Orange Cyberdefense – Market Positioning & Growth Outlook

23 September 2022

Key Insights

- Cybersecurity market is transitioning towards advisory services, managed security internet, event management services and managed SOC services. Specialist highlights Microsoft Azure Sentinel growth too, but Orange Cyberdefense needs to improve this area
- Competitive landscape varies by region – Nomios, Atos and Capgemini are strongest in France, Integrity and BCX in UK and others in Nordics. Orange struggles in DACH and southern Europe
- Orange Cyberdefense’s 14% revenue growth rate in 2021 is sustainable and should increase “through acquisition and through a bit more scale”. Company has right long-term strategy of growing services
- Orange Cyberdefense’s biggest growth area is on detect, respond and advise side. Equipment resell side, meanwhile, is lower-growth and lowest-margin area, due to high competition and commoditisation
- Orange Cyberdefense’s cross-sell level was historically low, so this is considered a growth avenue along with developing new services and acquiring into a new region

Specialist	Etienne Greeff (EG), Former Group CTO at Orange Cyberdefense
Moderator	Saad Maqsood (SM), Third Bridge Sector Analyst

Agenda

- Revenue segmentation and growth trajectories of Orange Cyberdefense’s offerings, highlighting SOC (security operations centre) and SIEM (security information and event management) services
- Orange Cyberdefense’s market positioning and key competitors
- Size and sector customer sweet spots
- Geographic focus and expansion opportunities
- Orange Cyberdefense's key vendors and partners

Contents

Orange Cyberdefense – Market Positioning & Growth Outlook

Transcription begins at 00:00:02 of the recorded material

SM: Welcome, everybody, to Third Bridge Forum's Interview entitled Orange Cyberdefense – Market Positioning & Growth Outlook. I am Saad Maqsood, and I will be facilitating today's Interview with Mr Etienne Greeff, who is the former Group CTO at Orange Cyberdefense.

Etienne, before we start today's Interview, could you please state I agree or I disagree to the following statement: You understand the definition of material non-public information and agree not to disclose any such information, or any other information which is confidential, during this Interview.

EG: I agree.

SM: Could you please begin with a brief introduction of your background?

EG: Good day, all, my name is Etienne Greeff. I've been involved in the cybersecurity industry from before it was called cybersecurity, since I guess the early '90s. More recently, I was the Chief Exec of a business called SecureData, which was a private equity-backed business which I grew and scaled out to just south of GBP 60m. The business was then sold to Orange Cyberdefense, and, upon the sale of the business to Orange Cyberdefense, I took a Group CTO role which I fulfilled for 18 months. I left that role 18 months ago to do another scale-out, another buy and build. I know the business well, because I was at exec level, and I've been involved in cyber for quite a long time.

[00:01:49]

Q: Could you outline the key cyber services customers are asking for nowadays, whether it be SOC [security operations centre] or SIEM [security information and event management]?

EG: I think the market at the moment is in massive transition, and what people asking for traditionally was advice on what security devices to buy, and then they needed help to install it and then subsequently to manage it. That's still a large part of the market, but the market is moving along now more towards advisory kinds of services, customers asking their provider what they should be doing to minimise risks, what they should be doing to protect themselves against cyber issues and also how they can transform their businesses to the cloud and using technologies in a secure fashion. Advisory services are quite a large part of what customers are demanding. Then, of course, managed security internet and event management services, which is really about taking a huge amount of data from the different security devices across a customer's network and trying to understand, make sense of it, to aggregate it, correlate it and to understand if there are potential issues.

Lastly, manage SOC services, which is really about levelling that up. It's about now saying it's not just about talking the information, aggregating it, correlating it and trying to make sense of it, it's also about being able to respond to it and advise the customer in terms of what they should do if you spot anything suspicious or something that looks anomalous on the face of it. There are also other services in terms of security review work. There's a very useful framework to think about when you think about cybersecurity, and it's called the NIST Cybersecurity Framework, which has been wildly adopted now by companies. It really talks about identifying potential issues, detecting potential issues, protecting against issues, responding and recovering from issues. I think those are the five broad areas where customers are looking to buy products and services in, but I see particular growth at the moment on the detection side, on the advisory side, because detection is really the managed SIEM and the managed SOC services.

[00:04:18]

Q: Where do you think the next wave of growth will come from? Do you think it'll be centred around the areas of managed detection, managed SOC services and so on?

EG: I think the next big wave, and we're starting to see it growing already, is really around helping customers to transform their businesses, to use the right compute models. At the moment, a lot of customers run a lot of their stuff within their own data centres, and are using dedicated lines connecting to data centres and to head offices, and we see a huge change towards software-defined wide area networking. In other words, using the internet as a network, using the cloud as a data centre and, of course, throughout it all you need to net security through that. I think the next big trend, which is starting to happen already, is really about this transformation of businesses, where they've tried to use technology in the optimum way and a bit more flexibly, because I think one of the key advantages that customers see, and I certainly did see this in my time with Orange Cyberdefense, is that cloud offers you agility and flexibility. You can scale up and down as your business requirements change. I think the move to cloud is a big thing.

