Speaker 1:	00:01	Okay.
Speaker 2:	00:03	What it is to be a Cloud Security Architect, how to become a onet. Um, I guess a bit of a background. The reason I'm not going to put this out to it's mainly because it's a lot of what I'm seeing is client demand is, you know, can you find those individuals who have skills of cloud security, architecture, but not just you know, how can we actually take someone who's not quite there yet and develop them into a cloud security architect? Because a lot of clients I'm understanding of actually aren't that many people out there with the skills. We may have to be a bit more flexible.
Speaker 1:	00:40	Yeah, no problem. So I guess it's, we take it back if we take it back. Probate, just to give some, some context if we take it back to, um, the idea of a, of a security architects, security is fundamentally just a hybrid. It's not just a role as such. But if you look at my background, I started as a trainer, a on network infrastructure, security and security used to be just followers, bowel roads, ips rules. So anything network security, centic and then you had a whole Shibang and focus on application security and they used to be two very, very different worlds. So infrastructure, network, normal admin stuff then you had the risk and compliance work and you had the application security architect or DEV with security security hat on. Those would be the three main categories of security people. Now if you collapse that into the cloud world, you effectively mixing up the three elements. So you mixing up network security is not any more bad relevant and you only have fundamentally ips ids, firewall rules. But setting them up is becoming a little bit more trivial. So you have that more into the data center world.
Speaker 1:	02:19	And will it become more and more relevant? It's actually application security because if you think about elements like, um, function as a service where you just throw some codes and it get executed, then it becomes much more relevant to the cloud. Security architect actually has a very, very good understanding of application security problems. So if you want, it's an evolution of what traditional, uh, security architect that still has a need to have an understanding of the CQ enterprise security or their challenges because it's still need to have a photo on prem unless he's a complete get on the cloud security stuff. But it is a much more complex because it needs to have contract and oversight on contractual stuff. Yeah. Uh, and Oversight on SLA and oversight on risk and compliance and oversight on a technical controls and technical stuff there is out there and work with the rest of the team. So it needs to be a little bit of a politician as well because need to influence and

work with the rest of the team because he's a figure that is, is a role that is so, so spread across the entire of the organization if it makes sense.

Speaker 2: 03:41 Yeah. Up to, I think one interesting thing that you mentioned, did you need, you need to be an implementer across the rest, rest of the team. Um, and I, I understand it's to not completely black and white, but where do you think of cloud security architectures set in Methuen?

Speaker 1: 03:59 That's another challenging question. So in all the client or the work with it tend to sit into role. So if he sees in the architecture space, then it ha then this is where it has the more influence. But the problem is in Sydney, in the architecture space and reporting or the head of architecture, it's curse. So our security architect as such, need to have the freedom to flash out and point out the challenges from a security perspective. So need to have that freedom by reporting to the CSO. So it needs to be in the architecture space, but has have a reporting line to the CSO that that's where the security architect is Muufri ineffective in an organization because otherwise it will be coerced by the delivery and a per project want to go ahead then the reporting line, uh, is on the project side. So on architecture in the architecture space, the tend to report to the, um, to the c level for the technical stuff. So the CEO or the CIO or the CTO, depending on how the organization is structured, but I tend to be focused on actually delivering the rendering and what the security are. There needs to be focused on actually risk and compliance and working with other hockey that, but if, if you spot something that is wrong and he said I had the freedom to actually flush it out.

Speaker 2: 05:22 Okay.

Speaker 1: 05:25 So just as a sound needs to sit in the architecture space needs to pay with all the other architects need to lead the security discussion in that word. But the reporting, I need to be on the CSO

Speaker 2: 05:39 and then testing taken one I don't see very often. Normally I, from what I see, you read the report directly into if you feel I'm working the architect of fit or reporting to the head of architecture and report directly into space and not really sit with security at all.

