewer

OK, got it. Thank you.