Coupled to that is the ability to detect threats across these heterogeneous environments, on-premise, data centre, cloud, devices connected to the internet directly, which brings me onto a second area which is growing quite rapidly at the moment, which is the whole concept of SASEs, secure access service edge, which was really about saying that you need to secure the edge of your network as devices connect to it, which is coupled with a thing called zero trust, where effectively you're saying that devices need to fend for themselves. The bigger picture thing is that there's absolutely a move to the cloud, and people need advice to do that. Then, on the one area which I'm seeing particular growth in at the moment, and it does resonate a little bit of Orange, because that's one area I think they need to improve on, is the whole growth of Microsoft and Microsoft Security Services through Azure Sentinel and so forth. That really competes with a lot of the traditional managed SIEM, managed SOC services, because Microsoft is providing the platform, and you now need to lay a service on top of that. For Orange, that's still embryonic. They do that in the Benelux region, but not so much in the rest of their territories.

[00:07:02]

Q: In regards to the other growth waves coming in – whether from the SASE [secure access service edge] side or just the transformation into cloud – how well-placed do you think Orange Cyberdefense is to accommodate these, with the exception of the Microsoft side, which you believe the company is building on?

EG: I think they're doing well there. They're not doing as well as the young, nimble competitors, but, certainly in terms of the larger players, the NTTs of the world and the Telefónicas and even the Secureworks of the world, I think they're doing particularly well, because they created the Qatar Centre of Excellence, which is headed up directly by the executive VP, Laurent Celerier. Even when he was my boss, I couldn't pronounce his name properly. I think there's a lot of focus in it. There's work to be done, but I think, in terms of their major big competitors, they're there or thereabouts, and maybe even slightly ahead of their main big competitors.

SM: Within the big competitor space, you'd get NTT [Nippon Telegraph and Telephone Corp], Telefónica Tech and so on?

EG: Yes, absolutely.

[00:08:21]

Q: Within the young, nimble competitors you mentioned, who would you consider to be the main players in the space?

EG: This goes to a number of a few other questions. I think it's important to understand how Orange Cyberdefense organises themselves. They are global, or a pan-European company, but they actually do operate locally. The individual territories have a lot of flexibility and a lot of autonomy in terms of what they do. The country managers tend to report into a regional executive vice president which looks after the different territories, which then reports, which is on the main board of Orange Cyberdefense. To answer your question, you can only look at that question by looking at each territory. For instance, in France, they'll compete with Nomios and Atos and Capgemini. In the UK, they'll compete with Integrity and with BCX and so forth. Globally, yes, we've got the competitors we talked about, but actually most of their competitors are regional, and it really depends on it per region who the competitors are. I think it's important to think of it that way.

That goes on to another point around Orange Cyberdefense, where I think the main scope of growth is, in territories where they acquired, like they did in the UK, like they did in the Nordics, like they did in Benelux, they are strong and they're doing well. In areas where they didn't acquire, they're struggling, so in DACH they're not getting the traction that they're looking to, in southern Europe they're not getting the traction too. I think, for me, that will be the main area of growth for Orange Cyberdefense, really, would be looking to acquire in those territories. I think there's a lot of scope to do so, because, despite the fact that they are very large, they will be approaching EUR 1bn now in revenue, there's still not a single dominant player across Europe. I think there's still ample runway for them to continue growing via acquisition.

[00:10:35]

Q: Orange Cyberdefense saw about 14% revenue growth in 2021. How sustainable do you think that growth rate is? As you mentioned, there's also scope to grow in different regions, so do you believe it could go even higher than this, or is there a certain rate where it would taper off?

EG: That's actually a really interesting and nuanced question. Of course, I'm sure there will be a prospectus and there will be a lot of information shared at the time when it goes to market, but in a way I think Orange Cyberdefense can actually grow quicker than the 14%. Why I say that is that that growth is a combination of services growth, managed services, managed SOC and product resell. If they just wanted to do product resell and, let's say, compete with Nomios in France, they could have grown quicker, but I think they're taking a longer-term view and prioritising growing services, which of course takes longer, because revenue recognition over the period of the contract. I think that's tempered growth. I think if they had a more short-term product strategy they could have grown quicker, but I think that's more sustainable, that growth that they are showing. I would also say this, is that that growth is an amalgam of different territories. They've traditionally grown quicker in France than they've grown in the rest of Europe, so some territories, again, I can't share the exact figures, because that wasn't public at that stage, but I know that in certain territories the growth was single digit and other territories it was higher, and that was 14% is an amalgam of it. I guess what I'm saying is the average growth, I think it is sustainable. I think, in fact, through acquisition and through a bit more scale, that growth actually should increase.