Speaker 1: 06:00 Yeah, it's wrong in a way because I mean, it's not wrong. It's, it is a rule that is evolving and we gonna find our footing and all space a while we go along. But you know that to be more

effective, that's the best way. And there are new ones on, on every kind of role where you might have, you know, a more, a more security focused on security wise. Um, architecture lead because you know, my talk, I said security is everyone's responsibility so that the architecture, the leads or the head of architecture cannot say I'm not interested in security. But there is always a challenge where maybe the lead is not interested in, in easy, it's more interested in delivering fast rather than delivering secure. So there needs to be that. Then freedom of action, AME reporting line.

Speaker 2: 07:05 Um, I guess two to one the questions I sent across before, um, the call will be what actually attracted you to cloud security.

Speaker 1: 07:17 So I started my journey in consecrating eight years ago when cloud was and consider clouds. So you had steel as you would loosen capabilities. Aws schools, I think back in 2006 in the infancy and I saw the opportunity to shape the future of the world. So I believe of living making the word secure one project at the time. And if you look at the other opportunity count securities effectively just to reset the clock, because security, if you look at 25, 20 to 25 years ago, security was not a big, big of a deal project where Netapp were not developed with security mindset. And that led to the, to the current status of insecure application insecure that ascent and everything that we'd done from 20 years ago to today. It's been basically just bolting on security in new project, uh, in trying to do new project better or bolting on security control on existing data center. Now on the seat on the cloud, you, I actually have a unique opportunity to start with security from scratch. So with secure, with a security mindset and it's a security focus and that's an opportunity. So that's what I say. I want to change the word. Where can I do it? I can do it.

Speaker 2: 08:52 Okay.

Speaker 1: 08:53 And also it's interesting. It's interesting. It's an interesting challenge. It's an interesting opportunity. And if you take for example controls, it's much, it's much more pro ball. There's somebody with, um, I use base like AWS or Azure has much more effective control, uh, their organization that has limited spending insecurity. So leveraging cloud control, you can actually make a real difference. Now there is, there is, there is a whole question of actually once you've done that, you locked in pretty much on the cloud provider because you want to maximize the use of the capability and you log in. So the cloud access strategy is a topic that is, uh, more and more relevant. But it's a, it could be a security challenge. It couldn't be

fundamentally a security architect. They just, it just the shape of every other architect. So we tend to have an opinion about a lot of stuff.

Speaker 2: 09:51 Yeah,

Speaker 1: 09:54 it's a risk. If you look at the, if you read it as a race to be looked in, your account provider is a risk,

Speaker 2: 10:01 I guess. Um, what would you say the current, you know, leading cloud platform or the emerging competitors?

Speaker 1: 10:11 That's a very interesting question. So I think it depends. So you have a lot of expertise on AWS, but AWS is not a very approachable, um, cloud platform because it's very, very complex. So they give you a fatty with engineering power and they give you the opportunity to do whatever you want, but you need to have the expertise to actually do that. And there is more and more expertise. But it's really complex to start on on AWS. While if you look at as you as your is more focused on enterprise, they want to jump on board and want to start leveraging on cloud functionality without tiring, um, um, an army of engineers to actually build that and the Reese and I had to say there is much more chances that you do that securely. I'll see my many more mistake on AWS rather than on a [inaudible] from a security perspective. And if you step into something without understanding what you're doing, you've been prone to make mistakes, security or not security wise, but I found it more if you want a little bit more user friendly or Microsoft has always been from back nothing in 2010 more focused on the graphic user interface. Well AWS in 2006 was pretty much just API based.

Speaker 2: 11:36 Yeah.

Speaker 1: 11:37 And then, and then you have the close follow either the Scougal cloud that is fundamentally not very focused on their on the compute side, but he's very, very focused on a analytics. So where where they show real capabilities actually unstructured data and stuff like that and management of, of of increased shinning keys. They, they do a wonderful job in that. So I think it depends on what you want to use, what culpability want you want to use.