[00:12:43]

Q: I understand the main revenue streams will differ by region, but at least in terms of services, the Orange Cyberdefense website splits them out across the assess and advise side, design and implement, detect and respond and so on. How would you split those out and rank them?

EG: Their biggest growth area is really on the detect, respond and advise side, is where the growth is. I think the area that is becoming not stagnant, but is lower growth, was certainly lowest margin, is the detect, the technology side, the equipment, Orange calls it ERS, equipment resell. That ERS side of it I think has become more challenging, just because there are a lot more competitors. As technology commoditises, you're now competing with Computacenter and Softcat, CDW, Optiv, the large resellers of technology, and although Orange Cyberdefense is large, they're not large compared to a Computacenter or to Softcat from a resell point of view. I think the growth really has been on the services side, and that's more sustainable growth, because that stuff, you've got customer intimacy, because your differentiation, there's a level of service you deliver, and how strategic you are to the customer, whereas on the equipment resell side your value is how much you sell it for, and it's not sticky.

[00:14:22]

Q: Would you say Orange Cyberdefense's core strengths would be around the services side and detect and respond, and even advising?

EG: Yes, absolutely. That is the core strength, the relationship-driven stuff, that is, but I also think one of the core strengths of Orange Cyberdefense is the fact that they have a comprehensive offering. They're really one of the very few large players that has end-to-end offering, those five areas of the NIST Framework that I talked about. A lot of the other players will be very strong on maybe the managed services side, or on the advisory side, or on the detect side, but Orange is strong on the SASE side, on the respond and the recover side, so they really do have a truly end-to-end offering. That's one other big differentiation for them. Then the other area also is that, because they operate this act-local model, they are pan-European but they do operate locally with customer intimacy, that does mean that the pan-European players, European-headquartered businesses, do like them, because BNP Paribas could have a contract with them signed in France, but BNP Paribas has a presence across Europe, and the local entities can fulfil the services for the customer. That's quite an attractive alternative to the large US integration houses.

[00:16:05]

Q: We touched on the weaknesses in Orange's offering, or perhaps where it's lacking. Do you think those gaps can be addressed organically or could it be a case of executing some M&A strategy?

EG: It's some and some. I would say that certainly the original gaps need to be filled, and I'll give an example there. Germany, or DACH region, has always been one that Orange Cyberdefense has not been strong in, and in a way that actually allowed other players to step into the market. The ex-SecureLink CEO, Thomas, Thomas is now the CEO of Deutsche Telekom Security, which is effectively a direct competitor to OCD. The only reason that was allowed to almost happen, and is gaining some traction, is because Orange is not really strong in that region. They only really do consultancy in Germany. They don't have a comprehensive offering there. Acting local is important for the German market, as an example. Again, in southern Europe, Telefónica doesn't really feature anywhere else in Europe against Orange, but they do in southern Europe. They definitely need to have presence.

The challenge is, cybersecurity, just give me a second just to describe it. Customer intimacy is important, because cybersecurity is all about trust. It's about trusting the advice, trusting that the person giving advice understands your local context, understands your business, and it really does boil down to trust. The whole notion of land and expand is really, really important. At one hand, you need to have that, and I think for that to work you need to have local presences in the country. Of course, what you tend to do is you tend to make sure that the people that interact with the customer is local to the customer, so the local advisory people, same language, same time, same area. Even some of the SOC services, where you need to have an engineer interacting with a customer or sitting even inside the customer's environment to investigate security issues and to help advise them on incidents, that needs to be local. What you can centralise, and what Orange is starting to do, you can centralise the back office functions, for instance, the aggregating and correlating data, taking initial calls for managed services. Even when I was there, they were talking about potentially taking some of the back-office service to Mauritius and to other territories and so forth. Going back to southern Europe, you need to have a local presence there in order to have that land and expand for you to then upsell and cross-sell the different services.

[00:19:07]

Q: Are there common opportunities for Orange in terms of cross-selling and upselling, or can Orange Cyberdefense leverage OBS's [Orange Business Services'] relationships to sell into?

EG: Yes, absolutely. OBS has been a really good source of growth for Orange Cyberdefense, because, although Orange Cyberdefense focuses on cyber, and on this call we're discussing cyber, customers don't segment it like that necessarily. They don't think of cyber necessarily all the time as separate. When Refinitiv wants to transform their network, or the London Stock Exchange wants to transform their network, they don't compartmentalise it into network, data centre, cloud, cyber, they just come to one party to help them to advise them to do it. For instance, I think the reference customer for Orange is GSK, they go to OBS, and OBS opts into the whole programme of transforming and monetising their IT system, and, of course, to do that, it's a multi-faceted area. It's on-premise work, it's data centre work, it's cloud work, it's cyber work, it's managed services, and, with OBS and Orange Cyberdefense, that can be presented as a seamless offering.