Speaker 2: 12:10 I see. I mean, yeah, I think certainly being the encryption side of Google, how to someone that could make it a more attractive option for organizations moving forward.

Speaker 1:	12:21	Yeah. I mean, if you want to use unstructured data and just throw data in, in, you know, database and create tables on the fine, not worry about security because this is kind of taking care of, then it becomes an attractive offer.
Speaker 2:	12:38	So I guess I'm going from, you're looking at how you were, uh, an issue before carries a real opportunity to build security and from a star and really shape how it, how it looks with in the cloud. How did you actually go about becoming a cloud security architect?
Speaker 1:	12:59	Um, I just riskier than myself. So doing, doing, doing, at the beginning there was no training. I think in 2006 there was no training, no material, no it, just try and run it and break stuff and use it and interact with the community. That's, that's how I became part of the consigliere lines because there was no documentation or on the couch. And 2010, Microsoft was exactly the same. So it was really, really painful to interact with some of this stuff and not having reference documentation. Um, because he also knew and that's why I joined the cloud security alliance. And I put the effort to actually do develop part and we my organization and you know, share that knowledge because ultimately that's the only way. So learn by breaking and testing and any seals the very effective way, even though nowadays there is, there has been massive adoption. So there is much more um, material out there. So there is IC square has private stair see, uh, CCSP, sorry, sees CSP certification. That is a good stepping stone. Consecrate Alliance has published their body of knowledge, the CCS case certification, um, and there is a lot more material out there. So, um, as you are, it is publishing a lot of reference material on the security side. They start doing a security truck on that step for upscaling. Aws is doing x, x is a close follow up.
Speaker 1:	14:38	So I think there is much more material. They just, it just looking at which one to use. So the recommendation is start from south, from framework like this is GSK because it give you an oversight, uh, then more to the CSP if you want to add a certification for z squared and then move to the technical certification. Like, uh, uh, the Microsoft product or data we struck, I don't think Google has a security security focus. Certification is a little bit scattered, but AWS and Microsoft are starting to train only on security because they have a massive amount of product now.
Speaker 2:	15:20	Okay, interesting. So yeah, take, take then I guess in neutralized version first before going down a specific tracking thing, I want to be a qualified through your professional opinion is you are

Speaker 1:	15:31	Oh, AWS and ultimately they gives you, that gives you the breathing space and say these are all the problem that I need to consider. So you, you ended up realizing really quickly they're not security problem. They're just problems with the security lens on it. That's why I say it's security is everybody's job because network has a security component in infrastructure as a security component in it. Um, application has a security component and in the cloud we touch all those elements. So it becomes the role of a security. Architects become a mile wide and an inch thing. So you need to be a little bit of a generalist with some verticals like network, like, uh, uh, development. So application security, um, or um,
Speaker 3:	16:18	right.
Speaker 1:	16:19	Yeah. Even though it's, it tends to be mixed. You tend to be an expert depending on your background. If it, if we were at there were or not mean those were the two main categories. Um, I will, they include risk and compliance because it's not a very technical role. Um, and then you develop those other skill as a light touch.
Speaker 2:	16:43	Okay. I guess just to confirm, you know, you'd see fest certified cloud security professional as I understand it. What does CCS case Downfall,
Speaker 1:	16:53	a certified cloud security knowledge.
Speaker 3:	16:57	Yeah.
Speaker 1:	17:00	Okay. So if you will on the CCS gaze, the base one and let's say it's certified or you know, stuff on the cloud, you understand the division of responsibility and, and, and things like that. And with the cost of your alliance, we are, we have, we published a body of knowledge. So there is a body of knowledge and the exam is online. Um, uh, well the IC square equivalent, they have another body of knowledge to this more or less on the same, on the same topic. So if you study one, you can actually take both certification, which is slightly different
Speaker 2:	17:40	on the cloud security alliance. It's a map when it came across very recently. Um, could, could you explain a bit more about that for me please?
Speaker 1:	17:49	Yeah, so we are a non for profit organization. Uh, we have done, uh, we had to stream of, or if you want three, three pillars. One is on the education, one is, uh, what we develop the body of