The reality is customers want to buy from less people. They want less complicated supply chains. The same argument that I had previously with one of the advantages that Orange Cyberdefense has of having a comprehensive offering, which means they can do more for a customer, is also true when you're now starting to think about transforming IT and integration work, where OBS I think works well. That's one of the areas, after the acquisition of SecureLink and SecureData, that didn't really work that well. The Orange-OBS relationship didn't really work that well. It took about 18 months for that relationship to start working, but, towards the end of my tenure at Orange Cyberdefense, that really started working, and I know that relationship has gone from strength to strength, the working relationship between OBS and OCD.

[00:21:26]

Q: There's such a comprehensive offering here on Orange Cyberdefense's end, as you mentioned, but have you seen instances of a customer taking one aspect of cybersecurity from the company and another component from a competitor?

EG: Yes, you do. There tended to be a dividing line between advisory services and operating, in other words, customers tended to have this view you want one person to advise you on your weaknesses and on your strategy, and you want somebody else to actually implement it and to manage it, so absolutely. Also, not every territory has all the capabilities. For instance, in France, they might not have the capability to manage Microsoft or Azure Sentinel. That capability is so-so, so those customers will buy it elsewhere because Orange Cyberdefense don't have the capability to do that, so a customer that wants to have Azure Sentinel managed service would have gone elsewhere. Then, of course, Orange then develops the capability and then they have the ability to cross-sell it. I guess what I'm saying is that, yes, customers do buy from multiple players, it's very rare for a customer to only buy from Orange Cyberdefense and buy nowhere else, but for me that's the upside, that's the runway that I see for Orange Cyberdefense, is to continue with a cross-sell and upsell journey.

SM: Could you see this becoming a trend across customers as well, to prefer to have it all coming from one place as opposed to separate providers for different aspects, in the sense of advisory vs the implementation, for example?

EG: Yes, absolutely, because I think we see it in other industries. I think when an industry is young and fragmented and new, people tend to go to specialists, but as stuff gets more mature, people tend to go to one place. It's one of the sad reasons why supermarkets are becoming dominant as opposed to specialist shops in city centres, it's just the overall trend, I think, people prefer to deal with fewer. It's simpler, because you can have your frameworks in place with the company, you can have a single contract, you have single SLAs. There are no hand-off points, pointing of fingers between network and data centre and cyber and everything else, it's one company that you deal with.

[00:24:16]

Q: Do you think there are certain sectors Orange Cyberdefense is best able to adapt or cater to?

EG: Yes, that's a good question, that. I think it, again, depends on region to region, but I don't think it's so much a sector focus as it is a company focus. In France, they tend to focus on the larger companies, the CAC 100 or the 40, the biggest companies within France. In the UK, they tend to be more mid-enterprise. In the Nordics, it's larger companies, again. I think it varies per territory, and it's more to do with the company's size and relevant experience of dealing with companies of that size. They get their really global customers, it's through OBS is where they get their really large customers, the global companies that are looking for a single supply solution that does multiple areas for them. I think it's that. The one area where Orange is putting a lot of investment and time in, which I think is interesting, which we haven't talked about yet, is the whole OT, operating technologies side, in other words, the stuff that runs factories and stuff like that. I think, in France in particular, Orange works extremely well with the manufacturing industry, so a lot of the car manufacturers, a lot of the industrial manufacturers are customers of Orange. They're also customers of Orange Cyberdefense, but I think they've been dragging Orange Cyberdefense into the whole OT market. I think that's a really, really interesting market, because there's a huge scope for growth in that space, because it's still very early days in that space.

[00:26:23]

Q: Can you see OTs [operating technologies] as a potential growth area itself or in cyberdefence, since Orange Cyberdefense already has some good relationships there?

EG: Absolutely. They really work with a lot of the large manufacturers, and even globally they'll work with people like PMI, Philip Morris International, they work with Maersk, they deal with some of the very larger global manufacturers, logistics people, so they're in a good position. They have relationships already, it's just really about broadening the offering. Really, in my mind, there are two avenues of growth, there are three avenues of growth, I guess. Let's talk organically. Organically, the avenues of growth is really about landing and expanding and selling more of the same to customers. One of the key questions I would ask myself when I look at Orange Cyberdefense, I've tried to evaluate how successful they are at cross-selling, and it's quite easy to do. You could just ask, in those five pillars that I mentioned for the top 100 customers, trending it from, let's say, the last three years, how many pillars did customers buy offerings from them? What percentage of the customers buy from one pillar, what percentage buy two, three, four, five pillars? That's a good way, and then you can trend that over the period. That will tell you how much runway there is within the customer, because I think new customer acquisition is expensive. It's a lot cheaper to sell, not new services, to sell different services to existing customers. That's scalable and that's effective, and that actually is very profitable to do that. I think that's one area of growth, is that cross-sell that I talked about. That actually is better and cheaper than trying to keep on delivering new solutions, partnering with new technology partners, all the rest of it.