knowledge and an exam. I think the latest iteration is the version four and it's all for free with the exception of the exam. The thing is $300. Then there is the evangelization. So making sure that the cloud adoption runs smoothly by making sure that everybody knows about uh, how to secure the cloud and you don't get, you get demystification and we engage in all the major conference. We run event, we making webinars and things like that. Awful frame. Uh, Eh, yeah, this is what we do. And then the third pillar is actually research where we, we have a pool of people that is interested in specific topics. So we the surface, the topic that we're interested in because we are all practitioner or a, we do research on existing topic.

Speaker 1: 19:01 So there is a, there is a research director that that um, has, um, I think we have running for the nodes or research, uh, at the current point in time. But that that was quite a bit. That was yeah, there was a point where uh, the cloud security alliance was born. Um, and then on the side of that we have um, uh, the star alliance and the CCM, the cloud control monitor. So the cloud control Maddix was born to actually map all the existing um, standards. So Iso 27,001 Kobe and so on and so forth, back to cloud specific topic. And then on the back of that we develop the star certification that is effectively an equivalent on ISO 27,001. And we have two level. One is a self is a self assessment and the second one is an official certification where you ask an auditor to come in and check you doing a dose control.

Speaker 1: 20:01 And is there the certification of pub they on there on the cloud security alliance website. So effectively becomes a um, a list of all the providers that actually are taking seriously security. So if you want to go and purchase a specific service, it could be a saas service or it could be a new service like Azure. Uh, you go there, you search. Is it secure enough? Yes. Can I see how do they do security? Because they had to revive a quite extensive, a spreadsheet of how do they do control and security and is available. So the latest version is available on the site and is full frame. There is a, is a way to check the due diligence that the cloud provided us. And the whole point of it was actually to incentivize the clouds, the cloud adoption. And we worked for fundamentally all the, all the members were non profit. We have, um, I don't remember the last number, but we have a quite wide spreads, um, uh, use based in, in most of the organization or member worst in most of the fortune five onwards. So we have a cool VCP the on the, on, on the existing problem and the problem that coming up

Speaker 2: 21:19 Coveo I guess a real knowledge sharing platform and with the overall aim of improving security across industry. Okay.

Speaker 1:	21:27	Yeah. Good. Then did the participation of the unconference and everything else you get the feeling they get the feeling of the latest problem, the latest headache that the company has. Okay. Musician.
Speaker 2:	21:44	Um, I guess my next question, um, you know, why, why would a security professional one to choose cloud is that SME domain, you know, in comparison to maybe identity and access management or network or general infrastructure within security.
Speaker 1:	22:05	Do you want to have a job in two years or not? That will be my question is around. I actually had, I can tell you a story I had this conversation with, it wasn't a security person but it was um, an infrastructure person and he was very, very knowledgeable about VM ware, but it was a very hard man in hot us and that was sticking to the um, to one specific topic. And I was talking through, I was trying to get him through the cloud transformation, everything else. And Pete told me that Francesco, I'm not interested in the cloud, I'm interested just in focusing on my area and keeping on my arrest. And then a applying to piece, like that's absolutely fine. You can become the maximum expert from VM ware, but then you're going to go out of job very, very quickly because you focus on a very, very specific area.
Speaker 1:	23:04	Well if you focus on on the future that is the clouds, then you can can have these mass adoption. So to take it back to the, to the contents of what we discussing, you can either decide to be a very, very special, it's like page one wanted to be and work and it might be a market for it. Actually very, very profitable market, but you need to be really on top of your game because there is such a niche market that even if there are two or three players, we probably won't find the GIG. And if you take it to cobalt, uh, x cobol develop. I was talking to frank the other day and he's very specialized cobal developer and he has a lot of opportunities. Well No, not that many opportunities but very, very remote area we opportunity but they're scattered around the year so it doesn't have continued it. So it really depends who you want to be. If you want to be somebody that helps the majority of the organization and help drive the conversation forward on a security aspect or if you want to be like frank and like Pete, very, very specialized on a specific topic.
Speaker 2:	24:18	Interesting. Um, what advice would you give to someone who's aspiring to become a code security architect? Or I guess a close to your professional in general?