The second avenue of growth, as I said, is developing new services, but that's more complicated, because you need to develop OT technologies, maybe you need to partner with new vendors, you need to develop service around it. That's one of the disadvantages of being large, is you're not nimble. It takes you longer to do stuff. It's easy to do if you only operate in one territory to launch a new service. You train 40 salespeople, you put it in your books and it's done, but if you're across 20 territories, you have to have international price book that works across all those territories, you need to have a model that allows you to have different languages to deal with different customers in different countries. It becomes complicated. I think that's the second area of growth, is really about expanding their portfolio. The third area of growth, of course, is to do acquisitive growth, and, potentially, if you buy into a country where the company that you buy hasn't sold a lot of services, that then gives you that cross-sell opportunity, getting to those customers.

[00:29:21]

Q: Given your comments around the sectors Orange Cyberdefense might be best able to cater to, would you say there's ample room to keep cross-selling and achieving the growth rate the company has seen so far?

EG: Absolutely. I know, not for sure, again, this is anecdotal, I can't share figures, but they'd probably be out of date by now anyway, but the level of cross-sell was low. It was low. There's a lot of runway there, but they started getting better towards the end. This goes onto one of the other questions I know we discussed previously, which is this whole how good Orange was at integrating acquisitions. I know that's something we discussed previously. I think being acquired gave me unique insight and perspective in the integration process. Orange actually did a very good job of integrating the businesses. They did what they said they would do, and they said what they would, and they stuck to their words. I think the reason why they were quite successful at integrating is that they really kept the regional autonomy, so they didn't change too much within the individual businesses. Of course, there's always a regiment change, because whenever there are acquisition opportunities, especially in a resource-constrained market, competitors will try to hire people, but, on the whole, I think their acquisition strategy and integration strategy worked. The businesses are still doing well, are still dealing with the customers they used to deal with. I've been on the buyer side and sell side, this is probably one of the better integrations I've seen, both of SecureLink and of SecureData, so I think that will give me confidence that they've got a recipe now to integrate. They just need to do more of it.

[00:31:26]

Q: Going back to your comment that Orange Cyberdefense perhaps hadn't executed enough on the cross-selling side, was it the case that the strategic focus at the time was more around going for new customers, or was it just difficult to execute the cross-sell? Was there any particular reason behind this?

EG: Yes, there was. I think the reason behind it is just momentum, lethargy, and let me explain what I mean by that. As I said already, Orange tended to keep the country managers in place, and they gave them a fair amount of autonomy, so there's not a real edict to those guys that they needed to start selling services from other companies. I'll give you a real example here. One of the key assets that Orange Cyberdefense acquired when they bought SecureData was the penetration testing business, SensePost, which were really high-end consultants, ethical hackers and trainers and thought leaders and real cybersecurity experts. That's a really fantastic quality business, but it took a good two years for those services to be sold into the Nordics and into Benelux and so forth. It takes a long time, because it's not just a switch. You don't just tell a salesperson, "You've got this new capability, sell it." They need to understand it, you need to train them in it, you need to train your pre-sales guys in it, then they need to talk to customers about it and the customers may not have a budget for it with you. Then you need to get onto the penetration testing panel and that takes a year. It just takes time, that's the thing. Anything can be done better, but I think they've done as good as you could, and the patience is now paying off, you're now starting to see that cross-sell happening. I think it's just momentum and lethargy and time for people to get to know the services before you can start cross-selling it.

[00:33:34]

Q: We've touched on how Orange Cyberdefense may operate in different regions, and may be stronger in some than others, but to confirm, what would you consider to be its strongest regional focus? Would that be France?

EG: France, for sure. They're a French company, but also the fact that pretty much every single large customer within France uses Orange, so there are strong existing relationships at board level with those customers, so it's a lot easier to sell into that. Also, the business that they bought in France, Atheos, at the time, which was Michel Van Den Berghe's business, was enterprise-focused, so they're really strong in France, it's the number one region for sure. Then, the next big region is really the Nordics. I think they're exceptionally strong in the Nordics, and I think that's more because of SecureLink, they had good acquisitions in the Nordics, so they've bought a really strong base there. They're not as strong as they can be in Benelux, not strong enough in DACH, and the UK, I suppose because of the local execution, I think there's room for improvement within Orange Cyberdefense in the UK.

[00:35:11]

Q: I understand the DACH region has been particularly tough to break into. Is it a matter of preference for local players in Germany? This country stands out for its stringent data protection and security requirements, so does the whole concept of security made in Germany become a differentiator there? Is that why the company might be struggling to break in? What would you highlight?

EG: Exactly that. I would say Germany of course does stand out for the stringent security and made in Germany and TÜV is kind of a thing, and that's fine, but I wouldn't say it's that different in the UK. Actually, in the Nordics, the Nordics don't mind, people from Sweden will buy from a company in Norway and vice versa and so forth, but I would say most companies prefer to deal with somebody local to them. You need to build up a trust relationship. It's unlikely for somebody in Germany to buy, they will, but it's unlikely for them to buy from a company outside Germany. The Swiss do, but not so much the Germans.