Speaker 1:	24:29	I think age is, go arounds, have an understanding of the widespread of the problem that you might encounter and where you should focus. Don't get lost. So understand where your expertise, where your background can actually help you develop your expertise. So if you're coming from a, from a developer, then that's your, that's your, your part to a application specific problem. The cloud or maybe infrastructure as a code or maybe things specific. So leverage your existing background is not, it's not all come from scratch but they just need to be repurposed on the cloud. So understand the cloud that is nothing else and actually did the center somewhere. But the reason, the reason, the level of obstruction that they need to be taken into account and then go out and talk to people. So there is a lot of material out there as you see in the consecrate alliance is publish a lot of stuff.
Speaker 1:	25:24	My organization [inaudible] is publishing a lot of Hatton's use and leverage the knowledge that's already out there. Don't get lost and PA with other, with other people. So participate in the cancer care alliance forum, participate in a cloud security or cloud specific conferences. Here we are the people, we are in most of the, we have the cloud security alliance very most of the organization, most of them, uh, cloud conferences. So K with us ask your question and you can free consultancy. We get free knowledge and I also have um, a mentoring call when I help people actually directly, not just on, on cloud security topic. Uh, but it's an effort that them, I'm doing with honesty square and Microsoft where I help people develop their path. So if you want to be a pen test that if you want to be account specialist, if you want to be an infrastructure, we want work in risk risking compliance. What part did you choose? Because I had a lot of mentee from my early days. They were asking what do I do next? I had our own asking for this. I had Amy ask him for this. It's like I'm here, I'm stuck. Go ahead do this. How do I go from here? And I help them develop in their passion and helping seeking the problem that they want to fix and then directing them on the specific topic.
Speaker 2:	26:52	Awesome. I think I've had a good service to provide to people, you know, um, but there's a lot of people out there who helps you. Um, don't really know why. Start with this kind of stuff. You know, it all seems, um, she'll broad the informational Siva.
Speaker 1:	27:07	It is a very broad subject and you can get lost very, very quickly if you're not careful. This is also an opportunity. So there is, there is, you can choose any kind of field you want to work on. So if you're in any of those fields you can put your security hat on and your Sunday get boosts, educate new challenge, a new

		opportunity. I mean security job nowadays, what are the most pay job. So there is an interest in actually getting APP scale. They're also the most challenging one.
Speaker 2:	27:40	Right.
Speaker 1:	27:43	But if you're up for a challenge
Speaker 2:	27:47	yeah. By Brian, um, we have from, from that was all I wanted to cover off from, from our interview. Um, you, I really, really appreciate your time. Any final bullets?
Speaker 1:	28:03	I will say give back to the community. So the community is giving a lot, uh, to people give back to the community. So even if you, if you want to volunteer, even if you want to just share, you know, her to research even any little effort is important to us. She takes secure is the next step, get involved and get on board on the secrets. The challenge there is a massive lack of people. So it doesn't necessarily mean you need to have a security background, securities, nothing else, and doing things right. And it's an exciting field to be on. Those will be my last, my last message to the aspiring security people. Security architecture, cloud security architect.
Speaker 3:	28:44	I know.
Speaker 2:	28:46	Fantastic. Well, yeah, fight, fight the MPA time. I will probably towards the end of the quarter or over the next month, I said, yeah, I'll share a copy with you and I'll let you know your contribution from my glove. Jessica.