That's because Orange didn't buy a business in Germany. That's its price.

SM: Would you say these difficulties, or a lack of focus on Germany, isn't necessarily particular to Orange Cyberdefense? Would you say other providers such as Telefónica Tech...

EG: Yes, that's why Deutsche Telekom Security, Thomas Fetten, is doing so well. They stepped into a void.

[00:37:04]

Q: How would you rate the competition across France and the Nordics, which seem to be Orange Cyberdefense's strongest regions? Would you highlight any key players? You mentioned others such as Atos and Nomios in France.

EG: The market is still so fragmented there. The competition, you've got people like I-Tracing and even Secureworks and things like that, and, of course, increasingly the vendors, believe it or not. When I say the vendors, people like Palo will do some stuff directly, and people like Zscaler will provide a lot of the service and you just become a reseller for it. You don't really lay a service on top of that. I would really say that the competition in those territories is the smaller players, the more specialist players, the people which maybe don't have such a comprehensive offering, but they've got a strong relationship with the companies, they've known the companies for a long time and they may be providing other services for them. I think, increasingly, those companies, scale really will become more important. It really will become more important. What I mean by scale, scale isn't just size, scale is also depth of technical knowledge, understanding. The cybersecurity challenge is becoming more complicated because, in a way, it was always complicated, but if you just have to protect all your assets and all your assets were in one location, was in a data centre, you could see where the assets were, you could walk around your assets, you could almost a draw a moat around your assets, you could protect them. Now, your asset sits everywhere, it sits on mobile devices, it sits on laptops all over the world, it sits in the cloud, it sits in different territories, it sits in different sovereignties, so now that problem is getting a lot more complicated. It becomes very, very difficult for a small company to have the breadth of knowledge and understanding to bring all these different threads together. That's why I think scale will become more important in this space, and that's why I think there's such a race for consolidation in this space.

SM: I suppose we'll have to see how that plays out in terms of consolidation.

EG: Yes.

[00:39:40]

Q: I understand it's very fragmented in France and the Nordics, but would you say the top players – those who Orange Cyberdefense may be competing with – have a certain market share in these regions or is that also difficult to distinguish?

EG: Yes, it's difficult to distinguish, but I would say this to you, Orange Cyberdefense, or any other player for that matter, is nowhere close to saturation. None of these businesses will run out of runway in any of their territories anytime soon. The simple reason being that the problem is getting bigger, it's becoming more complicated, and most companies have a huge amount of technical debt, or security debt. Technical debt or security debt is defined as the trade-off that you make when you have to move quickly, so if you have to move quickly, get a product to market quickly, maybe you make some technical trade-offs. You sacrifice security for speed, let's say. Universally, no CIO ever has ever said to anybody ever, "I've got too much money for cybersecurity." There's always a shortage of resources. I guess the runway isn't just taking business away from your competitors, but it's about solving more and more of a security problem. With the rise of ransomware, with the compromises, with an increasingly regulatory stance of government bodies, I think the spend in cyber will just go up. It's not just runway in terms of taking market share away from your competitors, it's also about solving more of a security problem. That's why I don't really tend to think in terms of market share, because I only think of market share if you think in terms of the market becoming constrained, but we're not there yet.

[00:41:49]

Q: In terms of the main competitive advantages Orange Cyberdefense may have against the more global players – Atos, Telefónica Tech and so on – is there a big differentiation in their capabilities, the technical side of things, or is it the fact that there's more of an end-to-end and comprehensive solution here?

EG: That's a really good question. Again, I chuckled a little bit here. Every business I've ever spoken to say they've got the smartest people. I've never met any business that says, "We've got mediocre people that we overcharge for and they deliver a mediocre service at the best of times." Nobody says that, do they? They always have the smartest people, have to deliver the greatest edge and everything else. Generally, having worked with them and been outside of them now for a while, I would say the following. I think, from a managed service point of view, and from a managed SIEM point of view, there's not that much to differentiate between any player, to be honest. It really is not. They all deliver a good service, because they wouldn't have been there, they wouldn't have survived and evolution wouldn't allow them to be there and grow to that size if they were delivering rubbish service, actually. At its core, it's all pretty much of a muchness. They all represent the same technology vendors. I know there's a question about CrowdStrike was another question, but they all deal with Palo and Fortinet and Check Point and Cisco, Splunk, they all deal with those same core of vendors. That's not a differentiation either.

I think the one area that genuinely does differentiate Orange away from other players is that I think they've got really smart advisory people within the business, and advisory at two levels, virtual CISO, in other words, providing strategic advice to customers in terms of how to really think about security, what steps to take. That's number one. Number two, their penetration testing business, both in terms of France and the Nordics, Benelux and most of the pen tests are based in South Africa, are really smart people. They're globally recognised to be some of the smartest people about. I think that whole ability to use that knowledge of how the bad guys operate and to then blend that into your service is really important. I think that there they are differentiated. I know everybody claims they're differentiated everywhere, but that's one area I think they truly are differentiated in, that one area.

I think the other area where they are differentiated, but that's transient, because if you're talking about a EUR 300m-400m business, or even a EUR 1bn business, you can stand its capabilities up. They do have a strong offering on the instant response side and on the recovery side, which I think is stronger than most of their competitors, but that's transitory. People can actually build on that. I think what could define success for them and continue growth for them will really be if they can take this recipe that's worked for them in Benelux, in France, and replicate that in the UK, replicate that in Benelux, replicate that in DACH and in southern Europe. Beyond that, I think these players are all the same, it really comes down to execution, but there's some differentiation, as I said, on the advisory side and on the penetration testing side, I would say.

[00:45:29]

Q: You said it would be good to see if Orange Cyberdefense can replicate into other regions where it's perhaps not as strong – the UK, Benelux and so on. Do you think any of these areas offers a much greater growth opportunity if the company manages to unlock it and replicate the recipe?

EG: Yes, I think if you just look at the relative size of the economies, Germany is the second or third biggest economy in Europe, isn't it, so, yes, for sure. I don't think Telefónica is doing a fantastic job in southern Europe either, to be honest. I think there's scope there, but there's maybe not as exciting potential as Germany. I think there's still huge scope in the UK. There's still huge scope in the UK. Let me explain what I mean by that, let me give you some numbers to that. I can't speak to what the numbers are now, but I can speak to what the numbers were with SecureData and SecureLink combined, because those, if you go to company sites you can look at those numbers, so there are no issues with that. In France, which is equivalent size to the UK economy, they're about EUR 300m revenue. In the UK, they're sub-EUR 100m, so there's scope for three times the growth there, isn't there? That's what I mean by that. That's why, again, I don't think market share is a good metric. It's really about just sharpening execution and growing and doing what you're doing in other territories, in the territories you're not as strong as in, in a way. I think you will run out of runway, eventually you will do, but I think acquisition can just turbocharge this, that's all.

[00:47:27]

Q: Within the vendors you mentioned – Palo Alto, CrowdStrike and so on – are there any particular leading cyber vendors you believe an MSSP [managed security service provider] should always be linked to?

EG: I don't know. Yes, but they all have them. If you have a look at the top vendors for all the big players, they all deal with exactly the same vendors. There's no real differentiation there. What you're just talking about is a good question, that's a question from when I started 20 years ago. 20 years ago, my success was defined by me selecting Check Point when there were 12 people, and I still met the founders. Then, product selection mattered. Now, it doesn't matter, because if you've got any size of any scale, those vendors will seek you out, because they're looking for a way to get to their big customers, aren't they?

SM: I can imagine across the board, with these managed service providers, they'll have the likes of Juniper, Cisco and Palo Alto.

EG: I would say this, again, this is just my opinion, I don't need to have a crystal ball to be successful in this space, I just need to predict what won't change. I think that, for me, the key vendors in this space really, Microsoft. You're going to laugh at this, but Microsoft is not a known security player. They're becoming more and more dominant in this space and they will become a major player, and that's one of the areas that I think Orange needs to work on, is the Microsoft strategy, number one. The second vendor which I think is really, really important in the space is, again, I'm talking the non-obvious ones, is Citrix, no, VMware. They have really, really good security technology, they're very strong on the SASE side, they're very strong on the SD-WAN side, and I don't think Orange deals with them a lot, where I think some of the other competitors do a little bit, does more VMware than Orange Cyberdefense does.

In terms of the rest of the vendors, the more traditional ones, I think the ones that are really going to be interesting and more relevant are people like Palo Alto Networks. The reason they're becoming interesting and more relevant is because they have an offering that does embrace a cloud. They have cloud-native solutions, which a lot of other vendors don't really have. Then, I think Fortinet is becoming quite interesting. Some very large companies, people like Barclays and so forth, have embraced Fortinet, in preference to something like Check Point. I think Fortinet, but I know that Orange Cyberdefense has a strong relationship with Fortinet. Fortinet is a really interesting player, which has not been that obvious, but their strategy is starting to work. I think the one that there is weakness in is Check Point, to be honest, just because Check Point is a security purist, and that's fine, but they're going to be like the sports car which is fantastic and works extremely well, but not a lot of people buy. You sell a lot more Priuses than you sell Ferraris, don't you?

[00:50:59]

Q: On the note of vendors, CrowdStrike recently accelerated its partner business, and it has a sort of invite-only tier, for now at least, in which Orange Cyberdefense, Deloitte and Cyber Defense Labs are included. Do you think this could play as a competitive advantage to Orange Cyberdefense in any way?

EG: No, it's PR, to be honest. I don't have a orderly row of customers at my door looking to buy CrowdStrike. There are five or six players in that space, all moderately okay, maybe not as good as CrowdStrike but good enough. Every morning I compromise, and it's a compromise between time, cost and resource. CrowdStrike is a good solution, but the fact that they've got limited people selling them, I don't think it's a good marketing strategy. While they do that, I think Microsoft with Defender is busy getting better and better, and at some stage the XDR endpoint vendors… I don't know, I don't think it's a differentiation, the fact the vendor chooses you.

[00:52:30]

Q: How is Orange Cyberdefense priced compared to competitors? Would you say it's almost at a premium, or is it on level? As you said, it can be hard to differentiate on the actual capabilities, and can sometimes come down to just the delivery, advisory and so on.

EG: I would say they are at a premium. I don't know what's public and what's not public, but they are at a premium. I think their services are at a premium. Certainly, Again this will come out when they share more detailed information with the market, I guess, I do know that they don't follow a model that some people do, which is to offshore a lot. A lot of what they deliver is delivered locally in-country. Yes, there's some level of offshoring happening, but that's only for back-end stuff, really, which means by definition the cost to deliver services is more expensive than it might be for a TCS or a Wipro and stuff like that. That's on that basis that I say that.

[00:53:54]

Q: Do you think the premium pricing is justified for a customer to take on, in the sense that it's onshoring?

EG: Yes, I think it is, but the fact is the market is moving away… The market is not moving away. Sorry. Let me just qualify myself. I think the value that you are delivering, I said from the beginning, I think where the market is going is towards the managed SOC, SIEM advisory services, and that you can't really offshore, that needs to be near-shored. The value that you deliver managing devices is diminishing, but in event for two reasons. First of all, it's become simpler. It has become simpler. When stuff is new it's complicated, then when it becomes more mature it becomes simpler. IPhone as an example, compare an iPhone today to your typical mobile phone, like your Blackberry 10 years ago. Much simpler to use. Technology becomes simpler as it becomes more mature. That's one reason. Second reason is that more and more stuff is going into the cloud, so there are less physical devices to manage and to swap out if they break, so actually that market is moving towards not just even the cybersecurity specialist, but the mass-market resellers like CDW and Softcat and those guys are starting to offer managed services. Their entry cost is a lot less than Orange Cyberdefense's cost is, so I think the market is busy evolving and changing.

SM: Would you say the fact that some of these players are offering the managed services themselves could play as a threat to Orange Cyberdefense in the long run?

EG: Yes, absolutely, and the way to assess that threat is just to look at how much portion of the revenue of Orange Cyberdefense comes from device management vs more advisory stuff like SOC, SIEM and advisory services, and to see how that's straining over the last couple of years, is how you would assess that risk.

[00:55:59]

Q: In terms of M&A strategy or the acquisition targets that Orange Cyberdefense filters out, do you think there's a particular criteria the company implies here, in terms of strategy? How would you define that?

EG: Size, really, because they're a big organisation, they're a big beast, they take a very French approach to acquisitions, very structured, very methodical, and it's not worth it for anything that they'd sell for EUR 50m. Actually, that's the first thing. Sorry, that sounded flippant, it wasn't intended to be flippant. First of all, it needs to meet that criteria, it needs to be that bar, but then the next criteria, really, is territory. I think their strategy really is focused on entering into areas where they're not.

[00:57:02]

Q: Do you have any concluding remarks on Orange Cyberdefense? What's your growth outlook for the company?

EG: I would say this, I've worked there for 18 months and I did sell a business to them, and they always say nobody has ever left a good company, so when people leave a company there are always other reasons, it's not because it's a great company, but, actually, I genuinely have a huge amount of respect for the people managing Orange Cyberdefense. I think the management team is really strong, and I can't think of a single person in that management team that's not a quality person, so they've got strong leadership. I genuinely think the company has got good potential, but what will define whether they rise to that potential is whether they get execution right in territories where they're weaker, that's number one.

[00:58:21]

SM: Perfect. We will conclude the Interview there, so let me close by saying thank you to the clients for joining Third Bridge Forum's Interview today, and also thank you very much, Etienne, for your input today. It was a very insightful Interview, and I hope to work with you again soon.

EG: Thanks a lot. A pleasure.

SM: Perfect. Take care, Etienne. Have a good one.

Transcription ends at 00:58:47 of the recorded material

If you'd like to speak to Etienne Greeff in a private call or meeting, please let your relationship manager know.

Disclaimer

The information, material and content contained in this transcript ("Content") is for information purposes only and does not constitute advice or an offer or inducement of any type or a trade recommendation and should not form the basis of any investment decision. This transcript has been edited by Third Bridge and may differ from the audio recording of the Interview. Third Bridge Group Limited and its affiliates (together "Third Bridge") make no representation and accept no liability for the Content or for any errors, omissions or inaccuracies in respect of it. The views of the specialist expressed in the Content are those of the specialist and they are not endorsed by, nor do they represent the opinion of, Third Bridge. Third Bridge reserves all copyright, intellectual and other property rights in the Content. Any modification, reformatting, copying, displaying, distributing, transmitting, publishing, licensing, creating derivative works from, transferring or selling any Content is strictly prohibited.